7 INSTRUMENTATION AND CONTROLS

This chapter presents the U.S. Nuclear Regulatory Commission (NRC or Commission) staff's (herein after referred to as the staff) review of the instrumentation and controls (I&C) for the NuScale Power, LLC (NuScale), small modular reactor (SMR) nuclear power reactor design certification application (DCA), Revision 2. This is part of the design certification review conducted by the NRC staff under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." The description of the I&C systems includes the overall design bases, system classifications, functional requirements[1], and system architecture, which encompasses all I&C systems and components (i.e., hardware, software, firmware, and other forms of complex logic) and areas such as software tools and equipment that are used for the I&C design or are connected to the I&C systems or components for testing.

The information provided emphasizes those instruments and associated equipment that constitute the safety systems as defined in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," which is endorsed by Regulatory Guide (RG) 1.153, Revision 1, "Criteria for Safety Systems." While the standard does not establish requirements for I&C systems that are non-safety-related (e.g., control systems), the criteria in IEEE Std. 603-1991 can be applied to any I&C system. As stated in Commission Paper SECY-11-0024, "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," (Agencywide Documents Access and Management System (ADAMS) Accession No. ML110110691) dated February 18, 2011, the review framework incorporates a more risk-informed approach to the staff's review by considering both the safety classification and risk-significance of each SSC (system, structure, or component) to help determine the appropriate level of review for each SSC. Consequently, as a starting point, the NRC staff used the concepts of IEEE Std. 603-1991 and the guidance in design-specific review standard (DSRS) Chapter 7, "Instrumentation and Controls," in reviewing I&C systems that are not safety-related but are risk significant. The NRC staff used a graded approach commensurate with the safety and risk significance of the system or component (see Section 7.0.4.1 of this report).

The NRC staff uses the term "non-safety-related" to refer to certain structures, systems and components (SSCs) that do not fall under the definition of "safety-related SSCs" described in 10 CFR 50.2. These non-safety-related SSCs include SSCs that both are and are not "important to safety" as that term is used in the General Design Criteria (GDC) listed in Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50.

Lastly, this chapter presents the NRC staff review of the disposition of 65 application-specific action items (ASAIs) specified by the safety evaluation (SE) (ADAMS Accession No. ML17116A097) of the NuScale Topical Report (TR)-1015-18653, "Design of the Highly Integrated Protection Platform," Revision 2, dated May 23, 2017 (ADAMS Accession

[1] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the General Design Criteria in Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, Appendix A, and 10 CFR 50.55a(h), which incorporates by reference Institute of Electrical and Electronics Engineers (IEEE) Std 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE Std 603-1991, are written in terms of so-called system, functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but, except as used in IEEE Std 603-1991, are not legal requirements. To avoid confusion, this safety evaluation report will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this safety evaluation report, should be understood as recommendations that NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance. The system, functional, performance, design, and other requirements of IEEE Std 603-1991, which are legal requirements, will be explicitly identified as originating from IEEE Std 603-1991.

No. ML17143A436). The NRC staff previously concluded that the Highly Integrated Protection System (HIPS) Platform meets the requirements of IEEE Std. 603-1991 and the correction sheet dated January 30, 1995, IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Digital I&C Interim NRC Staff Guidance 4, DI&C-ISG-04, "Highly Integrated Control Rooms & Digital Communication Systems," and the Staff Requirements Memorandum (SRM) to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." However, the SE of TR-1015-18653 stated that 65 ASAI analyses must be performed to ensure the generic approval granted by the SE remains valid for a specific system or plant application utilizing the HIPS platform. Section 7.1.6 of this report provides the disposition of the 65 ASAIs specified by the SE of TR-1015-18653. The NRC staff notes that the substantive staff evaluations of the individual ASAIs are set forth in various subsections of Chapter 7 of this safety evaluation report. Design Certification Application (DCA) Part 2, Tier 2, Table 7.0-2, "Highly Integrated Protection System Topical Report (HIPS TR) Application Specific Information Cross References," provides a cross-reference of the ASAIs with the Chapter 7 subsections in which the ASAIs are specifically addressed.

Introduction and Review Process

7.0.1 Introduction

As described below, the NuScale I&C systems control plant processes provide the capability to control the plant systems manually and automatically during normal operation, anticipated operational occurrences (AOOs), and accident conditions as appropriate. The I&C systems also provide initiating signals to mitigate the consequences of accident conditions.

7.0.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 2.5, "Module Protection System and Safety Display and Indication System," and Tier 1, Section 2.6, "Neutron Monitoring System."

DCA Part 2, Tier 2: The applicant provided a system description in DCA Part 2, Tier 2, Section 7.0, "Instrumentation and Controls—Introduction and Overview," which is summarized in the following discussion.

The NuScale I&C systems are implemented using three major platforms: (1) a safety-related field programmable gate array (FPGA)-based platform for the safety-related systems, (2) a non-safety-related FPGA-based platform for the plant protection system[2] (PPS), and (3) a non-safety-related distributed control system (DCS) platform for the data processing system and non-safety-related control systems.

The safety-related I&C systems consist of the module protection system (MPS) and the neutron monitoring system (NMS). These systems perform the functions necessary to maintain the plant within the prescribed safety limits (SLs) and provide indications to the operators for post-accident monitoring (PAM) functions.

[2] The applicant uses the term "protection system" as the name for the Plant Protection System (PPS), which is not a "protection system," as described in GDCs 20 to 25 to 10 CFR Part 50, Appendix A. The term "protection system" in GDCs 20 to 25 to 10 CFR Part 50, Appendix A, applies to safety-related systems. The PPS is a non-safety-related/non-risk-significant system that provides monitoring and control of plant systems that are common to multiple NuScale power modules. Specifically, the PPS provides automatic actuation functions for the control room habitability system and the normal control room heating ventilation and air conditioning system. The GDC "protection system" in the NuScale design is the Module Protection System.

The MPS is built on the HIPS platform, which is FPGA-based. TR-1015-18653, Revision 2, provides an overview of the HIPS platform. The NRC staff evaluated the HIPS platform and found it acceptable subject to certain limitations and conditions stated in the ASAIs for safety-related I&C applications in nuclear power plants, as documented in the staff's TR-1015-18653 SE.

DCA Part 2, Tier 2, Section 7.0, incorporates by reference NuScale TR-1015-18653, Revision 2. The applicant provided information specific to the NuScale design in DCA Part 2, Tier 2, Chapter 7.0, in addition to text from the referenced TR-1015-18653. Section 7.1.6 of this report describes the disposition of ASAIs 1, 2, 18, and 57, which relate to the I&C system design.

TR-1015-18653[3], Section 2.0, "Highly Integrated Protection System Platform," describes the basic HIPS platform hardware and communication bus design concepts.

The non-safety-related PPS is implemented using the HIPS platform to monitor variables at the plant level and execute actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to up to 12 NuScale power modules (NPMs).

The non-safety-related DCS provides monitoring and component-level control of NPM balance-of-plant control functions and non-NPM-specific plant components. The DCS uses a redundant and fault-tolerant architecture.

Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC): The ITAAC associated with DCA Part 2, Tier 2, Section 7.0, appear in DCA Part 2, Tier 1, Sections 2.5 and 2.6. The evaluation of ITAAC is in Section 14.3.5 of this report.

Initial Test Program (ITP): The ITPs associated with DCA Part 2, Tier 2, Section 7.0, appear in DCA Part 2, Tier 2, Section 14.2, Table 14.2-109, "List of Test Abstracts," and are as follows; Table 14.2-49, "In-core Instrumentation System," Table 14.2-61, "Module Control System," Table 14.2-62, "Plant Control System," Table 14.2-63, "Module Protection System," Table 14.2-64, "Plant Protection System," Table 14.2-65, "Neutron Monitoring System," and Table 14.2-66, "Safety Display and Indication System." The evaluation of ITPs is in Section 14.2 of this report.

Technical Specifications: The technical specifications associated with DCA Part 2, Tier 2, Section 7.1, appear in DCA Part 4, "Generic Technical Specifications," Section 3.3, "Instrumentation," and Section B.3.3, "Instrumentation."

Technical Reports: The technical report associated with DCA Part 2, Tier 2, Section 7.0.4.1.2, "Reactor Trip System," is TeR-0616-49121, Revision 0, "NuScale Instrument Setpoint Methodology," (ADAMS Accession Nos. ML17005A147 (Proprietary); ML17005A118 (Non-Proprietary)). The evaluation of NuScale Instrument Setpoint Methodology is in Section 7.2.7 of this report.

7.0.3 Regulatory Basis

The relevant requirements of the NRC regulations for this area of review, and the associated acceptance criteria, are given in Table 7.1, "Instrumentation and Controls—Mapping of Regulatory Requirements, Guidance and DSRS Review Criteria," of DSRS Section 7.0, "Instrumentation and Controls—Introduction and Overview Process." DSRS Section 7.0 also gives the review interfaces with other NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," (SRP)/DSRS sections. The following are the relevant NRC regulations:

[3] All citations in this report are based on TR-1015-18653, Revision 2.

- 10 CFR 50.55a(h), “Protection and Safety Systems,” as it relates to compliance with IEEE Std. 603-1991 and the January 30, 1995, correction sheet.

- 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” Appendix A, “General Design Criteria for Nuclear Power Plants,” General Design Criterion (GDC) 1, “Quality Standards and Records,” as it relates to ensuring that SSCs important to safety are designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

- 10 CFR Part 50, Appendix A, GDC 2, “Design Bases for Protection against Natural Phenomena,” as it relates to ensuring that SSCs important to safety shall be designed to withstand the effects of natural phenomena without loss of capability to perform their safety functions.

- 10 CFR Part 50, Appendix A, GDC 4, “Environmental and Dynamic Effects Design Bases,” as it relates to ensuring that SSCs important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.

- 10 CFR Part 50, Appendix A, GDC 13, “Instrumentation and Control,” as it relates to ensuring that instrumentation is provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.

- 10 CFR Part 50, Appendix A, GDC 20, “Protection System Functions,” as it relates to the protection system to be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to ensure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences, and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

- 10 CFR Part 50, Appendix A, GDC 21, “Protection System Reliability and Testability,” as it relates to ensuring that the protection system is designed for high functional reliability and inservice testability commensurate with the safety functions to be performed as well as redundancy and independence sufficient to ensure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy.

- 10 CFR Part 50, Appendix A, GDC 22, “Protection System Independence,” as it relates to the design of the protection system to assure that the effects of natural phenomena and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function.

- 10 CFR Part 50, Appendix A, GDC 23, “Protection System Failure Modes,” as it relates to the protection system, which shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced.

- 10 CFR Part 50, Appendix A, GDC 24, “Separation of Protection and Control Systems,” as it relates to the protection system, which shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

- 10 CFR Part 50, Appendix A, GDC 29, “Protection against Anticipated Operational Occurrences,” as it relates to protection and reactivity control systems, which shall be designed to assure an extremely high probability of accomplishing their safety functions in anticipated operational occurrences.

- 10 CFR 52.47(a)(2) requires, in part, that the applicant describe and analyze the SSCs of the facility, with emphasis on performance requirements; the bases, and their technical justification, for these requirements; and the evaluations required to show that safety functions will be accomplished.

- 10 CFR 52.47(a)(3)(i) requires applicants to provide information on the principal design criteria for the facility.

DSRS Section 7.0, item “DSRS Chapter 7 Acceptance Criteria and Review Process,” presents the acceptance criteria adequate to meet the above requirements.

7.0.4 Technical Evaluation

The objectives of the NRC staff’s review are to confirm that the I&C system design includes the functions necessary to provide reasonable assurance of adequate protection during operation of a nuclear power plant under normal conditions, AOOs and accident conditions; that these functions, the implementing systems, and the equipment have been properly classified; and that the commitments have been made to use appropriate quality standards for the I&C systems.

This section addresses several of the design considerations with references, as appropriate, for information contained in Sections 7.1 through 7.2 of this report. The NRC staff’s review of the I&C systems in this section is based on DCA, Revision 2. The following technical evaluation discusses the NRC staff’s review of the compliance of the proposed design with NRC regulations.

As documented in the NRC staff’s evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed DCA Part 2, Tier 2, Section 7.0, and checked the referenced TR-1015-18653 to ensure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information on this review topic. The NRC staff’s review confirmed that the information in the application and the information incorporated by reference from TR-1015-18653 address the required information relating to the I&C system design. The following describes the NRC staff’s evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.0.3 and to address aspects of ASAIs 1, 2, 18, and 57, that relate to the I&C system design. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The NRC staff has confirmed that the applicant listed the technical reports that contain analyses and other information that supplement the materials included in the DCA and has identified the regulatory requirements, guidance, and industry standards to which the NuScale I&C systems

are designed to. Based on the above, the NRC staff finds that the application satisfies the I&C system design aspects of ASAI 1. ASAI 1 is described in greater detail in Section 7.1.6 of this report.

7.0.4.1 System Classification

The NRC staff reviewed the design of the I&C systems in accordance with DSRS Chapter 7 and consistent with the graded review approach described in Section 1.1 of this report. Section 3.2.2, "System Quality Group Classification," Section 17.4, "Reliability Assurance Program," and Section 19.1, "Probabilistic Risk Assessment," of this report describe the basis for acceptability of the I&C systems' safety significance and risk significance categorization. With this determination, the review framework for I&C systems was implemented.

The NuScale design identifies no A2 and B1 I&C systems in Chapter 7 of DCA.

7.0.4.2 Architecture Evaluation

This section addresses Section 4 of IEEE Std. 603-1991, which requires, in part, that a specific basis be established for the design of each safety-related system. The architecture description described in DCA Part 2, Tier 2, Section 7.0.3, "System Architecture," provides a representation of the I&C system's properties, elements, functions, and the relationship among them. The architectural description contains the rationale, justification, or reasoning for architecture decisions that have been made, including potential consequences of such decisions.

The NRC staff considered the I&C system's overall architecture in concert with the Sections 7.1.2 to 7.1.5 of this report, relating to the fundamental design principles. In addition, the NRC staff considered other sections of the DCA that discuss the I&C system design basis (see Section 7.1.1 of this report), provide I&C system descriptions, and identify I&C system functions for consistency and additional information.

DCA Part 2, Tier 2, Figure 7.0-1, "Overall Instrumentation and Controls System Architecture Diagram," illustrates the I&C system architecture principles and concepts. The NRC staff confirmed that the system architecture includes (1) all of the safety-related systems and relevant control systems, (2) connections between the systems, and (3) identification of signal/data barrier devices.

The NRC staff has found that there are no deviations in the application-specific NuScale I&C architecture presented in DCA Part 2, Tier 2, Chapter 7, from what is described and approved in TR-1015-18653, Revision 2. Therefore, the NRC staff finds that ASAI 2, as described and evaluated in Section 7.1.6 of this report, is satisfied.

The MPS functional logic diagrams are shown in Figure 7.1-1a, "Module Protection System and Plant Protection System Trip or Bypass Switch Logic," through Figure 7.1-1ao, "Actuation Priority Logic Non-safety-related Input Control Logic." The functional diagrams include (1) major components from sensors to actuation devices, including various channels/divisions used for signal/data processing, voting units, and actuation devices and (2) signal/data flow paths.

The NRC staff confirmed that the I&C architecture provided a description of systems necessary to support the defense-in-depth concept of the plant, which provides layers of defensive capabilities to mitigate or prevent potential hazards. This included the following:

- all I&C functions that are part of the design basis (see Section 7.1.1 of this report);
- a description of the I&C systems, including their classification, technologies, boundaries, and interfaces with other systems;

- end-to-end signal flows and their descriptions (e.g., signal flow paths from sensor input through signal conditioning, data processing, voting, and actuation);

- key functional blocks that make up the I&C architecture, through which the data (e.g., plant process information or command signals) are transmitted and their descriptions;

- simplified logic diagrams;

- signal processing block diagrams and their descriptions;

- prioritization schemes for the reactor trip and actuation of engineered safety feature (ESF) components (the priority functions and their descriptions are provided in DCA Part 2, Tier 2, Sections 7.0.4.1.2, and 7.0.4.5, and Figures 7.0-17 and 7.0-20);

- interfaces and comparisons of electrical and I&C diagrams; and

- specific constraints identified in the I&C design resulting from the general plant safety approach that could affect compliance with regulatory requirements.

7.0.4.3 Systems Descriptions

This subsection outlines the I&C system as submitted by the applicant in the DCA. The description of the NuScale I&C Systems is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6, and DCA Part 2, Tier 2, Chapter 7, Revision 2.

DCA Part 2, Tier 2, Revision 2, Figure 7.0-1, illustrates the main I&C systems of the NuScale design used for control and monitoring in the plant. These I&C systems perform the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. These I&C systems also implement functional requirements specified by various plant mechanical and electrical systems.

The I&C systems of the NuScale design are implemented using three major platforms: (1) a safety-related FPGA-based platform for the safety-related systems, (2) a non-safety-related FPGA-based platform for the PPS and SDIS, and (3) a non-safety-related DCS platform for the data processing system and non-safety-related control systems.

The safety-related I&C systems consist of the MPS and NMS. These systems perform the necessary functions to maintain the plant within the prescribed SLs and provide indications to the operators for PAM functions. The MPS is built on the generic HIPS platform, which is FPGA based. The NRC staff evaluated the HIPS platform TR, including the 65 ASAIs described therein, and found it acceptable for use in safety-related I&C applications at nuclear power plants as documented in the NRC staff's SE (ADAMS Accession No. ML17116A097). The NMS supports the MPS by providing neutron flux data for various reactor trips and information signals for PAM.

The non-safety-related PPS is implemented using the HIPS platform to monitor variables at the plant level and executes actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to up to 12 NPMs.

The non-safety-related DCS provides for monitoring and component-level control of NPM balance-of-plant control functions and non-NPM-specific plant components. The DCS utilizes a redundant and fault-tolerant architecture.

7.0.4.3.1 Safety-Related Systems Descriptions

This section describes the safety-related I&C systems in the NuScale design. The evaluation of how these systems meet applicable NRC regulations is described in Sections 7.1 and 7.2 of this report. The information in this section addresses the application-specific information requirements for ASAIs 17 and 58.

Module Protection System

DCA Part 2, Tier 1, Section 2.5.1, states that "the primary purpose of the MPS is to monitor process variables and provide automatic initiating signals in response to out-of-normal conditions to provide protection against unsafe reactor operation during steady state and transient power operation. The MPS is a safety-related system."

DCA Part 2, Tier 2, Section 7.0.4.1, "Module Protection System," states that there is one MPS for each NPM. The MPS comprises the reactor trip system (RTS) and the engineered safety features actuation system (ESFAS).

DCA Part 2, Tier 2, Section 7.0.4.1, states that there are two major functions for the MPS:

- The RTS portion of MPS monitors plant variables and trips the reactor when specified setpoints, which are based on the plant safety analysis analytical limits described in DCA Part 2, Tier 2, Chapter 15, "Transient and Accident Analysis," are reached or exceeded during anticipated operational occurrences; and

- The ESFAS portion of MPS monitors plant variables and actuates ESFAS equipment when specified setpoints, which are based on the plant safety analysis analytical limits described in DCA Part 2, Tier 2, Chapter 15, are reached or exceeded during anticipated operational occurrences. Actuation of ESFAS equipment prevents or mitigates damage to the reactor core and reactor coolant system components and ensures containment integrity.

DCA Part 2, Tier 2, Section 7.0.4.1, states that the MPS incorporates the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth (D3) as described in TR-1015-18653 for the HIPS platform.

DCA Part 2, Tier 2, Section 7.0.4.1, states that the MPS consists of the following:

- separation group sensor electronics and input panels;

- four separation groups of signal conditioning;

- four separation groups of trip determination;

- manual actuation switches in the main control room (MCR);

- MCR isolation switches in the remote shutdown station (RSS);

- Class 1E components to provide isolation from the non-safety-related highly reliable direct current power system (EDSS) power supply;

- power supplies for sensors and MPS components, which also provide isolation from the non-safety-related EDSS;

- eight voltage sensors for detecting loss of 480 volts alternating current to the EDSS battery chargers;
- four reactor trip breakers (RTBs) and associated cabling;
- four pressurizer heater trip breakers and associated cabling;
- two non-safety-related maintenance work stations (MWSs);
- two non-safety-related MPS gateways;
- three 24-hour timers per division for PAM-only mode;
- two divisions of RTS voting and actuation equipment;
- two divisions of ESFAS voting and actuation equipment; and
- four under-the-bioshield temperature sensors.

The MPS boundary extends from the output connections of the sensors and detectors to the input connections of the actuated components, as described in DCA Part 2, Tier 2, Figure 7.0-2, "Module Protection System Boundaries."

Safety Function Module

The safety function module (SFM) performs three main functions: (1) signal conditioning, (2) trip determination, and (3) communication engines (i.e., input/output devices).

Signal Conditioning

DCA Part 2, Tier 2, Section 7.0.4.1, states that the signal conditioning function comprises input modules that are part of the SFM consisting of a signal conditioning circuit, an analog-to-digital converter, and a serial interface. The signal condition function is responsible for conditioning, measuring, filtering, and sampling field inputs.

Trip Determination

DCA Part 2, Tier 2, Section 7.0.4.1, states that the trip determination receives process and detector input values in a digital format through a serial interface from the signal conditioning block. The trip determination performs the safety function algorithm and makes a trip determination based on a predetermined setpoint and provides a trip or not-trip demand signal to each RTS division through isolated, redundant, transmit only, serial connections. The SFM also makes an ESFAS actuation determination based on a predetermined setpoint and provides an actuate or do-not-actuate demand signal to each ESFAS division through isolated, transmit only, serial connections.

Communication Engines

The SFM communication engine sends the trip or not-trip or actuate or do-not-actuate data to the three safety data buses (SDBs) (i.e., SDB1, SDB2, and SDB3) on the chassis backplane, and the data are received on the scheduling and bypass modules (SBMs) (i.e., SBM SD1, SBM SD2, and SBM SD3). The SBMs are the bus masters of their associated buses and are responsible for scheduling the communications.

There are two other logic functions within the SFM: (1) monitoring and indication bus (MIB) functionality and (2) calibration and testing bus (CTB) functionality. The MIB logic function obtains the parameters, trip determination, status, and diagnostic information from each of the core logic paths and provides that to the MIB. The CTB functional logic allows the MWS to update the tunable parameters in nonvolatile memory when the SFM is out of service.

All status and diagnostics information for the SFMs and SBMs is provided to the MIB. The MIB communication module is the bus master for the MIB and schedules the communications for the MIB. If the SFM identifies a failure on a communication bus, the SFM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for the SFM on that communication bus is to not respond to the bus master. By not receiving a response from an SFM, the MIB communication module also generates an alarm. The MIB communication module provides the status and diagnostics information to the MCS and the MPS gateway through one-way, transmit-only, isolated outputs. The MPS gateway sends the data to the MWS and SDIS. The MIB communication module also provides a communication path from the MWS to the SFM through the CTB to allow for calibration and parameter updates for each safety function. The safety function must be out of service and a temporary cable from the MWS to the MIB communication module is required to allow changing parameters or calibration of a channel. An MWS can access only one separation group at a time using a temporary cable. The evaluation of controls of access for the MWS is described in Section 7.2.9.1 of this report.

An MIB communication module is included for each separation group and each division. A divisional MIB communication module serves only the function of monitoring and indication as there is no calibration available for the divisional RTS and ESFAS.

Reactor Trip System

DCA Part 2, Tier 2, Section 7.0.4.1.2, “Reactor Trip System,” states that the RTS is responsible for monitoring plant variables and shutting down the reactor when specified setpoints, which are based on analytical limits, are reached or exceeded.

The RTS uses four redundant trip determination signals, one from each separation group, to complete the logic decisions necessary to automatically open the RTB.

The SFM for each separation group generates a trip signal that is sent through an SBM to a schedule and voting module (SVM) in both RTS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more trip determination signals generate a reactor trip, a trip signal is generated in the SVM and sent to the associated equipment interface modules (EIMs) to open the RTBs.

DCA Part 2, Tier 2, Section 7.0.4.1, “Module Protection System,” identifies the safe states for protective functions and the conditions that force the MPS to enter a fail-safe state.

The EIMs in the RTS are slaves to the SVMs on the safety data communication buses and slaves to the MIB-communication module (CM) on the monitoring and indication communication bus. If an EIM identifies a failure on a communication bus, the EIM generates an alarm and assumes a fail-safe state for that communication bus. The fail-safe state for that communication bus on the EIM is to demand a trip or actuation of all its protective functions. The fail-safe state for protective functions on EIMs is to demand a trip or actuation. The fail-safe state for the EIM on the monitoring and indication communication bus is to not respond to the communication bus master.

Each EIM in the RTS receives redundant trip signals from outputs created in the SFM and provides a trip signal based on two-out-of-three voting from the incoming signals. Two divisions

of RTS circuitry and RTBs are provided to ensure that a single failure does not cause the loss of an RTS function.

An EIM is included for each RTB in both RTS divisions that are actuated by the MPS. Each RTB EIM has two separate logic paths. The primary coil is connected to the undervoltage trip circuit, and the secondary coil is connected to the shunt trip circuit for each RTB. Each RTS division controls one RTB in each parallel path. This configuration allows for either division to accomplish a reactor trip.

When a reactor trip signal is generated, the EIM outputs to the undervoltage and shunt trip circuits are deenergized, causing the undervoltage coils and the shunt trip relays to deenergize. When the shunt trip relays drop out, the shunt trip coils are energized with power from the module-specific highly reliable direct current (dc) power system (EDSS-MS). Either action causes the RTBs to open. The shunt trip circuit and coil are provided as a non-safety-related diverse means to open the RTBs for increased reliability should deenergization of the undervoltage coil fail to cause an RTB to open, and non-safety-related electrical power from EDSS-MS is still available. Power from the control rod drive power supply is then interrupted, and the control rods are inserted into the core by gravity.

The RTS also provides manual trip capability. Manual switches in the MCR allow the operator to manually initiate a reactor trip. Two manual switches, one per division, are provided to manually initiate a reactor trip. The manual switches are input into the actuation and priority logic (APL) associated with the reactor trip system EIM via the hard-wired module (HWM).

The APL accepts commands from three sources: (1) digital trip signal from the SFM, (2) nondigital manual trip signal from its associated RTS division, and (3) nondigital manual control signals from the MCS.

The nondigital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single device based on the highest priority. Regardless of the state of the digital system, manual initiation can be performed at the division level at any time. If the enable non-safety-related control permissive is active and there are no automatic or manual actuation signals present, the MCS is capable of operating the RTBs.

The result from the APL is used to actuate equipment connected to the EIM. RTB status is transmitted to the EIM. Breaker status information is sent to the MIB, along with the status of the SDB signals.

Engineered Safety Features Actuation System

DCA Part 2, Tier 2, Section 7.0.4.1.3, “Engineered Safety Features Actuation System,” states that the ESFAS is responsible for initiating additional protective actions when a reactor trip alone cannot mitigate an event.

DCA Part 2, Tier 2, Section 7.0.4.1, “Module Protection System,” identifies the safe states for protective functions and the conditions that require the MPS to enter a fail-safe state.

When an ESFAS parameter exceeds a predetermined limit, the SFM for each separation group generates an actuation signal that is sent through an SBM to the SVM in both ESFAS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more actuation signals generate an actuation of an ESF system, an actuation signal is generated in the SVM. The signal is then sent to the associated EIMs to deenergize the solenoids of the associated ESF system or open the breakers of the associated ESF system.

An EIM is included in each division for each ESF component actuated by the MPS. Each EIM has two separate logic paths to allow for connection to separate ESF components. Each component is connected to two separate EIMs, resulting in two EIMs providing redundant control to each component. This allows an EIM to be taken out of service and replaced online without actuating the connected equipment.

When an ESFAS actuation signal is generated in the SVM, all four switching outputs from the EIM open, power is interrupted to the component solenoids, the solenoids are deenergized, and the components change state to their deenergized position. For the pressurizer heater, the undervoltage trip circuit is deenergized, and the shunt trip circuit is energized. Either action causes all four breakers to open. Power is then removed from the pressurizer heaters.

Similar to the RTBs, only one division of pressurizer heater breakers is required to trip to remove power to heaters. The pressurizer heater breakers are configured as two separate series connections.

The ESFAS also provides manual trip capability. Manual switches in the MCR allow the operator to manually initiate an ESF function. Two manual switches, one per division, are provided to manually initiate each ESF function. The manual switches are input into the APL associated with the RTS's EIM via the HWM.

The APL accepts commands from three sources: (1) digital trip signal from the SFM, (2) nondigital manual trip signal from its associated ESFAS division, and (3) nondigital manual control signals from the MCS.

The nondigital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single device based on the highest priority. Regardless of the state of the digital system, manual initiation can be performed at the division level at any time. If the enable non-safety-related control permissive is active and there are no automatic or manual actuation signals present, the MCS is capable of controlling ESF components.

The result from the APL is used to actuate equipment connected to the EIM. ESF component status is transmitted to each EIM. Component status information is sent to the MIB, along with the status of the SDB signals.

Module Protection System Support Systems

DCA Part 2, Tier 2, Section 7.0.4.1.4, "Module Protection System Support Systems," states that each MPS separation group and division, as well as the MPS gateway, has a dedicated HWM. The HWM accepts hard-wired signals external to the MPS cabinets and makes them available on the chassis backplane for the other modules. These signals include the manual actuation switches, operating bypass switches, override switches, and enable non-safety-related control switches from the MCR. The evaluation of the operational bypass and override switches is described in Section 7.2.4 of this report.

Each division of the MPS has a non-safety-related MWS for the purpose of maintenance and calibration. The one-way, read-only data are connected through the MPS gateway for its division and are available continuously on each division's MWS. The MWS is used to update tunable parameters in the SFMs when the safety function is out of service. The evaluation of access controls of the MWS is described in Section 7.2.9.1 of this report.

Each division of MPS has a non-safety-related MPS gateway that consolidates the information received from the four separation groups, the two divisions of RTS, and the ESFAS. The MPS gateway also collects equipment status feedback from the HWM for the PAM-only mode, as well as reading the status of the three 24-hour timers. All of the information transmitted to the MPS

gateway is consolidated by a single communication module that acts as a master on the MPS gateway backplane and then transmits the consolidated data through a qualified, isolated, one-way communication path to the MWS and the SDIS hubs. There is one MPS gateway for each division. The evaluation of the data communication independence from the safety-related system to non-safety-related systems is described in Section 7.1.2.4.3 of this report.

The EDSS is the power source for the MPS as described in Chapter 8 of this report. The dc-to-dc voltage converters are used for Class 1E isolation and protection of the MPS equipment. Division I MPS power is generated from power channels A and C through a dc-to-dc converter for Class 1E isolation and then auctioneered. Division II power is generated from power channels B and D, similar to Division I. Each of the separation groups is redundantly supplied and auctioneered by a single EDSS channel. The evaluation of redundancy is described in Section 7.1.3 of this report.

To ensure EDSS batteries supply power for their full mission time of 24 hours for A and D batteries and 72 hours for B and C batteries, only loads associated with maintaining the ECCS valves closed or the PAM instrumentation functional are required to be energized during ECCS hold mode and PAM-only mode. These loads include the MPS and NMS cabinets including power to sensors, ECCS valve solenoids, RM bioshield radiation monitors, and the EDSS battery monitors. If two out of four sensors detect a loss of voltage on both B and C battery charger switchgear, the MPS automatically generates a reactor trip, DHRS actuation, pressurizer heater trip, demineralized water supply isolation, and containment isolation and starts the three 24-hour timers per division. For the first 24 hours following a loss of voltage, the four separation groups of MPS equipment and both divisions of ESFAS and RTS remain energized. If an ECCS actuation is not required by plant conditions, then ECCS is not actuated (ECCS trip solenoid valves remain energized), which is defined as the ECCS hold mode, to allow time to restore alternate current (ac) power and prevent actuation of the ECCS. The ECCS still actuates if the associated ESFAS signal is generated during this 24-hour period. If power has not been restored within 24 hours to the B and C battery switchgear, the 24-hour timers time out. At this time, the ESFAS and RTS chassis and MWS for both MPS divisions are automatically deenergized. This action deenergizes the ECCS solenoid trip valves, and the ECCS is actuated. The PAM instrumentation remains powered by the B and C EDSS batteries for an additional 48 hours (for a total of 72 hours). This configuration is defined as the "PAM-only mode." The evaluation of the displays and monitoring systems is described in Section 7.2.13 of this report.

Neutron Monitoring System

DCA Part 2, Tier 1, Section 2.5.1, "Design Description," states that the NMS monitors the neutron flux level of the reactor core by detecting neutron leakage from the core. The NMS measures neutron flux as an indication of core power and provides safety-related inputs to the MPS. The NMS is a safety-related system. Each NPM has its own module-specific NMS.

DCA Part 2, Tier 2, Section 7.0.4.2, "Neutron Monitoring System," states that the NMS performs the following functions:

- provides neutron flux data to the MPS for various reactor trips;
- provides information signals to the MPS for PAM; and
- provides neutron flux signals to the PCS during refueling operations.

The NMS consists of the safety-related NMS-excore subsystem and the non-safety-related NMS-refuel and NMS-flood subsystems.

NMS-Excore

DCA Part 2, Tier 2, Section 7.0.4.2.1, “Neutron Monitoring System-Excore,” states that the neutron flux level signals generated by the NMS-excore equipment are used by the MPS to generate appropriate reactor trips, operating permissives, indications, and alarms for various modes of reactor operation, including shutdown conditions. The MPS sends neutron flux signals to other systems to provide nonprotective controls and indication.

The NMS-excore detectors are located in the reactor pool and are maneuvered into position (direct contact with) the reactor module against the outer containment wall. Because of the wide ranges associated with the neutron flux, there will be three distinct scales or ranges provided to the MPS. These are the source range, intermediate range, and power range. The four NMS-excore detectors placed symmetrically around each reactor core measure the neutrons leaking from the reactor module core. The level of neutrons detected is an indication of neutron flux in the reactor core, which is used as an indication of reactor power. A single neutron detector is used for all three ranges supplied to the MPS.

The NMS-excore detectors are qualified to seismic Category I and located within the operation bays of the Reactor Building. The detectors are placed outside the containment vessel (CNV) and are installed in support mechanisms that are connected to the NPM operating bay structure.

7.0.4.3.2 Non-safety-related Systems Descriptions

The following section describes the non-safety-related I&C systems in the NuScale design that perform specific regulatory required functions. The evaluation of how these systems meet these required functions is provided in Sections 7.1 and 7.2 of this report.

NMS-Refuel

DCA Part 2, Tier 2, Section 7.0.4.2.2, “NMS-Refuel,” states that the NMS-refuel detectors are located within the refueling bay of the plant. There is one NMS-refuel subsystem for the plant as each NPM is relocated to the refueling bay for the refueling process and only one NPM is refueled at a time. The NMS-refuel monitors neutron flux from the point of reactor pressure vessel (RPV) head lift until the replacement of the RPV head.

The NMS-refuel subsystem includes the detector array, preamplifiers, NMS-refuel cabinets with electronics, and associated cabling. The NMS-refuel detectors are proportional counter source range detectors located near the core midplane. The detectors monitor neutron flux in counts per second over a five-decade range from 10^0 to 10^5 counts per second with a 5 percent sensor accuracy.

The NMS-refuel neutron monitoring capability ensures that the neutron flux level is continuously monitored during the refueling process and also provides an audible count rate to the operator with the ability to detect and alert a spurious increase in count rate during fuel movement. The NMS-refuel provides neutron flux signals to the PCS.

The NMS-refuel detectors are located on the outside of the RPV. This mounting allows the NMS-refuel to be repeatedly replaced in the same location between each use, allowing for the movement of NPMs between operating bay and refueling bay.

NMS-Flood

DCA Part 2, Tier 2, Section 7.0.4.2.3, “NMS-Flood,” states that the NMS-flood subsystem is non-safety-related. The NMS-flood subsystem monitors neutron flux during specific conditions when the CNV is flooded during normal and accident conditions. The NMS-flood subsystem provides indication only; it performs no safety-related functions. The NMS-flood subsystem consists of two proportional neutron detectors with sufficient sensitivity to monitor neutron flux when the CNV is flooded, preamplifiers, cabling, and signal conditioning and processing equipment. The NMS-flood detectors monitor the neutron flux over a range of five decades.

The NMS-flood subsystem is powered by the non-safety-related EDSS and provides indication for monitoring neutron flux during the specific periods of time when the CNV is flooded during normal and accident conditions. The signals from the NMS-flood subsystem are provided to the MPS via isolated inputs to MPS separation groups B and C. The indication for the NMS-flood subsystem is also categorized as Type B and D PAM variables and provided to the SDIS to support PAM of neutron flux levels.

Plant Protection System

DCA Part 2, Tier 2, Section 7.0.4.3, “Plant Protection System,” states that the PPS monitors variables at the plant level and executes actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to up to 12 NPMs. Selected variables monitored and equipment actuated by the PPS require an augmented level of quality. The PPS consists of two independent and redundant divisions. Either of the divisions is capable of accomplishing PPS functions.

The PPS utilizes the HIPS platform, which is FPGA based. The PPS communication architecture is shown in DCA Part 2, Tier 2, Figure 7.0-13.

Division I and Division II of the PPS are located in separate rooms in the Control Building. The boundaries of the PPS extend from the output connections of the sensors and detectors to the input connections of the actuated devices. Also included in the PPS boundary are the low voltage ac electrical distribution system ac voltage sensors, which are classified as part of the PPS. The non-safety-related displays, which receive data from the PPS, are either part of the SDIS or the PCS.

Safety Display and Indication System

DCA Part 2, Tier 2, Section 7.0.4.4, “Safety Display and Indication System,” states that the SDIS provides accurate, complete, and timely information pertinent to MPS and PPS status and information displays to support the ability to initiate protective actions manually, if required. Display of information is designed to minimize the possibility of ambiguous indications and to enhance the human-system interface (HSI) for the operator.

The principal functions of the SDIS are the following:

- provide operators with the HSI and data to ensure that the plant is operating within the limits defined by safety analyses;
- notify operators when the ESFAS, RTS, and PPS setpoints are reached or exceeded;
- supply operators with the data necessary to ensure that the NPM is in a safe condition following an accident; and

- provide accurate, complete, and timely information pertinent to the MPS and PPS status and information displays to support PAM.

Information regarding process variable values and equipment status is provided to the SDIS from each separation group and each division of the MPS and PPS.

The SDIS interfaces with the MPS and PPS through communication modules. The MPS interface is through the MPS gateway, while the interface with the PPS is through an MIB communication module. The SDIS consists of two independent divisions of equipment. Each SDIS division consists of communication hubs, display interface modules (DIMs), and display panels. There is a data interface connection between the Division I MPS gateway to SDIS Division I and the Division II MPS gateway to SDIS Division II as shown in DCA Part 2, Tier 2, Figure 7.0-14. The evaluation of the data communication independence from the safety-related systems to non-safety-related systems is described in Section 7.1.2.4.3 of this report.

The SDIS hub receives data from the MPS gateway and plant protection system MIB communication module. Each NPM MPS gateway delivers data to a separate communication module within the SDIS hub. The SDIS hub distributes the data it receives from the MPS and PPS to the DIM associated with the respective NPM or PPS through one-way, optically isolated, fiber optic cables. Data from each of the communication modules on the SDIS hub for each SDIS hub rack are aggregated into a single communication module. This module polls each of the communication modules on its rack through the backplane for the rack. The communication module then sends the aggregated information to the PCS through a unidirectional, optically isolated interface.

Module Control System

DCA Part 2, Tier 2, Section 7.0.4.5, “Module Control System,” states that the MCS is a DCS, which allows monitoring and control of NPM-specific plant components that are associated with the NPM balance-of-plant control functions. The MCS includes manual controls and HSIs necessary to provide operator interaction with the process control mechanism. The HSIs are provided in the MCR and the RSS. The evaluation of the HSIs is described in Section 7.2.13 of this report. The evaluation of the RSS is described in Section 7.1.1.4.2 of this report.

The principal function of the MCS is to control and monitor non-safety-related systems and components. This encompasses non-safety-related primary and secondary systems, including chemical, utility, and support process systems to the NPM. The MCS is part of the non-safety-related network and includes the associated network equipment and appurtenances necessary for network communication.

The MCS provides component-level control and monitoring of safety-related components that are specific to an NPM. The monitoring of the safety-related components is achieved by receiving one-way communications from the MPS to the MCS through isolation one-way communication ports on the MIB communication module. The evaluation of the data communication independence from the MPS to the MCS is described in Section 7.1.2.4.3 of this report.

The control of safety-related components by the MCS are manual component-level manipulations used for maintenance, testing, or aligning the components following refueling or actuation and not for safety-related purposes. The control signal from the MCS is hard wired and sent through a qualified isolation device through the HWM to the EIM in the MPS, which contains priority logic that requires a safety-related enable signal before allowing control of the device from the MCS. The evaluation of allowing control of the device from the MCS is described in Section 7.1.2 of this report.

The MCS uses logic processing in the cases where redundant input/output (I/O) channels are used. Some logic supports the redundant-channel architecture used by the MPS, while other logic directly supports the process systems. The logic processing of multiple channels can include two, three, or four input signals.

Table 7.0-1 lists the MCS subsystems' control inputs and functions for each NPM.

Table 7.0-1: MCS Subsystems Control Inputs and Functions

MCS Subsystem(s)	Control Inputs and Functions
Turbine Trip, Throttle, and Governor Valve Control	1. Main turbine control system package sensors (case temperatures, drain valve position, eccentricity, speed sensing, shaft axial position, journal bearing displacement, journal bearing temperature, and other sensors). 2. Demand power level (main turbine generator load or reactor power) from MCS and main turbine control system. 3. Main steamline flow. 4. Turbine inlet steam pressure. 5. Secondary system calorimetric input. 6. Target reactor power and change rate via the MCR operator workstation. 7. Turbine generation limit and load change rate via the MCR operator workstation.
Turbine Bypass Valve Control	1. Turbine trip. 2. Reactor trip. 3. DHRS passive condenser steam pressure (below approximately 15-percent steam flow). 4. Turbine inlet steam pressure (above 15-percent steam flow). 5. Secondary system calorimetric. 6. Target reactor power and change rate via the MCR operator workstation. 7. Turbine generation power limit and load change rate via the MCR operator workstation.
Feedwater Pump Speed Control	1. Main steamline flow. 2. Feedwater line flow. 3. Feedwater pressure. 4. Turbine inlet steam pressure (above approximately 15-percent steam flow). 5. Main steam temperature (above approximately 15-percent steam flow). 6. Secondary system calorimetric. 7. Target reactor power and change rate via the MCR operator workstation. 8. Turbine generation limit and load change rate via the MCR operator workstation.
Feedwater Regulating Valve Control	1. Decay heat removal passive condenser condensate pressure. 2. Decay heat removal passive condenser steam pressure. 3. Main steamline flow. 4. Feedwater line flow.

MCS Subsystem(s)	Control Inputs and Functions
	5. Target reactor power and change rate via the MCR operator workstation. 6. Turbine generation limit and load change rate via the MCR operator workstation.
Control Rod Drive System Control	1. Reactor coolant system (RCS) flow. 2. RCS boron concentration. 3. RCS average coolant temperature. 4. Chemical and volume control system (CVCS) letdown line flow. 5. CVCS makeup line flow. 6. CVCS makeup boron concentration. 7. Source, intermediate, and power range nuclear instrumentation. 8. Main steamline flow.
RCS Boron Concentration (Chemical Shim) Control	1. RCS flow. 2. RCS boron concentration. 3. CVCS letdown line flow. 4. CVCS makeup line flow. 5. CVCS makeup boron concentration. 6. Boron addition system boron concentration.
Pressurizer Pressure Control	1. RCS pressure.
Pressurizer Level Control	1. Pressurizer level. 2. Reactor power.

DCA Part 2, Tier 2, Section 7.0.4.5, contains COL information item 7.0-1 that pertains to the stability of the NPM during normal and power maneuvering operations for closed-loop MCS subsystems that use reactor power as a control input. The NRC staff considers this COL information item acceptable because the operational aspects of the closed-loop MCS subsystems are site specific and should be addressed at the time of COL application.

Module Control System Segmentation

DCA Part 2, Tier 2, Section 7.0.4.5.1, "Module Control System Segmentation," describes the MCS segmentation. Segmentation of the MCS is important to ensure that a failure of the MCS does not adversely affect the MPS functions. The NRC staff evaluated the four MCS control segments and the technical basis of the segmentation analysis and found that a failure in any of the MCS control segments does not have an adverse impact on the MPS and NMS functions. Independence between the MPS and MCS is evaluated in Section 7.1.2 of this report. The MCS coping analysis is described in Section 7.1.5 of this report.

Plant Control System

DCA Part 2, Tier 2, Section 7.0.4.6, "Plant Control System," states that the PCS is a DCS, which allows monitoring and control of non-NPM-specific plant components. The PCS includes manual controls and HSIs necessary to provide operator interaction with the process control mechanism.

The principal function of the PCS is to control and monitor the non-safety-related control system components, which are not specific to an NPM. The PCS is composed of the central processor or processors, power supplies, mounting racks, I/O racks, and associated networking equipment.

The boundary of the PCS is at the terminations on the PCS hardware. The PCS supplies non-safety-related inputs to the HSIs for non-safety-related displays in the MCR, the RSS, and other locations where PCS HSIs are necessary. The boundary between the PPS and PCS is at the output connection of the optical isolators in the PPS. The PCS has a direct, bidirectional interface with the MCS. The network interface devices for the PCS domain controller/historian provide the interface between the human machine interface (HMI) network layer and the control network layer. A unidirectional data diode from the PCS to the plant network is provided.

The PCS control architecture is separated into multiple control segments based on their functions. The PCS coping analysis is described in Section 7.1.5 of this report.

Plant Control System Segmentation

DCA Part 2, Tier 2, Section 7.0.4.6.1, “Plant Control System Segmentation,” describes the PCS segmentation. Segmentation of the PCS is important to ensure that a failure of the PCS does not adversely affect the MPS functions. The NRC staff evaluated the two PCS control segments and the technical basis of the segmentation analysis and found that a failure in any of the PCS control segments does not have an adverse impact on the MPS and NMS functions. Independence between the MPS and PCS is evaluated in Section 7.1.2 of this report.

In-Core Instrumentation System

DCA Part 2, Tier 2, Section 7.0.4.7, “In-Core Instrumentation System,” states that the ICIS monitors the neutron flux distribution within the reactor core and provides core inlet and exit temperature information to the MPS for monitoring core cooling during postaccident conditions. The neutron flux information is also used to verify operation and calibrate the NMS-excore detectors. The ICIS has the ability to determine a power shape deviation caused by stuck or misaligned control rods, when the rod positions cannot be determined by the rod position indication system.

The ICIS includes: (1) self-powered neutron detectors located in the reactor core for monitoring neutron flux, (2) thermocouples located at the inlet and exit of the core to provide temperature information to the MPS for monitoring postaccident conditions, (3) instrument assemblies in which the neutron detectors and thermocouples are housed, and (4) signal conditioning and processing electronics.

The in-core instrumentation system has a total of six detectors integral to each instrument assembly. There are four self-powered neutron detectors and two thermocouples. The neutron detectors are equally spaced throughout the vertical height of the reactor core. One thermocouple is located at the inlet of the core, and one thermocouple is located at the exit of the core.

An NPM has a total of 12 in-core instrumentation guide tubes. These rigid tubes extend from the top of the containment to the bottom of the reactor to provide routing and structural support for the mineral-insulated, pressure-retaining cabling which contains the in-core instrumentation assemblies.

Health Physics Network

DCA Part 2, Tier 2, Section 7.0.4.8, “Health Physics Network,” states that the HPN is used to interconnect the radiological controls equipment as part of the Operational Radiation Protection Program, which is established to provide an effective means of radiation protection for station personnel, visitors, and the general public. The evaluation of radiation protection is described in Chapter 12, “Radiation Protection,” of this report.

The principal function of the HPN is to provide the permanently installed communications infrastructure necessary to support the Operational Radiation Protection Program.

The HPN includes communications cabling and equipment mounting racks.

Fixed Area Monitoring

DCA Part 2, Tier 2, Section 7.0.4.8, “Fixed Area Monitoring,” states that fixed area radiation monitors and continuous air monitors throughout the plant perform radiation monitoring.

The principal functions of radiation monitoring are the following:

- continuously monitoring in-plant radiation and airborne radioactivity as appropriate for routine and accident conditions;
- informing plant personnel immediately when predetermined exposure rates are exceeded in various areas within the plant; and
- alerting control room operators of changing plant radiation levels.

Area radiation monitors consist of a detector or detectors connected to an electronic control unit in local proximity. The electronic control unit interfaces with the corresponding I&C system depending on functionality. Airborne monitors are self-contained and consist of modular components that are assembled on an open frame for ease of accessibility. The detectors are connected to a local electronic control unit, which interfaces with the corresponding I&C system depending on functionality. The evaluation of the location of area and airborne radiation monitors is described in Section 11.5 of this report.

7.0.5 Combined License Information Item

DCA Part 2, Tier 2, Section 7.0.4.5, “Module Control System,” contains COL Item 7.0-1 pertaining to the stability of the NPM during normal and power maneuvering operations for closed-loop MCS subsystems that use reactor power as a control input. The COL information item is evaluated in Section 7.0.4.3.2 of this report.

7.0.6 *Conclusions*

The staff review confirms that the applicant has provided sufficient information to support the staff’s findings in Chapter 7 of this report. The applicant identified the I&C systems that are important to safety in accordance with RG 1.206, “Combined License Applications for Nuclear Power Plants (LWR Edition),” and identified the NRC regulations that apply to these systems.

The regulation in 10 CFR 50.55a(h)(3) states, in part, that applications filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. The application also identifies the requirements of IEEE Std. 603-1991 that apply to the NuScale I&C systems. The clauses within IEEE Std. 603-1991 address, among other requirements, single failure protection,

independence, quality, design bases, information displays, automatic and manual controls, operating and maintenance bypasses, and capability for test and calibration. The NRC staff concludes that the NuScale I&C design meets the I&C system design aspects of ASAIs 1, 2, 18, and 57 listed in TR-1015-18653, Revision 2. In conjunction with IEEE Std. 603-1991 applicability, the NRC staff confirmed that the applicant has committed to compliance of the design with GDC 1, 2, 4, 13, 20, 21, 22, 23, 24, and 29 of Appendix A to 10 CFR Part 50.

7.1 Instrumentation and Controls—Fundamental Design Principles

The review of I&C ensures that the application contains sufficiently detailed functional diagrams and explanations demonstrating that the hardware and software for I&C architectures incorporate the fundamental design principles—namely, independence, redundancy, predictability and repeatability, and D3.

7.1.1 Safety System Design Basis

7.1.1.1 Introduction

This section addresses the review of the specific design basis of each I&C safety-related system to ensure that the information provided is sufficient to enable the detailed evaluation of the I&C system. This review also verifies that the I&C design is consistent with the credit taken in the safety analysis for the I&C system, including design basis, postulated design-basis event (DBE) analyses, design descriptions, and operational characteristics of the safety systems.

7.1.1.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.1.1, "Design Bases and Additional Design Considerations," which states that the NuScale design is consistent with the following regulations: 10 CFR 50.34(b)(2)(i); 10 CFR 50.34(f)(2)(iv); 10 CFR 50.34(f)(2)(v); 10 CFR 50.34(f)(2)(xi); 10 CFR 50.34(f)(2)(xiv); 10 CFR 50.34(f)(2)(xvii); 10 CFR 50.34(f)(2)(xviii); 10 CFR 50.34(f)(2)(xix); 10 CFR 50.36(c)(1)(ii)(A); 10 CFR 50.36(c)(3); 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants;" 10 CFR 50.54(jj); 10 CFR 50.55(i); 10 CFR 50.55a(h); and 10 CFR Part 50, Appendix A, GDC 1, 2, 4, 5, 10, 13, 15, 16, 20, 21, 22, 23, 24, 25, 28, 29, 64 and GDC 19.

DCA Part 2, Tier 2, Section 7.1.1, incorporates by reference NuScale TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.1.1, in addition to text from the referenced TR-1015-18653. The disposition of aspects of ASAIs 1, 3, 4, 5, and 6 relating to safety system design basis is described in Sections 7.1.1 and 7.1.6 of this report.

DCA Part 2, Tier 2, Section 7.1.1.2, states that the safety systems are used to facilitate protective actions of the MPS (i.e., reactor trip and ESF functions) in response to monitored variables exceeding pre-established limits. Table 7.1-1 identifies the specific DBEs and classifications for which MPS protective actions are credited in Chapter 15 analyses. The DBEs, including AOOs, infrequent events (IEs), and postulated accidents (PAs) for the NuScale power plant design are listed in Table 15.0-2. The MPS functional logic diagrams are shown in Figure 7.1-1a through Figure 7.1-1ao. Table 7.1-2 identifies the specific NPM variables that provide input to the MPS and includes the instrument range for covering normal, AOOs, and accident conditions and the nominal operating value at 100-percent rated thermal power (RTP).

The NMS-excore subsystem monitors the continuous reactor neutron flux from shutdown to full-rated power across three overlapping detector ranges: the source range, intermediate range, and power range. Certain monitored variables are relied on to execute protective actions if setpoints based on the analytical limits are exceeded. The analytical limits and permissive conditions for operational bypasses are summarized in DCA Part 2, Tier 2, Tables 7.1-3 and 7.1-5 for the RTS and DCA Part 2, Tier 2, Tables 7.1-4 and 7.1-5 for the ESFAS. The NMS provides safety-related input to the MPS to support its functions.

The ESFAS delays are a product of sensor response time, signal processing time, and actuation device delays. A standard 1-second signal processing time is applied for all ESFAS signals. A 1-second delay is also added to the RTS signal, which includes RTB response time and control rod detach time. Additional sensor response delays are defined in Table 7.1-6.

There are manual trip or actuate switches for each automatic trip or actuate function in the MCR. These switches are connected to the HWMs in the RTS and ESFAS chassis where the signals are isolated and converted to logic-level signals and placed on the backplane. These signals are provided to the associated EIM actuation priority logic circuits downstream of the FPGA logic.

All of the variables monitored by the MPS listed in Table 7.1-2 are sent to the SDIS and the MCS to be displayed in the MCR as required by those systems. These variables include all that are needed for reactor trip and ESF actuations, and PAM variables that would be required for monitoring after an event.

When allowed by plant procedures to reconfigure systems after a reactor trip or an ESF actuation, the components can be repositioned using the non-safety-related MCS when the enable non-safety-related control switch is activated and no automatic or manual safety actuation signal is present. All required protective actions by the MPS are automatic. There are no credited manual actuations required for the MPS to accomplish its safety functions; however, manual initiation at the division level of the automatically initiated protective actions is provided in the MCR.

The MPS and NMS are designed to operate during normal, abnormal, AOOs, IE, and accident conditions for a minimum of 72 hours during a loss of ac power. The MPS operates in PAM-only mode after a loss of ac power for 24 hours. These systems are designed to function during a loss of heating, ventilation, and air conditioning (HVAC). Protection from natural phenomena is provided by the location of the MPS and NMS cabinets in the Reactor Building, which is a seismic Category I reinforced concrete structure. Separation Groups A and C and Division I equipment, and Separation Groups B and D and Division II equipment are in different rooms in the Reactor Building, protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.

A failure modes and effects analysis (FMEA) was conducted for both the MPS and the NMS. This is a systematic procedure for addressing failures of all components of a system and for evaluating their consequences. The essential function of an FMEA is to consider each part of the system, how it may fail, and what the effect of the failure on the system would be while considering the single-failure criterion. Application of the FMEA methodology to the MPS and NMS concluded that no failure modes were undetectable or would prevent (1) the MPS from performing its RTS and ESFAS functions, (2) the NMS from performing its safety functions, and (3) accident monitoring functions.

The MPS automatically initiates a reactor trip or actuation of ESF functions when the associated setpoint is reached or exceeded. Once initiated, safety functions continue until completed. The

completion of the safety function is satisfied once all equipment is in the actuated position and the plant conditions are stabilized. The NMS does not initiate any protective functions; it only provides safety-related input to the MPS.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.1.1.4.1.2, is given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 29. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: The technical specifications associated with DCA Part 2, Tier 2, Section 7.1.1, appear in DCA Part 4, "Generic Technical Specifications," Sections 3.3 and B.3.3.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.1.1.

7.1.1.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review of the safety systems' design basis. Compliance with additional regulations stated in DCA Part 2, Tier 2, Section 7.1.1, are evaluated in the relevant sections of this report:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 4, "Safety System Designation," which requires, in part, that a specific basis be established for the design of each safety system.

- 10 CFR Part 50, Appendix A, GDC 10, "Reactor Design," requires that the reactor core and associated coolant, control, and protection systems be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of AOOs.

- 10 CFR Part 50, Appendix A, GDC 15, "Reactor Coolant System Design," requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including AOOs.

- 10 CFR Part 50, Appendix A, GDC 16, "Containment Design," requires that reactor containment and associated systems be provided to establish an essentially leaktight 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.

- 10 CFR Part 50, Appendix A, GDC 19, "Control Room," requires, in part, that equipment at appropriate locations outside the control room shall be provided with a design capability for safe shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe shutdown condition.

- 10 CFR Part 50, Appendix A, GDC 20, "Protection System Functions," requires that the protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

7.1.1.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed Section 7.1.1 of the DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to ensure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The staff's review confirmed that the information in the application and the information incorporated by reference from TR-1015-18653 address the required information relating to safety-related system design basis. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.1.1.3 and to address aspects of ASAIs 1, 3, 4, 5, and 6 relating to safety system design basis. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The NRC staff confirmed that the design bases, system design descriptions, system operation characteristics, postulated DBE analyses, and other information given in the application for each of the I&C safety-related systems satisfy the requirements of GDC 10, 15, 16, 20, and GDC 19, and Section 4 of IEEE Std. 603-1991. The I&C system characteristics described in Section 7.2 of DCA Part 2, Tier 2 are directly associated with the design bases documentation prescribed in Section 4 of IEEE Std. 603-1991. These characteristics include, for example, identification of the I&C systems' safety functions and corresponding protective actions; all monitored variables used to control each protective action; the minimum number and location of sensors required for protective purposes; plant conditions; and the range of transient and steady-state conditions throughout which the safety systems must perform, including conditions having the potential for functional degradation of safety system performance.

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details, presented in Sections 7.1 and 7.2 of DCA Part 2, Tier 2, the NRC staff confirmed that the application contains information sufficient to demonstrate that the requirements in Section 4 of IEEE Std. 603-1991 are satisfied and meets ASAIs 3, 4, 5, and 6, as described in Section 7.1.6 of this report, which require the applicant to specify the design basis for the use of the HIPS platform in safety-related systems. In addition, the NRC staff confirmed that the design-basis descriptions in the application for each of the I&C safety-related systems have the following characteristics:

- Completeness: The design-basis descriptions of reactor trip functions outlined in DCA Part 2, Tier 2, Table 7.1-3, and ESFAS functions outlined in DCA Tier 2, Table 7.1-4, address all system functions necessary to fulfill the system's safety purpose.

- Consistency: The NRC staff finds that the information in the DCA Part 2, Tier 2, Table 7.1.1 conforms to the DBE analysis of Chapter 15 of DCA Part 2, Tier 2, the mechanical and electrical system designs, and other plant system designs. DCA Part 2, Tier 2, Table 7.1-1, outlines all of the DBEs along with corresponding references to the Sections of Chapter 15 that describe these DBE analyses. For safety evaluation of the corresponding Chapter 15 Sections, see Chapter 15 of this report.

- Correctness: Based on its review of consistency between the DBE analysis provided in Chapter 15 and protection of the safety functions described in Chapter 7, the NRC staff finds that the information provided for the design-basis items is technically accurate.

- Traceability: Based on review of the DBE analyses in Chapter 15 and safety system descriptions in Chapter 6, “Engineered Safety Features,” Chapter 8, “Electrical Power,” and Chapter 9, “Auxiliary Systems,” the NRC staff finds that the information in each design-basis item is traceable to the safety analyses, plant system design documents, regulatory requirements, application commitments, or other plant documents.

- Unambiguity: The NRC staff finds that the information provided for the design-basis items, taken alone and in combination, has one and only one interpretation. The design bases do not contain contradictory statements.

- Verifiability: The NRC staff finds that the information provided for the design-basis items is verifiable by the design descriptions, design commitments, and ITAAC provided in DCA Part 2, Tier 1 Section 2.1, “NuScale Power Module,” Section 2.5, and Section 2.6 and is evaluated in Section 14.3.5 of this report.

7.1.1.4.1 Additional Considerations in the Review of Design-Basis Information

The regulation in 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991. Section 4 of IEEE Std. 603-1991 is the design-bases requirement for safety I&C systems, which correspond to I&C systems parts of the requirements stipulated in GDC 10, “Reactor Design”; GDC 15, “Reactor Coolant System Design”; GDC 16, “Containment Design”; GDC 19, “Control Room”; and GDC 20, “Protection Systems.” Below is the NRC staff’s review of the safety analysis of design bases.

Section 4.1 of IEEE Std. 603-1991 requires 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 NRC staff confirmed that this information conforms to the analysis provided in Chapter 15 of the application. The NRC staff evaluation in Chapter 15 of this report included a review of the DBEs that are examined, the selection of plant variables that are used to initiate protective action, and functional and performance requirements for systems and components.

Section 4.2 of IEEE Std. 603-1991 requires identification of safety functions and corresponding protective actions of the execute features for each DBE. Additional information to address this requirement is derived from Section 4.4 of IEEE Std. 603-1991, which discusses the identification of variables that are monitored to provide protective action. The evaluation of the completion of protective action is described in Section 7.2.3.4.3 of this report.

The NRC staff reviewed all of the DBEs and corresponding safety functions discussed in Chapter 15 of the application to gain an understanding of the DBEs considered and the initiating events that are analyzed to identify safety functions and protective actions of both sense and command features as well as execute features. Based on the review of documentation in DCA Part 2, Tier 2, Chapter 15 analyses, and Sections 7.1 and 7.2 of DCA Part 2, Tier 2 design details for corresponding protective actions, the NRC staff finds that the design meets the requirements of Sections 4.1 and 4.2 of IEEE Std. 603-1991.

Section 4.3 of IEEE Std. 603-1991 requires, in part, the identification of the permissive conditions for each operating bypass capability that is to be provided. Permissive signals are used to enable, disable, or modify the operation of actuation functions based on plant conditions. DCA Part 2, Tier 2, Table 7.1-5, adequately outlines the MPS interlocks/permissives/overrides. The evaluation of interlocks is described in Section 7.2.5 of this report. The NRC staff finds that the application includes the necessary permissive signals that maintain safety-related interlocks, interlocks associated with plant operating modes, or interlocks that provide status and control signals to other systems and alarms.

Section 4.4 of IEEE Std. 603-1991 requires, in part, the identification of variables that are monitored to provide protective action. Performance requirements, including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action, should be identified in the system designation. The NRC staff confirmed that the application includes analyses, including the applicable portion provided in Chapter 15 of the application, demonstrating that system performance requirements are adequate to ensure completion of the protective actions. Additionally, variables that control each protective action by automatic means have been identified and documented using the criteria in Sections 6.1 and 7.1 of IEEE Std. 603-1991. The evaluation of completion of protective action is described in Section 7.2.3.4.3 of this report. Section 4.4 of IEEE Std. 603-1991 also requires, in part, the identification of the analytical limit associated with each variable. The evaluation of setpoint requirements is described in Section 7.2.7 of this report. The NRC staff confirmed that an adequate margin exists between the analytical limits and the setpoints. In this context, adequate margin means the proper allowance for instrument uncertainties between (1) the device setpoint and the process analytical limit such that the system initiates protective actions before SLs are exceeded and (2) operating limits and setpoints such that there is a low probability of inadvertent actuation of the system.

Section 4.5 of IEEE Std. 603-1991 describes the minimum criteria for determining whether manual initiation and control of protective actions are allowed. Specifically, the NRC staff confirmed that the application describes the following:

- Operator manual actions are not required for responding to any DBE. However, the NuScale design provides capabilities for system-level manual initiation of the safety functions. The DCA identifies these manual controls as a backup to the automatic functions provided by the MPS, since no credited manual actions are required to mitigate DBEs. DCA Part 2, Tier 2, Section 7.1.5, identifies these manual operator actions as defense in depth and diverse measures for achieving protective actions.

- Since operator manual actions are not required for responding to any DBE, no justification is required for permitting initiation or control subsequent to initiation solely by manual means.

- The range of environmental conditions imposed on the operator during normal, abnormal, and accident conditions throughout which the manual operations will be performed.

- The variables in Section 4.4 of IEEE Std. 603-1991 that must be displayed for the operator to use in taking manual action.

Section 4.6 of IEEE Std. 603-1991 requires, in part, the identification of the minimum number and location of sensors for those variables identified in Section 4.4 of IEEE Std. 603-1991 that have a spatial dependence. The NRC staff confirmed that the application's analyses demonstrate that the numbers and locations of sensors are adequate. The evaluation of the first-of-a-kind (FOAK) advanced sensors used in the nuclear reactor, containment, and steam supply system to measure temperature, pressure, flow, and level is described in Section 7.2.6 of this report.

Section 4.7 of IEEE Std. 603-1991 requires that the design-basis documentation include the range and steady-state transient 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 must perform. The evaluation of the equipment qualification (EQ) requirements is

described in Section 7.2.2 of this report. The NRC staff confirmed that the application provides information sufficient to address the range of steady-state and transient conditions during normal, abnormal, and accident conditions stated above.

Section 4.8 of IEEE Std. 603-1991 requires, in part, identification of the conditions having the potential for functional degradation of safety system performance (including missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, and failure in non-safety-related systems). The NRC staff confirmed that the application identifies conditions having the potential for functional degradation of safety system performance, as well as the provisions that are incorporated in the design to maintain each system's capability to perform its safety functions. The evaluation of the interaction between sense and command features and other systems is described in Section 7.2.10 of this report. The NRC staff finds that the application complies with the independence criteria in Section 5.6 of IEEE Std. 603-1991 and the criteria for interactions between sense and command features and other systems in Section 6.3 of that standard.

Section 4.9 of IEEE Std. 603-1991 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design and the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. The NRC staff finds that the application complies with the single-failure criterion requirements of Section 5.1 of IEEE Std. 603-1991 and the reliability criteria in Section 5.15 of that standard, and thus complies with Section 4.9 of IEEE Std. 603-1991.

Section 4.10 of IEEE Std. 603-1991 requires identification of plant conditions after the onset of a DBE including (1) plant conditions for which the protective actions of the safety system must be initiated, (2) plant conditions that define the proper completion of the safety function, (3) plant conditions that require automatic control of protective actions, and (4) plant conditions that allow the return of a safety system to normal. The NRC staff confirmed that the application includes sufficient information to address plant conditions outlined in items 1-4 listed above. Requirements for automatic and manual initiation and control of protective actions for sense and command features are given in Sections 6.1 and 6.2 of IEEE Std. 603-1991, respectively. Requirements for automatic and manual initiation and control of protective actions for execute features are in Sections 7.1 and 7.2 of IEEE Std. 603-1991, respectively.

Section 4.11 of IEEE Std. 603-1991 requires documentation of equipment protective provisions that can prevent the safety systems from accomplishing their safety functions. The safety-related systems must be designed to accomplish their safety-related functions in accordance with the single-failure criterion in Section 5.1 of IEEE Std. 603-1991. The NRC staff considered the system's capability for test and calibration and the hazard analyses performed on the system as part of this finding. The evaluation of the related test and calibration and hazard analyses is described in Sections 7.2.15 and 7.1.8 of this report, respectively.

Section 4.12 of IEEE Std. 603-1991 requires the documentation of any other special design basis that may be imposed on the system design, such as diversity, interlocks, or regulatory agency guidance criteria. The NuScale design requires the use of two diverse FPGA technologies for the MPS separation groups and divisions. DCA Part 2, Tier 2, Table 7.1-10, outlines the differences between the two FPGA architectures. The evaluation of the diversity in the MPS architecture is described in Section 7.1.5 of this report. The NRC staff finds that the application includes the special design-basis requirements for the built-in diversity in the MPS architecture.

7.1.1.4.2 Remote Shutdown Capability

DCA Part 2, Tier 2, Section 7.1.1.2.3, "Remote Shutdown Station," states that the RSS provides an alternate location to monitor the NPM status and to operate the MCS and PCS during an MCR evacuation. An MCR evacuation is a special event and is not postulated to occur simultaneously with any DBE, nor does it cause fuel damage or result in consequential loss of function of the reactor coolant pressure boundary or primary containment barriers. The RSS provides a safe alternate location during an MCR evacuation occurrence to allow monitoring of each NPM. Events for the RSS design and licensing basis include (1) smoke caused by fire in the MCR, (2) impact of a commercial aircraft into the Control Building, and (3) loss of the Control Building as part of the loss of a large area.

At the onset of an MCR evacuation, the operators trip the reactors and initiate decay heat removal and containment isolation for each reactor before they leave the MCR. Following evacuation of the MCR, the ability to isolate the MPS manual switches to prevent spurious actuations is provided in the RSS as evaluated in Section 7.2.12 of this report. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches in the RSS.

The MCS equipment in the RSS provides an independent alternative shutdown capability that is physically and electrically separate from the controls in the MCR. The MCS equipment in the RSS provides a non-safety-related HSI and an identical set of MCS and PCS displays of the process variables necessary to monitor safe shutdown of each NPM.

The controls necessary for the operator to monitor the plant status of an immediate hot shutdown of the reactor, maintain the unit in a safe condition during hot shutdown, and perform subsequent cold shutdown of the unit are provided in the RSS. SDIS displays are not provided in the RSS as there is no manual control of safety-related equipment allowed from the RSS. However, there is an identical set of MCS and PCS displays located in the RSS provided for the operator to monitor the plant operation if evacuation of the MCR is required.

Access to the RSS is under administrative controls, as described in Section 7.2.9.4.1 of this report.

7.1.1.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.1.6 Conclusions

The NRC staff concludes that the application conforms to the guidance identified above, including the coordination with those having primary review responsibility for the accident analysis. The NRC staff concludes that the application provides information sufficient to (1) demonstrate that a documented design basis is established for the design of each I&C safety system and (2) the proposed I&C design meets the safety systems' I&C requirements, including design basis, DBE analyses, design descriptions, and operational characteristics of the safety systems. Based on the discussion above NRC staff concludes that the application satisfies the safety system design basis aspects of ASAIs 1, 3, 4, 5, and 6 listed in TR-1015-18653, Revision 2. Therefore, the NRC staff finds that the design of I&C systems satisfies the applicable requirements of GDC 10, 15, 16, 20, and GDC 19 and Section 4 of IEEE Std. 603-1991.

7.1.2 Independence

7.1.2.1 Introduction

This Section addresses the review of methods described in the application used to demonstrate independence of the I&C systems (1) between redundant portions of a safety system, (2) between safety systems and the effects of a DBE, and (3) between safety systems and other systems, as required by 10 CFR 50.55a(h). The review also addresses the concepts of physical independence, electrical independence, communications independence, and functional independence.

The NRC staff's evaluation includes other fundamental design principles, such as redundancy, predictability and repeatability, and D3 that inform the review of independence. In addition, the staff considered the architectural description, simplicity, and hazard analysis techniques and how they inform the review of independence.

7.1.2.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2, Section 7.1.2, "Independence," describes the physical, electrical, communications, and functional independence attributes of the I&C systems.

DCA Part 2, Tier 2, Section 7.1.2, incorporates by reference TR-1015-18653, Revision 2. The applicant provided DCA application-specific information in Section 7.1.2, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 8, 9, 20, 22, 23, 46, 52, 53, 55, 60, and 61, which relate to independence, is described in Section 7.1.6 of this report.

DCA Part 2, Tier 2, Section 7.1.2.1, "Physical Independence," describes the physical independence attributes of the MPS and the NMS. DCA Part 2, Tier 2, Section 7.1.2.1, specifies that the MPS and NMS conform to the guidance in RG 1.75, "Criteria for Independence of Electrical Safety Systems," Revision 3, which endorses IEEE Std. 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits," with identified exceptions and clarifications.

DCA Part 2, Tier 2, Section 7.1.2.2, "Electrical Independence," describes the electrical independence attributes of the MPS and the NMS. DCA Part 2, Tier 2, Section 7.1.2.2, specifies that the MPS and NMS conform to the guidance in RG 1.75, Revision 3.

DCA Part 2, Tier 2, Section 7.1.2.3, "Communications Independence," describes the communication independence attributes of the MPS. DCA Part 2, Tier 2, Section 7.1.2.3, specifies that the MPS conforms to the guidance in RG 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std. 7-4.3.2-2003.

DCA Part 2, Tier 2, Section 7.1.2.4, "Functional Independence," describes the functional attributes of the MPS.

TR-1015-18653, Section 4.0, "Independence," describes the HIPS platform independence features: (1) to meet the independence requirements of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003, Section 5.6, and (2) to conform with the NRC staff positions of DI&C-ISG-04.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.1.2, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 3 through 7; and Section 2.6, Table 2.6-1, Items 1 through 3. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.1.2.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.1.2.

7.1.2.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55(a)(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55(a)(2). This standard includes Section 5.6, "Independence," which requires physical, electrical, and communication independence between redundant portions of safety systems, safety systems and the effects of DBEs, and safety systems and other systems.

- 10 CFR Part 50, Appendix A, GDC 13.

- 10 CFR Part 50, Appendix A, GDC 21.

- 10 CFR Part 50, Appendix A, GDC 22.

- 10 CFR Part 50, Appendix A, GDC 24.

The guidance in DSRS Section 7.1.2 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.75, Revision 3, endorses IEEE Std. 384-1992, with identified exceptions and clarifications.

- RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications.

7.1.2.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed Section 7.1.2 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to ensure that the combination of the information in the TR and the information in the NuScale DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference from TR-1015-18653 address the required information relating to independence. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.1.2.3 and the aspects of ASAIs 8, 9, 20, 22, 23, 46, 52, 53, 55, 60, and 61 that relate to independence. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The HIPS platform, as described in TR-1015-18653, Revision 2, has been approved for use by the NRC. The NRC staff's review of the HIPS platform evaluated all aspects of the internal platform features, including concepts implemented on the individual HIPS platform modules, isolation concepts used to support monitoring and indication features, and control of access features. The staff finds that the applicant has committed to implementing the electrical, physical, and communication independence features in the NuScale design in accordance with the functionality described in TR-1015-18653, Revision 2.

As explained in the discussion below, the NRC staff evaluated the I&C system design described in the application and finds that it complies with the independence requirements of GDC 13, 21, 22, and 24 in Appendix A to 10 CFR Part 50 and Section 5.6 of IEEE Std. 603-1991.

The NRC staff reviewed the NuScale DCA to verify that the requirements of IEEE Std. 603-1991 Section 5.6 and GDC 13, 21, 22, and 24 have been adequately addressed for the safety systems. GDC 13 requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety and that appropriate controls be provided to maintain these variables and systems within prescribed operating ranges. GDC 21 requires redundancy and independence designed into the protection system to be sufficient to assure that no single failure results in a loss of the protection function and that removal from service of any component or channel does not result in loss of the required minimum redundancy. GDC 22 requires the protection system to be designed to assure that the effects of natural phenomena and of normal operating, maintenance, testing, and PA conditions on redundant channels do not result in loss of the protection function. GDC 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or removal from service of any protection system component or channel common to control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Section 5.6 of IEEE Std. 603-1991 requires independence between (1) redundant portions of a safety system, (2) safety systems and effects of DBE, and (3) safety systems and other systems.

The following discussion explains how, through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details shown in DCA Part 2, Tier 2, Section 7.1.2, the NRC staff confirmed that the proposed design exhibits independence between (1) redundant portions of a safety system, (2) safety systems and the effects of DBEs, and (3) safety systems and other systems. For each of these areas, the NRC staff evaluated the following: (1) physical independence, (2) electrical independence, (3) communications independence, and (4) functional independence.

7.1.2.4.1 Physical Independence

Physical independence is attained by physical separation and physical barriers. The NRC staff considered whether the application contains sufficient information to demonstrate the separation of (1) redundant portions of the safety system and (2) safety (protection) and non-safety-related (control) systems to confirm that all interfaces among redundant portions of the safety system and between safety systems and non-safety-related systems have been properly identified and addressed.

The RG 1.75, Revision 3, describes a method acceptable to the NRC staff for complying with NRC regulations with respect to the physical independence requirements of the circuits and electrical equipment that comprise or are associated with safety systems. RG 1.75 endorses IEEE Std. 384-1992, with identified exceptions and clarifications. The review of physical separation of electrical cables is evaluated in Section 8.3 of this report.

Module Protection System

DCA Part 2, Tier 1, Section 2.5, states the following:

> *Physical separation exists between the redundant separation groups and divisions of the MPS Class 1E instrumentation and control current-carrying circuits, and between Class 1E instrumentation and control current-carrying circuits and non-Class 1E instrumentation and control current-carrying circuits*.

DCA Part 2, Tier 2, Section 7.1.2, describes conformance with IEEE Std. 384-1992 for the I&C systems, as endorsed by RG 1.75. DCA Part 2, Tier 2, Section 7.1.2.1, states that the "separation group and division independence is maintained throughout the system, extending from the sensor to the devices actuating the protective function." DCA Part 2, Tier 2, Section 7.1.2.1, further states that the "wiring for redundant divisions uses physical separation and isolation to provide independence of the circuits. Separation of wiring is achieved using separate wireways and cable trays." Because the design conforms to the methods described in RG 1.75, the NRC staff finds that separation group and division independence is maintained throughout the MPS.

The MPS equipment rooms are seismically qualified and located in separate fire zones. The rooms containing Separation Group A and C (Division I) MPS and NMS equipment are in a separate fire zone from the MPS equipment rooms containing Separation Group B and D (Division II) MPS and NMS equipment. The geographic separation and electrical isolation between these cabinets reduces the possibility of a common-cause failure (CCF). The outputs of each division are isolated from each other. Based on the above, the NRC staff finds that a loss of one division will not cause loss of the system function.

Neutron Monitoring System

DCA Part 2, Tier 1, Section 2.6, states the following:

> *Physical separation exists between the redundant divisions of the NMS Class 1E instrumentation and control current-carrying circuits, and between Class 1E instrumentation and control current-carrying circuits and non-Class 1E instrumentation and current-carrying circuits.*

DCA Part 2, Tier 2, Section 7.1.2.1, states that the NMS separation groups are physically independent and separate. The NMS-excore neutron detectors are installed 90 degrees equidistant around the NPM, and the associated cabling is routed in physically separate cable trays and raceways. The NMS hardware and signal processing equipment associated with the MPS divisions is installed in separate, seismically qualified equipment rooms. Because the design conforms to RG 1.75, the NRC staff finds that physical independence is maintained throughout the NMS.

DCA Part 2, Tier 2, Section 7.1.2.1, states that the SDIS has two separate and independent hubs. The SDIS hubs are located in the seismically qualified Control Building in the same divisionally separate rooms as the PPS.

Conclusion

The NRC staff finds that the safety I&C system design meets the physical independence requirements because (1) the safety system conforms to RG 1.75, (2) the design precludes the use of components that are common to redundant portions of the safety system, and (3) the safety systems have adequate physical separation and physical barriers. Based on the discussion above and the evaluation in Section 8.3 of this report, the NRC staff concludes that

the application satisfies the physical independence aspects of ASAIs 8, 20, 22, 23, and 60. Therefore, the NRC staff finds that the NuScale I&C design complies with the physical independence requirements of Section 5.6 of IEEE Std. 603-1991.

7.1.2.4.2 Electrical Independence

The NRC staff confirmed that the I&C systems conform to the electrical independence guidance of RG 1.75, Revision 3. The relevant guidance includes electrical isolation criteria for circuits and electrical equipment that comprises or is associated with safety systems.

DCA Part 2, Tier 2, Section 7.1.2, describes conformance with IEEE Std. 384-1992 for the I&C systems, as endorsed by RG 1.75. The review of physical separation of electrical cables is evaluated in Section 8.3 of this report.

DCA Part 2, Tier 1, Section 2.5, states the following:

> *Electrical isolation exists between the redundant separation groups and divisions of the MPS Class 1E instrumentation and control circuits, and between Class 1E instrumentation and control circuits and non-Class 1E instrumentation and control circuits to prevent the propagation of credible electrical faults.*

DCA Part 2, Tier 1, Section 2.6, states the following:

> *Electrical isolation exists between the redundant divisions of the NMS Class 1E instrumentation and control circuits as well as between Class 1E instrumentation and control circuits and non-Class 1E instrumentation and control circuits to prevent the propagation of credible electrical faults.*

Electrical isolation between the safety-related MPS and associated non-safety-related systems is provided by (1) galvanic isolation between the non-safety-related sensor inputs to the MPS, (2) transmit-only or receive-only fiber optic ports, (3) dc-to-dc and galvanic isolation at the HWM, and (4) isolation devices in the electrical power supply.

Galvanic Isolation between the Non-safety-related Sensor Inputs to the Module Protection System

The SFM provides Class 1E isolation by galvanic isolation between the non-safety-related sensor inputs to the MPS. In TR-1015-18653, Section 4.0, “Independence,” the applicant describes the HIPS platform galvanic isolation features used to isolate non-safety-related inputs. The NRC staff’s evaluation of the HIPS platform galvanic isolation features is documented in the SE for TR-1015-18653 (ADAMS Accession No. ML17116A097).

Safety-Related to Non-safety-related Communication Interface

DCA Part 2, Tier 2, Section 7.1.2.2, states that communication to non-safety-related systems is provided through transmit-only or receive-only fiber optic ports. These ports provide electrical isolation for either transmit-only or receive-only unidirectional communication links.

In TR-1015-18653, Section 4.6.2, “Communication Independence outside the Platform,” the applicant states that all data communications going out of or into the HIPS chassis are done through the one-way isolated communication ports on the CMs. The CMs are part of the safety-related HIPS platform and are qualified as safety-related modules and Class 1E to non-Class 1E isolation.

The MIB-CM provides Class 1E isolation between the Class 1E equipment and non-safety-related equipment via four copper-to-fiber-optic ports. The remaining copper-to-fiber-optic ports on the separation group MIB-CM are configured as receive-only and receive information from the MWS through a temporary cable that is connected during maintenance activities.

Communication to non-safety-related systems is provided through transmit-only or receive-only fiber optic ports. These ports provide electrical isolation for either transmit-only or receive-only unidirectional communication links.

Hard-Wired Inputs to the Module Protection System

In TR-1015-18653, Section 2.5.5, "Hard-Wired Module," the applicant described the HWM. DCA Part 2, Tier 2, Section 7.1.2.2, states that the HWM receives signals from the manual switches in the MCR, from the discrete, hard-wired non-safety-related control signals from the MCS, and from the trip/bypass switch panels.

The HWM provides dc-to-dc and galvanic isolation between the safety-related MPS and non-safety-related MCS. The HWM is constructed of discrete logic components only; there are no programmable devices.

The HWM performs a safety-related function to provide electrical isolation (i.e., dc-dc and galvanic isolation) for the backplane and modules from the external manual switches (e.g., enable non-safety-related switch) and the non-safety-related control signals. These isolation devices conform to RG 1.75, Rev. 3. The enable non-safety-related switch is classified as part of the MPS and is used to prevent spurious non-safety-related control signals from adversely affecting safety-related components.

The APL (which is constructed of discrete components and part of the EIM) is designed to provide priority to safety-related signals over non-safety-related signals. When the enable non-safety-related switch is not active, the non-safety-related control signal is ignored. If the enable non-safety-related is active, and no automatic or manual safety actuation command is present, the non-safety-related control signal can control the component. In this case, the HWM provides isolation for the non-safety-related signal path when the enable non-safety-related switch is active.

Electrical Power Supply

DCA Part 2, Tier 1, Section 2.5, states, "Electrical isolation exists between the highly reliable dc power system-module-specific (EDSS-MS) subsystem non-Class 1E circuits and connected MPS 1E circuits to prevent the propagation of credible electrical faults."

DCA Part 2, Tier 1, Section 2.6, states, "Electrical isolation exists between the NMS Class 1E circuits and connected non-Class 1E circuits to prevent the propagation of credible electrical faults."

DCA Part 2, Tier 2, Section 7.1.2.2, states that the MPS receives electrical power from the non-safety-related EDSS. It further states that the NMS separation groups receive isolated, independent power supplied by the EDSS through Class 1E isolation devices that are qualified as part of the NMS.

The NRC staff confirmed the use of redundant power sources within the MPS. Figures 7.0-11a, "Module Protection System Power Distribution," and Figure 7.0-11b, "Module Protection System Power Distribution," show that separate power feeds energize redundant protection divisions.

Interfaces between safety and non-safety-related systems use isolation devices to maintain electrical independence. The NRC staff confirmed that isolation devices used to transmit signals between independent divisions are classified as part of the safety system and powered in accordance with IEEE Std. 603-1991 and the guidelines of RG 1.75, Revision 3. Isolation devices are considered part of the safety system and are qualified as Class 1E. The NRC staff also confirmed that each isolation device is powered from a safety-related system (i.e., MPS and NMS).

The PPS, SDIS, ICIS, MCS, and PCS are non-safety-related systems and are separated from safety-related equipment.

DCA Part 2, Tier 2, Section 7.1.2.2, states that the SDIS receives electrical power from the EDSS. The SDIS divisions are powered from independent EDSS sources.

Conclusion

The NRC staff finds that the safety I&C system design meets the electrical independence requirements because the safety I&C system conforms to RG 1.75, Revision 3, and the NuScale design safety systems utilize separate and redundant power sources. Based on the discussion above and the evaluation in Section 8.3 of this report, the NRC staff concludes that the application satisfies the electrical independence aspects of ASAIs 20, 22, 23, 46, 60, and 61. Therefore, the NRC staff finds that the NuScale I&C design meets the electrical independence requirements of Section 5.6 of IEEE Std. 603-1991.

7.1.2.4.3 Communications Independence

The NuScale I&C systems consist of the MPS and NMS safety-related systems and the PPS, SDIS, MCS, PCS, ICIS, HPN, and RM non-safety-related systems.

DCA Part 2, Tier 1, Section 2.5, states that “communications independence exists between redundant separation groups and divisions of the Class 1E MPS.” It further states that “communications independence exists between the Class 1E MPS and non-Class 1E digital systems.”

DCA Part 2, Tier 2, Section 7.1.2.3, states that “with the exception of interdivisional voting, the communication within the MPS separation group is independent and does not rely on communication from outside the respective separation group or division to perform a safety function.” It further states that “the MPS separation groups perform independent signal conditioning and trip determination and provide that input to the scheduling and bypass module (SBM) which provides inputs to the schedule and voting module (SVM) for the two-out-of-four voting logic.” For voting purposes, the communication uses point-to-point fiber optics through the SDB connections between the SBM and SVMs. The divisions do share voting data with other divisions through the SVM. The division voters are not dependent on voting data from other divisions because the division voters will still be able to complete their safety function, even if the SVM voting data have errors or are not available. The division voters would apply a safe default for the missing inputs.

Module Protection System Communication Scheme

TR-1015-18653, Revision 2, provides an overview of the design of data communications within the MPS and communications between the MPS and non-safety-related systems. The NRC staff evaluated TR-1015-18653 and issued an SE (ADAMS Accession No. ML17116A097). TR-1015-18653 describes the communications buses of the HIPS modules.

The MPS communications architecture is rigorously segmented into five separate and distinct communication domains based on the safety function of the communication. These buses are:

- The three SDBs (i.e., SDB1, SDB2, and SDB3) are exclusively used for the automatic actuation path, communicating trip/actuate or no trip/actuate information. The SDB communication scheme is described in TR-1015-18653, Section 2.6.1, "Safety Data Bus."

- The MIB is used for communicating process values to the non-safety-related control system(s) and monitoring and indication information to safety displays and plant historians. The MIB communication scheme is described in TR-1015-18653, Section 2.6.2, "Monitoring and Indication Bus Protocol."

- The CTB is exclusively used for maintenance activities, such as calibrating or testing a module. The CTB communication scheme is described in TR-1015-18653, Section 2.6.3, "Calibration and Test Bus Protocol."

In the SE for TR-1015-18653, the NRC staff concluded that these three types of communications buses meet the requirements of IEEE Std. 603-1991, as supplemented by IEEE Std. 7-4.3.2-2003 and DI&C-ISG-04. The staff's review of these communications schemes supplements the conclusions made in the TR-1015-18653 SE. Specifically, the staff evaluated the application of these communications schemes for data communications within the NuScale I&C systems.

The five communication buses (i.e., SDB1, SDB2, SDB3, MIB, and CTB) use a master-slave communication protocol and are used only for intradivisional communication. This provides the capability for communication on the corresponding communication bus of the backplane. There can be only one master (e.g., SBM) on a communication bus, and it must be a communication engine on a CM. Each of the four fiber-to-copper physical layers can be configured as receive-only or transmit-only.

The MPS interdivisional communication is performed using point-to-point fiber optic communications through the SDB connections between the SBM and SVMs. Interdivisional communication must be through the transmit-only or receive-only fiber optic ports. Unlike the RS-485 buses, connections to and from the fiber optic ports are physical point-to-point connections.

Deterministic Communication

DCA Part 2, Tier 2, Section 7.1.2.3, states that communication is deterministic and does not use interrupts or handshaking. The NRC staff finds that the NuScale I&C safety-related systems design is adequate to provide for data communications reliability to meet Section 5.15 of IEEE Std. 603-1991. Specifically, the NRC staff finds that the use of deterministic cyclic processing without the use of process-driven interrupts for all safety applications enables deterministic data communications for NuScale I&C safety-related systems. The NRC staff's evaluation of TR-1015-18653 related to deterministic communication is described in an SE (ADAMS Accession No. ML17116A097). The evaluation of the isolation devices is documented in Sections 7.1.2.4.1 and 7.1.2.4.2 of this report.

Performance of Safety Functions

DSRS Section 7.1.2 states that communication faults should not adversely affect the performance of required safety functions. It also states that the design should identify and address potential hazards to and from the data communications equipment. Provisions for

communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

DCA Part 2, Tier 2, Section 7.1.2.3, states that the MPS interdivisional communication is performed using point-to-point fiber optic communications through the SDB connections between the SBM and SVMs. As discussed in the TR-1015-18653 SE, the NRC staff finds that the deterministic behavior of the system, as described in TR-1015-18653, Section 7, "Repeatability and Predictability," assures adequate performance of the data communications system to accomplish its safety functions to meet Section 5.5 of IEEE Std. 603-1991.

Communication Faults

Section 4.6 of TR-1015-18653 states that the communication within the MPS is performed by dedicated logic communication engines.

DCA Part 2, Tier 2, Section 7.2.3.2, states that the "MPS platform is designed with redundancy and embedded self-test capability to assure system integrity by detecting and alarming faults in the MCR." Thus, failures resulting in the MPS can be identified through anomalous indication and alarms in the MCR. The NRC staff also finds that the use of cyclic redundancy check (CRC) for error detection conforms to RG 1.152. The evaluation of the diagnostics and testing capabilities of the MPS platform is described in Section 7.2.15 of this report.

TR-1015-18653, Section 8, describes the self-testing capabilities of the HIPS platform. The TR-1015-18653 SE concluded that the built-in self-test (BIST) feature in the FPGA logic is separate and independent of the FPGA safety function logic; thus, the programming of the safety function FPGA logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic. The evaluation of the diagnostics and testing capabilities of the MPS platform is described in Section 7.2.15 of this report.

Therefore, the NRC staff finds that the communication processing faults in one safety division would not adversely affect performance of the safety function in other divisions. The review of functional independence is described in Section 7.1.2.4.4 of this report.

Completion of Protective Action

All safety functions are performed without interruption by any other signals, regardless of whether these signals are valid or erroneous. The SBM sequentially polls the individual SFMs to collect data. Once the data messages are received by the SBM, they are assembled into a single message that is transferred via triple redundant communication buses to the divisional level scheduling and voting module logic. This message is a one-way operation with no handshaking or receipt acknowledgment. The review of completion of protective action is evaluated in Section 7.2.3.4.3 of this report.

Communications from Non-safety-related Module Control System to the Safety-Related Module Protection System

As described in TR-1015-18653, there are no digital communications from the non-safety-related to the safety-related systems. Non-safety-related control signals from the MCS to the MPS are nondigital discrete signals routed and isolated through an HWM to the actuation priority logic within the EIM. During normal plant operation, non-safety-related control is prohibited and blocked by the enable non-safety-related control switch, thus providing electrical isolation between non-safety-related systems and the safety-related MPS.

Monitoring of the safety-related components is achieved by receiving one-way communications from the MPS to the MCS through isolation one-way communication ports on the MIB

communication module. DCA Part 2, Tier 2, Figure 7.0-1, shows a unidirectional data diode, firewalled connection from the MCS to the plant network. The review of control of access is evaluated in Section 7.2.9.1 of this report.

Each division of MPS has a non-safety-related MWS for the purpose of maintenance and calibration. The one-way, read-only data are connected through the MPS gateway for its division and are available continuously on each division's MWS. The MWS is used to update tunable parameters in the SFMs when the safety function is out of service. The evaluation of access controls of the MWS is described in Section 7.2.9.1 of this report.

Communication Independence between the Module Control System and the Plant Network

The network interface devices for each NuScale power module's MCS domain controller/ historian provide the interface between the HMI network layer and the control network layer. DCA Part 2, Tier 2, Figure 7.0-1, shows a unidirectional data diode, firewalled connection from each NuScale power module's MCS to the plant network. The NRC staff finds this approach acceptable because the information from each NuScale power module's MCS to the plant network is through one-way, transmit-only, isolated outputs. The review of control of access is evaluated in Section 7.2.9 of this report.

Actuation Priority Logic

DSRS Section 7.1.2 states that the priority modules should be safety related. A command initiating a safety function should have the highest priority and should override lower priority commands. Any instance in which a command initiating a safety function does not have the highest priority should be identified, and the conditions that justify the reduction in priority should be explained. All requirements that apply to safety software should also apply to priority module software. The priority module software should be stored in nonvolatile memory to prevent online alteration.

In DCA Part 2, Tier 2, Section 7.1.2, the applicant states that the APL is classified as part of the safety system and is constructed of discrete logic components. The APL accepts commands from three sources: (1) digital trip signal from the SFM, (2) nondigital manual trip signal from its associated RTS division, and (3) nondigital manual control signals from the MCS. Furthermore, DCA Part 2, Tier 2, Section 7.1.5.1.3, states that the "limitations on when the enable non-safety-related control switch can be positioned to allow control of safety-related components from non-safety-related controls are controlled by the plant operating procedures described in Section 13.5.2."

DCA Part 2, Tier 2, Section 7.2.3.3, states the following:

> *If the non-safety-related control inputs are disabled by the enable non-safety-related control switch, then non-safety-related control inputs are rejected and not processed by the APL circuit.*
>
> *For cases when the enable non-safety-related control switch is enabled to allow non-safety-related control inputs, there must be no active RTS or ESF manual or automatic active signal present. If the enable non-safety-related control switch is enabled, and there is no active RTS or ESF signal, then the non-safety-related manual control inputs from the MCS are used by the APL circuit to control the final component (e.g., containment isolation valve).*
>
> *During the time the non-safety-related control inputs are enabled, if an automatic or manual RTS or ESF signal is generated and received by the APL circuit, the actuation priority logic immediately disables the enable non-safety-related control*

logic permissive and rejects all non-safety-related control inputs. The actuation priority logic circuit processes the RTS or ESF command to position the final actuation device to its safe state.

Re-initiation of manual controls from non-safety-related equipment is possible only if the protective action has gone to completion and the operator deliberately blocks the safety signal using the override function via the manual override switches provided or the initiating signal is no longer present.

For the APL, the signals originating from the safety system have priority over signals from the non-safety-related system. The priority logic section of the EIM is developed using discrete analog components and is downstream of the automatic digital portion of the safety system. The NRC staff finds this approach acceptable because the automatic or manual RTS or ESF signal has the highest priority.

Neutron Monitoring System

DCA Part 2, Tier 2, Section 7.1.2.3, states that the "NMS is an analog system with no digital communication protocols." The NMS and MPS operate as independent analog systems, and there is no digital communication between the NMS and the MPS. The NRC staff finds this approach acceptable because the communications independence in the NMS is maintained by implementing hard-wired connections directly to the MPS.

Safety Display and Indication System

The SDIS hub receives data from the MPS gateway and PPS MIB communication module. Each NuScale power module's MPS gateway delivers data to a separate communication module within the SDIS hub. The SDIS hub distributes the data it receives from the MPS and PPS to the DIM associated with the respective NPM or PPS through one-way, optically isolated fiber optic cables. Data from each of the communication modules on the SDIS hub for each SDIS hub rack are aggregated into a single communication module. This module polls each of the communication modules on its rack through the backplane for the rack. The communication module then sends the aggregated information to the PCS through a unidirectional, optically isolated interface. The NRC staff finds this approach acceptable because the information from the MPS and PPS to the SDIS is through one-way, transmit-only, isolated outputs.

Communication Independence between the Plant Protection System and the Plant Control System

DCA Part 2, Tier 2, Section 7.1.2.3, states, "Independence between the PPS and PCS is maintained by establishing one-way communications from PPS to PCS through isolation devices that are components of the PPS." The NRC staff finds this approach acceptable because the information from the PPS to the PCS is through one-way, transmit-only, isolated outputs.

Communication Independence between the Plant Control System and the Plant Network

The network interface devices for the PCS domain controller/historian provide the interface between the HMI network layer and the control network layer. DCA Part 2, Tier 2, Figure 7.0-1, shows a unidirectional data diode, firewalled connection from the PCS to the plant network. The NRC staff finds this approach acceptable because the information from the PCS to the plant network is through one-way, transmit-only, isolated outputs. The review of control of access is evaluated in Section 7.2.9 of this report.

DCA Part 2, Tier 2, Section 7.0.4, provides information on configuration of the slave modules to alarm and assume a fail-safe state, as shown in Table 7.1-1 (below) of this report. The slave modules (e.g., SFMs and EIMs) are configured to provide an alarm in the MCR and assume a fail-safe state.

The MPS and PPS use communication schemes that are described in the NRC staff-approved TR-1015-18653. The NRC staff finds this acceptable because the communication schemes specific to the NuScale I&C architecture have been approved by staff in the SE for TR-1015-18653 (ADAMS Accession No. ML17116A097).

Table 7.1-1: Configuration of the Slave Modules to Alarm and Assume a Fail-Safe State

Slave Module	Fail-Safe State	Alarm
The SFMs are a slave to the SBM on the safety data communication bus.	The fail-safe state for the SFM on that communication bus is to not respond to the communication bus master.	If an SFM identifies a failure on a communication bus, the SFM generates an alarm to the SDIS and MCS.
The SFMs are a slave to the MIB-CM on the MIB bus.	The fail-safe state for the SFM on that communication bus is to not respond to the bus master.	If the SFM identifies a failure on a communication bus, the SFM generates an alarm to the SDIS and MCS. By not receiving a response from an SFM, the MIB-CM also generates an alarm.
The SVMs are slaves to the SBMs on the safety data communication bus.	The fail-safe state for that communication bus on the SVM is to demand a trip or actuation of all protective functions.	If an SVM identifies a failure on a communication bus, the SVM generates an alarm to the SDIS and MCS.
The SVMs are slaves to the MIB-CM on the monitoring and indication communication bus.	The fail-safe state for the SVM on the monitoring and indication communication bus is to not respond to the communication bus master.	The alarm and status information from the MPS is provided to the SDIS and MCS.
The EIMs in the RTS and ESFAS are slaves to the SVMs on the safety data communication bus.	The fail-safe state for protective functions on EIMs is to demand a trip or actuation.	The alarm and status information from the MPS is provided to the SDIS and MCS.
The EIMs in the RTS and ESFAS are slaves to the MIB-CM on the MIB bus.	The fail-safe state for the EIM on the monitoring and indication communication bus is to not respond to the communication bus master.	The alarm and status information from the MPS is provided to the SDIS and MCS.

Conclusion

The NRC staff finds that the NuScale safety I&C system design meets the communication independence requirements because it (1) meets the requirements of IEEE Std. 603-1991, Section 5.6 and (2) conforms to RG 1.152 and DI&C-ISG-04. Based on the discussion above, the NRC staff finds that the application satisfies the communications independence aspects of ASAIs 22, 52, 53, 55, 60, and 61.

7.1.2.4.4 Functional Independence

Functional independence provides additional assurance of the isolation of a safety system from other safety systems. Functional independence seeks to prevent safety function failures by ensuring that physically and electrically independent portions of safety systems (with the exception of coincidence voting) do not depend on information from other independent portions of the safety system. The concept of functional diversity (using different variables, different technologies, different logic or algorithms, or different actuation means to provide several ways of detecting and responding to a significant event) helps accomplish functional independence but does not totally address it.

Considering functional independence in the I&C system design helps demonstrate that the successful completion of the system's safety functions is not dependent on any behavior, including failures and the normal operation of another system, or on any signals, data, or information derived from another system. Functional independence could also be used as a means of achieving isolation between redundant systems.

TR-1015-18653, Section 4, provides an overview of the functional independence principles for the safety-related MPS architecture. The NRC staff evaluated TR-1015-18653 and issued an SE approving the HIPS platform (ADAMS Accession No. ML17116A097).

The MPS architecture consists of four separation groups and two divisions of the RTS and ESFAS in a safety system. Each bus is a differential bus with a single master and multiple slaves. The three CMs connected to SDBs are the bus masters for the three SDBs. The MIB-CM is the bus master for the MIB and the CTB.

In the MPS, voting logic is used to support reactor trip and ESF functions. Since a voting scheme is used for these safety functions, and any partial trip or ESF actuation function is accomplished before the voting function, the NRC staff finds that the MPS separation groups and divisions are self-reliant and have no dependency on functions outside the separation groups or divisions.

DCA Part 2, Tier 2, Section 7.1.1, states that the RTS and ESFAS protective functions listed in Tables 7.1-3 and 7.1-4 are assigned to a single and independent SFM within the MPS. For each protective function, the associated sensor, signal conditioning, and trip determination are performed by a single, independent SFM. There is one-to-one correspondence for each SFM and its associated protective function. The NRC staff finds that this approach is acceptable because it provides functional independence within each separation group from other protective safety functions, as well as independence across the separation groups and divisions within the MPS.

DCA Part 2, Tier 2, Section 7.1.2, states that the MPS separation group components (SFM, SBM, and SDB) are functionally independent from the division components (SVM, EIM) and are installed in physically separate cabinets providing functional independence between the separation group components and division components.

DCA Part 2, Tier 2, Section 7.1.2.4, states that there are no shared functions between the MPS separation groups or divisions. The MPS separation groups and divisions are self-reliant and have no dependency on functions outside the separation groups or divisions. The MPS communication architecture is isolated between the separation groups and other non-safety-related systems, which supports functional independence. The evaluation of isolation is described in Section 7.1.2.4.1 of this report.

DCA Part 2, Tier 2, Section 7.1.2.4, describes the various rules to support functional independence with the SFM and the EIM configurations within the MPS. These rules are

described in Table 7.1-2 of this report. The safety functions required for the MPS are distributed deliberately across several SFMs based on their inputs. The SBMs have the separate function of collecting and transmitting trip determination data. The SVMs have the separate function of collecting trip determination data, voting, and initiating protective actions. The allocation of field components to EIMs is a deliberate process for limiting the safety functions required for each EIM.

Table 7.1-2 of this report provides the general rules to support functional independence for the SFMs and EIMs.

- The safety functions required for the MPS are distributed deliberately across several SFMs based on their inputs.
- The SBMs have a separate function of collecting and transmitting trip determination data.
- The SVMs have a separate function of collecting trip determination data, voting, and initiating protective actions.
- The allocation of field components to EIMs is a deliberate process for limiting the safety functions required for each EIM.

Table 7.1-2: General Rules to Support Functional Independence in the SFM and EIM

Module	General Rules
SFM	Sensor inputs to input-sub modules on an SFM must all have the same safety classification (i.e., all safety-related sensor inputs or all non-safety-related sensor inputs). The intent is to keep non-safety-related sensor inputs on separate SFMs.
	For SFMs with multiple inputs, only process variable inputs that are related to the same function are assigned to the same SFM.
EIM	If one of the two groups of field components is used to perform a safety-related function, the other group must also be used to perform a safety-related function. The intent is to prevent a group that performs only non-safety-related functions from being actuated by an EIM performing a safety-related function.
	An EIM performs the same actuation on each group of field components regardless of which protective action is demanded. The intent is to have an EIM perform the same sequence of actuations regardless of which safety function is demanded.
	Where the primary group of components has a backup group, the primary and backup group is actuated by different EIMs. The intent is to keep backup groups (i.e., feedwater-regulating valves, secondary main steam isolation valves, and secondary main steam isolation bypass valves) separate from primary groups (i.e., feedwater isolation valves, main steam isolation valves, and main steam isolation bypass valves).

In Section 3.2.3, “Functional Independence,” of the TR-1015-18653 SE, the NRC staff found that the BIST feature in the FPGA logic is separate and independent of the FPGA safety function logic; thus, the programming of the safety function FPGA logic is not made more complex by the inclusion of the diagnostic and self-test FPGA logic.

Based on the discussion above, the NRC staff finds that the I&C safety-related systems design meets the functional independence aspects of ASAI 9. Therefore, the NRC staff finds that the I&C safety-related systems design meets the functional independence requirement of IEEE Std. 603-1991, Section 5.6.1.

7.1.2.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.2.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed I&C systems address the fundamental design principle of independence among safety divisions, between redundant portions of a safety system, between safety systems and the effects of a DBE, and between safety systems and other systems. Based on the discussion above, the NRC staff concludes that the NuScale I&C design meets the aspects of ASAIs 8, 9, 20, 22, 23, 46, 52, 53, 55, 60, and 61 listed in TR-1015-18653, Revision 2, that relate to independence. On this basis, the NRC staff finds that the design of I&C systems conforms to the guidance in RG 1.75, Revision 3; RG 1.152, Revision 3; RG 1.53, Revision 2, "Application of the Single-Failure Criterion to Safety Systems," and satisfies the independence requirements of GDC 13, 21, 22, and 24, as well as Section 5.6 of IEEE Std. 603-1991.

7.1.3 Redundancy

7.1.3.1 Introduction

This Section addresses the review of redundancy, which is commonly used in I&C safety systems to achieve system reliability goals and meets the single-failure criterion. The application should provide information that describes the level of redundancy used in the safety system to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. In addition to the redundancy, the application describes the means employed in the I&C design for guarding against CCF.

The NRC staff's evaluation includes other fundamental design principles, such as independence, predictability and repeatability, and D3 to inform the review of redundancy. In addition, the staff considered the architectural description, simplicity, and hazard analysis techniques and how they inform the review of redundancy.

7.1.3.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2, Section 7.1.3, "Redundancy," describes the redundancy attributes of the I&C systems.

DCA Part 2, Tier 2, Section 7.1.3, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in DCA Part 2, Tier 2, Section 7.1.3, in addition to the information from the referenced TR-1015-18653. The disposition of ASAIs 12, 13, 14, 21, and 32, which relate to redundancy, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 5.0, "Redundancy," describes the HIPS platform design concepts that address the fundamental design principle of redundancy to meet the single-failure criterion requirements of IEEE Std. 603-1991, Section 5.1.

ITAAC: There are no ITAAC associated with DCA Part 2, Tier 2, Section 7.1.3. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.1.3.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.1.3.

7.1.3.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.1, "Single-Failure Criterion." Section 5.1 states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but nondetectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

- 10 CFR Part 50, Appendix A, GDC 21

- 10 CFR Part 50, Appendix A, GDC 24

The guidance in DSRS Section 7.1.3 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance document provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.53, Revision 2, which endorses IEEE Std. 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," with identified exceptions and clarifications.

7.1.3.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed Section 7.1.3 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the NuScale DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application from TR-1015-18653 address the required information relating to redundancy. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.1.3.3 and to address aspects of ASAIs 12, 13, 14, 21, and 32, which relate to redundancy. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

Single-Failure Criterion

Through a review of design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details shown in DCA Part 2, Tier 2, Section 7.1.3, the NRC staff confirmed that the application provides information sufficient to conform with the single-failure criterion in RG 1.53. IEEE Std. 379-2000 provides a detailed discussion of how the safety I&C systems address the single-failure criterion that the NRC staff considered in the review.

The NRC staff's review confirmed that (1) an evaluation of the effects of each component failure mode on the overall system was performed, (2) any component failure mode that could contribute to a failure of the safety system was identified, (3) the design of the safety system is such that no single failure of a component resulted in unacceptable spurious actuations, and (4) necessary action was taken to eliminate, prevent, or control failure modes. This confirmation was achieved by reviewing the information in DCA Part 2, Tier 2, Section 7.1.3, and the FMEAs for the MPS and NMS. The NRC staff examined the MPS and NMS FMEAs in accordance with IEEE Std. 352-1998, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," and IEEE Std. 379-2000. The NRC staff confirmed that no failure modes of the MPS were identified that were undetectable or would prevent the MPS from performing its RTS, ESFAS, and accident monitoring functions. In addition, the staff confirmed that no single failure exists that would prevent the NMS from performing its safety function.

RG 1.53 states that central to meeting the single-failure criterion is the elimination of nondetectable failures. This is also stated in Section 1 of IEEE Std. 603-1991. TR-1015-18653, Section 8, "Calibration, Testing, and Diagnostics," describes the overlapping testing capabilities of the MPS platform to eliminate nondetectable failures (see Section 3.1.9 of the NRC staff's SE of TR-1015-18653). DCA Part 2, Tier 2, Section 7.2.15.2, "I&C system testing," describes the use of overlapping BIST and periodic surveillance testing to eliminate nondetectable failures. The calibration and testing capabilities of the MPS and NMS are evaluated in Section 7.2.15 of this report, which also addresses the requirements in 10 CFR Part 50, Appendix A, GDC 21, that the protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred. The NRC staff confirmed that the FMEAs provide a satisfactory demonstration of the system's fault tolerance under various scenarios. Based on the coverage of testing and the alarms described in TR-1015-18653, Revision 2, and the demonstration of the system's fault tolerance under various scenarios, the NRC staff finds that the NuScale design meets ASAIs 12, 13, and 14, as described in Section 7.1.6 of this report.

As described in RG 1.53, independence is also key to redundancy. DCA Part 2, Tier 2, Section 7.1.2.1, "Physical Independence," states, in part, that the "MPS Separation Groups A, C, and Division I equipment are located in rooms on the 75'-0" elevation of the Reactor Building (RB) and Separation Groups B, D, and Division II equipment are located on the 86'-0" elevation." Each room contains that division's RTS, ESFAS, MWS, and two of the separation groups containing SFMs, SBMs, and associated NMS-excore electronics cabinets. Physical independence is evaluated in detail in Section 7.1.2.4.1 of this report.

The two divisions are physically independent, with the exception that each division's SVMs receive inputs from all the separation groups. However, this particular connectivity was specifically addressed in TR-1015-18653 and reviewed in Section 3.2.2, "Communications Independence," of the NRC staff's SE for TR-1015-18653.

The use of data communication systems as single paths for multiple signals or data raises particular concerns about extensive consequential failures as the result of a single failure. The NRC staff confirmed that channel assignments to individual communication subsystems can assure that both redundancy and diversity requirements within the supported systems are met. This capability was evaluated in Sections 3.15, 3.3, 3.5, and 3.8 of the NRC staff's SE for TR-1015-18653.

At a high level, the ability of either division of MPS/NMS to achieve the required safety function independently allows them to broadly address single failures. This analysis is simplified by there being a fail-safe mode for the different components, equivalent to the positions they would attain on a loss of power. The NRC staff examined the FMEAs for the MPS and NMS to

evaluate cascaded and DBE-related CCFs as indicated in IEEE Std. 379-2000, as endorsed by RG 1.53, Revision 2. The NRC staff found both issues to be satisfactorily addressed and integrated into the FMEA results. Based on the above, the NRC staff concludes that ASAI 12 is met, as described in Section 7.1.6 of this report.

Based on the above evaluation, the NRC staff concluded that the design of I&C systems conforms to the guidance in RG 1.53, Revision 2, and satisfies the redundancy requirements in Section 5.1 of IEEE Std. 603-1991.

Common-Cause Failures

While CCFs resulting from design defects, such as digital-based CCFs, are not among the types of CCFs subject to single-failure analysis in IEEE Std. 379-2000 as endorsed by RG 1.53, Revision 2, the standard directs that provisions should be made to address such CCFs as part of assuring sufficient redundancy. The NuScale design has built-in diversity to accomplish safety functions when one division of the safety system is compromised. The evaluation of digital CCFs is described in Section 7.1.5, "Diversity and Defense in Depth," of this report. The effects of spurious actuations stemming from CCFs for sensors, safety blocks, and the MCS are also evaluated in that Section.

Interactions between Safety-Related and Non-safety-related Systems

The effects of sense, command, and other non-safety-related systems were considered by the NRC staff to assure that they could not degrade redundancy in the safety system and to confirm that these interactions comply with applicable regulations as described below.

While a non-safety-related system action could result in a condition that requires protective action, redundancy in terms of performing the safety function is maintained by the APL in the EIMs, which establish priority of safety signals over non-safety-related control systems. The evaluation of the interaction between sense and command features and other systems is described in Section 7.2.10 of this report. The NRC staff finds that the application complies with the independence criteria in Section 5.6 of IEEE Std. 603-1991 and the criteria for interactions between sense and command features and other systems in Section 6.3 of IEEE Std. 603-1991.

EDSS is classified as a non-safety-related system. However, a loss of power results in actuation of the RTS and ESF components as their solenoids lose power, and the breakers and components go to their deenergized states (including ECCS hold mode after 24 hours). The evaluation of the electrical power sources is in Section 7.1.2.4.2 of this report.

Discrete inputs from the MCS are connected to the HWMs in each division of RTS and ESFAS to provide for control of ESFAS components and the RTBs. The HWMs provide for electrical isolation of the signals. However, this logic is ignored by the APL in the presence of either an automatic or manual actuate signal and is also ignored unless that division's enable non-safety-related control switch is closed. Considerations of this configuration on the completion of the protective action are evaluated in Section 7.2.3 of this report. The NRC staff finds that the design satisfies the redundancy requirements contained in GDC 24.

Maintenance and Operational Bypass

In addition to satisfying the single-failure criterion, suitably implemented redundancy enables maintenance and operational bypass without loss of function as required in the regulations as evaluated below.

Section 6.7 of IEEE Std. 603-1991 provides maintenance bypass requirements for sense and command features as described in DCA Part 2, Tier 2, Section 7.2.4. This is evaluated in detail

in Section 7.2.4 of this report. The NRC staff confirmed that there is sufficient redundancy to allow for maintenance bypass of SFMs. DCA Part 2, Tier 2, Section 7.2.13.4, states that an alarm is sounded by the MCS if more than one MPS bypass is attempted for a given function.

The NuScale design has four channels of safety-related sensors allowing for channel checks and placing a channel into bypass while still meeting the single-failure criterion. To meet the requirement for redundancy, PAM sensors need only two channels to comply with the single-failure criterion. The evaluation of displays and monitoring is described in Section 7.2.13 of this report.

Section 7.5 of IEEE Std. 603-1991 provides maintenance bypass requirements for execute features. DCA Part 2, Tier 2, Section 7.2.4, states, in part, the following:

> *The MPS operating and maintenance bypasses conforms to Sections 5.8, 6.6, 6.7, 7.4 and 7.5 of IEEE-603-1991 and the guidance contained in RG 1.47, Revision 1. The display of bypassed and inoperable status information is described in Section 7.2.13, which conforms to 10 CFR 50.34(f)(2)(v).*

Section 7.2.4.4.2 of this report presents the evaluation of maintenance bypasses of the RTS, ESFAS, MPS, and NMS. The evaluation found that the provisions for maintenance bypasses are consistent with the technical specification action statements and confirmed that maintenance bypasses are designed to comply with Sections 6.7 and 7.5 of IEEE Std. 603-1991. Meeting the redundancy requirements of IEEE Std. 603-1991, Sections 6.7 and 7.5, demonstrates compliance with the requirement in GDC 21 that removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.

Shared Systems

IEEE Std. 379-2000, as endorsed by RG 1.53, directs consideration of shared systems. DCA Part 2, Tier 2, Section 7.1.1.1, “Design Bases and Additional Design Considerations,” states the following:

> *The plant control system (PCS) and plant protection system (PPS) are shared between multiple NPMs and are designed to not adversely affect the ability of I&C platforms that perform safety-related functions.*

There are shared I&C systems between the NPMs, specifically, between the PCS and the PPS; however, they are not designated as safety-related systems. These shared I&C systems are evaluated in Section 7.2.11 of this report.

NMS refuel is used by each NPM but never at the same time as the excore function, and it is not considered a safety-related system. NMS flood is used by two channels of the MPS, but it serves non-safety-related and PAM purposes only. Therefore, the NRC staff concludes that the application conforms to the shared system considerations in IEEE 379-2000, as endorsed by RG 1.53.

Test and Calibration Capabilities

The NRC staff considered the following IEEE Std. 603-1991 requirements in the review of redundancy as part of addressing the ASAIs 14 and 32 of TR-1015-18653:

- Section 5.7 of IEEE Std. 603-1991, which provides requirements for test and calibration of safety system equipment described in DCA Part 2, Tier 2, Section 7.2.15. Detailed review of testing and calibration against IEEE Std. 338-1987,

"Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," endorsed by RG 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems," and is evaluated in Section 7.2.15 of this report.

- Section 6.5 of IEEE Std. 603-1991, which provides requirements for test and calibration of sense and command feature sensors during reactor operations described in DCA Part 2, Tier 2, Section 7.2.15, is evaluated in detail in Section 7.2.15 of this report.

In Section 7.2.15 of this report, the NRC staff concludes that the design of I&C systems satisfies the requirements related to capability for test and calibration contained in Section 5.7 of IEEE Std. 603-1991 and confirmed that the use of self-diagnostics does not replace the capability for test and calibration as required by Section 6.5 of IEEE Std. 603-1991.

The portions of the MPS that require calibration are the SFMs. Provisions have been made for continuous self-test and to take an SFM out of service in either a trip or bypassed state via trip/bypass switches on the chassis below the SFM and an out-of-service switch on the SFM. This leaves the rest of the SFMs in that safety group (SG) operational and does not affect the operation of the other three SGs.

Based on the above, the NRC staff finds that ASAIs 14 and 32 are met.

Redundant Power Sources within the Module Protection System

DCA Part 2, Tier 2, Section 8.3 describes the EDSS-MS. The presence of two redundant power sources for each of the two divisions is established in DCA Part 2, Tier 2, Section 7.0.4.1.4. Therefore, the NRC staff concludes that the NuScale I&C design meets ASAI 21.

7.1.3.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.3.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the design has enough redundancy to assure that (1) no single failure results in loss of the safety function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the safety-related system can be otherwise demonstrated.

Based on evaluation in Sections 7.1.5, 7.2.13, and 8.3 of this report and the above discussion, the NRC staff finds that the design of I&C systems conforms to the guidance in RG 1.53, Revision 2, and satisfies the redundancy requirements in 10 CFR Part 50, Appendix A, GDC 21 and 24; Section 5.1 of IEEE Std. 603-1991; and ASAIs 12, 13, 14, 21, and 32 listed in TR-1015-18653, Revision 2, as described in Section 7.1.6 of this report.

7.1.4 Predictability and Repeatability

7.1.4.1 Introduction

This Section addresses the review of methods described in the application to demonstrate that the I&C safety system output is predictable and repeatable. Predictable and repeatable system behavior refers to the case in which input signals and system characteristics result in output signals through known relationships among the system states and responses to those states.

Such a system will produce the same outputs for a given set of input signals (and the sequence of inputs) within well-defined response time limits to allow timely completion of credited actions. I&C safety systems should be designed to operate in such a predictable and repeatable manner, which is also called “deterministic” behavior.

The NRC staff evaluated the predictability and repeatability of the output of the MPS. The objective of this review is to (1) verify that system timing derived from the analysis of DBEs has been allocated to the I&C system architecture as appropriate and has been satisfied in the I&C system design, (2) confirm that the I&C system design and communication protocols provide features to assure system (or logic) performance in terms of response to inputs and time to produce a response, and (3) confirm that hazards that could challenge predicted behavior have been adequately identified and accounted for in the design.

The NRC staff’s evaluation includes other fundamental design principles, such as independence, D3, and redundancy, to inform the review of I&C system output predictability and repeatability. In addition, the NRC staff considered the architectural description, simplicity, and hazard analysis techniques, and how they inform the NRC staff’s review of the I&C system output predictability and repeatability.

7.1.4.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2, Revision 2, Section 7.1.4, “Predictability and Repeatability,” describes the predictability and repeatability attributes of the I&C systems.

DCA Part 2, Tier 2, Section 7.1.4, states the following:

- The actuation delays assumed in the plant safety analysis are listed in DCA Part 2, Tier 2, Table 7.1-6. The RTS timing analysis is defined from the point in time when the monitoring process variable exceeds its predetermined setpoint to when the control rods fall into the reactor core. The MPS digital portion of the RTS function is allocated a timing budget in the safety analysis of 1 second. For this portion of the RTS, protective actuation function is defined from the sensor input to the SFM input terminals, to the opening of the RTBs, which includes the control rod de-latch time. The MPS is designed to complete this function in less than or equal to 1 second.

- For the ESFAS protective functions, the actuation delays in DCA Part 2, Tier 2, Table 7.1-6, are assumed in the plant safety analysis and are defined as the time from when the monitored process variable reaches or exceeds the predetermined setpoint until the actuation signal is received at the component (e.g., valve solenoid). The MPS digital portion of the ESFAS functions is allocated a timing budget in the safety analysis of 1 second. This time allocation is defined from the sensor input to the separation group input terminals to the EIM outputs. The MPS is designed to complete this function in less than or equal to 1 second. For the pressurizer heater trip function, this time requirement includes the time for the pressurizer heater trip breakers to open.

Section 7.1.4 of DCA Part 2, Tier 2, Revision 2, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.1.4, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 19, 56, and 59, which relate to repeatability and predictability, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 7.0, “Repeatability and Predictability,” describes the HIPS platform design concepts that address the fundamental design principle of repeatability and predictability (1) to meet the completion protective action requirements of IEEE Std. 603-1991, Section 5.2, and (2) to meet the system integrity requirements of IEEE Std. 603-1991, Section 5.5.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.1.4, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 14, 15, and 17. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.1.4.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.1.4.

7.1.4.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). IEEE Std. 603-1991 provides requirements related to safety system performance and the timing of safety system response. Section 4 of the standard requires the applicant to establish the design basis for each system, including documentation of the following: (1) the variables that are to be monitored to manually or automatically 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 (Section 4.4); and (2) the critical points in time after the onset of a DBE (Section 4.10). In addition, Section 5.5, “System Integrity,” of IEEE Std. 603-1991 requires safety systems to be designed to accomplish their safety-related functions under the range of conditions enumerated in the design basis. After initiation by either automatic or manual means, the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that performs the safety function) shall go to completion in compliance with Section 5.2, “Completion of Protective Action,” of IEEE Std. 603-1991.

- 10 CFR Part 50, Appendix A, GDC 13

- 10 CFR Part 50, Appendix A, GDC 21

- 10 CFR Part 50, Appendix A, GDC 29

There are no specific DSRS acceptance criteria in this Section.

7.1.4.4 Technical Evaluation

As documented in the NRC staff’s SE for TR-1015-18653 (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.1.4, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to predictability and

repeatability. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.1.4.3 and to address aspects of ASAIs 19, 56, and 59 that relate to predictability and repeatability. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.1.4.3 and ASAIs cited above.

From DCA Part 2, Tier 2, Section 7.1.4, and Table 7.1-6 design information, including functional block diagrams, descriptions of operation, architectural descriptions, and other design details provided in TR-1015-18653, the NRC staff confirmed that the MPS is designed to complete the RTS and ESFAS functions in less than or equal to 1 second, which satisfies the allocated timing budget in the safety analysis of 1 second for these functions in predictable and repeatable manner. Therefore, the NRC staff finds that the application complies with the performance and timing requirements for safety systems in IEEE Std. 603-1991. Additionally, the NRC staff confirmed that the design commitments demonstrated in the DCA for predictable and repeatable performance within the allocated timing requirements for each of the safety-related functions satisfy the applicable requirements of GDC 13, 21, and 29.

The NRC staff confirmed that the application provides a detailed timing analysis discussing how the I&C system and supporting communication systems address the concept of predictability and repeatability. The MPS architecture uses the HIPS platform. As evaluated in the TR-1015-18653 SE, the HIPS platform is designed to produce the same outputs for a given set of input signals within well-defined response time limits to allow timely completion of credited actions. TR-1015-18653, Section 7.0, describes how the platform and components function and provides functional block diagrams to demonstrate how they meet the criteria for predictability and repeatability. The MPS response time analysis demonstrates that the MPS performs and completes its required safety functions in a predictable and repeatable manner. TR-1015-18653, Section 7.0, describes the calculation used to determine the worst-case digital time response for an MPS channel. As DCA Part 2, Tier 2, Table 7.1-6, shows, the DBE actuation delays assumed in the plant safety analyses range from a minimum of 2.0 seconds to a maximum of 150.0 seconds, whereas the MPS is designed to complete the RTS and ESF functions in less than or equal to 1 second. DCA Part 2, Tier 2, Section 7.1.4, state that for the RTS protective function, the MPS time allocation response time budget comprises the analog input delay plus the digital time response delay plus the analog output delay and includes the reactor trip breaker cycle time and control rod drive mechanism de-latch time. The MPS digital time response delay is described in Section 7.7, "Design of the Highly Integrated Protection System Platform Topical Report," of TR-1015-18653, Revision 2. This time allocation budget comprises the analog input delay plus the digital time response delay plus the analog output delay and is defined from the sensor input to the SFM input terminals to the EIM output command to the final actuation device. For the pressurizer heater trip function, this time requirement includes the time for the pressurizer heater trip breakers to open. The MPS is designed to complete the pressurizer heater trip function in less than or equal to 1 second.

The NRC staff considered the following IEEE Std. 603-1991 Sections in the review of predictability and repeatability:

- Section 4.4, regarding limits, ranges, and rates of change of variables included in the design basis as described in DCA Part 2, Tier 2, Section 7.1.4, Tables 7.1-2 and 7.1-6, and TR-1015-18653.

- Section 4.10, regarding critical points in time after the onset of a DBE as described in DCA Part 2, Tier 2, Section 7.1.4, and Table 7.1-6.

- Section 5.5, regarding the capability of safety systems to accomplish their safety-related functions under the range of conditions enumerated in the design basis as described in DCA Part 2, Tier 2, Table 7.1-5 and Figures 7.1-1a to 7.1-1ao.

- Section 5.2, regarding the sequence of protective actions (from receipt of a signal from the sense and command features to the actuated equipment that performs the safety function) that will go to completion after initiation by either automatic or manual means as described in DCA Part 2, Tier 2, Tables 7.1-3, 7.1-4, and Figures 7.1-1a to 7.1-1ao.

The NRC staff confirmed that the application provides sufficient information (in the form of architectural descriptions, functional block diagrams, descriptions of operation, and others) as stated above to demonstrate that the proposed system's real-time performance is repeatable, predictable, and known at all times.

The NRC staff evaluated the following when assessing predictability and repeatability:

- The NRC staff confirmed that the digital I&C system timing analysis identifies limiting response times, digital component timing requirements, architecture, and design commitments.

- The digital I&C system timing analysis addresses all system components from signal collection to completion of protective action.

- The NRC staff confirmed that the timing of specific system responses credited in the safety analysis have been allocated to the digital I&C portion of the system, as appropriate, and have been satisfied in the digital system architectural design. Hardware and software design specifications reflect these functional timing requirements.

- The NRC staff confirmed that the digital I&C system timing analysis demonstrates that the protection safety functions are achieved within the times assumed in the safety analysis.

- The NRC staff confirmed that data communications system timing is predictable and repeatable and the error performance is specified.

- The cycle time for the safety function process is determined in consideration of the longest possible completion time assuming worst-case conditions. Failure of the system to meet the limiting cycle time is detected and alarmed. To assure predictable and repeatable behavior, a message packet is included in every transmit cycle, whether it has changed since the previous transmission or not.

- The NRC staff confirmed that the processing cycle is defined, predictable, and repeatable within a specified sample time. In addition, the timing analysis demonstrates that all safety functions are accomplished in each cycle.

- The NRC staff confirmed that the I&C architecture design does not diminish the design's conformance with the other fundamental design principles.

7.1.4.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.4.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the design of the I&C and data communication systems adequately addresses the fundamental design principle of predictability and repeatability at both the system and component levels as demonstrated in the applicant's timing analysis. The NRC staff reviewed the application against ASAIs 19, 56, and 59 listed in TR-1015-18653, Revision 2. Based on the discussion above, the NRC staff concludes that the NuScale I&C design meets aspects of ASAIs 19, 56, and 59 that relate to predictability and repeatability. On this basis, the NRC staff finds that the design of I&C systems satisfies the predictability and repeatability requirements of GDC 13, 21, and 29, and Sections 4.4, 4.10, 5.2, and 5.5 of IEEE Std. 603-1991.

7.1.5 Diversity and Defense in Depth

7.1.5.1 Introduction

This Section addresses the review of methods described in the application used to demonstrate that (1) the I&C safety systems have a level of D3 such that there are two or more diverse systems or components that will be able to perform the safety functions credited in the safety analysis, (2) the different systems or components will have different attributes so as to reduce the likelihood of CCF, and (3) the displays and manual controls for critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems. The NRC staff focused its review of D3 in digital I&C systems on whether the safety functions can be achieved in the event of a postulated CCF in the digital I&C system. Conformance to these objectives is sufficient to demonstrate compliance with the applicable requirements of 10 CFR 50.55a(a)(2). The applicant has requested an exemption from a portion of 10 CFR 50.62 "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," with respect to equipment used to address ATWS events. This exemption is evaluated as part of this Section.

The NRC staff's evaluation includes other fundamental design principles, such as independence, redundancy, and predictability and repeatability, which inform the review of D3. In addition, the NRC staff considered the architectural description, simplicity, and hazard analysis techniques and how they inform the staff's review of D3.

7.1.5.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2, Section 7.1.5, "Diversity and Defense-in-Depth," describes the D3 attributes of the I&C systems.

Section 7.1.5 of DCA Part 2, Tier 2, Revision 2 incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.1.5, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 6, 9, 10, 11, 62, 63, 64, and 65, which relate to D3, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 6.0, "Diversity," describes the HIPS platform design concepts that address the fundamental design principle of diversity (1) to meet the single-failure criterion requirements of IEEE Std. 603-1991, Section 5.1, and (2) to comply with the NRC SRM to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs."

The applicant has requested an exemption from the portion of 10 CFR 50.62(c)(1) requiring diverse equipment to initiate a turbine trip under conditions indicative of an ATWS. The applicant states that the NuScale power plant design does not include an auxiliary or emergency feedwater system, and therefore, the portion of the rule requiring diverse and automatic auxiliary feedwater system (AFWS) initiation is not applicable. The underlying purpose of 10 CFR 50.62 is to reduce the risk associated with ATWS events. The NuScale power plant is designed to reduce the risk of an ATWS event via redundancy, diversity, and independence within the NuScale MPS. The MPS design reduces the probability of a failure to scram. When combined with the NuScale power plant response to ATWS events, the MPS design results in an ATWS contribution to core damage frequency lower than the safety goal identified in 10 CFR 50.62 rulemaking documents. In summary, the applicant states that the underlying purpose of the rule is met without the diverse turbine trip capabilities specified in 10 CFR 50.62(c)(1).

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.1.5, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 28. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.1.5.

Technical Reports: The technical report associated with DCA Part 2, Tier 2, Section 7.1.5, is TeR-0316-22048, "Nuclear Steam Supply System Advanced Sensor Technical Report," Revision 0 (ADAMS Accession Nos. ML17005A151 (Proprietary); ML17005A126 (Non-Proprietary)).

7.1.5.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.1, "Single-Failure Criterion." This Section states, in part, that the safety system must perform all safety functions required for a DBE in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (2) all failures caused by the single failure, and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

- 10 CFR Part 50, Appendix A, GDC 13.

- 10 CFR Part 50, Appendix A, GDC 22.

- 10 CFR Part 50, Appendix A, GDC 24.

- 10 CFR 50.62 requires, in part, automatic initiation of ATWS mitigation systems and equipment that is diverse and independent from the RTS.

- 10 CFR 50.34(f)(2)(xiv), "Containment Isolation Systems," requires, in part, that all nonessential systems are isolated automatically by the containment isolation system.

The guidance in DSRS Section 7.1.5 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following

guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994, summarizes several D3 analyses performed after 1990 and presents an acceptable method for performing such analyses.

- SRM to SECY-93-087 describes the NRC position on D3 in Item 18.II.Q.

- Generic Letter (GL) 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," dated April 16, 1985, provides quality assurance guidance for non-safety-related ATWS equipment.

- RG 1.53, Revision 2 endorses IEEE Std. 379-2000, with identified exceptions and clarifications. Section 5.5 of IEEE Std. 379-2000 establishes the relationship between CCF and single failures by defining criteria for CCFs that are not subject to single-failure analysis and identifies defense in depth as a technique for addressing CCF.

- RG 1.62, Revision 1, "Manual Initiation of Protective Actions," includes information on diverse manual initiation of protective action.

- RG 1.152, Revision 3 endorses IEEE Std. 7-4.3.2-2003, which provides guidance on performing an engineering evaluation of software CCF for digital-based systems, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the CCF.

7.1.5.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed Section 7.1.5 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to D3. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.1.5.3 and to address aspects of ASAIs 6, 9, 10, 11, 62, 63, 64, and 65 that relate to diversity and defense in depth. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

As discussed further below, the NRC staff confirmed that the application has addressed vulnerabilities to CCF in accordance with the NRC position on D3 originating from the SRM to SECY-93-087, particularly Item 18.II.Q.

7.1.5.4.1 Defense-in-Depth Assessment

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAIs 6, 9, 10, 11, 62, 63, and 64.

DSRS Section 7.1.5 states that the NRC staff needs to confirm that a D3 assessment has been docketed for the proposed I&C system and that the assessment demonstrates that

vulnerabilities to CCFs have been adequately addressed. The D3 assessment should focus on the protection systems, along with other systems that are credited as providing diverse functions to protect against CCF in the protection systems.

The applicant has not docketed a separate technical report for the D3 assessment. Instead, the D3 assessment is summarized in DCA Part 2, Tier 2, Section 7.1.5.1. The NRC staff used NUREG/CR-6303 in evaluating the applicant's D3 assessment. Various aspects of the evaluation are explained below.

7.1.5.4.1.1 Choosing Blocks

NuScale has chosen five different blocks for the D3 assessment of its design. Figure 7.1-4 of DCA Part 2, Tier 2, Section 7.1.5, shows the various blocks and the connections between them. DCA Part 2, Tier 2, Section 7.1.5.1.1, states, in part, "Blocks have been selected to represent a physical subset of equipment and software whose internal failures can be assumed not to propagate to other blocks based on respective diversity attributes."

The Non-Class 1E Monitoring and Indication Block represents the soft controls and digital displays available to the operator in the MCR for module-specific systems controlled by the MCS. These displays and controls are used by the operators for day-to-day operations, and these operator workstations are on a human machine interface network separate from the MCS control network. This assures that any errors do not propagate to other equipment or software. The SDIS and manual control blocks represent the respective division of SDIS and manual controls available to the operators. The SDIS displays are for indication only and do not provide any control functionality. DCA Part 2, Tier 2, Section 7.0.4.4, states that each division of SDIS receives information from the gateway associated with the respective MPS division. Each gateway contains information from all four separation groups and both MPS divisions of RTS and ESFAS. Each protective action automatically initiated by the MPS can be manually actuated at the division level by safety-related manual switches. The safety-related manual controls within the manual control blocks provide division-level initiation of safety-related components

Safety Blocks I and II consist of the MPS with the exception of the manual controls in the MCR. The MPS utilizes the HIPS platform. Each block represents a different programmable technology. Safety Block I includes Separation Groups A and C and Division I of RTS and ESFAS. Safety Block II includes Separation Groups B and D, and Division II of RTS and ESFAS. Because each separation group provides a trip determination status to both divisions of RTS and ESFAS, links between both safety blocks are required. Also, information from each safety block is provided to the SDIS blocks via respective MPS gateways. Component-level control of safety-related components requires that the non-Class 1E control logic within the actuation priority logic of the EIM is enabled by a safety-related switch. This is described in DCA Part 2, Tier 2, Section 7.0.4.1, "Module Protection System." If the operator has enabled non-Class 1E controls in the actuation priority logic of an EIM and there are no active manual or automatic actuation signals present, the operator can use the MCS to control safety-related components.

Sensor Blocks I and II consist of the sensors that are used as inputs to the MPS. The inputs to the MPS are summarized in DCA Part 2, Tier 2, Table 7.1-9, "Sensor Inputs to Module Protection System." For the purpose of the D3 assessment, the evaluation of Sensor Block I and II focuses on digital sensors that have safety-related functions. Variables that are calculated by the MPS (e.g., degrees of subcooling, high power range positive rate) are not included as part of the sensor blocks. Analog and discrete sensors are identified for completeness, but they are not considered to be vulnerable to digital-based CCF which can affect the digital sensors. The MCS block consists of the control network, controllers, remote

I/O network, and remote I/O modules. The MCS block provides for NPM-specific control of non-safety-related systems and, with the appropriate permissives, control of safety-related equipment. The MCS block provides information to the operators and receives input from the operators through the Non-Class 1E Monitoring and Indication Block.

7.1.5.4.1.2 Determining Diversity

The different blocks were evaluated against the following diversity attributes: design diversity, equipment diversity, functional diversity, human diversity, signal diversity, and software diversity. Diversity attributes within a block, as well as between different blocks, were evaluated. Diversity attributes within the MPS are discussed in detail in TR-1015-18653. While evaluating diversity within blocks, the NRC staff found that the safety blocks and the sensor blocks had diversity within their respective blocks. This evaluation is explained below.

Diversity within Safety Blocks I and II

The diversity attributes within the safety blocks are explained in detail in TR-1015-18653. There is design diversity within the safety blocks because implementation of interdivisional and intradivisional communication within a safety block uses design diversity. Interdivisional communication from SBMs, EIMs, SVMs, and MIB communications modules uses copper-to-fiber conversion and one-way communication. Intradivisional communication between SFM and SBM uses a virtual point-to-point connection with the SBM acting as the bus master and the SFMs operating as slaves on the communication bus. Intradivisional communication between SVMs and EIMs uses a point-to-multipoint communication protocol that results in SVMs not having to request information from EIMs. Each EIM implements a digital and analog method for initiating protective actions. The automatic signal actuation is generated within the FPGA of the EIM. The manual signal actuation originates from the physical switches in the manual control blocks. In the EIM, both manual and automatic actuation signals are used by the APL, which is implemented using discrete analog components.

There is functional diversity within the safety blocks since the various FPGA modules have different functions. The SFMs are configured and programmed for different safety functions. The safety function or group of safety functions implemented within an SFM is based on its inputs. A good example of this is given in DCA Part 2, Tier 2, Section 7.1.5.1.2, “Guideline 2—Determining Diversity.” One SFM only monitors and makes a trip determination on containment pressure, while another SFM monitors and makes a trip determination on steamline conditions. Some SFMs are not required to perform a trip determination. Instead, these SFMs are used only to provide accident monitoring information to the SDIS blocks through the separation group MIB communications modules. Each EIM can control two groups of field components. The EIMs are configured for functions only associated with those groups of components by limiting the number of components that an EIM can control. A good example of this is given in DCA Part 2, Tier 2, Section 7.1.5.1.2. An EIM may be required to close valves on a containment system (CNTS) isolation signal, while another EIM is dedicated to tripping a breaker on a low pressurizer level signal. Although there are instances where EIMs implement different safety functions, certain EIMs implement more than one safety function.

There is software diversity within the safety blocks because each safety block is composed of three types of FPGA-based modules: SFMs, communications modules, and EIMs. Because each type of module performs different functions, the logic implementations also differ significantly. For example, the logic implemented for trip determination on an SFM is different than the logic implemented for two-out-of-four voting on an SVM.

Diversity within Sensor Blocks I and II

The various safety-related sensors in the NuScale design can be seen in DCA Part 2, Tier 2, Table 7.1-9. These digital sensors can be grouped into three different function types: digital-based level measurements, digital-based pressure measurements, and digital-based flow measurements. Sensors of the same function type within Sensor Blocks I and II are not diverse from each other except in the case of digital-based level sensors. The digital level sensors in Sensor Block I are diverse from the digital level sensors in Sensor Block II.

Each function type depends on different physical effects that require unique processing algorithms to obtain desired variables such as flow, pressure, and level. Within a sensor block, each function type is based on different designs from different manufacturers. Hence, there is equipment diversity. The equipment diversity within each sensor block creates inherent design diversity. Each function type is based on a different architecture of the underlying components. Hence, there is design diversity. Each function type is used for a particular function. Hence, there is functional diversity. Within a sensor block, each function type represents sensors from a different vendor or supplier. Hence, there is human diversity. Each function type relies on different physical effects that require different algorithms and logic to obtain the desired parameter. Hence, there is software or logic diversity. The equipment diversity within each sensor block also creates inherent signal diversity. Each function type represents different process variables sensed by different physical effects. Hence, there is signal diversity as well.

The evaluation of the diversity attributes between the different blocks is explained below based on the various diversity attributes built into the NuScale design.

Equipment Diversity

Safety Blocks I and II have different FPGA technologies associated with them. One block will have an architecture composed of one-time programmable or flash-based FPGA. The other block will have an architecture composed of a static random-access memory FPGA. This provides equipment diversity and assures that the same digital-based CCF does not affect both Safety Block I and II FPGA. This, coupled with the different development tools used for each FPGA technology, helps mitigate the digital-based CCF vulnerabilities present in the MPS. Further discussion and evaluation of this can also be found in the reviewed and approved TR-1015-18653, Revision 2. DCA Part 2, Tier 2, Table 7.1-17 describes the effect of a digital-based CCF across diverse FPGA technologies between each safety block. Between Sensor Block I and II, there are two sets of digital-based level measurement sensors, and each set is from a different design vendor or supplier. Although the process variable is sensed by the same level fluctuations within the reactor, the digital processing electronics from different companies result in different designs. Hence, a digital-based CCF would be limited to only one set of digital level sensors.

Functional Diversity

Safety Blocks I and II initiate, as needed, reactor trip and ESF actuations to mitigate a DBE.

The monitoring and indication blocks allow the operator to monitor and control both safety-related and non-safety-related systems. The operator can maintain a plant within operating limits or initiate necessary protective actions. The MCS provides automatic control of systems to maintain the plant within operating limits including constraining certain operational transients.

Sensor Block I and II function to provide parameter information to Safety Block I and II, respectively. Also, there is functional diversity within the two divisions of the MPS as described in TR-1015-18653.

Design Diversity

Safety Block I and the Division I SDIS block use a different FPGA chip architecture than that of Safety Block II and Division II SDIS block. The diverse FPGA technologies have additional design diversity attributes, as described in TR-1015-18653, Revision 2, and also summarized in DCA Part 2, Tier 2, Table 7.1-10. The MCS block and Non-Class 1E Monitoring and Indication Block are based on a programmable technology diverse from that of Safety Block I and II and Division I and II SDIS blocks.

Human Diversity

The SDIS and safety blocks are based on an FPGA platform while the Non-Class 1E Monitoring and Indication blocks and MCS blocks are based on a microprocessor-based or computer-based platform as described in DCA Part 2, Tier 2, Section 7.0.4.4. The use of different I&C platforms creates inherent human diversity between these blocks because different design and test teams are used for the two different kinds of platforms.

Signal Diversity

The MCS and Non-Class 1E Monitoring and Indication Blocks provide control at the component level while the manual control blocks provide control at the division level. Between blocks, signal diversity is provided by having automatic and manual means of actuating equipment and protective actions.

Software Diversity

Because of the design diversity of the FPGA equipment, the use of different programmable technologies results in the use of different design tools. This would prevent diverse FPGA equipment from being susceptible to the same digital-based CCF.

The diversity attributes between the two divisions of the MPS (and even within a division) can be better understood using the figure below. This figure is based on information in the reviewed and approved TR-1015-18653, Revision 2.

		Division 1		Division 2	
Event	**Module**	**A**	**C**	**B**	**D**
Transient or DBE with no DBC	SFM	✓	✓	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or DBE with DBC (modules exhibiting functional and equipment diversity)	SFM	✗	✗	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or DBE with DBC (modules exhibiting only equipment diversity)	SFM	✗	✗	✓	✓
	CM	✗	✗	✓	✓
	EIM	✗	✗	✓	✓

KEY

DBE: Design-Basis Event
SFM: Safety Function Module
CM: Communication Module
EIM: Equipment Interface Module
CCF: Common-Cause Failure
DBC: Digital-Based CCF

✓ - Available to perform function
✗ - Not available to perform function
- Division I modules
- Division II modules

Figure 7.1.5-1: Effect of digital-based CCF on MPS built-in diversity

Figure 7.1.5-1 shows that there is sufficient diversity between the two divisions of the MPS. Based on the built-in diversity within the MPS, it can be concluded that even if one division of the MPS is affected by a potential digital-based CCF, the other MPS division would not be affected by the same CCF, and the division is still available to perform its respective functions.

7.1.5.4.1.3 Postulated Common-Cause Failure of Blocks

The NRC staff used NUREG/CR-6303 in evaluating the applicant's D3 assessment. In accordance with NUREG/CR-6303, blocks have been selected to represent a physical subset of equipment and software whose internal failures can be assumed not to propagate to other blocks based on their respective diversity attributes. NRC staff's evaluation, to ensure that a postulated failure originating within a block is confined within the same block, is further described below.

7.1.5.4.1.3.1 Safety Display and Indication System Division I or II and Manual Controls Block

Since the manual controls in each manual control block are physical hard-wired switches, a digital-based CCF can be assumed not to affect them. The SDIS blocks are designed for indication only and do not have the capability to control equipment. The displays are used for accident monitoring, and there are no credited manual actions for mitigating DBEs.

A fail-as-is condition within one block before the start of a DBE results in one division of operator displays indicating false safe operating conditions. This would, however, not prevent protective actions from being automatically initiated by Safety Block I or II. The digital equipment within the block has no control capability, and hence, a CCF would not automatically

cause a spurious actuation. If there is a digital-based CCF, the operator will need to determine which of the displays are valid. To resolve this information discrepancy, the operator can use the non-Class 1E Monitoring and Indication Block since the information provided to the SDIS blocks from the safety blocks is also provided to the Non-Class 1E Monitoring and Indication Block through the MCS block.

Another possibility is a digital-based CCF that falsely indicates a transient occurring without automatic initiation of protective actions. In this scenario, the operator still has the redundant SDIS block available, as well as the non-Class 1E Monitoring and Indication Block. The operator is able to resolve the discrepancy in indication. DCA Part 2, Tier 2, Figure 7.1-7, "Common Cause Failure of Division I Safety Display and Indication System," highlights in red the blocks and signals assumed to be affected by CCF. The blocks and signals available to resolve information discrepancy if the SDIS had a CCF are highlighted in green. Hence, NRC staff finds that this block has been selected in accordance with NUREG/CR-6303.

7.1.5.4.1.3.2 Safety Blocks I or II

Four scenarios may be identified as a result of a digital-based CCF within a safety block as explained in DCA Part 2, Tier 2, Section 7.1.5.1.6, "Guideline 6—Postulated Common Cause Failure of Blocks":

- Scenario 1—Spurious initiation of protection action(s) with correct indication;
- Scenario 2—Spurious initiation of protective action(s) with false indication;
- Scenario 3—Failure to initiate protective action(s) with correct indication; and
- Scenario 4—Failure to initiate protective action(s) with false indication.

Spurious actuation signals from separation group modules within a safety block would result in a complete spurious actuation in the opposite safety block because of the two-out-of-four voting performed by each safety block. Because the APL within an EIM is composed of discrete components, it is not vulnerable to a digital-based CCF. However, the rest of the EIM is susceptible to a CCF. Hence, partial spurious actuation is credible for digital-based CCF postulated in the EIMs of a safety block.

To identify the extent of partial spurious actuations resulting from digital-based CCF, the EIMs are evaluated and grouped by the protective action(s) configured on the EIM. Such an approach results in seven possible partial spurious actuation scenarios. These are identified in DCA Part 2, Tier 2, Table 7.1-11, "Partial Spurious Actuation Scenarios for Engineered Safety Features Actuation System within Safety Block I." For Scenarios 1 and 2, a D3 coping analysis was performed to demonstrate that the spurious actuations result in conditions that are bounded by the plant safety analyses. This is discussed in DCA Part 2, Tier 2, Section 7.1.5.2.2, "Results of Coping Analyses for Postulated Digital-Based Common Cause Failure Vulnerability." Each division of RTS has two sets of RTBs. A partial spurious actuation of the RTS within a division does not result in a reactor trip. This is summarized in DCA Part 2, Tier 2, Table 7.1-12, "Consequences of Partial Spurious Reactor Trip."

Scenarios 3 and 4 do not prevent the unaffected safety block from initiating protective actions when required because of the diversity attributes between the two safety blocks. While Scenario 4 would result in conflicting information in the MCR, other blocks are available to resolve conflicting information. DCA Part 2, Tier 2, Figure 7.1-8 identifies the blocks relied on to automatically initiate safety-related functions when one of the safety blocks has a digital-based CCF. DCA Part 2, Tier 2, Figure 7.1-9, "Common Cause Failure of Safety Block I with False

Indication," identifies in green outline the available blocks used to resolve information discrepancy and to automatically initiate safety-related functions if a safety block had a CCF. Hence, NRC staff finds that this block has been selected in accordance with NUREG/CR-6303.

7.1.5.4.1.3.3 Non-Class 1E Monitoring and Indication Block

Any spurious actuation of a major control function caused by a digital-based CCF within the Non-Class 1E Monitoring and Indication Block is mitigated by Safety Blocks I or II. This is shown in DCA Part 2, Tier 2, Figure 7.1-10, "Common Cause Failure of Non-Class 1E Monitoring and Indication," where blocks affected by the assumed digital-based CCF are outlined in red while the green outline shows the available blocks and signals used to resolve the information discrepancy. Since the APL can be used for component-level control of safety-related components only when the enabled non-safety-related control permissive is active, a digital-based CCF within the Non-Class 1E Monitoring and Indication Block cannot directly prevent or spuriously initiate protective actions. As soon as there is an automatic or manual initiation, the non-safety-related control permissive is overridden, and the component goes to the state needed for the protective action. Hence, NRC staff finds that this block has been selected in accordance with NUREG/CR-6303.

7.1.5.4.1.3.4 Module Control System Block

The MCS block consists of the control network, controllers, remote I/O network, and remote I/O modules. These components are segmented or explicitly incorporate other functional defensive measures to inhibit the propagation of failures across major control functions. Hazards from MCS digital-based CCF are addressed in Section 7.1.8 of this report. Since the APL can be used for component-level control of safety-related components only when the enable non-safety-related control permissive is active, a digital-based CCF within the MCS block cannot directly prevent the MPS from initiating protective actions and cannot directly command the MPS to spuriously initiate protective actions. As soon as there is an automatic or manual initiation, the non-safety-related control permissive is overridden, and the component goes to the state needed for the protective action. Hence, NRC staff finds that this block has been selected in accordance with NUREG/CR-6303.

7.1.5.4.1.3.5 Sensor Block I or II

Safety-related level, pressure, and flow sensors that depend on digital electronics are used as inputs to the MPS and, hence, are susceptible to a digital-based CCF. Using the function types and the diversity attributes discussed in DCA Part 2, Tier 2, Section 7.1.5.1.2, Tables 7.1-13 through 7.1-16 identify how a digital-based CCF affects either one or both sensor blocks.

A digital-based CCF of either level, pressure, or flow function type for Sensor Block I causes the following:

- spurious actuations from the MPS;
- provision of incorrect information to the SDIS; and
- provision of incorrect information to the MCS.

A sensor block with a digital-based CCF can be postulated to have the following outputs: fail low, fail high, or fail as-is.

7.1.5.4.1.3.5.1 Digital-Based Common-Cause Failure of Level Sensors

Failed Low Signal

The affected parameters are pressurizer level, RPV water level, and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed low signal results in a spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, ECCS actuation, and pressurizer heater trip. Failed low signals received by Safety Block I are transmitted to the MCS, displayed in the MCR, and used for non-safety-related control functions. With the spurious actuation of a reactor trip, CNTS isolation, and pressurizer heater trip, the MCS response to two correct and two incorrect sensor values has no further impact. Out of the failed low signals, pressurizer level is the only signal used for non-safety-related controls. However, with the CVCS isolated, the MCS cannot use CVCS makeup and letdown pumps to change pressurizer level.

Failed High Signal

The affected parameters are pressurizer level, RPV water level, and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed high signal results in a spurious reactor trip, CVCS isolation, and ECCS actuation. Failed high signals received by Safety Block I are transmitted to the MCS, displayed in the MCR, and used for non-safety-related control functions. With the spurious actuation of a reactor trip and CVCS isolation, the MCS response to two correct and two incorrect sensor values has no further impact. Out of the failed high signals, pressurizer level is the only signal used for non-safety-related controls; however, with CVCS isolated, the MCS cannot use CVCS makeup and letdown pumps to change pressurizer level. With Sensor Block II still capable of actuating on low-level signals, the capability to initiate other ESFs is not lost.

Failed as-Is

The affected parameters are pressurizer level, RPV water level, and containment water level. The failed as-is condition for two of the four sensors for each affected parameter does not prevent the initiation of a reactor trip or ESF actuation. Sensor Block II is still capable of identifying plant conditions requiring protective actions. Failed as-is signals do not lead to spurious initiation of protective actions. Failed as-is signals may go unnoticed until the valid signals significantly deviate from the failed signals.

7.1.5.4.1.3.5.2 Digital-Based Common-Cause Failure of Pressure Sensors

Failed Low Signal

The affected parameters are pressurizer pressure and wide-range RCS pressure. Failed low signals in the four sensors for each affected parameter can result in a spurious reactor trip, DHRS actuation, CVCS isolation, and pressurizer heater trip. Failed low signals received by Safety Block I and II are provided to the MCS to be displayed in the MCR and to be used for non-safety-related controls. With the spurious reactor trip, DHRS actuation, and CVCS isolation, the MCS response to four incorrect sensor values has no further impact. The automatic MCS response to a drop in pressure is to turn on the pressurizer heaters. However, with the pressurizer heater trip, pressurizer heaters are unavailable.

Failed High Signal

The affected parameters are pressurizer pressure and wide-range RCS pressure. A failed high signal affecting the four sensors for the affected parameters can result in a spurious reactor trip,

CNTS isolation, DHRS actuation, CVCS isolation, and pressurizer heater trip. Failed high signals received by Safety Block I and II are provided to the MCS to be displayed in the MCR and to be used for non-safety-related controls. With the spurious reactor trip, CVCS isolation, and pressurizer heater trip, the MCS response to four incorrect sensor values has no further impact. The automatic MCS response to a rise in pressure is to use pressurizer spray; however, with the isolation of the CVCS, pressurizer spray is unavailable.

Failed as-Is

The affected parameters are pressurizer pressure and wide-range RCS pressure. The failed as-is condition for the four sensors of each affected parameter does not result in spurious actuations. However, it can prevent initiation of protective actions if a DBE were to occur. This failure can be considered a Type 3 failure. Type 3 failures are system failures which occur when the primary sensors expected to respond to a design-basis event instead produce anomalous readings for some reason. DCA Part 2, Tier 2, Table 7.1-18, indicates the different DBEs for which the digital pressure sensors are credited in both the deterministic analysis and the best-estimate coping analysis. As clarified by the table, other diverse sensors or sensors not susceptible to a digital-based CCF, along with the built-in diversity of the MPS divisions, provide the required safety function.

7.1.5.4.1.3.5.3 Digital-Based Common-Cause Failure of Flow Sensors

Failed Low Signal

The affected parameter is RCS flow. A failed low signal for the four channels results in a spurious demineralized water system (DWS) isolation and CVCS isolation. No further impact is associated with a failed low signal.

Failed High Signal

The affected parameter is RCS flow. A failed high signal for the four channels does not result in spurious actuations. However, the safety blocks would be unable to identify a low RCS flow condition, and the operator would have incorrect information. Failure to identify a low RCS flow condition failure can be considered a Type 3 failure. However, RCS flow is not relied upon for detection or mitigation of AOOs or PAs as described in DCA Part 2, Tier2, Section 7.1.5.2 and Table 7.1 18, Note 2.

Failed as-Is

The affected parameter is RCS flow. The failed as-is condition for the four channels does not result in spurious actuations; however, it can prevent initiation of protective actions if a DBE were to occur. This failure can be considered a Type 3 failure. However, RCS flow is not relied upon for detection or mitigation of AOOs or PAs as described in DCA Part 2, Tier2, Section 7.1.5.2 and Table 7.1 18, Note 2

Hence, NRC staff finds that this block has been selected in accordance with NUREG/CR-6303.

7.1.5.4.1.4 Results of Defense-in-Depth Assessment

The NRC staff finds that NuScale's D3 assessment conforms with the guidance in NUREG/CR-6303. The NRC staff also finds that since sufficient diversity exists between the two divisions of the MPS, potential for a software CCF within the divisions which concurrently prevents both MPS divisions from performing their protective functions, can be considered to be appropriately addressed. However, several potential vulnerabilities to spurious actuations resulting from digital CCFs were identified. These are summarized below.

- Potential digital-based CCF within a safety block may lead to spurious initiation of a protective action, including reactor trip, DHRS actuation, ECCS actuation, containment isolation, CVCS isolation, pressurizer heater trip, DWS isolation, and low temperature overpressure protection (LTOP).

- Potential digital-based CCF within a safety block may lead to spurious partial initiation of protective actions. The identified consequences are provided in DCA Part 2, Tier 2, Table 7.1-11.

- Potential digital-based CCF of level function type within Sensor Block I or II may result in one of the following (see DCA Part 2, Tier 2, Section 7.1.5.1.6): spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, ECCS actuation, and pressurizer heater trip, spurious reactor trip, CVCS isolation, and ECCS actuation.

- Potential digital-based CCF of pressure measuring system function type within Sensor Block I and II may result in one of the following:

  - spurious reactor trip, DHRS actuation, CVCS isolation, and pressurizer heater trip,

  - spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, and pressurizer heater trip, and

  - Type 3 failure for the digital-based pressure-measuring system function type sensors.

- Potential digital-based CCF of flow function type within Sensor Block I and II may result in one of the following: spurious DWS isolation, CVCS isolation, or Type 3 failure of flow function type sensors.

- Type 3 failures of digital sensors may lead to failure of the MPS to initiate protective action(s) during AOOs and PAs. DCA Part 2, Tier 2, Table 7.1-18, identifies the digital sensors credited for AOOs and PAs that were addressed with a D3 coping analysis. A failure of two of the four MPS separation groups that leads to the spurious initiation of a protective action or combination of protective actions was evaluated by the D3 coping analysis using best-estimate methods. While there are many possible actuation combinations, the analysis of these events can be simplified without addressing each possible combination specifically.

7.1.5.4.2 Analysis of Design-Basis Events as Part of Defense in Depth

For the AOOs and PAs identified in the accident analysis portion of the DCA, it is important to understand how the NuScale design would cope with a concurrent postulated digital-based CCF of the safety systems and/or sensors relied on to achieve the required protective functions. To understand this, the applicant performs a best-estimate coping to demonstrate that (1) any radiation release for each postulated CCF for AOO events evaluated in DCA Part 2, Tier 2, Chapter 15 does not exceed 10 percent of the applicable siting dose requirements in 10 CFR 52.47(a)(2)(iv), or that the integrity of the primary coolant pressure boundary will not be violated and (2) any radiation release for each postulated CCF for PA events evaluated in Chapter 15 does not exceed the applicable siting dose requirements in 10 CFR 52.47(a)(2)(iv), or that the integrity of the primary coolant pressure boundary and the integrity of the containment will not be violated.

Section 7.1.5.4.1.4 of this report explains the different postulated digital-based CCF vulnerabilities identified as part of the D3 assessment. These vulnerabilities required a coping analysis to verify whether the consequences of the digital-based CCFs were acceptable. Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," states, in part, "If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action." Since sufficient diversity exists between the two divisions of the MPS, the potential for a digital-based CCF within the divisions can be considered to be appropriately addressed, and no coping analysis is needed. However, the digital sensors are susceptible to a software CCF and hence require a coping analysis. DCA Part 2, Tier 2, Section 7.1.5.2.2, describes the results of the coping analysis performed by the applicant. To come to a safety conclusion, the NRC staff evaluated the results of the best-estimate coping analysis performed by the applicant and found it acceptable.

7.1.5.4.2.1 Diversity for Mitigating AOOs

A Type 2 failure within a safety block does not prevent the unaffected safety block from initiating the necessary protective actions. Type 2 failures are system failures that do not directly cause plant transients but are undetected until environmental effects or physical equipment failure cause a plant transient or design basis accident to which protective equipment may not respond. Failure to respond is due to postulated common-mode failure of redundant protection system divisions or portions thereof. Safety Block I or II alone can initiate necessary protective actions for AOOs. The diversity attributes between Safety Block I and II limit a digital-based CCF to only one safety block.

Safety Blocks I and II depend on both analog and digital sensors for detecting the need for protective actions. DCA Part 2, Tier 2, Table 7.1-9, identifies all the sensor inputs to the MPS. DCA Part 2, Tier 2, Table 7.1-16 identifies the digital safety-related input signals used by the MPS. These digital sensors are vulnerable to a Type 3 failure. However, a concurrent Type 3 failure of the digital sensors does not happen because of the diversity between the different sensor function types. Instead, a digital-based CCF is assumed to occur within a particular subset of the digital sensors. In other words, a digital-based CCF of pressure sensors and digital-based level sensors concurrent with an AOO is not considered credible. In addition, the NRC staff finds that there is sufficient diversity for the digital level sensors between Sensor Blocks I and II to prevent Type 3 failures from concurrently affecting the level sensors in both Sensor Blocks I and II. This is identified in DCA Part 2, Tier 2, Table 7.1-13.

The different AOOs and the digital sensors credited to mitigate these events are summarized in DCA Part 2, Tier 2, Table 7.1-18. For digital pressurizer pressure and RCS flow sensors, a D3 coping analysis was performed to demonstrate that a Type 3 failure concurrent with an AOO does not result in a radiation release exceeding 10 percent of the applicable siting dose requirements in 10 CFR 52.47(a)(2)(iv) or violate the integrity of the primary coolant pressure boundary. The D3 coping analysis considered an AOO concurrent with a digital-based CCF of a credited signal and digital sensors of the same type. The NRC staff finds that (as clarified by table 7.1-18) the required safety function is provided by other diverse sensors or sensors not susceptible to a digital-based CCF, along with the built-in diversity of the MPS divisions.

7.1.5.4.2.2 Diversity for Mitigating Postulated Accidents

The explanation of the diversity between sensors in Section 7.1.5.4.2.1 of this report applies to PA events as well. A D3 coping analysis was used to demonstrate that a Type 3 failure concurrent with a PA does not result in a radiation release exceeding the applicable siting dose requirements in 10 CFR 52.47(a)(2)(iv), or violating the integrity of the primary coolant pressure boundary, or violating the integrity of the containment. The D3 coping analysis considered a PA

concurrent with a digital-based CCF of a credited signal and digital sensors of the same function type. The different PAs and the digital sensors credited to mitigate these events are summarized in DCA Part 2, Tier 2, Table 7.1-18. The NRC staff finds that (as clarified by table 7.1-18) the required safety function is provided by other diverse sensors or sensors not susceptible to a digital-based CCF, along with the built-in diversity of the MPS divisions.

7.1.5.4.2.3 Results of D3 Best-Estimate Coping Analysis

DCA Part 2, Tier 2, Table 7.1-18, shows the various AOOs and PAs that were analyzed with postulated digital-based CCFs of the identified sensors that are relied on and credited for the respective event. The D3 coping analysis determined that the spurious actuation of the containment isolation system (CIS) resulting from a digital-based CCF is the bounding analysis with regard to the reactor coolant pressure boundary integrity. Concurrent actuations of any combination of RTS, DHRS, or pressurizer (PZR) heater trip have been evaluated to be less limiting because of the additional heatup effects on the delay of reactor trip, DHRS actuation valve opening, or PZR heaters being tripped off. CIS actuation includes CVCS actuation, which increases the heatup event slightly and negates any possible effects of DWS actuation. The NRC staff determined that a spurious CIS is the limiting event in terms of peak RCS pressure. The applicant's D3 coping analysis shows that the peak RCS pressure for a spurious CIS remains below 120 percent of the RCS design pressure. Based on these results, and the information summarized in DCA Part 2, Tier 2, Section 7.1.5.2.2, the NRC staff finds that the D3 coping analysis demonstrates that a postulated digital-based CCF affecting digital-based sensors leading to a partial spurious initiation of protective actions at normal operating pressure and temperature does not violate the integrity of the primary coolant pressure boundary, or result in radiation release exceeding 10 percent of the applicable siting dose requirements in 10 CFR 52.47(a)(2)(iv) for AOOs and for PAs. For the postulated spurious actuations analyzed, none of the events resulted in a plant response that created conditions that were not bounded by the plant safety analysis described in DCA Part 2, Tier 2, Chapter 15. A summary of the description in DCA Part 2, Tier 2, Section 7.1.5.2.2, and the NRC staff's evaluation of it is provided below.

<u>High Pressurizer Pressure</u>

The plant safety analyses described in Chapter 15 credit high PZR pressure for detection and mitigation of heatup and reactivity excursion DBEs. The best-estimate transient analysis concluded that credit for the pressure mitigating effect of the PZR spray system would exclude the high-pressure trip from being the primary credited signal. Even if the spray was insufficient to mitigate the pressure response, the result would be the lifting of a reactor safety valve.

There are two reactor safety valves, each of which is sized to relieve the pressure generated by a total loss of secondary cooling without credit for a reactor trip. The D3 coping analysis concluded that a conservative postulated heatup event that did not trip on high pressure would not violate the RCS pressure boundary integrity because of the sizing of the reactor safety valves.

For the events described in DCA Part 2, Tier 2, Chapter 15 and listed in DCA Part 2, Tier 2, Table 7.1-18, that result in a high RCS pressure condition, the analyses conservatively do not take credit for normal pressurizer spray control. In the secondary plant events that result in the loss of main steam flow, the high main steam pressure signal is credited to generate reactor trip and DHRS actuations in addition to the high PZR pressure. In loss of feedwater and feedwater line break events, the high RCS temperature is a diverse signal. Therefore, the NRC staff finds that sufficient signal diversity exists such that postulated digital-based CCFs of the high-pressurizer pressure function are bounded by the plant safety analyses in DCA Part 2, Tier 2, Chapter 15. In most of these scenarios, the best-estimate analysis determined that the plant

response would not reach the high-pressurizer pressure actuation setpoint because of the realistic treatment of PZR spray and its ability to control the RCS pressure increase.

Low Pressurizer Pressure

The plant safety analyses described in DCA Part 2, Tier 2, Chapter 15 credit low PZR pressure in the steam generator tube failure and CVCS line breaks outside containment events. The limiting radiological scenarios include assumed loss of ac power concurrent with the breaks that result in an RCS pressurization that delays the low pressurizer level and low pressurizer pressure trips. This assumption bounds the cases where loss of offsite power is not assumed in a best-estimate analysis, and the D3 coping analysis concluded that the plant safety analyses are bounding. For the events described in DCA Part 2, Tier 2, Chapter 15 and listed in DCA Part 2, Tier 2, Table 7.1-18, that result in a low RCS pressure condition, the analyses do not credit normal operation of the PZR heaters. The best-estimate analysis of these events concludes that pressurizer heaters are able to mitigate events. Low pressurizer pressure is also credited for generating a CVCS isolation signal for a small CVCS line failure event and a DHRS actuation signal for the steam generator tube failure event after the RTS and PZR heater trip occurs on low RPV water level. In these cases, the low-low PZR level trip is identified as the diverse signal for CNV isolation to mitigate the consequences of the radiological release.

The best-estimate analysis of a larger break of the PZR spray line outside containment does generate a condition that relies on the low pressurizer pressure function because of the back flow and overflow prevention (check valves) located on the CVCS lines inside containment. If the CVCS pressure drops sufficiently to seat these valves, then the RCS inventory will be preserved, and the NPM will continue to operate until operators notice the failed CVCS line. For breaks or leaks in the CVCS lines that are small enough not to generate the system pressure drop required to seat the check valves, the transient response is a slow degradation of the RCS inventory that is detected and mitigated by the low PZR level actuation function. Hence, the NRC staff finds that the plant safety analyses is bounding for this scenario which is analyzed in the best estimate space.

Low Reactor Coolant System Flow

RCS flow rate is a function of reactor power in the NuScale design, such that low RCS flow is only possible during startup conditions. In part, DCA Part 2, Tier 2, Section 7.1.5.2.2, states the following:

> *The low RCS flow ESFAS actuation is used as a boron dilution initial condition but is not credited as part of the transient detection or mitigation. The minimum RCS flow is specified in order to generate the appropriate response time as part of the safety analysis evaluation but the change in neutron flux ultimately generates the mitigating actuations of RTS and/or DWS isolation.*

The low-low RCS flow protective function is credited for actuating RTS and CVCS isolation in the event of a module heatup system (MHS) malfunction that causes an RCS flow reversal. This event is not considered credible by the applicant in combination with a digital-based CCF of the RCS flow sensor because of the very short and limited operating window in which the MHS failure could occur.

DCA Tier 2, Section 7.1.5.2 states that RCS flow rate is a function of reactor power in the NuScale design, such that low RCS flow is only possible during startup conditions. Sufficient RCS flow is required to ensure timely detection of an inadvertent dilution event. During startup conditions, the MHS adds heat to the CVCS injection path and is combined with simultaneous heat removal in the steam generator (via feedwater flow) to

establish and maintain natural circulation RCS flow as described in DCA Part 2, Tier 2, Section 9.3.4.2.3. Since the reactor operates for a very short period of time in startup and very low power level conditions that need the MHS to function, such an event is not credible. However, there was still a need to understand what happens if there is a loss of RCS flow sensors/indications because of a digital-based CCF and the MHS malfunctions simultaneously resulting in a flow stagnation or flow reversal. Note 2 of DCA Part 2, Tier 2, Table 7.1-18 provides the following information:

> *The design basis for the digital-based RCS flow sensors in the plant safety analysis described in Section 15.4.6 is to ensure minimum RCS flow rates exist during dilution events to ensure proper mixing within the RCS; therefore, the RCS flow sensors are not included in Table 7.1-18 as they are not relied upon for detection or mitigation of AOOs or PAs as described in Section 7.1.5.2. The plant safety analysis credits the high subcritical multiplication protective function for detection and mitigation of an uncontrolled RCS dilution. Best-estimate analysis of this event concludes the event is non-limiting and does not rely on the digital-based RCS flow sensor to function. The consequences of RCS flow stagnation or reversal during low power conditions are addressed in NuScale Power, LLC topical report, "Non-Loss -of-Coolant Accident Analysis Methodology," TR-0516-49416. The FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function.*

The NRC staff agrees that RCS flow and reactor power are directly related to each other. If there is flow stagnation or reversal, then there would be no power either. The RCS flow indication is used as a boron dilution initial condition but is not credited as part of the transient detection or mitigation. Even if there are no RCS flow indications available, and the reactor power increases, the change in neutron flux ultimately generates the protective actuations. Because the required protective actuations occur even without the availability of the RCS flow indications, the NRC staff finds that the information provided by DCA Part 2, Tier 2, Table 7.1-18 is acceptable.

7.1.5.4.3 Diverse System Characteristics

If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should be capable of performing either the same function or a different function that will accomplish the same protection action. The diverse or different function may be performed by a non-safety-related system if the system is of sufficient quality to perform the necessary function under the associated event conditions. When a diverse means is needed to be available to replace an automated system used to accomplish a credited safety function as a result of the D3 assessment identifying a potential CCF, the NRC staff confirmed that the credited safety functions can be accomplished via an automated system.

The NuScale design has built-in diversity to accomplish safety functions when one division of the safety system is compromised. There is sufficient diversity within the MPS to prevent a postulated digital-based CCF from disabling the capability to perform any of the safety-related functions. Since the diverse means is safety related and part of the safety division, it is required to meet divisional independence and automatic control requirements as defined in IEEE Std. 603-1991. The evaluation of the divisional independence of the diverse means is discussed in Section 7.1.2 this report. In all cases, the diverse means is independent such that a CCF of the safety system would not affect the diverse system.

Use of Automation as a Diverse Means

The evaluation of automatic control of the diverse means is described in Section 7.1.5.4.1 of this report. The NRC staff also confirmed that the functions are provided by equipment that is not affected by the postulated CCF, and the functions are sufficient to maintain plant conditions within recommended acceptance criteria for the particular AOO or PA.

Use of Manual Action as a Diverse Means

Manual controls are available in the MCR to provide division-level control of safety components. These are hardwired physical switches, which are not susceptible to a digital-based CCF. However, these controls are not needed to bring the plant to a safe state. The NuScale reactor design has no Type A variables because there are no operator actions credited in any DCA Part 2, Tier 2, Chapter 15 AOO, IE, or PA, nor the station blackout or ATWS analysis. Type A variables are the variables which provide information essential for the direct accomplishment of critical safety functions that require manual or operator action. The evaluation of the identification of accident monitoring variables is described in Section 7.2.13 of this report.

7.1.5.4.4 Displays and Controls

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAIs 6 and 65.

DSRS Section 7.1.5 states in part that a set of displays and controls located in the MCR should be provided for manual, system-level actuation of critical safety functions and monitoring of variables that support the safety functions. The displays and controls should be independent and diverse from the safety computer system identified in Point 1 and Point 3 of the SRM to SECY-93-087, Item II.Q.

Division I and II manual control switches are provided to manually initiate safety-related functions at the division level. Manual actuation signals are input directly into the APL within an EIM and are downstream of the automatic digital portion of the safety system. The APL within the EIMs is implemented with discrete analog components. SDIS I and II are provided as diverse displays from the non-class 1E monitoring and indication displays. SDIS I is diverse and uses different FPGA technology from SDIS II. In addition, faults cannot propagate from the SDIS to the MPS and in turn influence the functioning of the RTS or ESFAS. Hence, the SDIS and manual controls are sufficiently diverse that any failure does not prevent the operator from obtaining or resolving conflicting information.

Even if SDIS I and SDIS II are not diverse from each other and succumb to the same failure, the availability of the MCS provides a set of displays in the MCR to monitor variables that support safety functions. Since the SDIS is diverse from the MCS and both are available to the operators in the MCR, the NRC staff finds that the aspects of ASAIs 6 and 65 that relate to displays and controls and Point 4 of the SRM to SECY-93-087 are met.

DCA Part 2, Tier 2, Section 7.1.5.3, states, in part, the following:

> *In the unlikely event that a postulated fault in one MPS division could adversely affect both MPS gateways ability to provide information to the SDIS for display in the main control room, there is an additional level of redundancy in providing information from MPS for display to the plant operators via the module control system (MCS). The data interface between the MPS to the MCS is provided by one-way, isolated data communication links from the MIB-CM in each MPS separation group and RTS and ESFAS Division as described in FSAR Section 7.0.4 and shown in FSAR Figure 7.0-5. The data interface between the*

MIB-CM to the MCS is completely separate from the MPS gateway, such that any combination of postulated failures of the MPS gateways does not affect the display information that is provided to the MCS for each MPS division. If the source of the information is incorrect for an MPS division, SDIS and MCS can be used to validate the information from the other MPS division.

The NRC staff finds the above acceptable since the availability of information via the MCS helps the plant operator resolve potentially conflicting SDIS display information.

7.1.5.4.5 Additional Considerations for Defense-in-Depth Review

The DSRS for the NuScale SMR design provides additional information that must be considered when reviewing the design's D3 aspect. These have been addressed in other parts of Section 7.1.5 of this report.

7.1.5.4.5.1 Exemption from 10 CFR 50.62

As defined in 10 CFR 50.62, an ATWS event is an AOO followed by failure of the reactor trip portion of the protection system. An ATWS was considered in the design of I&C systems as it relates to the design provisions of 10 CFR 50.62(c)(1). Part 7, "Exemptions," of the DCA, Section 3, "10 CFR 50.62(c)(1) Reduction of Risk from Anticipated Transients Without Scram," discusses NuScale's request for an exemption to 10 CFR 50.62(c)(1). The applicant requests an exemption from the portion of 10 CFR 50.62(c)(1) requiring equipment diverse and independent from the reactor trip system to automatically initiate a turbine trip under conditions indicative of an ATWS. The applicant also states that the portion of 10 CFR 50.62(c)(1) related to automatic initiation of the auxiliary (emergency) feedwater system is not applicable to the NuScale design.

Pursuant to 10 CFR 52.7, "[t]he Commission's consideration of requests for exemptions from requirements of the regulations of other parts in this chapter, which are applicable by virtue of this part, shall be governed by the exemption requirements of those parts." The exemption requirements for 10 CFR Part 50 regulations are found in 10 CFR 50.12, "Specific exemptions." As 10 CFR 50.12 states, an exemption may be granted when: (1) the exemptions are authorized by law, will not present an undue risk to the public health and safety, and are consistent with the common defense and security; and (2) special circumstances are present. Specifically, 10 CFR 50.12(a)(2) lists six circumstances for which an exemption may be granted. It is necessary for one of these bases to be present in order for the NRC to consider granting an exemption request.

7.1.5.4.5.1.1 Authorized by Law

The applicant has stated in the DCA that the requested exemption is authorized by law (10 CFR 50.12(a)(1)). Applicant also states that this exemption is consistent with the Atomic Energy Act of 1954, as amended. The NRC has authority under 10 CFR 52.7 and 10 CFR 50.12 to grant exemptions from the requirements of this regulation. Therefore, the requested exemption is authorized by law.

7.1.5.4.5.1.2 No Undue Risk to Public Health and Safety

The requested exemption will not present an undue risk to the public health and safety (10 CFR 50.12(a)(1)). The NuScale Power Plant design incorporates diversity within the MPS, reducing the risk from common-cause failures leading to a failure to scram. The NuScale design does not rely on diverse turbine trip functionality to reduce the risks associated with an ATWS.

Built-in Diversity of the Module Protection System

The diversity internal to the MPS assures safety function performance in the presence of CCF. The description and evaluation of the built-in diversity of the MPS are addressed in Section 7.1.5.4.1 of this report. The MPS design leads to a simpler overall I&C architecture than other previously accepted solutions for 10 CFR 50.62 that involved separate diverse actuation systems. The MPS design also results in higher quality and simpler system interfaces than other previously accepted solutions for 10 CFR 50.62 that involved non-safety-related diverse actuation systems. The NRC staff evaluated the technical basis document of the D3 coping analysis for postulated digital-based CCF vulnerability and found it acceptable.

Anticipated Transient without Scram Response

Since ATWS is considered a beyond-design-basis event, and is documented in DCA Part 2, Tier 2, Chapter 19, the NRC staff examined calculations supporting the ATWS turbine trip exemption request. The NRC staff observed that estimated NRELAP code model input values were used for the reactor safety valve (RSV) throat areas and flow coefficients (C_v). Although the detailed valve specifications were not yet completed, the staff notes that Table 5.2-2 of the DCA Part 2, Tier 2 specifies the minimum design capacity and setpoints for the RSVs. This provides assurance that the valve design will be consistent with its assumed function in the NRELAP ATWS calculations.

Anticipated Transient without Scram Contribution to Core Damage Frequency

In Section 3.2, “Technical Basis,” of the exemption request, the applicant stated that the spectrum of ATWS event sequences were modeled in the NuScale probabilistic risk assessment (PRA) and are described in DCA Part 2, Tier 2, Section 19.2.2. The applicant also stated that features have been included in the NuScale design for protection against fuel damage during an ATWS event which limits the risk of an ATWS. The applicant asserted the following:

> *Without the design attributes required by 10 CFR 50.62(c)(1) and without relying on diverse and independent decay heat removal system actuation, the NuScale ATWS contribution to single module core damage frequency is significantly less than the target of 1.0E-5 per reactor year provided in SECY 83-293.*

In consideration of the applicant’s assertion, the NRC staff has reviewed the accident sequence analyses for ATWS events provided in DCA Part 2, Tier 2, Section 19.2.2. From that review the NRC staff observed that those features in the NuScale design credited to prevent core damage during an ATWS are the same features credited to prevent core damage during an anticipated transient followed by successful actuation of the module protection system and insertion of the shutdown rods. These features include the safety-related RSVs, which provide reactor vessel overpressure protection, and the safety-related ECCS. For the more likely anticipated transients, the non-safety-related containment flood and drain system and the injection capability of the CVCS are also capable of preventing core damage should the safety-related systems fail. The descriptions provided in the NuScale DCA indicate that all of these systems include a redundant capability for mitigating core damage. Accordingly, a failure of redundant equipment in multiple mitigation systems would need to occur for core damage to occur following an ATWS. The overpressure protection system and the ECCS both perform their safety function using only RSVs in redundant configurations. The RSVs, each of which provides overpressure protection for the reactor vessel, are pilot-operated valves similar to those used in many operating boiling-water reactor plants. The ECCS vent and recirculation valves are solenoid-actuated relief valves that are hydraulically closed, spring-assist to open, normally closed, and fail in the open position upon loss of dc power. The CCF probabilities for these

valve-based systems are typically taken to be less than $1x10^{-5}$. Therefore, since the frequency of transients in NuScale is expected to be similar to such frequencies in other new reactor designs (i.e., less than two per reactor-year), the combined failure probability for multiple redundant systems would drive the core damage frequency attributable to ATWS in the NuScale design well below the target core damage frequency of $1x10^{-5}$/reactor-year provided in SECY-83-293. Based on this evaluation, the NRC staff finds the applicant's assertion above to be reasonable.

As part of its review of Chapter 19 of the applicant's DCA, the NRC staff performed independent analyses to confirm the validity of the success criteria for redundant safety related systems applied by the applicant in its accident sequence analysis. These analyses include an ATWS case that assumes the failure of DHRS and a single RSV (similar to Thermal-hydraulic Simulation TRN-14A-0D0E0C0F1S-00-S from DCA Part 2, Tier 2, Table 19.1-6). The results of NRC staff's confirmatory analyses showed an end state consistent with that reported by the applicant in DCA Part 2, Tier 2, Table 19.1-6.

Therefore, exemption from the provisions of 10 CFR 50.62(c)(1) requiring diverse turbine trip capabilities will not present an undue risk to the public health and safety.

7.1.5.4.5.1.3 Consistent with Common Defense and Security

The requested exemption is consistent with the common defense and security (10 CFR 50.12(a)(1)). The exemption does not affect the design, function, or operation of structures or plant equipment that are necessary to maintain the secure status of the plant. The proposed exemption has no impact on plant security or safeguards procedures. Therefore, the requested exemption is consistent with the common defense and security.

7.1.5.4.5.1.4 Special Circumstances

Special circumstances are present in accordance with 10 CFR 50.12(a)(2)(ii). Hence, the application of the regulation in this particular circumstance would not serve the underlying purpose of the rule or is not necessary to achieve the underlying purpose of the rule. The NuScale Power Plant design does not rely on diverse turbine trip functionality to reduce the risks associated with ATWS. The NuScale design incorporates diversity within the MPS that sufficiently reduces the risk of common-cause failures leading to a failure to scram. The provisions of 10 CFR 50.62(c)(1) requiring diverse turbine trip capabilities are therefore not required for NuScale to meet the underlying purpose of the rule.

Further, special circumstances are present (10 CFR 50.12(a)(2)(vi)) in that other material circumstances are present which were not considered when the regulation was adopted. 10 CFR 50.62 establishes requirements to incorporate additional safety features for "existing reactor trip system[s]," i.e., designs that were established at the time of the issuance of the rule. The nuclear plant design features that formed the basis of 10 CFR 50.62(c)(1) were evaluated via design-specific value-impact calculations for the nuclear plant designs under review at the time the rule was drafted, as documented in SECY-83-293 and NUREG-1780. These designs do not reflect the NuScale design. The NuScale design includes enhanced safety features that sufficiently reduce the risk from ATWS events and also maintains a simpler I&C configuration than the separate equipment considered at the time of the adoption of 10 CFR 50.62. Therefore, it is in the public interest to grant an exemption from the diverse turbine trip feature required by 10 CFR 50.62(c)(1).

7.1.5.4.5.2 Compliance with 10 CFR 50.34(f)(2)(xiv)

Signal diversity is provided for the containment isolation function as shown by DCA Part 2, Tier 2, Section 7.1.5.1.1. Section 7.1.5.1.1 states, in part, the following:

Each protective action automatically initiated by MPS can be manually actuated at the division level by safety-related manual switches. There is a Division I CNTS isolation switch that closes Division I containment isolation valves (CIVs). There is also a Division II CIV switch that closes Division II CIVs. Successful closure of one Division completes the intended safety function.

The NRC staff confirmed that the containment isolation functions of the ESFAS automatically close each isolation device on each essential penetration.

7.1.5.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.5.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed I&C systems are designed with enough diversity to cope with a DBE concurrent with a CCF that disables the safety function. The NRC staff reviewed the application against ASAIs 1, 3, 4, 6, 9, 10, 11, 62, 63, 64, and 65 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets the aspects of ASAIs 6, 9, 10, 11, 62, 63, 64, and 65 listed in TR-1015-18653, Revision 2 that relate to diversity and defense in depth. On this basis, the NRC staff finds that the design of I&C systems satisfies the guidelines in the SRM to SECY-93-087 and NUREG/CR-6303 with regard to D3 and the D3 requirements in 10 CFR Part 50, Appendix A, GDC 13, 22, 24; 10 CFR 50.34(f)(2)(xiv); and Section 5.1 of IEEE Std. 603-1991. In addition, the NRC staff concludes that the 10 CFR 50.62 exemption request complies with the requirements of 10 CFR 52.7.

7.1.6 Disposition of Application-Specific Action Items in the Topical Report Safety Evaluation "Design of Highly Integrated Protection Platform"

7.1.6.1 Introduction

This Section addresses the disposition of the ASAIs specified by TR-1015-18653, Revision 2. The safety-related MPS uses the HIPS platform, as described in TR-1015-18653. This TR describes the conformance to NRC regulatory guides and IEEE standards applicable to safety-related I&C applications. Specifically, the HIPS platform conforms to RG 1.153, Revision 1, which endorses IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Because the HIPS platform uses programmable digital devices, RG 1.152, Revision 3, which endorses IEEE Std. 7-4.3.2-2003, D&IC-ISG-04, and the SRM to SECY-93-087 were also used for the generic HIPS platform design.

7.1.6.2 Summary of Application

DCA Part 2, Tier 1: There is no DCA Part 2, Tier 1 information associated with this Section.

DCA Part 2, Tier 2: DCA Part 2, Tier 2, Sections 7.0 to 7.2, incorporate by reference TR-1015-18653, Revision 2. DCA Part 2, Tier 2, Table 7.0-2, "Highly Integrated Protection System Topical Report (HIPS TR) Application Specific Information Cross References," provides a cross-reference of the ASAIs with the Chapter 7 subsections in which the ASAIs are specifically addressed.

ITAAC: There are no ITAAC associated with DCA Part 2, Tier 2, Section 7.0.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.0.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.0.

7.1.6.3 Regulatory Basis

The NRC staff's evaluation of TR-1015-18653 stated that application-specific analyses must be performed to assure that the generic approval granted by TR-1015-18653, Revision 2, remain valid for a specific system or plant application utilizing the HIPS platform (ADAMS Accession No. ML17116A097). Section 4.0, "Limitations and Conditions," of the SE for TR-1015-18653 identifies 65 ASAIs to be addressed by the applicant during the development of a safety-related system using this platform. Section 7.1.6.4 of this report presents the NRC staff's evaluation of the DCA's satisfaction of the 65 ASAIs specified by the TR-1015-18653 SE.

7.1.6.4 Technical Evaluation

Assessment of Applicant's Compliance with Application-Specific Action Items

The following is the NRC staff's assessment of the applicant's compliance with each ASAI:

1. ASAI 1: *An applicant or licensee referencing this SE must establish full compliance with the design criteria and regulations identified in NuScale DSRS Chapter 7, Table 7.1, or the appropriate plant design criteria that are relevant to the specific application(s) of the HIPS platform as a safety-related I&C system in an NPP as defined in 10 CFR 50.55a(h)*.

   The applicant provided the disposition of ASAI 1 in DCA Part 2, Tier 2, Section 7.0.1, "Regulatory Requirements," and DCA Part 2, Tier 2, Section 7.1.1, "Design Bases and Additional Design Considerations." The NRC staff reviewed the disposition and found it acceptable because DCA Part 2, Tier 2, Table 7.0-1 provides a cross-reference of regulatory requirements, guidance, and industry standards with the Chapter 7 subsections in which the requirements and guidance are specifically addressed. Therefore, the NRC staff finds that ASAI 1 is met.

2. ASAI 2: *An applicant or licensee referencing this SE must demonstrate that the HIPS platform used to implement the application-specific or plant-specific system is unchanged from the base platform addressed in this SE. Otherwise, the applicant or licensee must clearly and completely identify any modification or addition to the base HIPS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes.*

   The applicant provided the disposition of ASAI 2 in DCA Part 2, Tier 2, Section 7.0.4.1, "Module Protection System." The NRC staff reviewed the disposition and found it acceptable because there are no deviations in the application-specific NuScale I&C architecture presented in DCA Part 2, Tier 2, Chapter 7, from that described and approved in TR-1015-18653. Therefore, the NRC staff finds that ASAI 2 is met.

3. ASAI 3: *Although the NRC staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991. Because this SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences, an applicant or*

licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 603-1991 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

The applicant provided the disposition of ASAI 3 in DCA Part 2, Tier 2, Section 7.1.1. The evaluation of the application-specific design basis for the NuScale I&C safety system and the applicability of each IEEE Std. 603-1991 Section are described in Section 7.1.1 of this report. Therefore, the NRC staff finds that ASAI 3 is met.

4. ASAI 4: *Although the NRC staff determined that the HIPS platform supports satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this SE must identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std. 7-4.3.2-2003 clause to its application-specific HIPS platform-based safety system or component. Furthermore, the applicant or licensee must demonstrate that the plant-specific and application-specific use of the HIPS platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.*

   The applicant provided the disposition of ASAI 4 in DCA Part 2, Tier 2, Section 7.1.1. The evaluation of the application-specific design basis for the NuScale I&C safety system and the applicability of each IEEE Std. 7-4.3.2-2003 Section are described in Section 7.1.1 of this report. Therefore, the NRC staff finds that ASAI 4 is met.

5. ASAI 5: *Although the NRC staff determined that the HIPS platform includes features to support satisfying various sections and clauses of DI&C-ISG-04, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full conformance against this guidance. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.*

   The applicant provided the disposition of ASAI 5 in DCA Part 2, Tier 2, Section 7.1.1. The evaluation of the application-specific design basis for the NuScale I&C safety system and the applicability of the various sections and clauses of DI&C-ISG-04 is described in Section 7.1.1 of this report. Therefore, the NRC staff finds that ASAI 5 is met.

6. ASAI 6: *Although the NRC staff determined that the HIPS platform includes features to support satisfying various sections of the SRM to SECY-93-087, an applicant or licensee referencing this SE must evaluate the HIPS platform-based system for full compliance against this requirement. The applicant or licensee should consider its plant-specific design basis. This SE does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences.*

The applicant provided the disposition of ASAI 6 in DCA Part 2, Tier 2, Sections 7.1.1 and 7.1.5. The evaluation of the application-specific design basis for the NuScale I&C safety system and the applicability of the various sections of the SRM to SECY-93-087 is described in Sections 7.1.1 and 7.1.5 of this report. Therefore, the NRC staff finds that ASAI 6 is met.

7. ASAI 7: *An applicant or licensee referencing this SE must provide administrative controls (e.g., procedures, technical specifications) to prevent an operator from placing the same SFM across more than one division into maintenance bypass concurrent with a single failure of a different division.*

   The applicant provided the disposition of ASAI 7 in DCA Part 2, Tier 2, Section 7.2.4, "Operating and Maintenance Bypasses." The NRC staff reviewed the disposition of ASAI 7 and found it acceptable because the removal from service of an SFM, corrective maintenance, parameter update, and return to service processes are administratively controlled with approved plant procedures. Therefore, the NRC staff finds that ASAI 7 is met.

8. ASAI 8: *An applicant or licensee referencing this SE should verify having appropriate physical independence between non-safety-related and safety-related equipment to satisfy the Class 1E to non-Class 1E separation requirements, consistent with the guidelines of Regulatory Guide 1.75, Revision 3.*

   The applicant provided the disposition of ASAI 8 in DCA Part 2, Tier 2, Section 7.1.2, "Independence." The physical independence attributes of the MPS and NMS conform to the guidance in RG 1.75, Revision 3. The evaluation of the physical independence is described in Section 7.1.2 of this report. Therefore, the NRC staff finds that ASAI 8 is met.

9. ASAI 9: *An applicant or licensee referencing this SE must provide the basis for the allocation of safety functions between the two diverse divisions to mitigate the effects of a postulated CCF concurrent with Chapter 15 events of its final safety analysis report.*

   The applicant provided the disposition of ASAI 9 in DCA Part 2, Tier 2, Sections 7.1.2 and 7.1.5, "Diversity and Defense-in-Depth." The NuScale I&C system design includes features and processes to mitigate a CCF in the MPS because of digital-based failures that could disable a safety function. In addition, the applicant's D3 assessment of the NuScale I&C design is consistent with the guidelines in NUREG/CR-6303. The evaluation of D3 is described in Section 7.1.5 of this report.

   The safety function or group of safety functions implemented within an SFM is based on its inputs. There is one-to-one correspondence for each SFM and its associated protective function. This provides functional independence within each separation group from other protective safety functions, as well as independence across the separation groups and divisions within the MPS. The evaluation of functional independence within the MPS is described in Section 7.1.2 of this report. Therefore, the NRC staff finds that ASAI 9 is met.

10. ASAI 10: *An applicant or licensee referencing this SE must verify that all diversity attributes of a HIPS platform (i.e., equipment diversity, design diversity, and functional diversity) conform to the diversity design details provided in the TR.*

    The applicant provided the disposition of ASAI 10 in DCA Part 2, Tier 2, Section 7.1.5. The NRC staff reviewed the disposition of ASAI 10 and found it acceptable because all diversity attributes of the MPS conform to the diversity design details described in

TR-1015-18653. The evaluation of diversity attributes of the MPS is described in Section 7.1.5 of this report. Therefore, the NRC staff finds that ASAI 10 is met.

11. ASAI 11: *An applicant or licensee referencing this SE must verify that the diverse FPGA technologies have unique identification.*

    The applicant provided the disposition of ASAI 11 in DCA Part 2, Tier 2, Section 7.1.5. DCA Part 2, Tier 2, Section 7.2.9.2, "Identification," describes the identification requirements of the MPS. The evaluation of the diversity attributes of the MPS is described in Section 7.1.5 of this report. The evaluation of the identification requirements of the MPS is described in Section 7.2.9.4.2 of this report. Therefore, the NRC staff finds that ASAI 11 is met.

12. ASAI 12: *An applicant or licensee referencing this SE should perform a system-level FMEA to demonstrate that the application-specific use of the HIPS platform identifies each potential failure mode and determines the effects of each failure. The FMEA should demonstrate that single failures, including those with the potential to cause a non-safety-related system action (i.e., a control function) resulting in a condition requiring protective action (i.e., a protection function), cannot adversely affect the protection functions, as applicable.*

    The applicant provided the disposition of ASAI 12 in DCA Part 2, Tier 2, Section 7.1.3, "Redundancy." The applicant performed system-level FMEAs for the MPS and NMS. The NRC staff examined the FMEAs for the MPS and NMS and confirmed that the FMEA identifies each potential failure mode of the MPS and NMS and determines the effects of each. The FMEA demonstrates that single failures resulting in a condition requiring an MPS subsystem protective action do not adversely affect the MPS protection functions needed for each analyzed condition. The evaluation of how the MPS and NMS meet the single-failure criterion in Section 5.1 of IEEE Std. 603-1991 is described in Section 7.1.3 of this report. Therefore, the NRC staff finds that ASAI 12 is met.

13. ASAI 13: *An applicant or licensee referencing this SE should demonstrate that the application-specific diagnostic, self-test, and manually initiated test and calibration features will not adversely affect channel independence, system integrity, or the system's ability to meet the single-failure criterion.*

    The applicant provided the disposition of ASAI 13 in DCA Part 2, Tier 2, Section 7.1.3. The evaluation of how the MPS and NMS meet the single-failure criterion in Section 5.1 of IEEE Std. 603-1991 is described in Section 7.1.3 of this report. Based on the above, the NRC staff finds that ASAI 13 is met.

14. ASAI 14: *An applicant or licensee referencing this SE must review the actions to be taken when failures and errors are detected during tests and self-tests and ensure that these actions are consistent with system requirements. In addition, the applicant or licensee should describe how errors and failures are indicated and managed after they are detected. Finally, the applicant or licensee should confirm that this information is provided in the single-failure analysis for the plant-specific application.*

    The applicant provided the disposition of ASAI 14 in DCA Part 2, Tier 2, Sections 7.1.3 and 7.2.15, "Capability for Test and Calibration." The MPS and NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions.

Chapter 16 of this report addresses the technical specifications. The evaluation of the test and calibration of the safety systems is described in Section 7.2.15 of this report.

The evaluation of how the MPS and NMS meets the single-failure criterion in Section 5.1 of IEEE Std. 603-1991 is described in Section 7.1.3 of this report. Based on the above, the NRC staff finds that ASAI 14 is met.

15. ASAI 15: *An applicant or licensee referencing this SE must demonstrate that the application-specific logic satisfies the completion of protective action requirements.*

The applicant provided the disposition of ASAI 15 in DCA Part 2, Tier 2, Section 7.2.3, "Reliability, Integrity, and Completion of Protective Action." The NRC staff's evaluation of the completion of protective actions requirements for safety systems is described in Section 7.2.3.4.3 of this report. Therefore, the NRC staff finds that ASAI-15 is met.

16. ASAI 16: *An applicant or licensee referencing this SE must confirm that the HIPS platform manufacturer is currently on the Nuclear Procurement Issues Committee list or confirm that the HIPS manufacturing quality processes conform to the applicant's or licensee's program that is compliant with 10 CFR Part 50, Appendix B (i.e., vendor is included in the applicant's Approved Vendor List). The applicant or licensee will need to demonstrate that the HIPS software and associated development life cycle meet the applicable regulatory requirements.*

The applicant provided the disposition of ASAI 16 in DCA Part 2, Tier 2, Section 7.2.1, "Quality." The evaluation of the quality processes specific to the I&C system development is described in Section 7.2.1 of this report. The NRC staff's review of the overall quality assurance program is described in Chapter 17 of this report. Therefore, the NRC staff finds that ASAI 16 is met.

17. ASAI 17: *An applicant or licensee referencing this SE must confirm that the HIPS platform equipment is qualified to the applicable regulatory requirements.*

The applicant provided the disposition of ASAI 17 in DCA Part 2, Tier 2, Section 7.2.2, "Equipment Qualification." Section 7.2.2 of this report addresses the NRC staff's evaluation of I&C EQ. The overall EQ program is evaluated in Sections 3.10 and 3.11 of this report. Therefore, the NRC staff finds that ASAI 17 is met.

18. ASAI 18: *An applicant or licensee referencing this SE must identify the safe states for protective functions and the conditions that require the system to enter a fail-safe state. The applicant or licensee must also demonstrate system qualification for installation and operation in mild environment locations.*

The applicant provided the disposition of ASAI 18 in DCA Part 2, Tier 2, Sections 7.0.4, "Systems Descriptions," 7.2.2, and 7.2.3. DCA Part 2, Tier 2, Section 7.0.4.1, "Module Protection System," identifies the safe states for protective functions and the conditions that require the MPS to enter a fail-safe state. The evaluation of the safe states for the MPS is described in Section 7.0.4 of this report.

The evaluation of the quality processes specific to the I&C system development is described in Section 7.2.1 of this report. Section 7.2.2 of this report addresses the NRC staff's evaluation of I&C EQ. The overall EQ program is evaluated in Sections 3.10 and 3.11 of this report. The NRC staff's evaluation of the completion of protective actions requirements for safety systems is described in Section 7.2.3.4.3 of this report. Based on the above, the NRC staff finds that ASAI 18 is met.

19. ASAI 19: *An applicant or licensee referencing this SE must confirm that system real-time performance is adequate to ensure completion of protective actions within critical time frames required by the plant safety analyses.*

The applicant provided the disposition of ASAI 19 in DCA Part 2, Tier 2, Sections 7.1.4, "Predictability and Repeatability," and 7.2.3. The NRC staff's evaluation of the I&C output predictability and repeatability is described in Section 7.1.4 of this report. The NRC staff's evaluation of the completion of protective actions requirements for safety systems is described in Section 7.2.3.4.3 of this report. Based on the above, the NRC staff finds that ASAI 19 is met.

20. ASAI 20: *An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the power distribution architecture provide the required independence.*

The applicant provided the disposition of ASAI 20 in DCA Part 2, Tier 2, Section 7.1.2. The physical and electrical independence attributes of the MPS and NMS conform to the guidance in RG 1.75, Revision 3. The evaluation of the physical and electrical independence is described in Section 7.1.2 of this report. The NRC staff's evaluation of the electrical power systems is described in Chapter 8 of this report. Based on the above, the NRC staff finds that ASAI 20 is met.

21. ASAI 21: *An applicant or licensee referencing this SE must provide redundant power sources to separately supply the redundant power conversion features within the HIPS platform (i.e., the two redundant power sources are connected to a single division in a multi-division system). These power sources are provided to improve reliability and maintainability of the HIPS modules.*

The applicant provided the disposition of ASAI 21 in DCA Part 2, Tier 2, Section 7.1.3. In DCA Part 2, Tier 2, Figures 7.0-11a, "Module Protection System Power Distribution," and 7.0-11b, "Module Protection System Power Distribution," show the redundant power sources to the MPS. Section 7.1.2.4.2 of this report addresses the NRC staff's evaluation of the two redundant power sources to the MPS. Therefore, the NRC staff finds that ASAI 21 is met.

22. ASAI 22: *An applicant or licensee referencing this SE must verify that the safety network provides electrical, physical, and communications independence and security requirements for communication from safety- to non-safety-related systems.*

The applicant provided the disposition of ASAI 22 in DCA Part 2, Tier 2, Sections 7.1.2 and 7.2.9. The NRC staff's evaluation of electrical, physical, and communications independence is described in Section 7.1.2 of this report. DCA Part 2, Tier 2, Section 7.2.9, provides information to address the communication security requirements for safety- to non-safety-related systems. The NRC staff's evaluation of the control of access to the MPS and NMS is described in Section 7.2.9.4.1 of this report. Therefore, the NRC staff finds that ASAI 22 is met.

23. ASAI 23: *An applicant or licensee referencing this SE must perform isolation testing on the HIPS platform equipment to demonstrate the capability to satisfy the Class 1E to non-Class 1E isolation requirements, consistent with the guidelines of Regulatory Guide 1.75, Revision 3.*

The applicant provided the disposition of ASAI 23 in DCA Part 2, Tier 2, Sections 7.1.2 and 7.2.2. DCA Part 2, Tier 2, Section 7.1.2, states conformance to IEEE Std. 384-1992 for NuScale I&C systems, which is endorsed by RG 1.75, Revision 3. Section 7.1.2 of

this report addresses the NRC staff's evaluation of safety-related isolation devices. Section 7.2.2 of this report addresses the NRC staff's evaluation of I&C EQ. The overall EQ program is evaluated in Section 3.10 of this report. Therefore, the NRC staff finds that ASAI-23 is met.

24. ASAI 24: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for testing and calibration of safety-related features.*

The applicant provided the disposition of ASAI 24 in DCA Part 2, Tier 2, Section 7.2.15. Section 7.2.15 of this report addresses the NRC staff's evaluation of the capability for test and calibration of the MPS and NMS. Therefore, the NRC staff finds that ASAI 24 is met.

25. ASAI 25: *An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (i.e., self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance.*

The applicant provided the disposition of ASAI 25 in DCA Part 2, Tier 2, Section 7.2.15. The MPS and NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions. Section 7.2.15 of this report addresses the NRC staff's evaluation of the capability for test and calibration of the MPS and NMS. Chapter 16 of this report addresses the technical specifications. Therefore, the NRC staff finds that ASAI 25 is met.

26. ASAI 26: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for any automatic sensor cross-check as a credited surveillance test function and the provisions to confirm the continued execution of the automatic tests during plant operations.*

The applicant provided the disposition of ASAI 26 in DCA Part 2, Tier 2, Section 7.2.15. The MPS provides a means for checking the operational availability of the sense and command feature input sensors relied on for a safety function during reactor operation. This capability is provided by cross-checking between channels that have a known relationship (i.e., channel check). Section 7.2.15 of this report addresses the NRC staff's evaluation of the capability for test and calibration of the MPS and NMS. Therefore, the NRC staff finds that ASAI 26 is met.

27. ASAI 27: *An applicant or licensee referencing this SE must describe any manual controls and associated displays used to support manually controlled safety actions necessary to accomplish a safety function for which no automatic control is provided.*

The applicant provided the disposition of ASAI 27 in DCA Part 2, Tier 2, Section 7.2.13, "Displays and Monitoring." The MPS provides a means for automatic and manual initiation of required functions; however, no credited manual actions are required to enable the plant to mitigate AOOs and PAs. Section 7.2.13 of this report addresses the NRC staff's evaluation of displays and monitoring systems. Therefore, the NRC staff finds that ASAI 27 is met.

28. ASAI 28: *An applicant or licensee referencing this SE must describe how the HIPS platform safety system status information is used in displays to provide unambiguous, accurate, complete, and timely status of safety system protective actions*.

The applicant provided the disposition of ASAI 28 in DCA Part 2, Tier 2, Section 7.2.13, "Displays and Monitoring." The MPS provides outputs of monitored variables to two redundant divisions of the MCR SDIS displays for accident monitoring and to aid in manual operations. Section 7.2.13 of this report addresses the NRC staff's evaluation of the displays and monitoring systems. Therefore, the NRC staff finds that ASAI-28 is met.

29. ASAI 29: *An applicant or licensee referencing this SE must describe how the HIPS platform bypass status information is used to automatically actuate the bypass indication for bypassed or inoperable conditions, when required, and provide the capability to manually activate the bypass indication from within the control room.*

The applicant provided the disposition of ASAI 29 in DCA Part 2, Tier 2, Section 7.2.13. The MPS includes interlocks, permissives, and operational and maintenance bypasses that prohibit or permit certain protective actions either automatically or through a combination of automatic and manual actions to allow plant mode changes. The NRC's staff evaluation of the operational and maintenance bypasses is described in Section 7.2.4 of this report. Section 7.2.13 of this report addresses the NRC staff's evaluation of displays and monitoring systems. Therefore, the NRC staff finds that ASAI 29 is met.

30. ASAI 30: *An applicant or licensee referencing this SE must describe how the information displays are accessible to the operator and are visible from the location of any controls used to affect a manually controlled protective action provided by the front panel controls of a HIPS-based system.*

The applicant provided the disposition of ASAI 30 in DCA Part 2, Tier 2, Section 7.2.13. The SDIS provides display panels of the MPS's PAM variables to support manually controlled protective actions if required. Section 7.2.13 of this report addresses the NRC staff's evaluation of the displays and monitoring systems. Therefore, the NRC staff finds that ASAI 30 is met.

31. ASAI 31: *An applicant or licensee referencing this SE must provide additional control of access features to address the system-level aspects for a safety system using the HIPS platform.*

The applicant provided the disposition of ASAI 31 in DCA Part 2, Tier 2, Section 7.2.9. Section 7.2.9.4.1 of this report addresses the NRC staff's evaluation of control of access. Therefore, the NRC staff finds that ASAI 31 is met.

32. ASAI 32: *An applicant or licensee referencing this SE must provide additional diagnostics or testing functions (self-tests or periodic surveillance tests) to address any system-level failures that are identified as detectable only through periodic surveillance. The applicant or licensee must also ensure that failures detected by these additional diagnostics or testing functions are consistent with the assumed failure detection methods of the application-specific single-failure analysis.*

The applicant provided the disposition of ASAI 32 in DCA Part 2, Tier 2, Sections 7.1.3, 7.2.9, and 7.2.15. The evaluation of how the MPS and NMS meet the single-failure criterion in Section 5.1 of IEEE Std. 603-1991 is described in Section 7.1.3 of this report.

The MPS and NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions. Chapter 16 of this report addresses the NRC

staff's evaluation of the technical specifications. Section 7.2.9.4.3 of this report describes the repair features of the safety-related systems. Section 7.2.15 of this report addresses the NRC staff's evaluation of the capability for test and calibration of the safety systems. Based on the above, the NRC staff finds that ASAI 32 is met.

33. ASAI 33: *An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and cabling for a safety system.*

The applicant provided the disposition of ASAI 33 in DCA Part 2, Tier 2, Section 7.2.9. Redundant divisions of MPS equipment are marked so that equipment can be clearly identified without frequent referral to reference material. Redundant divisions are distinguished by color-coded equipment tags or nameplates. Class 1E cable and cable raceways are marked with the division color and with their proper identification at periodic intervals. For computer systems, software and hardware identification is used to verify that the correct software is installed in the correct hardware component. A configuration control document or drawing is used to identify the correct software, including version, installed in digital I&C systems in accordance with IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3. Section 7.2.9.4.2 of this report addresses the NRC staff's evaluation of identification and coding requirements of the MPS. Therefore, the NRC staff finds that ASAI 33 is met.

34. ASAI 34: *An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for auxiliary features.*

The applicant provided the disposition of ASAI 34 in DCA Part 2, Tier 2, Section 7.2.8. The design of the MPS meets the requirements of Section 5.12 of IEEE Std. 603-1991 and 10 CFR 50.34(f)(2)(xxiii). The evaluation of the auxiliary features of the MPS is described in Section 7.2.8 of this report. Therefore, the NRC staff finds that ASAI 34 is met.

35. ASAI 35: *An applicant or licensee referencing this SE must demonstrate that the application-specific system design implemented with the HIPS platform meets the applicable regulatory requirements for shared systems.*

The applicant provided the disposition of ASAI 35 in DCA Part 2, Tier 2, Section 7.2.8. The safety-related MPS is module specific. There are no safety-related MPSs that share functions across multiple NPMs. The evaluation of multiunit stations is described in Section 7.2.11 of this report. Therefore, the NRC staff finds that ASAI 35 is met.

36. ASAI 36: *An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified human factors requirements.*

The applicant provided the disposition of ASAI 36 in DCA Part 2, Tier 2, Section 7.2.14. Section 7.2.14 of this report addresses the NRC staff's evaluation of human factors engineering (HFE) principles applied to the selection and design of the displays and controls. NUREG-0711, "Human Factors Engineering Program Review Model," provides guidance for establishing a program for the application of HFE to systems, equipment, and facilities of nuclear power generating stations. NUREG-0711 contains the review criteria referenced in SRP Chapter 18. The NRC staff's evaluation of the NuScale HFE program is described in Chapter 18 of this report. Based on the above, the NRC staff finds that ASAI 36 is met.

37. ASAI 37: *An applicant or licensee referencing this SE must confirm that the HIPS platform equipment meets any specified quantitative or qualitative reliability goals.*

The applicant provided the disposition of ASAI 37 in DCA Part 2, Tier 2, Section 7.2.3. Qualitative reliability goals have been established for the MPS to meet the single-failure criterion. The MPS meets the qualitative reliability goals and the requirements of IEEE Std. 379-2000 to satisfy the single-failure criterion through the addition of redundancy (see Section 7.1.3 of this report), diversity (see Section 7.1.5 of this report), and testability (see Section 7.2.15 of this report). The NRC staff's evaluation of reliability goals for I&C components and systems is further described in Section 7.2.3.4.1 of this report. Therefore, the NRC staff finds that ASAI 37 is met.

38. ASAI 38: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide automatic safety system sense and command features for required safety functions.*

The applicant provided the disposition of ASAI 38 in DCA Part 2, Tier 2, Section 7.2.12, "Automatic and Manual Control." The MPS provides a means for automatic initiation of required functions. The automatic features accomplish the reactor trip and ESF actuation functions necessary to shut down and maintain the reactor in a safe condition. The evaluation of the automatic initiation of protective actions is described in Section 7.2.12.4.1 of this report. Therefore, the NRC staff finds that ASAI 38 is met.

39. ASAI 39: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide manual safety system sense and command features for required safety functions.*

The applicant provided the disposition of ASAI 39 in DCA Part 2, Tier 2, Section 7.2.12. The MPS provides a means for manual initiation of required safety-related functions. The manual features accomplish the reactor trip and ESF actuation functions necessary to shut down and maintain the reactor in a safe condition. The evaluation of the manual initiation of protective actions is described in Section 7.2.12.4.2 of this report. Therefore, the NRC staff finds that ASAI 39 is met.

40. ASAI 40: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for sense and command features to provide protection against the resulting condition of a non-safety-related system action that has been caused by a single credible event, including its direct and indirect consequences.*

The applicant provided the disposition of ASAI 40 in DCA Part 2, Tier 2, Section 7.2.10, "Interaction between Sense and Command Features and Other Systems." The boundaries between safety-related and non-safety-related systems are formed by isolation devices that prevent failures or malfunctions in the non-safety-related systems from interfering with the safety-related systems. Therefore, conditions that prevent the safety-related systems from completing protective functions within the sense and command features do not exist in the MPS. The evaluation of the interaction between sense and command features and other systems is described in Section 7.2.10 of this report. Therefore, the NRC staff finds that ASAI 40 is met.

41. ASAI 41: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to acquire and condition field sensor measurements of the required variables.*

The applicant provided the disposition of ASAI 41 in DCA Part 2, Tier 2, Section 7.2.6, "Derivation of System Inputs." The MPS and NMS sensor and process measurement design meets the requirements of Section 6.4 of IEEE Std. 603-1991. The NRC staff's

evaluation of the methods used for the derivation of system inputs is described in Section 7.2.6 of this report. Therefore, the NRC staff finds that ASAI 41 is met.

42. ASAI 42: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for operating bypasses.*

The applicant provided the disposition of ASAI 42 in DCA Part 2, Tier 2, Section 7.2.4. The MPS operating bypasses meet Sections 6.6 and 7.4 of IEEE Std. 603-1991 and the guidance in RG 1.47, Revision 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems." The NRC staff's evaluation of the operating bypasses is described in Section 7.2.4.4.1 of this report. Therefore, the NRC staff finds that ASAI 42 is met.

43. ASAI 43: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses and provide the technical specification requirements.*

The applicant provided the disposition of ASAI 43 in DCA Part 2, Tier 2, Section 7.2.4. The MPS maintenance bypasses meet Sections 6.7 and 7.5 of IEEE Std. 603-1991 and the guidance contained in RG 1.47, Revision 1. The NRC staff's evaluation of the maintenance bypasses is described in Section 7.2.4.4.2 of this report. Technical specification requirements related to the MPS are evaluated in Chapter 16 of this report. Therefore, the NRC staff finds that ASAI 43 is met.

44. ASAI 44: *An applicant or licensee referencing this SE must describe the setpoints, setpoint methodologies, or HIPS platform module accuracies used for a safety system implemented with the HIPS platform equipment.*

The applicant provided the disposition of ASAI 44 in DCA Part 2, Tier 2, Section 7.2.7, "Setpoints." The NRC staff agrees with the approach the applicant selected regarding the NuScale setpoint methodology in TeR-0616-49121, Revision 1. The NRC staff's evaluation of setpoints is described in Section 7.2.7 of this report. Since the DCA provides an acceptable setpoint methodology and ITAAC to verify setpoints and response time, the NRC finds that ASAI 44 is met.

45. ASAI 45: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used for maintenance bypasses.*

The applicant provided the disposition of ASAI 45 in DCA Part 2, Tier 2, Section 7.2.4. The MPS maintenance bypasses meet Sections 6.7 and 7.5 of IEEE Std. 603-1991 and the guidance contained in RG 1.47, Revision 1. The NRC staff's evaluation of the maintenance bypasses is described in Section 7.2.4.4.2 of this report. Therefore, the NRC staff finds that ASAI 45 is met.

46. ASAI 46: *An applicant or licensee referencing this SE must describe power sources to the HIPS platform equipment and how they meet applicable regulatory requirements.*

The applicant provided the disposition of ASAI 46 in DCA Part 2, Tier 2, Section 7.1.2. DCA Part 2, Tier 2, Figures 7.0-11a, "Module Protection System Power Distribution," and 7.0-11b, "Module Protection System Power Distribution," show the redundant power sources to the MPS. Section 7.1.2.4.2 of this report addresses the NRC staff's evaluation of the two redundant power sources to the MPS. Therefore, the NRC staff finds that ASAI 46 is met.

47. ASAI 47: *An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V (independent verification and validation) processes for test and calibration functions as for all other HIPS platform functions.*

The applicant provided the disposition of ASAI 47 in DCA Part 2, Tier 2, Sections 7.2.1, 7.2.8, and 7.2.15. The design, development, and independent verification and validation (iV&V) requirements of the MPS are described in DCA Part 2, Tier 2, Section 7.2.1. The NRC staff's evaluation of the design, development, and iV&V requirements for the MPS is described in Section 7.2.1 of this report. The test and calibration functions described in DCA Part 2, Tier 2, Section 7.2.15, are classified as other auxiliary features of the MPS that are not required for the MPS to perform its safety functions; however, as described in DCA Part 2, Tier 2, Section 7.2.8, these functions are designed and qualified as part of the MPS. The evaluation of the auxiliary features of the MPS is described in Section 7.2.8 of this report. The NRC staff's evaluation of the test and calibration functions is described in Section 7.2.15 of this report. Therefore, the NRC staff finds that ASAI 47 is met.

48. ASAI 48: *An applicant or licensee referencing this SE that relies on a separate computer for the sole verification of test and calibration data should ensure adequate iV&V, configuration management, and quality assurance for the test and calibration functions of the separate computer.*

DCA Part 2, Tier 2, Table 7.0-2 reflects that ASAI 48 is not applicable. The NRC staff agrees that the MPS does not rely on a separate computer as the sole verification of test and calibration data. Based on the above, the NRC staff considers ASAI 48 closed.

49. ASAI 49: *An applicant or licensee referencing this SE must confirm that the manufacturer followed the same design, development, and iV&V processes for self-diagnostics functions as for all other HIPS platform functions.*

The applicant provided the disposition of ASAI 49 in DCA Part 2, Tier 2, Sections 7.2.1, 7.2.8, and 7.2.15. The design, development, and iV&V requirements of the MPS are described in DCA Part 2, Tier 2, Section 7.2.1. The NRC staff's evaluation of the design, development, and iV&V requirements for the MPS is described in Section 7.2.1 of this report. The self-diagnostic functions described in DCA Part 2, Tier 2, Section 7.2.15, are classified as other auxiliary features of the MPS that are not required for the MPS to perform its safety functions; however, as described in DCA T Part 2, Tier 2, Section 7.2.8, these functions are designed and qualified as part of the MPS. The evaluation of the auxiliary features of the MPS is described in Section 7.2.8 of this report. The NRC staff's evaluation of the self-diagnostic functions is described in Section 7.2.15 of this report. Therefore, the NRC staff finds that ASAI 49 is met.

50. ASAI 50: *An applicant or licensee referencing this SE must verify that the manufacturer included the self-diagnostic functions within its type testing of the HIPS platform standardized circuit boards during EQ.*

The applicant provided the disposition of ASAI 50 in DCA Part 2, Tier 2, Sections 7.2.1 and 7.2.15. The design, development, and iV&V requirements of the MPS are described in DCA Part 2, Tier 2, Section 7.2.1. Section 7.2.2 of this report addresses the NRC staff's evaluation of I&C EQ. The overall EQ program is evaluated in Sections 3.10 and 3.11 of this report. The self-diagnostic functions of the MPS are described in DCA Part 2, Tier 2, Section 7.2.15. Therefore, the NRC staff finds that ASAI 50 is met.

51. ASAI 51: *An applicant or licensee referencing this SE must demonstrate that the combination of HIPS platform self-tests and system surveillance testing provide the necessary test coverage to ensure that there are no undetectable failures that could adversely affect a required safety function.*

The applicant provided the disposition of ASAI 51 in DCA Part 2, Tier 2, Sections 7.2.1 and 7.2.15. The MPS and NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions. Section 7.2.15 of this report addresses the NRC staff's evaluation of the capability for test and calibration of the safety systems. Chapter 16 of this report addresses the technical specifications. Therefore, the NRC staff finds that ASAI 51 is met.

52. ASAI 52: *An applicant or licensee referencing this SE must demonstrate that the full system design, any use of a shared component, the equipment's installation, and the communication bus architecture provide the required independence.*

The applicant provided the disposition of ASAI 52 in DCA Part 2, Tier 2, Section 7.1.2. Section 7.1.2 of this report addresses the NRC staff's evaluation of independence. The physical and electrical independence attributes of the MPS and NMS conform to the guidance in RG 1.75, Revision 3, which endorses IEEE Std. 384-1992. The communication independence attributes of the MPS conform to the guidance in RG 1.152, which endorses IEEE Std. 7-4.3.2-2003. Therefore, the NRC staff finds that ASAI 52 is met.

53. ASAI 53: *An applicant or licensee referencing this SE must verify that the safety network provides communications independence and security requirements for communication from safety- to non-safety-related systems.*

The applicant provided the disposition of ASAI 53 in DCA Part 2, Tier 2, Section 7.1.2. Section 7.1.2 of this report addresses the NRC staff's evaluation of independence. The communication independence attributes of the MPS conform to the guidance in RG 1.152, which endorses IEEE Std. 7-4.3.2-2003. The applicant stated that DCA Tier 2, Section 7.2.9, provides information to address the communication security requirements for safety- to non-safety-related systems. Therefore, the NRC staff finds that ASAI 53 is met.

54. ASAI 54: *An applicant or licensee referencing this SE must establish the identification and coding requirements for cabinets and components for a safety system and the methods to verify that the correct firmware or software is installed in the correct hardware component.*

The applicant provided the disposition of ASAI 54 in DCA Part 2, Tier 2, Section 7.2.9. A configuration control document or drawing is used to identify the correct software, including version, installed in digital I&C systems in accordance with IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3. Section 7.2.9.4.2 of this report addresses the NRC staff's evaluation of identification and coding requirements of the MPS. Therefore, the NRC staff finds that ASAI 54 is met.

55. ASAI 55: *An applicant or licensee referencing this SE must demonstrate that a full system design does not, with the exception of division voting logic, depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.*

The applicant provided the disposition of ASAI 55 in DCA Part 2, Tier 2, Section 7.1.2. With the exception of interdivisional voting, the communication within the MPS separation group is independent and does not rely on communication from outside the respective separation group or division to perform a safety function. The MPS separation groups perform independent signal conditioning and trip determination and provide that input to the SBM, which provides inputs to the SVM for the two-out-of-four voting logic. The NRC staff's evaluation of communication independence is described in Section 7.1.2 of this report. Therefore, the NRC staff finds that ASAI 55 is met.

56. ASAI 56: *An applicant or licensee referencing this SE must confirm that system real-time performance is adequate, assuming the longest possible completion time to ensure the completion of protective actions within the critical time frames required by the plant safety analyses.*

The applicant provided the disposition of ASAI 56 in DCA Part 2, Tier 2, Section 7.1.4. The MPS architecture uses the HIPS platform. The MPS response time analysis demonstrates that the MPS performs and completes its required safety functions in a predictable and repeatable manner. TR-1015-18653, Section 7.7, describes the calculation used to determine the worst-case digital time response for an MPS channel. Section 7.1.4 of this report addresses the NRC staff's evaluation of I&C output predictability and repeatability. Therefore, the NRC staff finds that ASAI 56 is met.

57. ASAI 57: *An applicant or licensee referencing this SE must configure the slave modules (e.g., SFMs and EIMs) to alarm and assume a fail-safe state.*

DCA Part 2, Tier 2, Section 7.0.4 provides the configuration of the slave modules to alarm and assume a fail-safe state, as shown in Table 7.1-1 of this report. The NRC staff confirmed that the slave modules (e.g., SFMs and EIMs) are configured to provide an alarm in the MCR and assume a fail-safe state. DCA Part 2, Tier 2, Section 7.0.4.1, "Module Protection System," identifies the safe states for protective functions and the conditions that require the MPS to enter a fail-safe state. The evaluation of the safe states for the MPS is described in Section 7.0.4 of this report. Therefore, the NRC staff finds that ASAI 57 is met.

58. ASAI 58: *An applicant or licensee referencing this SE should verify having appropriate physical, logical, and programmatic controls during the system development phases to ensure that unwanted, unneeded, and undocumented functionality is not introduced into digital safety systems.*

The applicant provided the disposition of ASAI 58 in DCA Part 2, Tier 2, Section 7.2.9. Section 7.2.9.4.1 of this report addresses the NRC staff's evaluation of secure development and operational environment (SDOE). Therefore, the NRC staff finds that ASAI-58 is met.

59. ASAI 59: *An applicant or licensee referencing this SE must describe how the HIPS platform equipment is used to provide a deterministic communication structure for required safety functions.*

The applicant provided the disposition of ASAI 59 in DCA Part 2, Tier 2, Section 7.1.4. The MPS architecture uses the HIPS platform. The MPS response time analysis demonstrates that the MPS performs and completes its required safety functions in a predictable and repeatable manner. Section 7.1.4 of this report addresses the NRC staff's evaluation of I&C output predictability and repeatability. Therefore, the NRC staff finds that ASAI 59 is met.

60. ASAI 60: *An applicant or licensee referencing this SE must demonstrate that the full system design supports cross-divisional and non-safety-related communication with the appropriate independence and isolation.*

The applicant provided the disposition of ASAI 60 in DCA Part 2, Tier 2, Section 7.1.2. The NRC staff's evaluation of electrical, physical, and communications independence is described in Section 7.1.2 of this report. Therefore, the NRC staff finds that ASAI 60 is met.

61. ASAI 61: *An applicant or licensee referencing this SE must demonstrate that the application-specific use of an enable non-safety-related switch and its configuration details will not adversely affect the channel independence nor the operation of safety-related equipment when the safety-related equipment is performing its safety function. In addition, the applicant or licensee must demonstrate that the application-specific use of an enable non-safety-related switch should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.*

The applicant provided the disposition of ASAI 61 in DCA Part 2, Tier 2, Section 7.1.2. While discrete actuations may be sent from the non-safety-related systems, the use of the safety-related "enable non-safety-related control switch" is required for actuation signals to pass through to the safety-related actuation logic, which is prioritized such that the safety-related actuations are passed in the absence of a required protective action. When allowed by plant procedures to reconfigure systems after a reactor trip or an ESF actuation, the components can be repositioned using the non-safety-related MCS when the "enable non-safety-related control switch" is activated and no automatic or manual safety actuation signal is present. Therefore, the NRC staff finds that ASAI 61 is met.

62. ASAI 62: *An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the systems to eliminate HIPS platform digital CCF vulnerabilities.*

The applicant provided the disposition of ASAI 62 in DCA Part 2, Tier 2, Section 7.1.5. Two of the four separation groups and one of the two divisions of RTS and ESFAS will utilize a different programmable technology. Section 7.1.5 of this report addresses the NRC staff's evaluation of diversity. Therefore, the NRC staff finds that ASAI 62 is met.

63. ASAI 63: *An applicant or licensee referencing this SE must address any other digital CCF vulnerabilities in the application-specific D3 analysis.*

The applicant provided the disposition of ASAI 63 in DCA Part 2, Tier 2, Section 7.1.5. The D3 assessment demonstrates that there is adequate diversity within the MPS for each event evaluated in Chapter 15 of this report. A D3 coping analysis was performed to address identified vulnerabilities and demonstrates adequate diversity within the design. The evaluation of the coping analysis is described in Section 7.1.5 of this report. The analysis concluded that plant response to vulnerabilities is either bounded by Chapter 15 analyses or is within acceptable limits. Therefore, the NRC staff finds that ASAI 63 is met.

64. ASAI 64: *An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide FPGA diversity between redundant portions of the system architecture (e.g., in each of two redundancies in a four-fold redundant system or in one redundancy in a two-fold redundant system) to ensure HIPS platform safety performance in the presence of a digital CCF.*

The applicant provided the disposition of ASAI 64 in DCA Part 2, Tier 2, Section 7.1.5. The D3 assessment demonstrates that sufficient diversity exists within the MPS to prevent a postulated digital-based CCF from disabling the capability to perform any of its safety-related functions. The D3 coping analysis identifies different sensors not vulnerable to the same digital-based CCF that exist to mitigate the associated event conditions without requiring a separate I&C system. The evaluation of the coping analysis is described in Section 7.1.5 of this report. Therefore, the NRC staff finds that ASAI 64 is met.

65. ASAI 65: *An applicant or licensee referencing this SE must demonstrate that the HIPS platform equipment is used to provide diversity for indication and component control signals to ensure HIPS platform monitoring and control performance in the presence of a digital CCF.*

The applicant provided the disposition of ASAI 65 in DCA Part 2, Tier 2, Section 7.1.5. Division I and II manual control switches are provided to manually initiate at the division level the automatic safety-related functions. Manual actuation signals are inputs to the APL within an EIM. The APL within the EIMs is implemented in discrete analog components and is downstream of the automatic digital portion of the safety system. The MCS, SDIS, and manual controls are sufficiently diverse that any failure does not prevent the operator from obtaining or resolving conflicting information. Section 7.1.5 of this report addresses the NRC staff's evaluation of diversity. Therefore, the NRC staff finds that ASAI 65 is met.

7.1.6.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.6.6 Conclusions

The NRC staff concludes that the application satisfies the application-specific information requirements in TR-1015-18653, Revision 2 and are reflected in DCA Tier 2, Table 7.0 2. Therefore, the NRC staff considers ASAIs 1 to 65 closed.

7.1.7 Not Used

7.1.8 Hazard Analysis

7.1.8.1 Introduction

This Section contains the NRC staff's evaluation of hazard analysis (HA) information to determine if the applicant's HA adequately (1) describes and defines each I&C system to be analyzed, (2) identifies each loss or impairment of safety function that the I&C system should prevent, and (3) assures that all safety functions identified in the application are allocated to the appropriate I&C system. In addition, the NRC staff considered the I&C system architecture in its review of the HA.

7.1.8.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.1.9, "Hazard Analysis."

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.1.8, is given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 1 and is evaluated in Section 14.3.5 of this report

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.1.8.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.1.8.

7.1.8.3 Regulatory Basis

HA performed during an I&C system design development is a part of quality assurance activities. The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.3, "Quality," which requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. It also requires that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program.

- 10 CFR Part 50, Appendix A, GDC 1.

- Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establishes QA requirements for the design, manufacture, construction, and operation of safety-related SSCs.

Appendix A, "Hazard Analysis," to the DSRS provides guidance for evaluating HA performed during an I&C design development. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.28, Revision 4, "Quality Assurance Program Criteria (Design and Construction)," endorses American Society of Mechanical Engineers (ASME) NQA-1-2008, "Quality Assurance Requirements for Nuclear Facility Applications," and ASME NQA-1a-2009, "Addenda A to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications," with identified exceptions and clarifications.

- RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications.

7.1.8.4 Technical Evaluation

DCA Part 2, Tier 2, Section 7.1.8, describes the HA methodology applied to the design of the NuScale I&C systems and how the HA has been incorporated into the I&C design and architecture. It also states that a system HA was performed for the I&C systems described in DCA Part 2, Tier 2, Section 7.0, and considered the hardware, software, organizations, and processes used to develop the system.

The NRC staff's evaluation of the external hazards for the NuScale design is described in Section 2.2 of this report. The NRC staff's evaluation of the internal hazards for the NuScale design is described in Chapter 3 of this report. The NRC staff's evaluation of the electrical power system design conditions is described in Section 8.3.2 of this report. The NRC staff's

evaluation of independence is described in Section 7.1.2 of this report. The NRC staff's evaluation of the EQ requirements for I&C systems is described in Section 7.2.2 of this report.

7.1.8.4.1 Software-Related Contributory Hazards

DCA Part 2, Tier 2, Section 7.1.8.1, "Software-Related Contributory Hazards," provides information associated with contributory hazards as the system is developed, and the NRC staff evaluated this information for adequacy during the review of the application. The NRC staff considered the hazard controls and commitments associated with life-cycle phases for the I&C safety systems.

Concept Phase

As part of the concept phase in the software life cycle, the applicant states that a preliminary hazards list is prepared on the system that identifies (1) hazardous states of the system, (2) sequences of actions that can cause the system to enter a hazardous state, (3) sequences of actions intended to return the system from a hazardous state to a nonhazardous state, and (4) actions intended to mitigate the consequences of accidents.

Requirements Phase

During the requirements phase of the software life cycle, a requirement traceability matrix (RTM) is used in accordance with the Software Requirements Management Plan, as the tracking system to assure that hazards, their responsibility assignment, and their status can be tracked throughout the software life cycle, including retirement.

Design Phase

Software safety design analysis is performed during the design phase of the software life cycle to confirm that the safety-critical portion of the software design correctly implements the software integrity level (SIL) 3 and 4 software or configurable logic device logic functional requirements identified during the requirements phase and that the design introduces no new hazards.

Implementation Phase

Software safety logic analysis is performed during the implementation phase of the software life cycle to confirm that the SIL 3 and 4 portions of the logic design are correctly implemented in the logic and that the logic introduces no new hazards.

Testing Phase

Software safety test analysis is performed during the test phase to confirm that the SIL 3 and 4 portions of the software or configurable logic device logic design are correctly implemented in the logic and that the logic introduces no new hazards. Throughout each phase, software verification and validation (V&V) activities are performed, and the results of the software life-cycle phase are matched against the system safety requirements and system HA to assure that (1) system safety requirements have been satisfied within the software life-cycle phases, and (2) no additional hazards have been introduced by the work done during the software life-cycle activity.

The HA described in DCA Part 2, Tier 2, Section 7.1.8 is a living process that is performed throughout the I&C safety system development life cycle. DCA Part 2, Tier 2, Section 7.2.1.1 states that the system HA is reviewed when any system design information is changed to determine whether the changes impact the inputs or results of the HA.

7.1.8.4.2 Hazard Analysis Methodology

DCA Part 2, Tier 2, Section 7.1.8.2, "Hazard Analysis Methodology," states the following:

> *NuScale I&C system hazard analysis is intended to evaluate those conditions and factors associated with the system under analysis and the systems that directly interact with it that can result in unintended or unwanted system operation, including a failure to initiate a protective action.*

The applicant designated these conditions in the analysis as "unsafe." The applicant also stated that additional analysis is performed to provide guidance for the development process where a control action could affect continuity of operation or create other abnormal operating conditions without causing failure of a required protective action. The applicant designated these conditions in the analysis as "undesired."

The NRC staff evaluated the I&C system design described in the application to confirm that the applicant has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control these hazards. The NRC staff reviewed the HA of the MPS and NMS and confirmed that the HA information includes the necessary controls for the various contributory hazards and the associated commitments for each phase of the development process.

DCA Part 2, Tier 2, Section 7.1.8.2 states that the MPS and NMS HAs are to be performed for all modes of system operation.

7.1.8.4.3 Hazard Analysis Process

In DCA Part 2, Tier 2, Section 7.1.8.3, "Hazard Analysis Process," the applicant states that the "NuScale I&C system hazard analysis is based on a view of the processes that are performed by the systems described in Section 7.0." The cross-referencing of hazard conditions, safety constraints, and functional design requirements assures that potentially hazardous conditions not previously identified by other analysis methods are mitigated by feedback into the design of the system functional requirements.

The HA methodology described in the application is a living process, performed and verified throughout the I&C safety system development life cycle.

The NRC staff agrees with the applicant's conclusion that the HA does not explicitly analyze the effects of redundancy and defense in depth; however, the hazard conditions identified in the HA are partially or fully mitigated through application of the fundamental design principles of redundancy and D3 (see Sections 7.1.3 and 7.1.5 of this report).

7.1.8.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.1.8.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed HA has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control the hazards. The NRC staff also concludes that the HA information includes the necessary controls for the various contributory hazards, including design and implementation constraints, and the associated commitments. The NRC staff finds that the proposed HA for developing the I&C system design conforms to the quality assurance

guidance in RG 1.28, Revision 4; and RG 1.152, Revision 3. On this basis, the NRC staff concludes that the application provides information sufficient to demonstrate that the QA measures applied to the HA for I&C system and software life cycle meet the applicable QA requirements of GDC 1 of Appendix A to 10 CFR Part 50; Appendix B to 10 CFR Part 50; and Section 5.3 of IEEE Std. 603-1991.

7.2 Instrumentation and Controls—System Characteristics

This Section provides guidance associated with I&C safety system characteristics described in Sections 5, 6, and 7 of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3.

7.2.1 Quality

7.2.1.1 Introduction

This Section contains the NRC staff's evaluation of information provided to assure that I&C safety system equipment will be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed.

This Section is focused on those quality processes specific to I&C system development. The overall quality assurance (QA) program is evaluated in Chapter 17 of this report.

7.2.1.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.1, "Quality," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.2, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.1, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 4, 16, 17, 47, 49, 50, and 51, which relate to quality, are described in Section 7.1.6 of this report.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.1, is given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 1. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.1.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.1.

7.2.1.3 Regulatory Basis

The following regulations apply to the NRC staff's evaluation of quality standards applied to the development of instrumentation and control systems:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.3, "Quality," which requires that components and modules shall be of a quality that is consistent with minimum

maintenance requirements and low failure rates. It also requires that safety system equipment be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed QA program.

- 10 CFR Part 50, Appendix A, GDC 1.

- Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," to 10 CFR Part 50 establishes QA requirements for the design, manufacture, construction, and operation of safety-related SSCs.

The guidance in DSRS Section 7.2.1 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.28, Revision 4, "Quality Assurance Program Criteria (Design and Construction)," endorses American Society of Mechanical Engineers (ASME) NQA-1-2008, "Quality Assurance Requirements for Nuclear Facility Applications," and ASME NQA-1a-2009, "Addenda A to ASME NQA-1-2008, Quality Assurance Requirements for Nuclear Facility Applications," with identified exceptions and clarifications.

- RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications.

- RG 1.168, Revision 2, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," and IEEE Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," with identified exceptions and clarifications.

- RG 1.169, Revision 1, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 828-2005, "IEEE Standard for Software Configuration Management Plans," with identified exceptions and clarifications.

- RG 1.170, Revision 1, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 829-2008, "IEEE Standard for Software Test Documentation," with identified exceptions and clarifications.

- RG 1.171, Revision 1, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing," with identified exceptions and clarifications.

- RG 1.172, Revision 1, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 830-1998, "IEEE Recommended Practice for Software Requirements Specifications," with identified exceptions and clarifications.

- RG 1.173, Revision 1, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1074-2006, "IEEE Standard for Developing a Software Project Life Cycle Process," with identified exceptions and clarifications.

7.2.1.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed Section 7.2.1 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the NuScale DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to quality. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.1.3 and to address aspects of ASAIs 4, 16, 47, 49, 50, and 51 that relate to quality. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

7.2.1.4.1 System and Software Development Activities

Plant Safety Analyses and I&C System and Software Safety Analyses

Plant safety analyses and software safety analyses are mainly discussed in DCA Part 2, Tier 2, Section 7.2.1.2.

Section 4 of IEEE Std. 603-1991 requires, in part, that a specific basis be established for the design of each safety I&C system. This information is provided in DCA Part 2, Tier 2, Section 7.1.1.1. The design basis is consistent with the requirements of Section 4 of IEEE Std. 603-1991.

The I&C system, hardware, and software safety analyses have been conducted for each phase of the development life cycle and include the identification of hazards associated with the chosen I&C design. Subsequent I&C system, hardware, and software safety analyses consider whether software is a potential cause of a hazard or whether it is used to support the control of a hazard. The NRC staff finds this approach acceptable because it conforms to RG 1.173, Revision 1. Software-related contributory hazards are evaluated in Section 7.1.8.4.1 of this report.

As part of the software safety analyses, the application defines an SIL scheme to quantify software criticality, as defined in the endorsed IEEE Std. 1012-2004. DCA Part 2, Tier 2, Section 7.2.1.2, defines SIL classification based on the NuScale software classification procedure that governs the criticality analysis. DCA Part 2, Tier 2, Section 7.2.1.2, states that the software development activities are adjusted based on the software classification. SILs are classified to the highest SIL appropriate for the supported system safety function. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

I&C System Requirements

I&C system requirements are mainly discussed in DCA Part 2, Tier 2, Section 7.2.1.1.1.1 and Section 7.2.1.2 and its subsection 7.2.1.2.2.

DCA Part 2, Tier 2, Section 7.2.1.2.2, discusses a digital I&C system requirement specification that describes the identification, development, documentation, review, approval, and maintenance of I&C system requirements. The NRC staff finds this approach is acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.2, describes the I&C system requirement specification, which includes system and software safety analyses throughout the life cycle; functions and capabilities of the I&C system during operations; system boundaries; safety classification; safety

functional properties and additional features not performing a safety function; customer-requested features; safety, security, and human-machine interfaces; operations and maintenance measures, including intended fault identification, test, calibration and repair; design constraints; qualification requirements; results from hazard analyses; and restrictions and constraints placed on the system to assure compatibility with other plant systems. The NRC staff finds this acceptable because it conforms to RG 1.152, Revision 3, which endorses IEEE Std. 7-4.3.2-2003.

DCA Part 2, Tier 2, Section 7.2.1.1.1.1, states that an RTM is initially populated from the system functional specifications and software design description (SDD) and/or I&C system requirements and then documented, tracked, and maintained. DCA Part 2, Tier 2, Section 7.2.1.2.2, indicates that the RTM facilitates bidirectional traceability (from requirements to system validation testing) of all system requirements. Moreover, the RTM identifies references to analyses and supporting documentation that establish the bases for system requirements. The NRC staff finds this acceptable because it conforms to RG 1.173, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.2, states that all identified system requirements are evaluated, baselined, updated as necessary, and placed under configuration management. DCA Part 2, Tier 2, Section 7.2.1.2.2, also states that inconsistencies between system requirements and other system-related elements such as hardware and software are identified and evaluated. Finally, it indicates that the completed I&C system requirement specification is used as input to the ongoing I&C system safety analysis activity.

Based on the above, the NRC staff finds this acceptable because it conforms to RG 1.169, Revision 1.

I&C System Architecture

The evaluation of I&C system architecture is provided in Section 7.0.4.2 of this report.

DCA Part 2, Tier 2, Section 7.2.1.2.3, states that the SDD (including I&C system architecture) is documented, baselined, updated as necessary, and placed under configuration management. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1, which endorses IEEE Std. 828-2005.

DCA Part 2, Tier 2, Section 7.2.1.2.3, indicates that the SDD (including I&C system architecture) is used as input to the ongoing I&C system safety analysis activity. The NRC staff finds this approach acceptable because it conforms to RG 1.173, Revision 1.

I&C System Design

The I&C system design is described in DCA Part 2, Tier 2, Section 7.2.1.1.1.2 and Section 7.2.1.2 and its subsections 7.2.1.2.3 through 7.2.1.2.5.

DCA Part 2, Tier 2, Section 7.2.1.1.1.2, states that the SDD documents the system architecture and design details and is developed on the system functional specifications. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.4, indicates that the equipment requirement specification (ERS) is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. Bidirectional traceability is established between the ERS and the SDD. The ERS is used as input to the ongoing system safety analyses according to the NuScale Digital I&C Software Safety Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.1 states the following:

> *A software safety analysis is conducted and is documented in a Software Safety Analysis Report, which is initiated in the concepts phase of the system development life cycle with the Preliminary Hazards Analysis and updated throughout subsequent life cycle phases. When the Software Safety Analysis Report is first initiated or subsequently updated, an independent V&V Team performs V&V pursuant to the hazards analysis V&V tasks as specified in the NuScale Digital I&C Software Verification and Validation Plan.*

The NRC staff found this acceptable because it conforms to RG 1.170, Revision 1; RG 1.172, Revision 1; and RG 1.173, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.1.1.2, indicates that the I&C system design description is analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.5, indicates that the software requirements specification (SRS) is derived from, and traceability is assured with, the system design, I&C system architecture, SDD, and Digital I&C System Requirements Specification. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.3, indicates that the SDD is used as input to the ongoing system safety analyses. The NRC staff finds this approach acceptable because it conforms to RG 1.173, Revision 1.

Software Requirements

Software requirements are mainly discussed in DCA Part 2, Tier 2, Section 7.2.1 and its subsections 7.2.1.2.5 through 7.2.1.2.6.

DCA Part 2, Tier 2, Section 7.2.1, states that the NuScale Digital I&C Software Development Plan specifies the requirements to develop the SRS for the safety-related digital I&C systems, which is consistent with the guidance in RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that the SRSs are baselined, updated as necessary, and placed under configuration management in accordance with the Digital I&C Software Configuration Management Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1, which endorses IEEE Std. 828-2005.

DCA Part 2, Tier 2, Section 7.2.1.2.5, states that the SRSs are derived from, and traceability is assured with, the system design, I&C system architecture, SDD, and Digital I&C System Requirements Specification. Where appropriate, the RTM identifies references to analyses and or supporting documentation that establish the basis for software requirements. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1, which endorses IEEE Std. 830-1998.

DCA Part 2, Tier 2, Section 7.2.1.2.5, states that the completed SRSs are used as input to the ongoing I&C software safety analysis activity for SIL 3 and 4 software or complex logic device (CLD) logic. The NRC staff finds this approach acceptable because it conforms to RG 1.173, Revision 1.

Software Design

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that an SDD is developed for the software product to document the detailed design for the software or CLD logic elements of the software system and how the software units are to be constructed. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that the SDD addresses the methods by which software units are refined into lower levels including software modules to allow coding programming, compiling (not applicable to CLD logic), and testing. The software or CLD logic is also divided into a set of interacting units, including the description of those units, the interfaces, and dependencies in a structured fashion. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3, which endorses IEEE Std. 7-4.3.2-2003.

DCA Part 2, Tier 2, Section 7.2.1.2.6, indicates that the design of a software module is restricted to one clearly identified function that involves only minimum interaction with other functions, thus minimizing the impact of changes. The interfaces between the various units are simple, completely identified, and documented. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.6, indicates that the applicable software design is incorporated from the software requirements phase into the software design and implementation. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that traceability is established between software unit(s) and software module(s). The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that the software design is assessed to assure that it adequately covers the requirements in the SRSs and does not contain unnecessary functions. For predeveloped digital platforms, preexisting software (e.g., operating system software) may contain features that are not used (or not configured for use) in a specific I&C system. In those instances, the preexisting software is assessed to (1) identify those unused capabilities, (2) evaluate whether those functions may impact performance of the safety function, and (3) identify any compensatory measures taken. The evaluation of these capabilities is described in Section 7.2.9.4.1 of this report.

DCA Part 2, Tier 2, Section 7.2.1.2.6, indicates that the Digital I&C Software Configuration Management Plan governs the process for controlling code change requests and modifications. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.6, indicates that the SDD and interface design descriptions (IDDs) are analyzed, reviewed, approved, baselined, updated as necessary, and placed under configuration management according to the NuScale Digital I&C Software Configuration Management Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.6, indicates that the SDD is also used as input to the ongoing I&C system safety analyses per the NuScale Digital I&C Software Safety Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.173, Revision 1.

Software Implementation

The NuScale Digital I&C Software Integration Plan is a product of the equipment requirements specification phase described in DCA Tier 2, Section 7.2.1.1.1.4, which provides the framework for developing, performing and documenting software component (or unit) testing. The NuScale software development plans use the terminology of component testing and unit testing interchangeably.

The NRC staff finds the software integration plan acceptable because it conforms to RG 1.171, Revision 1.

The NuScale safety-related module protection system (MPS) design is based on field programmable gate array technology that is programmed using hardware description language. The translation of the detailed MPS design into the applicable hardware description language is addressed in DCA Part 2, Tier 2, Section 7.2.1.1.2.7, for the software implementation phase of the system development life cycle activities. The NRC staff finds the software implantation phase acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.7, indicates that the code capability of executing the safety design features and methods developed during the software design process is confirmed and is documented within the SDD and Software Safety Analysis Report. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.7, states that an analysis is performed on the software to identify potential hazards in accordance with the NuScale Digital I&C Software Safety Plan. The code is confirmed using the coding rules, methods, standards, and other applicable criteria of the NuScale Software Coding and Hardware Description Language Coding Guidelines. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.7, indicates that the software code or CLD logic is designed to facilitate analysis, testing, and readability. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.7, indicates that the correct implementation of the SRS is validated during software component tests with the software development and simulation tools and during testing on the test and development system. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1 indicates that the software unit testing will be performed to assure that it satisfies design requirements, consistent with the guidance in RG 1.170, Revision 1. The NuScale software development plans use the terminology of component testing and unit testing interchangeably. The NRC staff finds that the software unit testing acceptable because it conforms to RG 1.170, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.5, indicates that the completed SRS is used as input to the ongoing I&C software safety analysis activity for SIL 3 and 4 software or CLD logic. The NRC staff finds this approach acceptable because it conforms to RG 1.172, Revision 1.

Software Integration

DCA T Part 2, Tier 2, Section 7.2.1 describes the NuScale Digital I&C Software Master Test Plan, which specifies the requirements for performing software component or unit testing for the safety-related digital I&C systems. This is consistent with the guidance in RG 1.171, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1 describes the following critical elements of software integration.

> *The independent V&V engineer develops the integration testing documentation and conducts integration testing for software and complex logic device (CLD) logic classified as software integrity level (SIL) 3 and 4.*

The NRC staff finds the critical elements of software integration acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that, for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team identifies and resolves discrepancies between actual and expected results in integration testing. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

I&C System Testing

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team assures that the integrated software or CLD logic modules have successfully passed integration testing and that the software system is integrated with applicable hardware systems. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.9, indicates that a digital I&C system installation and site test plan is used which documents the methods by which the I&C safety system is installed and connected to other plant systems. The NRC staff finds this approach acceptable because it conforms to RG 1.170, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.9, indicates that the site acceptance test (SAT) demonstrates that the installed system performs in accordance with the system design basis. The NRC staff finds this approach acceptable because it conforms to RG 1.170, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.9, indicates that, for SIL 3 and 4 software or CLD logic, the independent V&V team works with the licensee to assure that the SAT demonstrates that the installed system performs the safety function described in the system design basis. For SIL 1 and 2 software or CLD logic, the engineering team SAT demonstrates that the installed system performs the safety function described in the system design basis. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team assures the detection of any inconsistencies between the software or CLD logic and the hardware. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.9, indicates that the SAT report is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan (DCA Part 2, Tier 2, Section 7.2.1.2.9). The NRC staff finds this approach acceptable because it conforms to RG 1.170, Revision 1, and RG 1.169, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team demonstrates that hazards identified in the Software Safety Analysis Report have been eliminated or controlled to an acceptable level of risk and assures that additional hazardous states identified during testing undergo analysis before

software delivery or use. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team evaluates and assures the correction of identified test discrepancies and makes provisions available for appropriate regression testing following changes made to resolve discrepancies. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.2.8, indicates that for SIL 3 and 4 software or CLD logic, a test engineer from an independent V&V team provides the completed system test results in the system test report to the engineering team as an input to the ongoing digital I&C system safety analysis activity of the NuScale Digital I&C Software Safety Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2, and RG 1.172, Revision 1.

I&C System Installation

DCA Part 2, Tier 2, Section 7.2.1.1.2.9, indicates that a digital I&C system installation and site test plan is used which documents the methods by which the I&C safety system is installed and connected to other plant systems. The NRC staff finds this approach acceptable because it conforms to RG 1.170, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1.1.2.9, indicates that the engineering team assures that the system installation plan describes the procedures for software installation, combined hardware and software installation, and systems installation; the confirmation measures to assure the computer system is functional, sensors and actuators are functional, and the required cards are present and installed in the correct slots (when applicable); the communication system is correctly installed; and correct software versions (i.e., consistent with the versions used for final system testing) are installed on the correct digital I&C system. The NRC staff finds this approach acceptable because it conforms to DSRS Section 7.2.1 and RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.1.2.9, indicates that, for SIL 3 and 4 software or CLD logic, a team performs V&V of the installation package and documents the results on corresponding V&V task reports pursuant to the NuScale Digital I&C Software V&V Plan. For SIL 1 and 2 software or CLD logic, an independent verifier within the engineering team does the V&V and documents the results. The NRC staff finds this approach acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.1.1.1, describes how anomalies discovered during installation would be reported to the developer and resolved before placing the system into operation.

> *When anomalies and deviations are identified during the V&V activities, V&V anomaly reports are generated by the independent V&V engineer. The responsible design engineering team member is required to review and resolve all anomalies reported.*

The NRC staff finds the anomalies resolution process acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.1.1.1, describes the control of software modifications during installation. Once the independent V&V engineer concurs with the resolutions to the anomalies identified, a V&V task report is issued for the completed activities of each life cycle phase. The NRC staff finds the control of software modification process acceptable because it conforms to RG 1.168, Revision 2.

DCA Part 2, Tier 2, Section 7.2.1.1.2.9, states that the SAT report is baselined and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan. The NRC staff finds this approach acceptable because it conforms to RG 1.169, Revision 1.

I&C System Operations

DCA Part 2, Tier 2, Section 7.2.1.2.10, contains COL Information Item 7.2-1 pertaining to implementation of the life-cycle processes for the operation phase of I&C systems. As indicated, the applicant specifies the operation phase of the I&C systems as a COL information item. The NRC staff considers this COL information item acceptable, as the operation aspects of the I&C systems are unique to the COL applicant and should be addressed at the time of COL application.

I&C System Maintenance

DCA Part 2, Tier 2, Section 7.2.1.2.11, contains COL Information Item 7.2-2 pertaining to implementation of the life-cycle processes for the system maintenance phase of I&C systems. As indicated, the applicant specifies the maintenance phase of the I&C systems as a COL information item. The NRC staff considers this COL information item acceptable, as the maintenance aspects of the I&C systems are unique to the COL applicant and should be addressed at the time of COL application.

I&C System Retirement

DCA Part 2, Tier 2, Section 7.2.1.2.12, contains COL Information Item 7.2-3 pertaining to implementation of the life-cycle processes for the retirement phase of I&C systems. As indicated, the applicant specifies the retirement phase of the I&C systems as a COL information item. The NRC staff considers this COL information item acceptable, as the retirement aspects of the I&C systems are unique to the COL applicant and should be addressed at the time of COL application.

7.2.1.4.2 Project Management and Organizational Processes

DCA Part 2, Tier 2, Section 7.2.1.3, describes the project management and organizational processes that will be employed by the QA program and used to define the project's organization, planning, execution, monitoring, control, and closure activities of the entire I&C safety system development effort.

DCA Part 2, Tier 2, Section 7.2.1 describes the NuScale Digital I&C Software Management Plan that governs the software project life cycle activities, and implements the guidance provided in IEEE Std.1074-2006 as endorsed by RG 1.173, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1 also describes the following provisions for the establishment, documentation, and maintenance of a schedule that considers the overall project as well as interactions of milestones.

> *The Digital I&C Software Management Plan, in conjunction with the overall Project Management Plan provides the framework for development of the project schedule, including major milestones and baseline reviews at each phase of the software life cycle, work products and project deliverables at each phase of the software life cycle.*

The NRC staff finds the software management plan acceptable because it conforms to RG 1.173, Revision 1.

DCA Part 2, Tier 2, Section 7.2.1, describes the provisions for risk management, including problem identification, impact assessment, and development of risk mitigation plans for risks that have the potential to significantly impact system quality goals, with appropriate metrics for tracking resolution progress. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.3, discusses the establishment of quality metrics throughout the life cycle to assess whether the quality requirements of IEEE Std. 603-1991 and IEEE Std. 7-4.3.2-2003 are being met. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.3, discusses adequate control of software tools to support system development and V&V processes and conform to the guidance of IEEE Std. 7-4.3.2-2003. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1.2.8, gives provisions for the documentation and resolution of problems and nonconformances found in the system elements. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

DCA Part 2, Tier 2, Section 7.2.1, gives provisions for effective oversight of all life-cycle-related activities. The NRC staff finds this approach acceptable because it conforms to RG 1.152, Revision 3.

7.2.1.4.3 Software Quality Assurance Processes

By definition, QA includes software quality assurance. RG 1.152, Revision 3, indicates, in part, that conformance with the recommendations of IEEE Std. 7-4.3.2-2003 is a method acceptable for providing high functional reliability and fulfilling design requirements for computers used in the safety systems of nuclear power plants. IEEE Std. 7-4.3.2-2003, Section 5.3.1, states, in part, that "computer software shall be developed, modified, or accepted in accordance with an approved software QA plan."

The application describes measures to satisfy the applicable requirements of Appendix B to 10 CFR Part 50 with respect to software QA. In particular, the application describes how the software QA plan is implemented throughout the software development life cycle, which is evaluated in Section 17.5 of this report.

The application addresses the QA process in DCA Part 2, Tier 2, Section 7.2.1, which describes in detail how the endorsed codes and standards are used to provide reasonable assurance that the DI&C systems and components will satisfactorily perform their safety functions and how to appropriately record the design, fabrication, and testing of the I&C systems and components important to safety. The NRC staff finds this approach acceptable because it meets Criteria I, "Organization," of 10 CFR Part 50, Appendix B.

7.2.1.4.4 Software Verification and Validation Processes

RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, subject to the exceptions and clarifications identified in the regulatory guide. Sections 5.3.3 and 5.3.4 of IEEE Std. 7-4.3.2-2003 provide guidance on V&V activities and independent V&V, respectively.

RG 1.168, Revision 2, endorses IEEE Std. 1012-2004 and IEEE Std. 1028-2008, with the exceptions and clarifications stated in the regulatory positions. IEEE Std. 1012-2004 describes a method acceptable to the NRC staff for complying with the NRC's regulations for promoting high functional reliability and design quality in software used in safety systems. In particular, the

IEEE Std. 1012-2004 method, if correctly applied, will assure compliance with GDC 1 in Appendix A to 10 CFR Part 50 and the criteria for QA programs in Appendix B, as they apply to software V&V. IEEE Std. 1028-2008 provides guidance acceptable to the NRC staff for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. RG 1.152, Revision 3, and RG 1.168, Revision 2, are used to review processes and activities associated with software V&V and software reviews.

The application addresses the V&V process in DCA Part 2, Tier 2, Sections 7.2.1.4.4 and 7.2.1, which provide details of V&V and review process and methods for DI&C systems and components. The NRC staff finds the QA process approach acceptable because it conforms to RG 1.152, Revision 3, and RG 1.168, Revision 2.

7.2.1.4.5 Software Configuration Management Processes

RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, subject to the exceptions and clarifications identified in the regulatory guide. IEEE Std. 7-4.3.2-2003, Section 5.3.5, provides guidance on software configuration management. RG 1.169, Revision 1, endorses IEEE Std. 828-2005, subject to the exceptions and clarifications identified in the regulatory guide. IEEE Std. 828-2005 describes methods acceptable to the NRC staff for use in complying with the NRC's regulations for quality standards, which promote high functional reliability and design quality in software used in safety systems. RG 1.169, Revision 1, provides an acceptable way of complying with GDC 1 in Appendix A to 10 CFR Part 50 and the criteria for QA programs in Appendix B to 10 CFR Part 50 as they apply to the maintenance and control of appropriate records of software development activities. RG 1.152, Revision 3, and RG 1.169, Revision 1, are used to evaluate processes and activities associated with software configuration management processes.

The application addresses software configuration management process in DCA Part 2, Tier 2, Section 7.2.1.4.5 and Section 7.2.1, which provide details of configuration management plans for computer software used in safety systems. The NRC staff finds this software configuration management process approach acceptable because it conforms to RG 1.152, Revision 3, and RG 1.169, Revision 1.

7.2.1.5 COL Information Items

DCA Part 2, Tier 2, Section 7.2.1, contains the following three COL information items pertaining to quality. The acceptability of the COL information items is evaluated in Section 7.2.1.4.1 of this report. The NRC staff concluded that no additional COL information items were needed.

Table 7.2-1: NuScale COL Information Items for Section 7.2.1

Item No.	Description	DCA Part 2, Tier 2 Section
COL Item 7.2-1:	A COL applicant that references the NuScale power plant design certification is responsible for the implementation of the life-cycle processes for the operation phase of the I&C systems, as defined in IEEE Std. 1074-2006 and IEEE Std. 1012-2004.	7.2.1.2.10, "Instrumentation and Controls System Operations"
COL Item 7.2-2:	A COL applicant that references the NuScale power plant design certification is responsible for the implementation of the life-cycle processes for the maintenance phase of the I&C systems, as defined in IEEE Std. 1074-2006 and IEEE Std. 1012-2004.	7.2.1.2.11, "Instrumentation System Maintenance"

COL Item 7.2-3:	The NuScale Digital I&C Software Configuration Management Plan provides guidance for the retirement and removal of a software product from use. A COL applicant that references the NuScale power plant design certification is responsible for the implementation of the life-cycle processes for the retirement phase of the I&C systems, as defined in IEEE Std. 1074-2006 and IEEE Std. 1012-2004. The NuScale Digital I&C Software Configuration Management Plan provides guidance for the retirement and removal of a software product from use.	7.2.1.2.12, "Instrumentation System Retirement"

7.2.1.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed I&C system design conforms to the guidance in RG 1.28, Revision 4; RG 1.152, Revision 3; RG 1.168, Revision 2; RG 1.169, Revision 1; RG 1.170, Revision 1; RG 1.171, Revision 1; and RG 1.172, Revision 1. The NRC staff reviewed the application against ASAIs 4, 16, 17, 47, 49, 50, and 51, which relate to quality listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets the quality aspects of ASAIs 4, 16, 17, 47, 49, 50, and 51 listed in TR-1015-18653, Revision 2. On this basis, the NRC staff concludes that the application provides information sufficient to demonstrate that the QA measures applied to the proposed I&C system and software life cycle satisfy the applicable QA requirements of GDC 1 of Appendix A to 10 CFR Part 50; Appendix B to 10 CFR Part 50; and Section 5.3 of IEEE Std. 603-1991.

7.2.2 Equipment Qualification

7.2.2.1 Introduction

This Section addresses the review of I&C safety system equipment design to confirm that it meets the functional performance requirements credited in the safety analysis over the range of environmental conditions postulated for the area in which it is located. The I&C safety system equipment is designed in accordance with GDC 2 and GDC 4 of Appendix A to 10 CFR Part 50. The EQ program includes (1) seismic qualification in accordance with Criterion III, "Design Control," of Appendix B to 10 CFR Part 50, (2) qualification of equipment such as sensors, cables, and certain PAM equipment located in harsh environments in accordance with 10 CFR 50.49, and (3) qualification of digital I&C equipment located in mild environments under IEEE Std. 603-1991.

The NRC staff's evaluation includes confirmation that (1) I&C equipment (including isolation devices) located in areas subject to seismic and environmental qualification requirements has been identified and design criteria established (i.e., seismic, environmental) in the application, (2) computer-based I&C system EQ criteria in Section 5.4 of IEEE Std. 603-1991 and Section 5.4 of IEEE Std. 7-4.3.2-2003 as endorsed by RG 1.152, Revision 3, have been considered, where applicable, as part of the process for the qualification of digital computers, and (3) the I&C system design includes the design and installation of safety-related instrument sensing lines and lightning protection systems.

Whether I&C equipment meets the substantive requirements for seismic and environmental qualification is evaluated as part of Chapter 3 and is not included in this Section. The evaluation of the review of seismic and environmental qualification is provided in Sections 3.10 and 3.11 of this report.

7.2.2.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5, 2.6, and 2.8, "Equipment Qualification."

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.2, "Equipment Qualification," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.2, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.2, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 17, 18, and 23, which relate to EQ, is described in Section 7.1.6 of this report.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.2, are given in DCA Part 2, Tier 1, Section 2.8, Table 2.8.2, "Equipment Qualification Inspections, Tests, Analyses, and Acceptance," Items 4 and 5. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.2.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.2.

7.2.2.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR Part 50, Appendix B, Criterion III.
- 10 CFR 50.49.
- 10 CFR Part 50, Appendix A, GDC 2.
- 10 CFR Part 50, Appendix A, GDC 4.
- 10 CFR 50.55(a)(h) requires compliance with IEEE Std. 603-1991, including the correction sheet dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(h)(2). This standard includes Section 5.4, "Equipment Qualification," which requires that safety equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods.

The guidance in DSRS Section 7.2.2 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.152, Revision 3, endorses IEEE Std. 7-4.3.2-2003, with identified exceptions and clarifications.
- RG 1.209, Revision 0, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," endorses IEEE Std. 323-2003, "IEEE Standards for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," with identified exceptions and clarifications.

- RG 1.151, Revision 1, “Instrument Sensing Lines,” endorses American National Standards Institute (ANSI)/ISA-67.02.01-1999, “Instrument-Sensing Line Piping and Tubing Standard for Use in Nuclear Power Plants,” with identified exceptions and clarifications.

- RG 1.180, Revision 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.”

- RG 1.204, Revision 0, “Guidelines for Lightning Protection of Nuclear Power Plants.”

7.2.2.4 Technical Evaluation

The staff reviewed DCA Part 2, Tier 2, Section 7.2.2, and the referenced HIPS platform TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff’s review confirmed that the information in the application and the information incorporated by reference address the required information relating to EQ. The following describes the NRC staff’s evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.2.4 and to address aspects of ASAIs 17, 18, and 23 that relate to EQ. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff’s evaluation of the information provided by the applicant against the regulations in SE Section 7.2.2.3 and ASAIs cited above.

7.2.2.4.1 Equipment Qualification

In DCA Part 2, Tier 2, Sections 3.10 and 3.11, Tables 3.2-1, “Classification of Structures, Systems, and Components,” and 3.11-1, “List of Environmentally Qualified Electrical/I&C and Mechanical Equipment Located in Harsh Environments,” describe the seismic and environmental qualification programs and list the equipment that will be subject to classification/qualification. The MPS and NMS-excore rack-mounted equipment and the processing electronics portion of the NMS-excore detectors are located in equipment rooms in the reactor building, which is classified as seismic Category I and is designated as a mild environment. DCA Part 2, Tier 2, Section 7.2.2.1 states that the MPS and NMS-excore equipment rooms provide an environment that would at no time be more severe than the environment that would occur during normal plant operation, including AOOs. The NMS-excore detectors are located in support mechanisms submerged in the reactor pool next to the reactor module, which is a harsh environment.

DCA Part 2, Tier 2, Section 7.2.2.1 states, in part, that the MPS and NMS-excore components are environmentally qualified in accordance with IEEE Std. 323-2003 as endorsed by RG 1.209 for mild environments and in accordance with IEEE Std. 323-1974 as endorsed by RG 1.89, Revision 1, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” for harsh environments. RG 1.89 focuses on the environmental qualification of equipment intended for use in harsh environments, while RG 1.209 applies to safety-related computer-based I&C systems intended for implementation in mild environments. The EQ program (both seismic and environmental) is evaluated in Sections 3.10 and 3.11 of this report.

DCA Part 2, Tier 2, Section 7.2.2, states that the safety I&C systems and components are designed to perform their safety-related functional requirements over the range of environmental conditions postulated for the area in which the components are located and during the time period when this performance is required. The NRC staff reviewed DCA Part 2, Tier 2, Tables 3.2-1 and 3.11-1, and confirmed that the I&C equipment (including isolation devices)

subject to seismic and environmental qualification requirements has been identified and design criteria established.

DCA Part 2, Tier 2, Section 7.2.2.1, states, in part, that the MPS is an FPGA-based system, which does not use software in a traditional manner; however, FPGAs are programmed, and qualification testing is performed, in accordance with IEEE Std. 7-4.3.2-2003. The NMS-excore contains sensors and analog signal processing equipment and is not a digital computer system; therefore, the commitments of IEEE Std. 7-4.3.2-2003 do not apply. The NRC staff confirmed that computer-based I&C system EQ criteria in Section 5.4 of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3, have been considered, where applicable, as part of the process for the qualification of digital computers.

DCA Part 2, Tier 2, Section 7.2.2.1 states that the MPS equipment and cable routing are designed to meet the separation requirements of IEEE Std. 384-1992 as endorsed by RG 1.75, Revision 3. Other fire and smoke exposure protection methods utilized for the MPS and NMS-excore equipment are separate rooms and cable runs, isolation and detection practices, minimization of combustible materials in the MPS rooms and cabinets, and absence of forced cooling of internal MPS or NMS-excore hardware equipment. The NRC staff confirmed that smoke tolerance and fire protection criteria contained in RG 1.209, Revision 0, have been considered, where applicable, as part of the safety system qualification. The evaluation of the fire protection design guidelines is part of Chapter 9 of the DSRS and is evaluated in Section 9.5 of this report.

7.2.2.4.2 Instrument Sensing Lines

The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.2.1, “Instrumentation and Controls Qualification,” and TR-0316-22048, Chapter 5, “Pressure Measurement in the NPM,” to identify how instrument sensing lines design and installation are addressed in the application.

DCA Part 2, Tier 2, Section 7.2.2.1, states that the instrument sensing lines are designed in accordance with ANSI/ISA-67.02.01-1999, “Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants,” as endorsed by RG 1.151, Revision 1. This standard establishes acceptance criteria for the design and installation of safety-related instrument sensing lines that provide connections to the reactor coolant system for measuring process variables (e.g., pressure, level, and flow). The NuScale I&C system sensors that utilize instrument sensing lines are pressurizer pressure narrow range, reactor coolant system pressure wide range, main steam pressure, feedwater outlet pressure, and DHRS outlet pressure. The applicant states that the instrument sensing lines are designed to conform to the guidance in ANSI/ISA-67.02.01-1999, as endorsed by RG 1.151, Revision 1.

7.2.2.4.3 Environmental Control Systems

DCA Part 2, Tier 2, Section 7.2.2.1 states that the MPS and NMS rack-mounted equipment do not require environmental controls to perform their safety functions.

7.2.2.4.4 Electromagnetic and Radiofrequency Interference

The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.2.1, “Instrumentation and Controls Qualification,” to identify how MPS and NMS equipment electromagnetic interference (EMI) and radiofrequency interference (RFI) qualifications are addressed in the application.

DCA Part 2, Tier 2, Section 7.2.2.1, states that the MPS and NMS-excore equipment is designed and qualified in accordance with the guidance in RG 1.180, Revision 1, for compliance with NRC regulations regarding EMI and RFI and power surges on safety-related I&C systems.

The NRC staff confirmed that EMI qualification is performed in accordance with the guidance in RG 1.180, Revision 1.

DCA Part 2, Tier 2, Section 7.2.2.1, states that for conformance to RG 1.204, NuScale applies the guidance for EMI/RFI protection from IEEE Std. 1050-1996, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations," to the design of the I&C systems. The MPS and NMS-excore equipment is designed with a single point ground system, with the cabinet safety grounds being separate from the instrument ground to the ground mat. Based on the applicant's commitment to conform to RG 1.204, the NRC staff finds that the design of the I&C systems addresses EMI/RFI testing to assure that safety systems are not adversely impacted by EMI/RFI effects.

7.2.2.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.2.6 Conclusions

The NRC staff concludes that the application (1) identified I&C equipment (including isolation devices) subject to seismic and environmental qualification requirements, (2) demonstrated the seismic and environmental qualification of I&C equipment, (3) demonstrated that specific qualification testing criteria for computer systems recommended by the NRC have been considered as part of environmental qualification, and (4) demonstrated the adequacy of the design of safety-related instrument sensing lines and environmental control systems. The staff reviewed the application against ASAIs 17, 18, and 23 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets the ASAIs. Therefore, the NRC staff finds that the design of I&C systems conforms to the EQ guidance in Section 5.4 of IEEE Std. 7-4.3.2-2003 and the guidance in RG 1.151, Revision 1; RG 1.180, Revision 1; RG 1.204, Revision 0; and RG 1.209, Revision 0. The design therefore meets the requirements of 10 CFR Part 50, Appendix B, Criterion III; 10 CFR 50.49; 10 CFR Part 50, Appendix A, GDC 2 and 4; and Section 5.4 of IEEE Std. 603-1991.

7.2.3 Reliability, Integrity, and Completion of Protective Action

7.2.3.1 Introduction

This Section addresses the review of the reliability and integrity of I&C components and systems and their ability to complete protective action once initiated to confirm that I&C components and systems are sufficiently reliable to accomplish their safety functions.

The NRC staff considers an I&C component or system adequately reliable if there is a high probability that a component or system will be available when needed and remain capable of performing the functions it was designed to achieve. The staff considers an I&C component or system to have adequate integrity if it has the capability to perform all of its intended functions with the accuracy and resulting outputs credited in the safety analyses. The staff considers a safety system to have completed protective action if, upon manual or automatic initiation, the system performs the entire sequence of protective actions or all execute features provided in the design that are necessary to achieve the result credited in the safety analyses.

7.2.3.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.2, "Reliability, Integrity, and Completion of Protective Action," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.3.1, "Reliability Characteristics," describes the reliability characteristics of the MPS and NMS.

DCA Part 2, Tier 2, Section 7.2.3.2, "System Integrity Characteristics," describes the integrity attributes of the MPS and NMS.

DCA Part 2, Tier 2, Section 7.2.3.3, "Completion of Proactive Action," describes the ability of the MPS to complete a protective action once initiated to accomplish the safety functions.

DCA Part 2, Tier 2, Section 7.2.3, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.3, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 15, 18, 19, and 37, which relate to reliability, integrity, and completion of protective action, is described in Section 7.1.6 of this report.

In TR-1015-18653, Sections 7.0, "Repeatability and Predictability," and 8.0, "Calibration, Testing and Diagnostics," describe the HIPS platform integrity characteristics and design features to meet the completion of protective action requirements of IEEE Std. 603-1991, Section 5.5.

TR-1015-18653, Section 2.5.4, "Equipment Interface Module," describes the HIPS platform design features for implementing coincidence logic and the platform response time characteristics to meet the integrity requirements of IEEE Std. 603-1991, Sections 5.2 and 7.3.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.3, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 16. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.3.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.3.

7.2.3.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes three Sections that are covered as part of this review: Section 5.15, "Reliability;" Section 5.5, "System Integrity;" and Section 5.2 and 7.3, "Completion of Protective Action." Section 5.15 of IEEE 603-1991 requires that, for those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed to confirm that such goals have been achieved. Section 5.5 states that safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Sections 5.2 and 7.3 require that safety systems and execute features be designed such that, once initiated, the intended sequence of protective actions shall continue to completion.

The guidance in DSRS Section 7.2.3 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- Digital I&C safety systems should conform to the reliability, integrity, and completion of protective action guidance in Sections 5.2, 5.5, and 5.15 of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3.

In addition, the fundamental design principles described in DSRS Section 7.1 as well as the appendices to Chapter 7 of the DSRS, inform the review of reliability, integrity, and completion of protective actions of the I&C systems.

7.2.3.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed DCA Part 2, Tier 2, Section 7.2.3, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA, appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to reliability, integrity, and completion of protective action. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.3.3 and to address the aspects of ASAIs 15, 18, 19, and 37 that relate to reliability, integrity, and completion of protective action. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.2.3.3 and ASAIs cited above.

7.2.3.4.1 Reliability Characteristics

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAI 37.

IEEE 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3, states that when reliability goals are identified, the proof of meeting the goals shall include the software. DCA Part 2, Tier 2, Section 7.2.3.1, states, in part, the following:

> *Qualitative reliability goals have been established for the MPS to meet the single failure criterion. The MPS meets the qualitative reliability goals and the requirements of IEEE Std. 379-2000 "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems" (Reference 7.2-9) to satisfy the single failure criterion through the addition of redundancy (see Section 7.1.3), diversity (see Section 7.1.5) and testability (see Section 7.2.15).*

The NRC staff reviewed the applicant's reliability analysis and I&C design documentation to verify that the qualitative reliability goal has been achieved. The NRC staff examined the FMEAs for the MPS and the NMS against the criteria in IEEE Std. 379-2000, as endorsed by RG 1.53, Revision 2, and IEEE Std. 352-1987. This evaluation of the FMEAs is described in Section 7.1.3 of this report. The NRC staff confirmed that the MPS's FMEA demonstrates the

ability of the MPS to function in the presence of a single failure within the scope of IEEE Std. 603-1991, Section 5.1.

The NRC staff examined ER-E000-4937, Revision 0, "Module Protection System Digital-Based Common Cause Failure Coping Analysis," which contains information on potential CCFs of digital sensors and the results of spurious actuations that could occur in the MPS, and ER-E000-4335, Revision 0, "Analysis of Common-Cause Failure in Process Control Systems," which analyzed worst-case effects of digital-based CCF in the MCS and PCS to assure that the effects do not exceed the design basis. Digital-based CCFs and the D3 assessment are evaluated in Section 7.1.5 of this report. Specifically, Section 7.1.5.4.2 of this report evaluates the technical basis as to why an MHS malfunction event, in combination with a digital-based CCF of the RCS flow, is not credible.

DCA Part 2, Tier 2, Section 7.2.3.1, also states, in part, the following:

> *An MPS hazard analysis was also performed using the methodology described in Section 7.1.8 to evaluate potential hazards from connected systems and establish safety constraints to meet the qualitative reliability goals established for the system. No failure modes of the MPS were identified in the FMEA or hazard analysis that were undetectable or prevented the MPS from performing its RTS, ESFAS and post-accident monitoring (PAM) functions.*

It further states the following:

> *The NMS hazard analysis (see Section 7.1.8) was also performed to evaluate potential hazards from connected systems and establish safety constraints to meet the qualitative reliability goals established for the system. Failures resulting in a loss of neutron flux information can be identified through anomalous indication, alarms in the MCR, or periodic testing. No failure modes of the NMS were identified in the FMEA or hazard analysis that were undetectable or prevented the NMS from performing required functions.*

The NRC staff examined ER-E011-2477, Revision 1, "Module Protection System Hazard Analysis," and ER-E013-3847, Revision 0, "Neutron Monitoring System Hazard Analysis." The NRC staff finds that the method of addressing hazards based on the design and safety constraints is acceptable.

Based on the above and the NRC staff's evaluation in Section 7.2.3.4.2 of this report, and the staff's evaluation of redundancy and the single-failure criterion in Section 7.1.3 of this report, the staff finds that the I&C systems are capable of functioning in all plant conditions including normal operation, abnormal, and accident conditions. The NRC staff has verified that the I&C systems have been conservatively designed with adequate reliability such that the effects of possible hardware and software failures, including the software and firmware, have been addressed and any design features provided to prevent or limit the effects of these failures will assure that the I&C systems are still capable of performing their safety functions.

Based on the above review, the NRC staff finds that ASAI 37 is met, as described in Section 7.1.6 of this report. Therefore, the NRC staff concludes that the I&C systems comply with the reliability requirements in Section 5.15 of IEEE Std. 603-1991, and the guidance contained in Section 5.15 of IEEE Std. 7-4.3.2-2003.

7.2.3.4.2 System Integrity Characteristics

The NRC staff's evaluation of this Section concludes that the application-specific information requirements for ASAIs 18 and 19, which relate to system integrity, are satisfied.

Range of Service Conditions

DCA Part 2, Tier 2, Section 7.2.2, states that the equipment is environmentally and seismically qualified in accordance with RG 1.209, Revision 0, and IEEE Std. 323-1974. The NRC staff's evaluation of the I&C EQ requirements is in Section 7.2.2 of this report.

DCA Part 2, Tier 2, Section 7.1.1.2.1, states the following:

> *The MPS and NMS are designed to operate during normal, abnormal, AOO, IE, and accident conditions for a minimum of 72 hours during a loss of alternating current (AC) power. The MPS operates in PAM-Only mode after a loss of AC power for 24 hours. These systems are designed to function during a loss of heating ventilation and air conditioning (HVAC). Protection from natural phenomena is provided by the location of the MPS and NMS cabinets in the Reactor Building, which is a Seismic Category I, reinforced concrete structure. Separation Groups A and C and Division I equipment, and Separation Groups B and D and Division II equipment are in different rooms in the Reactor Building, protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit.*
>
> *The MPS and NMS rack-mounted equipment is installed in a mild environment. The MPS rooms provide an environment that would at no time be more severe than the environment that would occur during normal plant operation, including AOOs. The environmental qualification requirements for the MPS and NMS rack mounted equipment are identified in Section 3.11.*

DCA Part 2, Tier 2, Table 3.11-1, indicates that the MPS equipment located in a harsh environment is only the four separation groups under-the-bioshield temperature sensors and the main control isolation switches, which need not function in that environment, but need only to not fail such that they spuriously execute their function. DCA Part 2, Tier 2, Figure 7.0-2, and DCA Part 2, Tier 2, Section 7.0.4.1, include the under-the-bioshield temperature sensors as part of the MPS boundary.

DCA Part 2, Tier 2, Table 3.11-1, indicates that the NMS equipment located in a harsh environment is the safety-related excore neutron detectors and the NMS flood highly sensitive neutron detectors. Their location, EQ environment, EQ program, PAM variable types, and required operating time are evaluated in Sections 3.11, 7.0.4, 7.2.2, and 7.2.13 of this report. The NRC staff examined the HA for the MPS and confirmed that the applicant identified hazards that could be introduced in the software development process and described the integration of software safety and HA.

As evaluated in Section 7.2.1 of this report, the software safety analysis activities cover the range of service conditions established by the design basis. Thus, the NRC staff concludes that computer system software integrity is demonstrated by the application's software safety analysis activities over the range of service conditions established in the I&C system's design bases.

The NRC staff has confirmed that the safety system components are conservatively designed to operate over the range of service conditions established in the I&C system's design bases. Based on the above, the NRC staff finds that the NuScale I&C design meets ASAI 18, as described in Section 7.1.6 of this report.

Real-Time Performance

The NRC staff's evaluation of the HIPS TR-1015-18653 found that the HIPS platform demonstrates calculated response time characteristics and supports the definition and demonstration of maximum and minimum response time performance to meet safety system performance and determinism requirements. The evaluation concluded that the HIPS platform's response time and determinism support meeting the criteria of Section 5.5 of IEEE Std. 603-1991 at the platform level and are suitable for support safety applications. DCA Part 2, Tier 2, Section 7.1.4, designates a 1-second timing budget for the digital portion of the MPS. DCA Part 2, Tier 2, Table 7.1-6, shows how that time limit fits into NuScale's analysis of DBEs. The detailed evaluation of the response time of the MPS is in Section 7.1.4 of this report. Thus, the NRC staff finds that the application provides information sufficient to confirm that digital computer-based I&C systems' real-time performance is adequate to assure completion of protective actions within the critical points in time identified in Section 4.10 of IEEE Std. 603-1991 and concludes that the design meets ASAI 19, as described in Section 7.1.6 of this report.

Fail-Safe State

The NRC staff's SE for TR-1015-18653 (ADAMS Accession No. ML17116A097) found that when a fault is detected, the specific response to particular failures depends on the application-specific system design. It is, therefore, reviewed here.

DCA Part 2, Tier 2, Section 7.2.3.2, states the following:

> *The MPS is designed such that in the event of a condition such as a system disconnection or loss of power, it fails into a safe state. The equipment interface module (EIM) outputs are designed to remove power to the final actuation devices causing them to go to a safe-state (e.g., RTBs open, ECCS valves open). This ensures that a loss of power or other detected fault that causes the EIM to go into a faulted state also causes the interface to remove power to the final actuated device.*

It further states the following:

> *Failure of NMS-excore components generate a fault signal and an actuate/trip signal for that particular NMS-excore channel. The fault signal is transmitted to the MPS for display to the control room operators.*

DCA Part 2, Tier 2, Section 7.0.4, provides information on configuration of the slave modules to alarm and assume a fail-safe state, as shown in Table 7.1-1 of this report. The NRC staff finds that the slave modules (e.g., SFMs and EIMs) are configured to provide an alarm in the MCR and assume a fail-safe state.

DCA Part 2, Tier 2, Section 7.2.15, provides further information on I&C testing and fault detection, which is evaluated in Section 7.2.15 of this report. Therefore, the NRC staff finds that the application provides information sufficient to confirm that, upon detection of inoperable input instruments, provisions are included to automatically place the protective functions associated with the failed instrument(s) into a safe state.

As documented in evaluation of the HIPS TR-1015-18653, the NRC staff found the provisions for the HIPS platform, which provides self-diagnostics and test failure reporting during system startup, to be acceptable. Periodic self-diagnostics and self-diagnostic test failure reporting, fault detection, test and calibration are described in DCA Part 2, Tier 2, Section 7.2.15, and evaluated in Section 7.2.15 of this report. Noninterference of these features with the safety

function of the system is evaluated in Section 7.2.8 of this report. The APL logic in the EIMs assure that a failure of the computer does not preclude the safety system from being placed into its preferred fail-safe mode. Thus, the NRC staff concludes that the application provides information sufficient to confirm that the computer integrity, test and calibration, fault detection, and self-diagnostics described in the application comply with the guidance in Section 5.5 of IEEE Std. 7-4.3.2-2003.

Based on the above, the NRC staff concludes that the application provides information sufficient to confirm that the I&C design incorporates protective measures that provide for the I&C safety systems to fail into a safe state in compliance with 10 CFR Part 50, Appendix A, GDC 23.

Secure Development and Operational Environment

DCA Part 2, Tier 2, Section 7.2.2.1, states the following:

> *The MPS is an FPGA-based system, which does not use software in a traditional manner; therefore, there is no software which executes while the system is in operation. However, FPGAs are programmed, and qualification testing is performed in accordance with IEEE Std. 7-4.3.2-2003 (see Section 7.2.1).*
>
> *The NMS-excore contains sensors and analog signal processing equipment and is not a digital computer system; therefore, the requirements of IEEE Std. 7-4.3.2-2003 do not apply.*

Software quality and its secure development and operational environment are evaluated in Sections 7.2.1 and 7.2.9.4.1 of this report.

Conclusion

Based on the above, the NRC staff concludes that ASAIs 18 and 19 are met, as described in Section 7.1.6 of this report. Therefore, the staff finds that the I&C systems satisfy the system integrity requirements in Section 5.5 of IEEE Std. 603-1991 and the guidance contained in Section 5.5 of IEEE Std. 7-4.3.2-2003.

7.2.3.4.3 Completion of Protective Action

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAI 15.

During the review for the completion of protective actions requirement for safety systems, the NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.3.3, and Figures 7.1-1b through 7.1-1ao.

DCA Part 2, Tier 2, Section 7.1.6, states the following:

> *Containment isolation is initiated by two diverse signals from the MPS that ensure the isolation valves do not re-open upon logic reset, as shown in Table 7.1-4 and Section 7.1.5.*

The NRC staff reviewed the functional and logic diagrams to verify that "seal-in" features are provided in the design to enable system-level protective actions to go to completion to the extent that position feedback is used as a discrete input that seals in the logic until such time as the component has actuated (valve closed/opened, breaker tripped).

DCA Part 2, Tier 2, Section 7.2.3.3 and Figure 7.1-1 indicates that the enable non-safety control switch has momentary contacts, which upon actuation return to center switch position. Based

on the design information provided, it can be seen that the operator must actuate the momentary contact non-safety-related control switch to reconfigure actuated equipment, and that this is only possible after the actuation has completed and the initiating signal is either not present or is overridden by deliberate operator intervention as allowed in Sections 7.3 and 5.2 of IEEE Std. 603-1991.

Conclusion

Based on the above, the NRC staff has determined that the I&C systems satisfy the completion of protective actions requirements in Sections 5.2 and 7.3 of IEEE Std. 603-1991 and the guidance in Sections 5.2 and 7.3 of IEEE Std. 7-4.3.2-2003, and ASAI 15 is satisfied, as described in Section 7.1.6 of this report.

7.2.3.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.3.6 Conclusions

The NRC staff concludes that the application provides information sufficient to (1) demonstrate that I&C components and systems will be reliable and available when needed and remain capable of performing the functions they are designed to achieve, (2) demonstrate that I&C components and systems will have adequate integrity to perform all of their intended functions with the accuracy and resulting outputs credited in the safety analyses, and (3) I&C safety systems will perform the entire sequence of protective actions or all execute features that are necessary to achieve the results credited in the safety analyses. The NRC staff reviewed the application against ASAIs 15, 18, 19, and 37 listed in TR-1015-18653, Revision 2.

Based on the above discussion, the NRC staff finds that the design of I&C systems satisfies the reliability, system integrity, and completion of protective action guidance in Sections 5.2, 5.5, and 5.15 of IEEE Std. 7-4.3.2-2003; the requirements of Sections 5.2, 5.5, 5.15, and 7.3 of IEEE Std. 603-1991, and that the NuScale I&C design meets the ASAIs.

7.2.4 Operating and Maintenance Bypasses

7.2.4.1 Introduction

This Section addresses the review of the I&C system's proposed operating bypasses that should be designed to automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s) whenever the applicable permissive conditions are not met. In addition, the review will evaluate the I&C system's proposed maintenance bypasses that provide the capability for a safety system to accomplish its safety function while sense and command and execute features equipment is in maintenance bypass. A bypass is a device that deliberately but temporarily inhibits the functioning of a circuit or system. An operational bypass is the bypass of certain protective actions when they are not necessary in a particular mode of plant operation. A maintenance bypass is a bypass of safety system equipment during maintenance, testing, or repair. A permissive is a set of conditions that must be satisfied before a decision is made or an action is taken.

The NRC staff's evaluation considered the provisions for these bypasses to be consistent with the required actions of the proposed plant technical specifications.

7.2.4.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.4, "Operating and Maintenance Bypasses," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.4, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.4, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 7, 42, 43, and 45, which relate to operating and maintenance bypasses, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 2.5.2, "Bypass or Trip Operation," describes the HIPS platform design concepts that address the signal processing and bypass features to meet the maintenance bypass requirements of IEEE Std. 603-1991, Sections 6.7 and 7.5.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.4, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 19 through 23. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: The technical specifications associated with DCA Part 2, Tier 2, Section 7.2.4, are given in DCA Part 2, Tier 2, Chapter 16, "Technical Specifications." Specifically, the following Sections address operating and maintenance bypasses: Technical Specifications, Section 3.3.1, "MODULE Protection System (MPS) Instrumentation;" Section 3.3.2, "Reactor Trip System (RTS) Logic and Actuation;" Section 3.3.3, "Engineered Safety Features Actuation System (ESFAS) Logic and Actuation;" Section B.3.3.1, "MODULE Protection System (MPS) Instrumentation;" Section B.3.3.2, "Reactor Trip System (RTS) Logic and Actuation;" and Section B.3.3.3, "Engineered Safety Features Actuation System (ESFAS) Logic and Actuation."

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.3.

7.2.4.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Sections 6.6 and 7.4, "Operating Bypasses," and Sections 6.7 and 7.5, "Maintenance Bypass." Sections 6.6 and 6.7 provide requirements for operating and maintenance bypasses applicable to sense and command features. Sections 7.4 and 7.5 provide requirements for operating and maintenance bypasses applicable to execute features.

- 10 CFR 50.34(f)(2)(v), "Additional Three Mile Island (TMI)-Related Requirements," requires automatic indication of the bypassed and operable status of safety systems.

The guidance in DSRS Section 7.2.4 lists the acceptance criteria adequate to meet the above requirements. In addition, the following guidance document provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.47, Revision 1.

7.2.4.4 Technical Evaluation

The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.4, and the incorporated by reference HIPS TR-1015-18653 to assure that the combination of the information appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that this combined information addresses the required design information relating to operating and maintenance bypasses. The following describes the NRC staff's evaluation of the information provided in the application to meet the regulations stated in Section 7.2.4.3 of this report and to address aspects of ASAIs 7, 42, 43, and 45 that relate to operating and maintenance bypasses. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

7.2.4.4.1 Operating Bypasses

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAI 42. The review focused on evaluating the provisions included in the I&C system design addressing operating bypasses.

DCA Part 2, Tier 2, Section 7.2.4.1, states that the MPS includes interlocks, permissive, and operational and maintenance bypasses that prohibit or permit certain protective actions either automatically or through a combination of automatic and manual actions to allow plant mode changes. In DCA Part 2, Tier 2, Section 7.2.4.1, and Table 7.1-5 describe that when permissive and interlock conditions are met and a protective function is not required, the MPS logic automatically bypasses the function. When permissive and interlock conditions are not met, the MPS logic automatically prevents the activation of the bypass or initiates the appropriate safety function. Further, DCA Part 2, Tier 2, Section 7.2.4.1, and Table 7.1-5, describe that when plant conditions change such that an active operating bypass is no longer permissible, operating bypasses are automatically deactivated with operator control of only certain functions, as required in IEEE Std. 603-1991, Sections 6.6 and 7.4. DCA Part 2, Tier 2, Section 7.2.4, states that the MPS operating and maintenance bypasses comply with Sections 6.6, 6.7, 7.4, and 7.5 of IEEE Std. 603-1991. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.4.1, Table 7.1-5, and TR-1015-18653, and confirmed that operating bypasses are designed to comply with Sections 6.6 and 7.4 of IEEE Std. 603-1991. The evaluation of Sections 6.6 and 7.4 for operating bypasses is also part of TR-1015-18653 and is also evaluated in Sections 3.6.3.6 and 3.6.4.4 of the NRC staff's SE of TR-1015-18653 (ADAMS Accession No. ML17116A097).

DCA Part 2, Tier 2, Section 7.2.4, states, in part, that the MPS operating and maintenance bypasses conform to the guidance in RG 1.47, Revision 1. DCA Part 2, Tier 2, Section 7.2.4.1, describes that if some part of the system has been bypassed or taken out of service, indication will be provided in the control room. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.4.1, and Table 7.1-5, and confirmed that features for bypassed and inoperable status indication conform to the guidance in RG 1.47, Revision 1. The evaluation of display system bypass status is part of Chapter 7 of the DSRS and is evaluated in Section 7.2.13 of this report.

DCA Part 2, Tier 2, Section 7.2.4.1, states that the manual operational bypasses have two switches, one per division. Failures of the operational bypass switches are limited to one of two MPS divisions, with no single failure capable of disabling a safety function. A trip determination is used for the permissive or interlock from the separation group with a three-out-of-four coincidence to determine when an operating bypass is warranted, and a two-out-of-four coincidence to remove the operating bypass.

7.2.4.4.2 Maintenance Bypass

The NRC staff's evaluation in this Section addresses the application-specific information requirements for ASAIs 7, 43, and 45. The review focused on evaluating how the provisions included in the I&C system design address maintenance bypasses.

DCA Part 2, Tier 2, Section 7.2.4.2, states that MPS variables are monitored by four redundant channels, which actuate the protective functions utilizing two-out-of-four coincident logic. In DCA Part 2, Tier 2, Section 7.2.4.2, Table 7.1-5 describes that there is a trip/bypass switch and an out-of-service switch that allow the removal of the SFM from service for maintenance and repair. With the out-of-service switch activated, the safety function is placed in trip or bypass, based on the position of the trip/bypass switch for that SFM. If the SFM is out of service and the trip/bypass switch is in bypass, the channel provides a no trip to the SVM, requiring two of the remaining three channels received by the SVM to vote to trip/actuate for the particular safety function. If the SFM is out of service and the trip/bypass switch is in trip/actuate, the channel provides a trip/actuate signal to the SVM, requiring one of the remaining three channels received by the SVM to vote to trip/actuate for the particular safety function. For both cases, DCA Part 2, Tier 2, Section 7.2.4.2, states that the MPS is still capable of performing the safety function with the required level of redundancy and continues to meet single-failure criteria. Additionally, DCA Part 2, Tier 2, Section 7.2.4, states that the MPS operating and maintenance bypasses comply with Sections 6.6, 6.7, 7.4, and 7.5 of IEEE Std. 603-1991. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.4.2, Table 7.1-5, and TR-1015-18653 and confirmed that maintenance bypasses are designed to comply with Sections 6.7 and 7.5 of IEEE Std. 603-1991. The evaluation of Sections 6.7 and 7.5 for operating bypass is also part of TR-1015-18653 and is evaluated in Sections 3.6.3.7 and 3.6.4.5 of the NRC staff's SE of TR-1015-18653 (ADAMS Accession No. ML17116A097).

DCA Part 2, Tier 2, Section 7.2.4.2, describes that, for periodic and corrective maintenance on the MPS, the safety function must be removed from service. The affected channel is placed in a trip condition or bypass subject to technical specification limitations. Furthermore, DCA Part 2, Tier 2, Section 7.2.4.2, states that the time period allowed for removal from service in maintenance bypass is administratively controlled by the technical specifications. The NRC staff reviewed the maintenance bypasses for RTS, ESFAS, MPS, and NMS, described in DCA Part 2, Tier 2, Section 7.2.4.2, Table 7.1-5, and found that the provisions for maintenance bypass are consistent with the technical specification action statements.

DCA Part 2, Tier 2, Section 7.2.4.2, states that the MPS conforms to the guidance in RG 1.47, Revision 1. The MCS and SDIS will provide the operator with continuous control room indication of MPS channel administrative bypass, trip, and out-of-service status. The operator can identify the operability of the safety function through the display of the status information. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.4.2, and Table 7.1-5, and confirmed that features for bypassed and inoperable status indication conform to the guidance in RG 1.47, Revision 1. The evaluation of display system bypass status is part of Chapter 7 of the DSRS and is evaluated in Section 7.2.13 of this report.

7.2.4.4.3 Technical Specifications

DCA Part 2, Tier 2, Section 7.4.2.2, states that the provisions for operating and maintenance bypasses are consistent with the required actions of the proposed plant technical specifications. The NRC staff's evaluation for the technical specifications is described in Chapter 16 of this report.

7.2.4.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.4.6 Conclusions

The NRC staff concludes that the application provides information sufficient to (1) demonstrate that the design of operating and maintenance bypasses assures the initiation of the appropriate safety function(s) under the conditions described above, (2) demonstrate that the proposed operating and maintenance bypasses are consistent with the required actions of the proposed plant technical specifications, and (3) demonstrate that adequate indication for bypassed status is provided in the control room. The NRC staff reviewed the application against ASAIs 7, 42, 43, and 45 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the I&C design meets the ASAIs. Therefore, the NRC staff concludes that the design of I&C systems conforms to the bypassed and inoperable status indication guidance in RG 1.47, Revision 1, and satisfies the requirements of Sections 6.6, 6.7, 7.4, and 7.5 of IEEE Std. 603-1991 and 10 CFR 50.34(f)(2)(v).

7.2.5 Interlocks

7.2.5.1 Introduction

This Section addresses the review of the acceptability of interlocks that (1) operate to reduce the probability of occurrence of specific events, (2) maintain variables within the ranges of values specified in the safety analyses, (3) assure proper system alignment during plant operation, or (4) maintain safety systems in a state that assures their availability in an accident. The scope of this review includes mechanical as well as computer-based interlocks.

The I&C evaluation assesses whether the design of interlocks is compatible with the functions and performance assumed in Chapter 15 of the application. Additionally, the evaluation confirms the adequacy of all proposed controls and instrumentation associated with mechanical interlocks.

7.2.5.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.5, “Interlocks.”

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.5, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 18. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.5.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.5.

7.2.5.3 Regulatory Basis

The following NRC regulation contains the relevant requirements for this review:

- Interlocks must satisfy the requirements of 10 CFR 50.55a(h), which requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2).

The guidance in DSRS Section 7.2.5.3 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance document provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- For computer-based interlocks, the components and system should conform to the guidance for digital computers in IEEE Std. 7-4.3.2-2003 as endorsed (with identified exceptions and clarifications) by RG 1.152, Revision 3.

7.2.5.4 Technical Evaluation

7.2.5.4.1 I&C Interlocks

DCA Part 2, Tier 1, Section 2.5, Table 2.5-1, and DCA Part 2, Tier 2, Section 7.2.5.1 and Table 7.1-5 list and describe the I&C interlocks. The IEEE Std. 603-1991 requirements for I&C interlocks are redundancy, independence, single-failure criterion, qualification, bypasses, status indication, and testing. These are evaluated in Sections 7.1.3 (redundancy and single-failure criterion), 7.1.2 (independence), 7.2.2 (qualification), 7.2.4 (bypasses), 7.2.13 (status indication), and 7.2.15 (testing) of this report. DCA Part 2, Tier 2, Section 7.2.5, states, in part, that the MPS interlocks and operating bypasses are implemented within the individual divisions, which assures that the applicable requirements of IEEE Std. 603-1991 are met. DCA Part 2, Tier 2, Section 7.2.5, states that the design of MPS interlocks complies with the requirements of IEEE Std. 603-1991. Computer-based interlocks conform to the guidance of IEEE Std. 7-4.3.2-2003. The NRC staff reviewed DCA Part 2, Tier 1, Table 2.5-1, and DCA Part 2, Tier 2, Section 7.2.5.1, and confirmed that the I&C interlocks conform to the guidance in IEEE Std. 7-4.3.2-2003.

Although the primary I&C review emphasis is on equipment comprising the interlocks, the NRC staff considered the interlock functions at the system level. In addition to evaluating interlocks against the criteria of IEEE Std. 603-1991, the staff coordinated the review of interlocks that are credited in the design-basis accident analyses with the review of Chapter 15 of this report.

7.2.5.4.2 Mechanical Systems Interlocks

DCA Part 2, Tier 2, Section 7.2.5.2, describes controls and instrumentation associated with mechanical interlocks that are described in DCA Part 2, Tier 2, Chapter 6, Section 6.3.2.2 and Figure 6.3-3.

DCA Part 2, Tier 2, Section 7.2.5.2, states that the ECCS valves contain an inadvertent actuation block feature, which minimizes the probability of a spurious opening of an ECCS valve at operating pressure. During an inadvertent signal, the ECCS valves will not open until a sufficiently low differential pressure between the RPV and the CNV is reached. During a valid signal, the completion of the ECCS protective action will occur only after the inadvertent actuation block is satisfied. DCA Part 2, Tier 2, Section 7.2.5.2, states that there are no other safety-related mechanical system interlocks. The NRC staff confirmed the adequacy of all proposed I&C associated with mechanical interlocks.

7.2.5.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.5.6 Conclusions

The NRC staff concludes that the design incorporates interlocks that (1) operate to reduce the probability of occurrence of specific events, (2) maintain variables within the ranges of values specified in the safety analyses, (3) assure proper system alignment during plant operation, or (4) maintain safety systems in a state that assures their availability in an accident. The NRC staff concludes that the design of interlocks satisfies the applicable guidance in IEEE Std. 7-4.3.2-2003, and the applicable requirements in IEEE Std. 603-1991.

7.2.6 Derivation of System Inputs

7.2.6.1 Introduction

This Section addresses the review of methods described in the application that are used for the derivation of system inputs to assure, to the extent feasible and practical, that sense and command feature inputs are derived from signals that are direct measures of the variables specified in the design basis.

The NRC staff's evaluation includes review of the DCA Part 2, Tier 2, Chapter 15, to assure that system inputs are direct measures of specified process variables in the design basis, to the extent feasible and practical.

7.2.6.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Part 2, Section 2.5.

DCA Part 2, Tier 2: DCA Tier 2 information associated with this Section is found in DCA Part 2, Tier 2, Section 7.2.6, "Derivation of System Inputs."

DCA Part 2, Tier 2, Section 7.2.6, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.6, in addition to text from the referenced TR-1015-18653. The disposition of ASAI 41, which relates to derivation of system inputs, is described in Section 7.1.6 of this report.

In TR-1015-18653, Section 2.5.1, "Safety Function Module," Section 2.5.3, "Communication Module," Section 7, "Repeatability and Predictability," and Section 8, "Calibration, Testing and Diagnostics," describe the HIPS platform design features to acquire and condition field sensor measurements of the required variables to meet the derivative of system inputs requirements of IEEE Std. 603-1991, Section 6.4.

ITAAC: There are no ITAAC directly associated with DCA Part 2, Tier 2, Section 7.2.6. However, DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 8 and 9, and Section 2.8, Table 2.8-2, Items 1, 2, and 4, are relevant to TeR-0316-22048. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.6.

Technical Reports: The technical report associated with DCA Part 2, Tier 2, Section 7.2.6, is TeR-0316-22048, Revision 0.

7.2.6.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 6.4, "Derivation of System Inputs." This requirement 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.

In addition to 10 CFR 50.55(a)(2), the following regulations apply to TeR-0316-22048:

- 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants."
- 10 CFR Part 50, Appendix A, GDC 2.
- 10 CFR Part 50, Appendix A, GDC 4.
- 10 CFR Part 50, Appendix A, GDC 13.
- 10 CFR 52.47(c)(2) states, in part, that an application for certification of a nuclear power reactor design that differs significantly from the light-water reactor designs, or uses simplified, inherent, passive, or other innovative means to accomplish its safety functions, must provide an essentially complete nuclear power reactor design and must meet the requirements of 10 CFR 50.43(e).

There are no specific DSRS acceptance criteria in this Section.

7.2.6.4 Technical Evaluation

The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.6, and the incorporated by reference HIPS TR-1015-18653 to assure that the combination appropriately represents the complete scope of information relating to this review topic. The staff's review confirmed that this combined information addresses the required design information relating to derivation of system inputs. The following describes the NRC staff's evaluation of the information provided by the applicant for meeting the regulations stated in Section 7.2.6.3 of this report and to address ASAI 41, which is described in Section 7.1.6 of this report.

DCA Part 2, Tier 2, Sections 7.0.4.1, "Module Protection System," 7.1.1.2, "Additional Design Considerations," 7.1.2.4, "Functional Independence," 7.2.6, "Derivation of System Inputs," and Tables 7.1-3 and 7.1-4 show sense and command feature inputs and measured variables for applicable systems. The design considerations of IEEE Std. 603-1991 for sense and command features are redundancy, independence, single-failure criterion, qualification, bypasses, status indication, and testing. These are evaluated in Sections 7.1.3, 7.1.2, 7.2.2, 7.2.4, 7.2.13, and 7.2.15 of this report.

In DCA Part 2, Tier 2, Section 7.2.6, "Derivation of System Inputs," Tables 7.1-2, 7.1-3, and 7.1-4 state that system inputs are derived from signals that are direct measures of the desired variables that reflect the physical processes of interest, as specified by the design bases. The

only exception is the steam superheat, which is a parameter calculated from steam pressure and steam temperature.

DCA Part 2, Tier 2, Section 7.2.6, states that the indirect parameters used are a valid representation of the corresponding direct parameters for all events. Additionally, for both direct and indirect parameters, the characteristics of the instruments that produce the safety system inputs, such as range, accuracy, resolution, response time, and sample rate, correctly reflect the applicable analyses provided in DCA Part 2, Tier 2, Tables 7.1-3 and 7.1-4, and TeR-0316-22048.

Regulatory Evaluation of TeR-0316-22048

In 10 CFR 50.55a(h)(3), the regulation states, in part, the following:

> *Applications filed on or after May 13, 1999…for design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995.*

Sections 4.12 and 5.1 of IEEE Std. 603-1991 are applicable to TeR-0316-22048. Single-failure scenarios related to the advanced sensors are analyzed in DCA Part 2, Tier 2, Section 7.1.3. The D3 assessment is discussed in DCA Part 2, Tier 2, Section 7.1.5. The analysis of the digital sensors credited for mitigating AOOs and PAs is summarized in DCA Part 2, Tier 2, Table 7.1-18. Based on this analysis, TeR-0316-22048 proposed two different types (digital and analog) sensors for containment pressure (see TeR-0316-22048, Section 3.1.3) and two different (vendors) level sensors (see TeR-0316-22048, Section 3.1.5.1) to address single-failure and CCF scenarios. For possible flow rate sensor CCF scenarios, if there is a loss of RCS flow sensors/indications, the neutron flux sensor (as part of defense-in-depth design) ultimately generates the protective actuations in the form of a source range trip (see Note 2 of DCA Part 2, Tier 2, Table 7.1-18).

The NuScale design using redundancy and diversity in the advanced sensors provides reasonable assurance of protection against postulated single-failure and CCF scenarios. Therefore, the NRC staff reviewed the redundancy and diversity features of the NuScale advanced sensor design and finds that the design meets Sections 4.12 and 5.1 of IEEE Std. 603-1991.

In Appendix A to 10 CFR Part 50, GDC 2 states, in part, the following:

> *Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions.*

All advanced sensors are inside the CNV and will withstand earthquakes. TeR-0316-22048 requires seismic classification, which is consistent with DCA Part 2, Tier 2, Table 3.2-1. The NRC staff reviewed seismic classification of the sensors and confirmed that the seismic program includes the sensors that will be subject to classification/qualification.

In Appendix A to 10 CFR Part 50, GDC 4 states, in part, the following:

> *Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents.*

TeR-0316-22048 describes the design and development of these sensors to withstand the harsher environmental conditions of normal operation, maintenance, testing, and PAs.

- For temperature sensors, the design considered [redacted] (see TeR-0316-22048, Section 4.0).
- For pressure sensors, the design [redacted] (see TeR-0316-22048, Section 5.0).
- For flow sensors, the design considered [redacted] (see TeR-0316-22048, Section 6.0).
- For level sensors, [redacted] (see TeR-0316-22048, Section 7.0).

In 10 CFR Part 50, Appendix A, GDC 13 states, in part, the following:

> *Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.*

Variables to be monitored and controlled are identified in DCA Part 2, Tier 2, Section 7.2.4, and TeR-0316-22048, where the range and accuracy of the instruments are all provided. The as-built test for flow, level, and pressure sensors will verify that the designed advanced sensors meet the requirements over their anticipated ranges.

TeR-0316-22048 Four-Phase Process

TeR-0316-22048 describes the design concepts for the first-of-a-kind (FOAK) advanced sensors used in the nuclear reactor, containment, and steam supply system to measure temperature, pressure, flow, and level. The FOAK sensors are based on existing technologies but have not been used in an environment similar to that of the conventional PWR. The FOAK sensors described in TeR-0316-22048 are composed of hardware, cables, and electronics.

TeR-0316-22048 describes the four-phase process for the development of these FOAK advanced sensors:

- Phase 1—Technology Selection;
- Phase 2—Proof-of-Concept;
- Phase 3—Collaborative Product Development; and
- Phase 4—Environmental Qualification.

Phase 1 describes the four primary process variables of interest: temperature, pressure, flow, and level. Phase 2 (proof-of-concept) and Phase 3 (collaborative product development) are considered outside the scope of 10 CFR 52.47, “Contents of Applications; Technical Information.” Phase 4 discusses the qualification process of the FOAK sensors. The EQ of the sensors is covered under the applicant’s EQ program. The evaluation of the EQ of the sensors is described in Section 7.2.2 of this report. Therefore, the NRC staff’s review in this Section is

focused only on the Phase 1 process. The sensors for the four primary process variables are further described below.

(1) Temperature Sensors

The purpose of the Phase 1 temperature study was to present conceptual designs for in-vessel temperature measurement that meets the requirements of NPM. The parameters to be measured by temperature sensors are discussed in TeR-0316-22048, Section 4.

The Phase 1 report for temperature measurement recommended [redacted]

(2) Pressure Sensors

[redacted]

The outside containment pressure sensors (i.e., main steam pressure and feedwater pressure) use conventional transmitter technology combined with a requalification of the transmitters to envelop the normal and postaccident containment operating environments for the respective areas.

(3) Flow Sensors

Four channels of reactor coolant flow signals are required for the RTS and ESFAS functions, and these flow signals are passed to the MCS for control functions, alarms, displays, and plant historian.

The four nozzles are mounted in four vessel quadrants on the reactor vessel outer shell below the steam generators. The eight transducers, two per separation group, make up four RCS flowmeters. Each transducer pair makes up one RCS flowmeter. The transducers are located below the steam generators and above the RPV flange. They are in the proximity of the RCS T_{cold} RTDs. This location was chosen to give a straight annulus for the reflection of the signal and also to maximize the turbulent flow for a more homogenous flow profile.

The baseline reactor coolant flowmeter concept requires the mounting of ultrasonic flowmeter transducers into a [redacted]

To assure accessibility of the transducers for maintenance and replacement, the transducers are located in the lower downcomer region that is exposed when the upper reactor module is separated for refueling. The transducers can be removed and replaced, via access to the side of the vessel, should that be necessary.

[redacted].]

(4) Level Sensors

Radar technology was selected from the Phase 1 study as the best solution for level measurement. Radar technology is currently used widely by the nuclear industry to measure spent fuel pool water level and has promising accuracy capability for the required level measurements within the NPM.

The NRC staff reviewed and evaluated the Phase 1 results described in TeR-0316-22048, which contains the level of design information needed to assure that the sensors satisfying the given requirements will perform the safety function in the environment where they will work. For example, TeR-0316-22048, Section 3.1.2, states that the temperature sensors are RTDs that are conventional for use in existing reactors, but for T_{hot} and T_{cold}, the NuScale sensor operating environment (inside the reactor vessel) is different from the conventional PWR operating environment (outside the reactor vessel), and radiation hardened design is considered. TeR-0316-22048, Section 3.1.3, states that the pressure sensors are similar to conventional sensors, but they are located outside the CNV where the environment is suitable for the signal processing electronics. TeR-0316-22048, Section 3.1.4, states that the flow sensor technology has been used in other applications, but the modification proposed is for an application environment, which is different from existing applications. TeR-0316-22048, Section 3.1.5, states that the level sensors technologies have also been used in other applications, but the modifications are proposed for an environment that requires stricter EQ testing than for the existing applications.

All sensors' accuracy and range are consistent with those in DCA Part 2, Tier 2, Table 15.0-6 of Chapter 15, with reasonable margin; sensor response times are consistent with those in DCA Part 2, Tier 2, Table 15.0-7 of Chapter 15, with reasonable margin; and sensors' seismic classification and safety classification follow the definitions in DCA Part 2, Tier 2, Table 3.2-1 of Chapter 3.

The NRC staff finds that TeR-0316-22048 meets the requirements of 10 CFR 52.47, which states, in part, the following:

> *The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant.*

Because the advanced sensor development has four phases and the TeR includes only the first phase (the concept design phase), the NRC staff's evaluation in this report focuses on the sensors' design performances. The NRC staff finds the Phase 1 results described in TeR-0316-22048 to be sufficient to enable the Commission to make a decision on the applicant's proposed means of ensuring that construction meets the design and to reach a final conclusion on safety questions associated with the design.

NRC staff evaluated the RCS flowmeter uncertainty study in accordance with the requirements of 10 CFR 52.47 and 10 CFR 50.43(e). The RCS flow uncertainties are presented in TR-0616-

49121, which is evaluated in Section 7.2.7 of this report. Several factors make up the uncertainty associated directly with the flow sensors and the reference accuracy value used for the low RCS flow protective function is conservative. The NRC staff finds that the instrument specifications are in accordance with the system functional requirements, and therefore, the design complies with the performance requirements of 10 CFR 52.47(c)(2) and 10 CFR 50.43(e).

7.2.6.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.6.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that sense and command feature inputs are derived from signals that are, to the extent feasible and practical, direct measures of the variables specified in the design basis, with only one exception of steam superheat, which is a valid representation of the corresponding direct parameter for all events. The NRC staff reviewed the application against ASAI 41, which relates to the derivation of system inputs, listed in TR-1015-18653, Revision 2. The staff concludes that the I&C design meets ASAI 41. On this basis, the NRC staff concludes that the design of I&C systems satisfies the requirements related to derivation of system inputs in Section 6.4 of IEEE Std. 603-1991.

7.2.7 Setpoints

7.2.7.1 Introduction

This Section addresses the review of the setpoint values assigned to the I&C devices that perform automatic protective actions or alarm abnormal plant conditions. The setpoints of concern in this review include (1) setpoints specified for process variables on which SLs have been placed, or a process variable that functions as a surrogate for one on which an SL has been placed, and (2) setpoints related to process variables that are associated with safety functions but do not protect any SLs.

Establishing setpoints involves determination of the proper allowance for uncertainties between the device setpoint and the process analytical limit (AL) or documented nominal process limit. The calculation of device uncertainties is documented and the device setpoint determined using a documented methodology. The setpoint analysis set forth in the setpoint methodology confirms that an adequate margin exists between setpoints and SLs or normal process limits (for variables with no related SL). Furthermore, the analysis should confirm that an adequate margin exists between operating limits and setpoints to avoid inadvertent actuation of the system.

A setpoint methodology developed in accordance with RG 1.105, Revision 3, “Setpoints for Safety-Related Instrumentation,” provides a method acceptable to the NRC staff for complying with the NRC’s regulations for ensuring that setpoints for safety-related instrumentation are initially within and remain within the technical specification limits.

The NRC staff’s I&C evaluation includes a coordinated setpoint review with the organization responsible for the technical specifications and basis Sections in DCA Part 2, Tier 2, Chapter 16 of the application, including the setpoint control program, and the organization responsible for accident analysis in DCA Part 2, Tier 2, Chapter 15 of the application.

7.2.7.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: The applicant provided a system description in DCA Part 2, Tier 2, Section 7.2.7, "Setpoints," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.7, incorporates by reference TR-1015-18653. The applicant provides NuScale DCA application-specific information in Section 7.2.7, in addition to text from the referenced TR-1015-18653. The disposition of ASAI 44, which relates to setpoints, is described in Section 7.1.6 of this report.

ITAAC: There are no ITAAC associated with DCA Part 2, Tier 2, Section 7.2.7.

Technical Specifications: The technical specifications associated with DCA Part 2, Tier 2, Section 7.2.7, are given in DCA Part 2, Tier 2, Chapter 16. Specifically, these are Sections 3.3.1; 3.3.2; 3.3.3; 5.5.10, "Setpoint Program (SP);" 5.5.11, "Surveillance Frequency Control Program;" B.3.3.1; B.3.3.2; and B.3.3.3.

Technical Reports: The technical reports associated with DCA Part 2, Tier 2, Section 7.2.7, are TeR-0616-49121, Revision 0, (ADAMS Accession Nos. ML17005A147 and TR-1015-18177, Revision 0, "Pressure and Temperature Limits Methodology," (ADAMS Accession Nos. ML17005A153 (Proprietary); ML17005A130 (Non-Proprietary)).

7.2.7.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). Section 4.4 of the standard requires identification of the analytical limit associated with each variable. Section 6.8.1 requires that allowances for uncertainties between the AL of the safety system and device setpoints be determined using a documented methodology. Section 6.8.2 requires that, for processes that may be subject to multiple setpoints, the design provide a positive means of ensuring that the more restrictive setpoint is used when required.

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

- 10 CFR 50.36(c)(3) states that surveillance requirements are related to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within SLs, and that the LCOs will be met.

- 10 CFR Part 50, Appendix A, GDC 13.

- 10 CFR Part 50, Appendix A, GDC 20.

The guidance in DSRS Section 7.2.7 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS Sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- The setpoint methodology should conform to RG 1.105, Revision 3, which endorses ISA-S67.04, Part 1—1994, "Setpoints for Nuclear Safety-Related Instrumentation," with identified exceptions and clarifications.

- Regulatory Issue Summary (RIS) 2006-17, "NRC Staff Position on the Requirements of 10 CFR 50.36, 'Technical Specifications,' Regarding Limiting Safety System Settings during Periodic Testing and Calibration of Instrument Channels."

- Generic Letter (GL) 91-04, "Guidance on Preparation of a Licensee Amendment Request for Changes in Surveillance Intervals to Accommodate a 24-Month Fuel Cycle."

- Technical Specification Task Force (TSTF) Traveler 493, Revision 4, "Clarify Application of Setpoint Methodology for LSSS Functions."

7.2.7.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.7, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference address the required information relating to setpoints. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.7.3 and to address ASAI 44, which relates to setpoints and that is discussed in greater detail in Section 7.1.6 of this report

7.2.7.4.1 Review of IEEE Std. 603-1991

DCA Part 2, Tier 2, Section 7.0.4.1, states that the safety-related MPS both trips the reactor and actuates the ESFAS based on plant safety analysis ALs described in Chapter 15 of the DCA. In DCA Part 2, Tier 2, Tables 7.1-3 and 7.1-4 identify the RTS and ESFAS variables with the corresponding ALs. The ALs were verified with DCA Part 2, Tier 2, Chapter 15, Section 15.0.0.4 and Table 15.0-7. TeR-0616-49121 provides the methodology to generate the setpoint calculations that will establish the final setpoints. Placeholders for the final calculated values are controlled by the Setpoint Program described in DCA Part 2, Tier 2, Chapter 16, Section 5.5.10, "Setpoint Program (SP)." The evaluation of the ALs and technical specifications are described in Sections 15 and 16 of this report.

TeR-1015-18177 provides the analytical methods to establish the algorithms used for the LTOP setpoint for the ESFAS. TeR-1015-18177 is evaluated in Chapter 5 of this report.

The operating bypasses described in DCA Part 2, Tier 2, Section 7.2.4.1, and shown in Table 7.1-5 provide adequate protection for the mode of operation and operating conditions for the NuScale design. The operating bypasses are described in DCA Part 2, Tier 2, Section 7.1.1.2, and shown in Table 7.1-5. The operating bypasses are further evaluated in Section 7.1.1 of this report.

DCA Part 2, Tier 2, Section 7.2.7, states that the methodology in TeR-0616-49121 and the operating bypasses meet IEEE Std. 603-1991, Clauses 6.8.1 and 6.8.2. The NRC staff finds the DCA Part 2, Tier 2, Section 7.2.7, acceptable because they meet the criteria in IEEE Std. 603-1991.

7.2.7.4.2 Review of Setpoint Methodology

The establishment of setpoints and the relationships between nominal trip setpoints (NTSPs), limiting trip setpoints (LTSPs), allowable value, as-left values, as-found values, as-left tolerance (ALT), as-found tolerance (AFT), AL, and SL are discussed in this report. A thorough understanding of these terms is important to properly utilize the total instrument channel uncertainty in the establishment of setpoints.

The SLs are chosen to protect the integrity of physical barriers that guard against the uncontrolled release of radioactivity. The SLs are typically provided in the plant safety analyses. The AL is established to assure that the SL is not exceeded. The ALs are developed from event analysis models that consider parameters such as process delays, rod insertion times, reactivity changes, analysis margin, transient response, modeling error, and instrument response times. They are provided in DCA Part 2, Tier 2, Chapter 15. A properly established setpoint initiates a plant protective action before the process variable exceeds its AL. This, in turn, assures that the transient will be avoided and/or terminated before the process variables exceed the established SLs.

TeR-0616-49121 is based on following the guidance in RG 1.105, Revision 3, which describes a method acceptable to the NRC for complying with the applicable regulations. However, the TeR states conformance to ANSI/ISA-67.04.01-2006 rather than to ISA-S67.04-1994, Part I, as endorsed by RG 1.105, Revision 3. In DCA Part 2, Tier 2, Table 1.9.2 for RG 1.105 reflects this exception and provides the following basis:

> *The NuScale Instrument Setpoint Methodology Technical Report (TR-0616-49121) applies the guidance contained in ISA-67.04.01-2006. A key difference is that the 1994 version of ISA-67.04.01 uses an allowable value to determine instrument channel operability during surveillance testing and calibration. The 2006 version of ISA-67.04.01 provides updated guidance for evaluating instrument channel operability based on the comparison of the as-found to the as-left value from the previous instrument calibration for the instrument setpoint.*

The NRC staff finds the use of ANSI/ISA-67.04.01-2006, as proposed by TeR-0616-49121, to be acceptable in lieu of ISA-S67.04-1994, Part I, because it follows TSTF-493, Revision 4, and the guidance in RIS 2006-17, which provides a more conservative approach to evaluating instrument operability.

DCA Part 2, Tier 2, Table 1.9-2 and Section 7.2.7 describe the partial conformance with RG 1.105, Revision 3, with respect to the use of ISA-67.04.01-2006. The NRC staff finds the partial conformance as described acceptable because it conforms to the guidance in RIS 2006-17, which is a conservative alternative to the use of an allowable value.

Additionally, the TeR references ISA-RP67.04.02-2000, “Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation.” Although ISA-RP67.04.02-2000 is not endorsed by the NRC, the NRC staff finds its use to be consistent with RG 1.105, Revision 3, and ANSI/ISA-67.04.01-2006.

In the NuScale methodology, the AL is established to assure that a trip occurs before the SL is reached. The purpose of an LSSS is to assure that a protective action is initiated before the

process conditions reach the AL. NTSPs are chosen based on the LSSS and to minimize spurious trips close to the normal operating point of the process. Figure 7.2.7-1 below provides a pictorial representation of the NuScale setpoint methodology relationships.

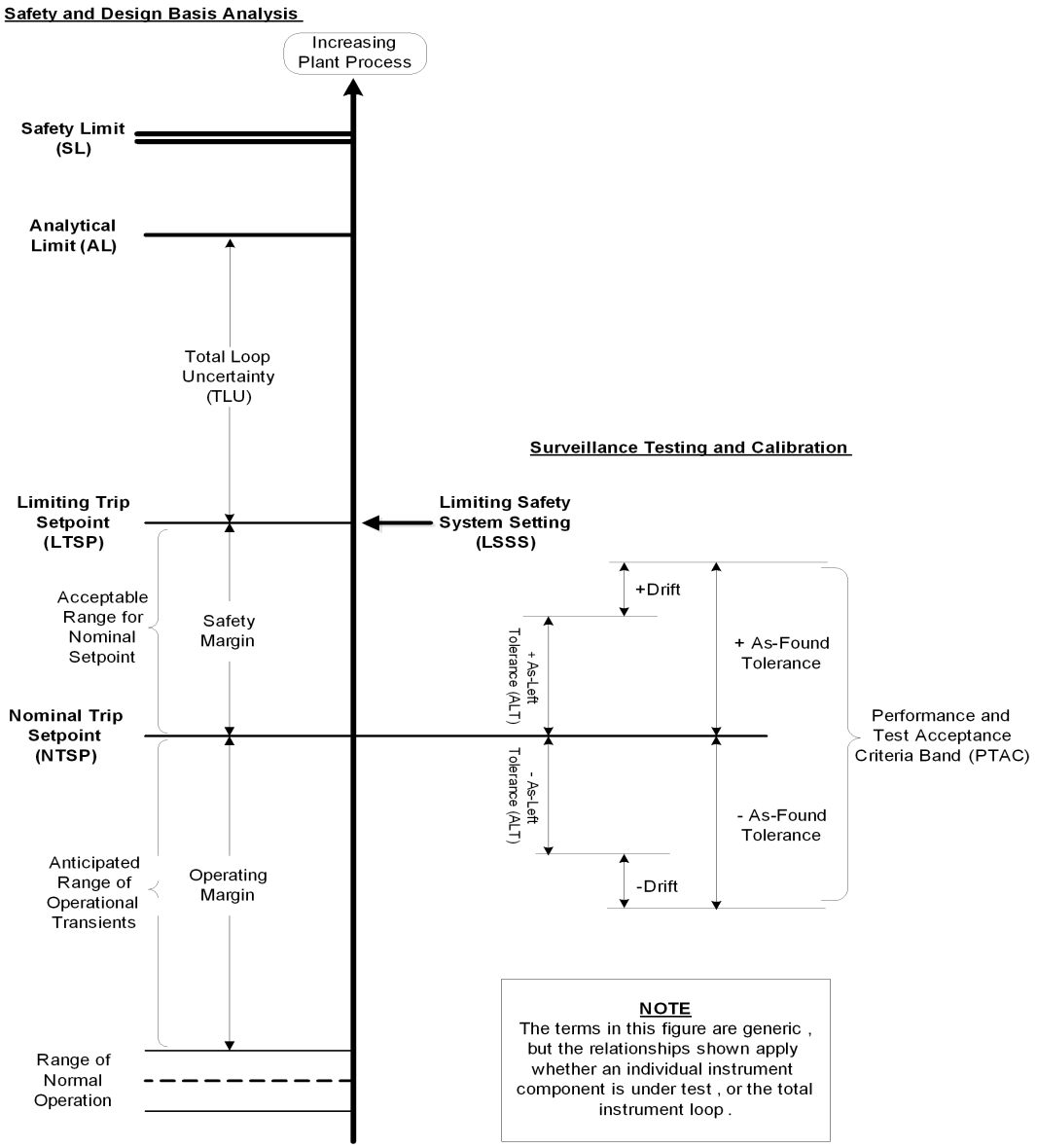

Figure 7.2.7-1: Setpoint relationships during surveillance testing and calibration[4]

This figure is intended to provide relative position and not to imply direction. Sections 4.1.3 and 4.1.4 in TeR-0616-49121 define LTSP as an LSSS and also define NTSP as the desired value of the measured variable at which an actuation occurs. The calculation of the LTSP value is given in TeR-0616-49121, Section 4.2, Equation 4-1, as LTSP = AL +/- TLU, where TLU is the total channel uncertainty.

The NTSP includes additional margin such that it is more conservative than the LTSP. In all cases, the margin must be greater than or equal to the total AFT: NTSP = AL + (| TLU | + Margin) (Equation 4-2 in Section 4.2 of TeR-0616-49121).

[4] Source: Figure 4 of TeR 0616-49121, Revision 1.

TeR-0616-49121, Section 4.3, describes how the ALT and AFT are calculated for each device and then combined to establish the total ALT and AFT. TeR-0616-49121, Section 4.4, defines performance and test acceptance criteria (PTAC) the total AFT as double-sided bands around the NTSP ± $PTAC_{Total}$ = NTSP ± AFT_{Total} (Equation 4-18 in Section 4.2 of TeR-0616-49121).

The NRC staff finds that this approach is consistent with the guidance in RG 1.105, Revision 3, and ANSI/ISA-67.04.01-2006.

Based on the discussion, sample calculations, and figures in TeR-0616-49121, the NRC staff finds that the NuScale setpoint methodology demonstrates that the correct relationships between the SL, AL, NTSP, LTSP, and PTAC will be assured, that the basis for the trip setpoint is correct, and that the requirements of 10 CFR Part 50, Appendix A, GDC 13 and 20, are met.

The NuScale setpoint methodology allows for a minimum set of assumptions to be used as referenced in TeR-0616-49121, Sections 5.1, 5.2, 5.3, 5.4, and 5.5. This minimum set of assumptions will yield conservative uncertainties used in the calculations and less chance of error during calibration of instrument channels, which the NRC staff finds reasonable and acceptable. The remaining assumptions listed were used to establish initial setpoint values that will be finalized by the setpoint calculations generated using TeR-0616-49121.

Following the setpoint calculation flow depicted in TeR-0616-49121, Figure 6.1, the pertinent information required to be documented for each calculation is collected in a typical table format as shown in Table 3.1 of the TeR. This table also provides traceability and documentation of the loop data and uncertainties used. The results of the calculation are documented in accordance with controlled plant procedures and programs (such as the Setpoint Program) with adequate detail so that all bases, equations, and conclusions are fully understood and documented.

The surveillance and calibration intervals are established in accordance with the Surveillance Frequency Control Program and are part of the development of the reference technical specifications, which is evaluated in Chapter 16 of this report. Determination of surveillance and calibration intervals takes into account the uncertainty resulting from instrument drift. As described in this report, there is reasonable assurance that the module protection system instrumentation is functioning as expected between the surveillance intervals. Plant-specific procedures will include required methods to evaluate the historical performance of the drift for each instrument channel and confirm that the surveillance and calibration intervals do not exceed the assumptions in the plant safety analysis. The guidance in GL 91-04 is used to evaluate and determine the acceptable surveillance and calibration intervals for each instrument channel as needed. For these reasons, the NRC staff finds that the NuScale setpoint methodology conforms to ANSI/ISA-67.04.01-2006 and RG 1.105, Revision 3, with respect to the assumptions and data used to determine the uncertainties and select the trip setpoint.

The NuScale setpoint methodology combines the uncertainty of the instrument loop components to determine the TLU for the functions of the reactor trip functions and the ESFAS function setpoints. All appropriate and applicable uncertainties are considered for each setpoint function. TeR-0616-49121, Table 3.1, includes a minimum list of uncertainties when calculating the TLU that are considered typical, but not inclusive, and the list is consistent with ANSI/ISA-67.04.01-2006. Other considerations that contribute to the uncertainty, such as environmental conditions and installation details of the components, are also factored into the TLU. For these reasons, the NRC staff finds that the NuScale setpoint methodology conforms to ANSI/ISA-67.04.01-2006 and RG 1.105, Revision 3, with respect to uncertainty terms, bias values, and correction factors used to select the trip setpoint.

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

Random, independent uncertainties are eligible for the square-root-sum-of-squares (SRSS) method combination, propagated from the process measurement module through the signal conditioning module of the instrument channel to the device that initiates the actuation (see TeR-0616-49121, Sections 2.1.2.1 and 2.1.2.2).

Dependent uncertainties are combined algebraically to create a larger independent uncertainty that is eligible for SRSS method combination (see TeR-0616-49121, Section 2.1.2.3).

Nonrandom bias and abnormally distributed uncertainties are those that consistently have the same algebraic sign. If they are predictable for a given set of conditions because of a known positive or negative direction, they are classified as bias with a known sign. If they do not have a known sign, they are treated conservatively by algebraically adding the bias to the TLU of interest (negative bias for increasing setpoints and positive bias for decreasing setpoints) as shown in the equation in TeR-0616-49121, Section 2.1.6. These are classified as bias with an unknown sign (see TeR-0616-49121, Sections 2.1.3 and 2.1.4).

The NRC staff finds that the described method of statistical combination of uncertainties conforms to ANSI/ISA-67.04.01-2006 and RG 1.105, Revision 3.

The equations shown in the TeR for determining module and channel uncertainty and trip setpoint conform to ANSI/ISA-67.04.01-2006 and RG 1.105, Revision 3.

Based on the discussion above, the NRC staff finds that, with respect to setpoint methodology, TeR-0616-49121 follows the guidance of RG 1.105, Revision 3; RIS 2006-17; GL 94-01; and ANSI/ISA-67.04.01-2006. It therefore complies with the NRC regulations for ensuring that setpoints for safety-related instruments are initially within and remain within the technical specification limits.

7.2.7.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.7.6 Conclusions

The NRC staff concludes that the application provides information sufficient to (1) demonstrate that the setpoint calculation methods are adequate to assure that protective actions are initiated before the associated plant process variables exceed their analytical limits, (2) demonstrate that the setpoint calculation methods are adequate to assure that control and monitoring setpoints are consistent with their system specifications, and (3) show that the established calibration intervals and methods are consistent with safety analysis assumptions. The NRC staff reviewed the application against ASAI 44 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets ASAI 44. The NRC staff also confirmed that the applicant's approach conforms to the guidance in RG 1.105, Revision 3.

Based on the above discussion, the NRC staff finds that the setpoint methodology satisfies the requirements of IEEE Std. 603-1991, Section 6.8; GDC 13 and 20 in Appendix A to 10 CFR Part 50; 10 CFR 50.36(c)(1)(ii)(A); and 10 CFR 50.36(c)(3).

7.2.8 Auxiliary Features

7.2.8.1 Introduction

This Section addresses the review of the auxiliary features. The Section is divided into two portions: evaluation of auxiliary supporting features and evaluation of other auxiliary features. Auxiliary supporting features are systems or components that provide services on which safety systems rely in accomplishing their safety functions. Auxiliary supporting features typically include, for example, electric power systems, diesel generator fuel storage and transfer systems, instrument air systems, HVAC systems, and essential service water and component cooling water systems. Other auxiliary features are systems or components that perform a function on which the safety systems do not rely to accomplish their safety functions, but which cannot be isolated from the safety system and are designated as part of the safety systems by association.

7.2.8.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this Section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: The applicant provided a system description in DCA Part 2, Tier 2, Section 7.2.8, "Auxiliary Features," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.8, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.8, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 34, 47, and 49, which relate to auxiliary systems, is described in Section 7.1.6 of this report.

In TR-1015-18653, Sections 2.5.1, "Safety Function Module," 4.8, "Access Control Features," and 8.1, "Calibration," describe the internal HIPS platform auxiliary support features to meet the auxiliary features requirements of IEEE Std. 603-1991, Section 5.12.

DCA Part 2, Tier 2, Section 7.2.8, states that for the MPS, there are no auxiliary supporting features. The other auxiliary features for the MPS are the following:

- continuous online checking and self-diagnostics communication from SFMs, SBM, SVMs, or EIMs to the MIB communications module to provide data to non-safety-related systems and non-safety-related displays;
- capability for control of safety-related components by using non-safety-related controls via the APL function within the EIM;
- isolation devices and circuitry;
- shunt trip relay/coil circuitry in RTBs and pressurizer heater breakers; and
- 24-hour timers for PAM-only mode.

For the NMS, there are no auxiliary supporting features. The other auxiliary features for the NMS include the isolation devices and circuitry.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.8, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 27. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.8.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.8.

7.2.8.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.12, "Auxiliary Features." This section indicates that auxiliary supporting features shall meet the requirements of IEEE Std. 603-1991 and that other auxiliary features that perform a function on which the safety systems do not rely to accomplish their safety functions and that are part of the safety systems by association shall be designed so that they do not degrade the safety systems below an acceptable level.

- 10 CFR 52.47(a)(2) states, in part, that the application shall discuss such items as auxiliary systems insofar as they are pertinent.

7.2.8.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed Section 7.2.8 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653, Revision 2, and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to auxiliary features. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.8.3 and to address aspects of ASAIs 34, 47, and 49 that relate to auxiliary features. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.2.8.3 and ASAIs cited above.

DCA Part 2, Tier 2, Section 7.2.8.1, states the following:

> *There are no auxiliary supporting features that are part of the safety-related module protection system (MPS) or neutron monitoring system (NMS). The MPS and NMS are designed to not rely on auxiliary supporting features such as electrical power or environmental controls to perform their safety functions; therefore, IEEE Std. 603-1991 subclause 5.12.1 does not apply to the design of the MPS and NMS.*

This is reflected in the NRC staff's evaluation of the NuScale TR-0815-1649, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," (ADAMS Accession No. ML17233A246). The NRC staff agrees with the applicant's conclusion that there are no auxiliary supporting features are relied upon for the MPS and NMS to perform their safety functions. Therefore, the NRC staff finds that the requirements of IEEE Std. 603-1991, Section 5.12.1 do not apply to the MPS and NMS design.

DCA Part 2, Tier 2, Section 7.2.8.2, describes other auxiliary features for the MPS and NMS, which are evaluated below.

The continuous online checking and self-diagnostics of the MPS were reviewed as part of the staff's evaluation of the HIPS platform and are further reviewed in Section 7.2.15 of this report. As such, the NRC staff finds that these auxiliary functions do not degrade the MPS's ability to perform its safety functions below an acceptable level.

The communication from SFMs, SBM, SVMs, or EIMs to the MIB communications module***s*** was reviewed as part of the staff's evaluation of the HIPS platform and in Section 7.1.2 of this report. The NRC staff finds that these auxiliary functions do not degrade the MPS's ability to perform its safety functions below an acceptable level.

The capability for control of safety-related components by using non-safety-related controls via the EIM was reviewed as part of the staff's evaluation of the HIPS platform and was further evaluated in Sections 7.1.2, 7.2.3, and 7.1.2.4.3 of this report. The NRC staff finds that these auxiliary functions do not degrade the MPS's ability to perform its safety functions below an acceptable level.

The isolation devices and circuitry for the MPS and NMS are reviewed in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097) and are further evaluated in Section 7.1.2 of this report. Based on those evaluations the staff finds that these auxiliary functions do not degrade the MPS's ability to perform its safety functions below an acceptable level.

DCA Part 2, Tier 2, Section 7.2.8.1, states the following:

> *The shunt trip coil and relay are non-safety-related diverse means for opening the reactor trip and pressurizer heater trip breakers and are not capable of closing these breakers once opened.*

Similarly, the 24-hour timers support non-safety-related functions of the MPS. Both auxiliary features are capable of causing spurious actuations, but are not capable of preventing the actuation of the safety functions of the MPS. As such, the NRC staff finds that these auxiliary functions do not degrade the MPS's ability to perform its safety functions below an acceptable level.

<u>Additional Other Auxiliary Features</u>

The NRC staff notes that there are additional features within the MPS and NMS that could be considered other auxiliary features. These are evaluated below.

The NMS contains health monitoring circuits. DCA Part 2, Tier 2, Section 7.2.15.3, states the following:

> *The NMS uses a health monitoring circuit in the electronic process blocks that checks the continuity of the circuit inputs. Detected faults within the NMS are provided to the MPS to trip the channel and for alarm and display in the MCR.*

The health monitoring circuits are not digital. Their inputs into the SFMs are isolated, and each has the ability to put a channel into trip but does not have the ability to prevent a safety actuation. A failure of a health monitoring circuit would at most affect only one of the four redundant NMS channels. Therefore, the staff finds that the NMS health monitoring circuits do not degrade the MPS and NMS abilities below an acceptable level to perform its safety functions.

The MPS receives a number of non-safety-related inputs. These are to allow for PAM variables, diagnostics, and to provide indications required in TMI action items. These inputs are evaluated for electrical and communications independence in Sections 7.1.2.4.2 and 7.1.2.4.3 of this report.

Certain non-safety-related valve position indicator sensors would have the ability, through the APL, to prevent removing valves from their fail-safe positions, but these do not have the ability to prevent a safety actuation.

The MPS also actuates valves that are considered non-safety-related as part of DHRS actuation and containment isolation. This is a one-way interaction through EIM solenoid valves.

These safety-to-non-safety-related interactions are evaluated in Section 7.2.10 of this report.

The portions of the MPS dedicated to processing these signals are designed as reviewed in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097) and would be developed according to the quality requirements evaluated in Section 7.2.1 of this report. Thus, the NRC staff finds that these auxiliary functions do not degrade the MPS's ability below an acceptable level to perform its safety functions.

This technical evaluation documents the staff's evaluation against ASAI 34 and concludes that the I&C design meets ASAI 34, as described in Section 7.1.6 of this report, and Section 5.12 of IEEE Std. 603-1991.

The applicant provided the disposition for ASAI 47 and ASAI 49 which require that the plans and commitments, at the level of detail found within a DCA, demonstrate that the same design, development, and iV&V processes for test, calibration, and self-diagnostic functions were followed as for all other HIPS platform functions. Therefore, the NRC staff finds these ASAIs to have been met, as described in Section 7.1.6.4 of this report.

7.2.8.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.8.6 Conclusions

Based on the above discussion and Sections 7.2.3 (reliability), 7.1.3 (single-failure criterion), 7.2.2 (qualification), and 7.1.2 (independence) of this report, the NRC staff concludes that the application provides information sufficient to (1) demonstrate that auxiliary supporting features are designed consistent with the applicable requirements of IEEE Std. 603-1991 and (2) demonstrate that other auxiliary features are designed such that they do not degrade safety systems below an acceptable level. The NRC staff reviewed the application against ASAIs 34, 47, and 49 listed in TR-1015-18653, Revision 2. The staff concludes that the I&C design meets the auxiliary features aspects of these ASAIs. On this basis, the NRC staff concludes that the design of auxiliary features satisfies the requirements of Section 5.12 of IEEE Std. 603-1991 and 10 CFR 52.47(a)(2).

7.2.9 Control of Access, Identification, and Repair

7.2.9.1 Introduction

This section addresses the review of the area of administrative control of the I&C system hardware and software, identification of safety equipment, and equipment repair features. Control of access to I&C system hardware and software allows a licensee to limit access to the

means for bypassing safety system functions to qualified plant personnel. "Identification" refers to the naming and labeling of I&C-related systems and components and I&C system documentation, software, and firmware to assure adequate control of safety system equipment. The review also includes evaluation of the capability to repair I&C safety systems.

7.2.9.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.9, "Control of Access, Identification, and Repair," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.9, incorporates by reference TR-1015-18653, Revision 2. The applicant provides NuScale DCA application-specific information in Section 7.2.9, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 11, 22, 31, 32, 33, 53, 54, and 58, which relate to control of access, identification, and repair, are described in Section 7.1.6 of this report.

TR-1015-18653, Section 4.8, "Access Control Features," describes the HIPS platform design concepts that address the internal platform access control features to meet the control of access requirements of IEEE Std. 603-1991, Section 5.9.

TR-1015-18653, Section 8.2.7, "Module Testing," describes the HIPS platform design concepts that address the firmware identification features to meet the identification requirements of IEEE Std. 603-1991, Section 5.11.

TR-1015-18653, Sections 2.2, "HIPS Module," and 8.2, "Testing," describe the HIPS platform design concepts that address the internal platform repair features to meet the repair requirements of IEEE Std. 603-1991, Section 5.10.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.9.4.1, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 1 and 2. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.9.

7.2.9.3 Regulatory Basis

The following NRC regulation contains the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.9, "Control of Access," Section 5.10, "Repair," and Section 5.11, "Identification." Section 5.9 of IEEE Std. 603-1991 states, in part, that the design shall permit the administrative control of access to safety system equipment. Section 5.10 requires that safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. Section 5.11 contains requirements for the identification of safety system equipment.

The guidance in DSRS Section 7.2.9 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS sections. In addition, the following

guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- Digital I&C safety systems and components should conform to the identification guidance in Section 5.11 of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3.

- I&C safety systems and components should conform to the identification guidance in IEEE Std. 384-1992, as endorsed (with identified exceptions and clarifications) by RG 1.75, Revision 3.

7.2.9.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.9, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application from TR-1015-18653 address the required information relating to control of access, identification, and repair. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.9.3 and to address aspects of ASAIs 11, 22, 31, 33, 53, 54, and 58 that relate to control of access, identification, and repair. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.2.9.3 and ASAIs cited above.

7.2.9.4.1 Control of Access

The NRC staff's evaluation in this section addresses the application-specific information requirements for ASAIs 22, 31, 53, and 58.

DCA Part 2, Tier 2, Section 7.2.9.1, describes how access to I&C safety systems will be controlled and how such controls satisfy the requirements of Section 5.9 of IEEE Std. 603-1991 and the guidance in RG 1.152 for digital-based I&C safety systems. The NRC staff confirmed that the design allows for the administrative control of access to I&C safety system equipment. These administrative controls are supported by provisions within the safety systems, by provisions in the generating station design, or by a combination thereof. These administrative controls are more specifically described below.

DCA Part 2, Tier 2, Section 7.2.9.1, "Control of Access," states, in part, the following:

> *Protection from a faulted MWS when not in use is provided through a qualified physical hardware disconnect and a qualified safety-related isolation device. To enable MWS communication, the hardware disconnect must be physically enabled and the affected safety channel must be placed into bypass, either of which generates an alarm in the control room. By placing the safety channel in bypass, the channel is no longer being relied upon to perform a safety function.*

The MPS parameters are adjusted in accordance with plant operating procedures that govern the parameter's adjustment, including procedures that establish the minimum number of redundant safety channels that must remain operable for the current operating mode and conditions (see Section 13.5 of this report). Each safety division has a dedicated non-safety-

related MWS to prevent connection to multiple safety divisions with the FPGA logic circuits, and configuration settings for digital data communication interfaces are not adjustable. As a result, the FPGA logic is protected from alterations while in operation. The NRC staff finds the physical control of access features (e.g., key locks) provided are acceptable based on their ability to prevent inadvertent or unauthorized physical access to the safety system.

DCA Part 2, Tier 2, Section 7.2.9.1, "Control of Access," states, in part, the following:

> *Remote access to the MPS is prohibited. However, the MPS permits administrative control of direct access to safety system equipment. Access to manually bypassed protection channels and manually blocked protective functions is limited by administrative controls. Administrative controls are also provided for access to MWS test points, setpoint adjustments, and channel calibration.*

The NRC staff finds that the electronic control of access features provided is acceptable based on its ability to prevent inadvertent or unauthorized physical access to the safety system.

The I&C architecture is designed with four security levels of which Security Level 4 is the highest. The MPS is identified as a Security Level 4 digital system. The design of the MPS prohibits remote access to systems within the Security Level 4 domain. The NRC staff's evaluation of physical security is addressed in Section 13.6 of this report.

The NRC staff finds that the security features provided are acceptable based on their ability to prevent an unauthorized electronic path by which personnel can change plant software or display erroneous plant status information to the operators.

Secure Development and Operational Environment

For digital safety systems, establishment of a secure development environment includes the protection of digital computer-based systems throughout the development life cycle of the system to prevent unauthorized, unintended, and unsafe modifications. During development, operation, and maintenance, measures should be taken to protect safety systems from inadvertent actions that may result in unintended consequences to the system. "Secure development environment" is defined as the condition of having appropriate physical, logical, and programmatic controls during the system development phases (i.e., concepts, requirements, design, implementation, testing) to assure that unwanted, unneeded, and undocumented functionality (e.g., superfluous code) is not introduced into digital safety systems.

The guidance for establishing an SDOE for digital safety systems is provided in RG 1.152. DCA Part 2, Tier 2, Sections 7.2.1 and 7.2.9.1 describe the process for establishing an SDOE during for the digital safety I&C system development software life-cycle phases (requirements, design, implementation, and test phases) in accordance with RG 1.152, Revision 3. The NRC staff's evaluation of the Regulatory Positions 2.1 through 2.5 of RG 1.152 is shown below.

(1) Concepts Phase, Regulatory Position 2.1 of RG 1.152, Revision 3

Regulatory Position 2.1, Part I

This position states the following:

> *In the concepts phase, the licensee should identify digital safety system design features required to establish a secure operational environment for the system. A licensee should describe these design features as part of its application.*

DCA Part 2, Tier 2, Section 7.2.9.1, describes the design features that prevent unintended changes to hardware or software code and that detect unintended changes if they occur. It also provides the attributes of system design features that minimize the potential for security vulnerabilities. These features includes physical access controls, electronic access controls, software alteration controls, and deterministic performance controls. The NRC staff's evaluation of the SDOE provisions imposed on the design process for later life-cycle phases are discussed in this section. The NRC staff finds the concept phase acceptable since there are design features to secure the operational environment as discussed above. The applicant has adequately described the design features required to establish a secure operational environment consistent with Regulatory Position 2.1 of RG 1.152, Revision 3.

Regulatory Position 2.1, Part II

This position states the following:

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

DCA Part 2, Tier 2, Section 7.2.1, describes the processes implemented during each software life-cycle phase for the safety I&C system that prevent inclusion of unintended functions in documents and software code. The applicant outlines generic defenses established during the concept phase to defend against undesired software changes throughout each phase of the software development life cycle. Furthermore, the applicant states that a vulnerability assessment process shall be carried out for each development life-cycle phase, and countermeasures from the assessment shall be applied as design features or management controls. The NRC staff finds the assessment process acceptable in identifying potential vulnerabilities and identifying measures to mitigate those undesired and unintended changes.

DCA Part 2, Tier 2, Section 7.2.1.2.5, describes defenses against unauthorized changes in the requirements phase. The SRS fully documents the security design requirements established during the concept phase. The requirements traceability matrix is created in this phase to capture all of the system requirements. The design team is responsible for developing, maintaining, and updating the SRS. It also states that the V&V team shall independently verify the SRS and assure that there are no functions in the SRS that are not traceable to the system requirements. The NRC staff finds this approach acceptable since the V&V team would be able to detect insertion of undesired requirements and initiate appropriate corrective actions.

DCA Part 2, Tier 2, Section 7.2.1.2.6, describes defense against unauthorized changes in the design phase. The SDD is developed during this phase and reflects the requirements documented in the SRS. The SDD fully documents the security design requirements established during the requirements phase. The design team is responsible for developing, maintaining, and updating the SDD. It also states that the V&V team shall independently verify the SDD and assure that all application software

requirements identified in the SRS are properly reflected in the SDD. The NRC staff finds the approach acceptable since the V&V team would be able to detect insertion of undesired designs and initiate appropriate corrective actions.

DCA Part 2, Tier 2, Section 7.2.1.2.7, describes defense against unauthorized changes in the implementation phase. The design team is responsible for developing, maintaining, and updating the application software in accordance with the design documented in the SRS and SDD and the design process. It states that the V&V team shall independently verify each application software unit, which includes graphical block diagrams and source code listings. The NRC staff finds the approach acceptable since the V&V team would be able to detect additional functions that are not traceable to the SRS and SDD and initiate appropriate corrective actions.

DCA Part 2, Tier 2, Section 7.2.1.2.8, describes defense against unauthorized changes in the test phase. During this phase, common system platform operating system and application software is integrated with the common digital platform hardware for each system. This phase also covers factory acceptance testing. Test reports are an output of this phase. The V&V team is responsible for the test reports or results. The applicant states that the application software test reports and results are version controlled and are released in accordance with the Digital I&C Software Configuration Management Plan. The NRC staff finds the approach acceptable since the V&V team would be able to detect any unauthorized changes in the test phase.

Regulatory Position 2.1, Part III

This position states:

> *The licensee should not allow remote access to the safety system. For the purposes of this guidance, remote access is defined as the ability to access a computer, node, or network resource that performs a safety function or that can affect the safety function from a computer or node that is located in an area with less physical security than the safety system (e.g., outside the protected area).*

Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and non-safety-related digital systems.

DCA Part 2, Tier 2, Section 7.2.9.1, states that remote access to the MPS is prohibited. In response to the ACRS concerns, NuScale in their letter LO-1018-62193, dated October 24, 2018 (ADAMS Accession No. ML182198A222), submitted proposed changes to DCA Part 2, Tier 2, Sections 7.0 and 7.2. Proposed revision to Section 7.2.13.7, “Other Information Systems,” states that “there is a unidirectional communication interface between the MCS and PCS networks and the plant network and is shown in Figure 7.0-1. The one-way deterministic isolation devices transmits network traffic from the MCS and PCS to the plant network in one direction only, which is enforced in the hardware design, not software. No software configuration or misconfiguration will cause the boundary device to reverse the direction of data flow.” The NRC staff finds this acceptable to conform to this regulatory position. The NRC staff’s evaluation of communication independence is discussed in Section 7.1.2.4.3 of this report.

(2) Requirements Phase, Regulatory Position 2.2 of RG 1.152

Regulatory Position 2.2.1, System Features, Part I

This position states:

> *The licensee should define the functional performance requirements and system configuration for a secure operational environment; interfaces external to the system; and requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.*

DCA Part 2, Tier 2, Section 7.2.1, states that secure operational environment design concepts are developed into system requirements during the concept and requirements phases. DCA Part 2, Tier 2, Section 7.2.1.2.5, states that the SRS fully documents the security design requirements established during the concept phase, including the design features that minimize the potential for security vulnerabilities. The NRC staff finds the applicant's approach acceptable to define functional performance requirements and system configuration for a secure operational environment according to RG 1.152, Revision 3.

Regulatory Position 2.2.1, System Features, Part II

This position states:

> *The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's SDOE feature.*

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that the independent V&V assures that all security design features and requirements are properly documented and assures the correctness, completeness, accuracy, and testability of all requirements. The NRC staff finds the approach acceptable to meet this regulatory position because the independent V&V team will confirm that design feature requirements are implemented correctly.

Regulatory Position 2.2.1, System Features, Part III

This position states the following:

> *Requirements specifying the use of pre-developed software and systems (e.g., reused software and COTS systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).*

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that in cases where previously developed software or COTS software is used, the NuScale Digital Safety System SDOE and Digital I&C Software Development Plans contain requirements during the implementation phase of software development for evaluating and assessing that both developed code and previously developed or COTS software meets the specified design requirements for system reliability and SDOE. For COTS software, previously developed software or complex programmable logic classified as SIL 4, the NuScale Digital I&C Quality

Assurance Plan requires an evaluation of vendors and suppliers of digital I&C systems to verify that the software or complex programmable logic adheres to the SDOE design requirements and does not adversely affect system reliability. The NRC staff finds that use of pre-developed or COTS software in NuScale design acceptable because they conform to RG 1.152, Revision 3.

Regulatory Position 2.2.2, Development Activities

This position states the following:

> *During the requirements phase, the licensee should prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.*

DCA Part 2, Tier 2, Section 7.2.1.6, states that the iV&V of the requirements documents assures that there are no unintended requirements. The NRC staff finds this approach acceptable to meet this regulatory position.

(3) Regulatory Position 2.3, Design Phase

Regulatory Position 2.3.1, System Features, Part I

This position states:

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

DCA Part 2, Tier 2, Section 7.2.1.1.2.5, states that the SDD fully documents the security design requirements established during the requirement phase and is independently reviewed by the V&V team to assure that all requirements in the SDD, including (1) physical access control, (2) data communication controls with other systems, (3) protection against software alteration, and (4) protection of deterministic performance, are described in sufficient detail to support the implementation phase and to assure that all design features are captured in accordance with the SRS. Since there are design features for controlling access and an independent V&V activity to assure such access, the NRC staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.3.1, System Features, Part II

This position states:

> *Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life cycle. The results of this assessment may identify the need for more complex access control measures, such as a combination of knowledge*

(e.g., password), property (e.g., key and smart card), or personal features (e.g., fingerprints), rather than just a password.

DCA Part 2, Tier 2, Section 7.2.9.1, discusses planned physical and logical access control features such as key switches, control room alarms, the safety-related I&C equipment location and the safety-related I&C communication interfaces. During each development life-cycle phase, assessment shall be performed to confirm that there are adequate physical and logical controls to prevent unintended software changes, and as a result, the NRC staff finds this approach acceptable to meet this regulatory position.

(4) Regulatory Position 2.4, Implementation Phase

Regulatory Position 2.4.1, System Features

This position states:

The developer should ensure that the transformation from the system design specification to the design configuration items of the secure operational environment is correct, accurate, and complete.

DCA Part 2, Tier 2, Section 7.2.1.1.2.7, "Software Implementation," states that the software code created during the implementation phase reflects the detailed designs documented in the SDD, which is developed during the design phase. All software codes are independently verified and validated on a component-by-component basis. Security analysis verification is performed as part of the V&V activities to assure that the secure development environment requirements are met and the developer has removed hidden functions or code that may have been used in development or unit testing and is not required to meet the system design requirements. The NRC staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.4.2, Development Activities, Part I

This position states:

The developer should implement secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. The developer's standards and procedures should include testing (such as scanning), as appropriate, to address undocumented codes or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner.

The developer should account for hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the FMEA of the application code) to prevent any unauthorized access or degradation of the reliability of the safety system.

DCA Part 2, Tier 2, Section 7.2.1.2.6, provides information on the defensive strategies planned for the implementation phase to prevent undocumented code and unauthorized and undocumented functions or application. The Digital Safety System SDOE Plan requires that vulnerability assessments be performed on software and complex programmable logic that is developed and classified as SIL 4. The vulnerability assessments evaluate that the design configuration items of the secure development environment are reviewed to assure they are correctly translated from the system design specification and are accurate and complete. Details of the secure development environment are described in DCA Part 2, Tier 2, Section 7.2.9.1. The NRC staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.4.2, Development Activities, Part II

This position states:

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

DCA Part 2, Tier 2, Section 7.2.1.2.6, states that for COTS software, previously developed software, or complex programmable logic classified as SIL 4, the Digital I&C QA Plan requires an evaluation of vendors and suppliers of digital I&C systems to verify that the software or complex programmable logic adheres to the SDOE design requirements and does not adversely affect system reliability. The NRC staff finds the NuScale's treatment of COTS and pre-developed software acceptable because it conforms to RG 1.152, Revision 3.

(5) Regulatory Position 2.5, Test Phase

This position states:

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

DCA Part 2, Tier 2, Section 7.2.1.2.8, states that the factory acceptance testing of the fully integrated system will validate that the system meets the system requirements related to the software. The system test is conducted with all connected system interfaces, including those that pose security threats. The applicant also stated that the independent validation testing demonstrates that all system requirements related to the software function correctly in the final integrated system. Since independent testing is

performed to assure that design requirements and configuration items are implemented correctly, the NRC staff finds this approach acceptable to meet this regulatory position.

Regulatory Position 2.5.1, System Features

This position states:

> *The developer should correctly configure and enable the design features of the secure operational environment. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.*

DCA Part 2, Tier 2, Section 7.2.1.2.8, states that the testing methodology assures that the software and data secure operational environment design requirements features have been designed and implemented in accordance with this regulatory position, including but not limited to, external hardware connections and external communication gateways. This testing methodology includes application-level testing and independent validation testing, and as a result, the NRC staff finds this approach acceptable to meet this regulatory position.

7.2.9.4.2 Identification

The NRC staff's evaluation in this section addresses the application-specific information requirements for ASAIs 11 and 54.

The NRC staff reviewed the DCA Part 2, Tier 2, Section 7.2.9, to verify that IEEE Std. 603-1991, Section 5.11, has been adequately addressed for the safety-related systems. IEEE Std. 603-1991, Section 5.11, requires that (1) safety system equipment be distinctly identified in accordance with the acceptance criteria of IEEE Std. 384-1981, (2) components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification, (3) identification of safety system equipment be distinguishable from other purposes, (4) identification of safety system equipment does not require frequent use of reference material, and (5) the associated documentation be distinctly identified in accordance with the acceptance criteria of IEEE Std. 494-1974. DSRS Section 7.2.9, provides NRC staff review criteria on meeting the identification requirements of IEEE Std. 603-1991.

DCA Part 2, Tier 2, Section 7.2.9.2, states that all equipment, including panels, modules, and cables associated with the MPS and NMS, be marked to facilitate identification. The safety-related I&C systems are configured in accordance with specific identification requirements that provide a standardized method for identifying equipment. The safety-related I&C systems are also configured using diagrams and signals for the purpose of consistency during the installation process. Interconnecting cabling is color coded. The cables and raceways for Class 1E systems are tagged at periodic intervals, durably marked, and colored to uniquely identify the division (or non-division) of the cable. The physical identification is provided so that an operator can confirm whether the safety I&C system cabinets and related cables are in the safety class. The safety-related I&C system cabinets are distinguished by nameplates. The safety I&C system components are uniquely identified by designations according to project procedures and as defined in contract specifications. The physically isolated cable that connects sensors to actuation devices is identified by different colors between divisions. The configuration identification of software is assured by identification provisions as discussed in DCA Part 2, Tier 2, Section 7.2.1.

Based on the information provided in DCA Part 2, Tier 2, Section 7.2.9.2, the NRC staff finds that the hardware and software identification controls for I&C safety equipment satisfies ASAIs 11 and 54, the guidance in RG 1.75, and the requirements of Section 5.11 of IEEE Std. 603-1991.

7.2.9.4.3 Repair

The NRC staff's evaluation in this section addresses the application-specific information requirements for ASAI 32.

DCA Part 2, Tier 2, Section 7.2.9.3, "Repair," describes the capability to repair I&C safety systems to assure that the requirements in Section 5.10 of IEEE Std. 603-1991 are met. The NRC staff reviewed the NuScale DCA to verify that IEEE Std. 603-1991, Section 5.10, has been adequately addressed for the NuScale safety-related systems. This standard requires that the safety-related systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

DCA Part 2, Tier 2, Section 7.2.9.1, describes software controls in place to detect potential alteration of various system aspects, including memory alteration.

DCA Part 2, Tier 2, Section 7.2.9.3, states the following:

> *The MPS facilitates the recognition, location, replacement, repair, and adjustment of malfunctioning components or modules. The built-in diagnostics support timely recognition of problems by providing a mechanism for periodically verifying the operability of MPS modules, and of rapidly locating malfunctioning assemblies. Continuous online error checking detects and locates failures. Channel bypass for the MPS permits replacement of malfunctioning sensors or channel components without jeopardizing plant availability.*

DCA Part 2, Tier 2, Section 7.2.9.3, also states that the MPS incorporates a combination of continuous self-checking features and periodic surveillance. Examples of these features include the use of the BIST feature in the FPGA logic and CRC checks as described in Section 8 of TR-1015-18653, periodic surveillance testing, and other tests in each type of module, as appropriate, to verify normal operation.

DCA Part 2, Tier 2, Section 7.2.15, states, in part, that safety-related I&C systems comply with the guidance of RG 1.22, Revision 0, "Periodic Testing of Protection System Actuation Functions," dated February 1972 (ADAMS Accession No. ML083300530), which provides criteria for the design to incorporate provisions to permit periodic testing of the complete safety-related I&C systems, as well as bypassed channel status indication being available in the MCR.

The applicant has adequately demonstrated that the NuScale design contains both automatic fault tolerance features, manual (e.g., MWS) testing measures, and equipment status indication to facilitate timely repairs of the safety related I&C systems.

The NRC staff finds that the I&C design satisfies ASAI 32 and the requirements of IEEE Std. 603-1991, Section 5.10. The applicant has adequately stated conformance to relevant guidance with regard to testing of the safety-related I&C systems.

7.2.9.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.9.6 Conclusions

The NRC staff concludes that the design provides information sufficient to (1) demonstrate that the proposed administrative provisions for controlling access to I&C safety systems and equipment are adequate to prevent unauthorized access and modification to the safety I&C systems, (2) demonstrate that I&C safety systems are distinctively marked, versions of hardware are marked accordingly, and configuration management is used for maintaining identification of safety-related software, and (3) demonstrate that safety system design facilitates timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. The NRC staff reviewed the application against ASAIs 11, 22, 31, 32, 33, 53, 54, and 58 listed in TR-1015-18653, Revision 2. The staff concludes that the NuScale I&C design satisfies the aspects of these ASAIs that relate to control of access, identification, and repair. On this basis, the staff concludes that the design of I&C systems conforms to the control of access guidance of RG 1.152, Revision 3; the identification guidance in RG 1.75, Revision 3; and satisfies the control of access, identification, and repair requirements of Sections 5.9, 5.10, and 5.11 of IEEE Std. 603-1991.

7.2.10 Interaction between Sense and Command Features and Other Systems

7.2.10.1 Introduction

This section addresses the review of the interaction between sense and command features and other systems to confirm that non-safety-related system interactions with I&C safety systems do not adversely affect the I&C safety systems. The fundamental design principles described in Section 7.1 of this report, as well as the appendices to Chapter 7 of the DSRS, inform this review.

7.2.10.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.10, “Interaction between Sense and Command Features and Other Systems.”

DCA Part 2, Tier 2, Section 7.2.10, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.2.10, in addition to text from the referenced TR-1015-18653. The disposition of ASAI 40, which relates to the interaction between sense and command features and other systems, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 2.5.2, “Bypass or Trip Operation,” and Section 4.5, “Hard-Wired Module,” describe the configuration capabilities and bypass features of the HIPS platform components to meet the sense and command requirements of IEEE Std. 603-1991, Section 6.3.

ITAAC: There are no ITAAC associated with DCA Part 2, Tier 2, Section 7.2.10.

Technical Specifications: There are no technical specifications associated with DCA Tier 2, Section 7.2.10.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.10.

7.2.10.3 Regulatory Basis

10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991, including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 6.3, "Interaction between Sense and Command Features and Other Systems." Section 6.3 states that, if a single credible event can both cause a non-safety-related system action that results in a condition requiring protective action and concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to this failure or equipment not subject to failure caused by the same single credible event will be provided.

There are no specific DSRS acceptance criteria in this section. However, the guidance provided below should be used to review the acceptability of the information associated with interaction between sense and command features and other systems.

7.2.10.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed Section 7.2.10 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information provided in the application and the documents incorporated by reference address the required information relating to interactions between sense and command features and other systems. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.10.3 and to address ASAI 40, which is discussed in greater detail in Section 7.1.6 of this report.

In DCA Part 2, Tier 2, Sections 7.1.1, 7.1.2, 7.1.5, and 7.2.10 describe the controls to assure that non-safety-related system interactions with safety systems are limited. Section 6.3 of IEEE Std. 603-1991 indicates that if a single credible event can both (1) cause a non-safety-related system action that results in a condition that needs protective action and (2) concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, either alternate channels not subject to this failure or equipment not subject to failure caused by the same single credible event will be provided.

DCA Part 2, Tier 2, Section 7.2.10, "Interaction between Sense and Command Features and Other Systems," states, in part, the following:

> *The boundaries between safety and non-safety-related systems are formed by isolation devices that prevent failures or malfunctions in the non-safety-related systems from interfering with the safety systems; therefore, conditions that prevent the safety systems from completing protective functions within the sense and command features do not exist in the MPS. The interactions between the MPS sense and command features and other non-safety-related systems are designed to meet the requirements of IEEE-603-1991, Section 6.3.*

Variables used for both protection and control are first input into the MPS for monitoring, signal conditioning, and trip determination functions. These variables are then provided to the MCS for plant control functions through isolated, one-way communication paths. Isolated output signals maintain MPS channel independence. This is already evaluated in Section 7.1.2.4 of this report. To prevent a single failure in the MPS from causing a transient in the control system

(that would require a protective action), the MCS uses a median signal select algorithm. The algorithm prevents a malfunctioning protection channel from causing a spurious control system action within the MCS. The MCS median select algorithm rejects the failed input and uses the remaining redundant MPS channels monitoring that variable for control.

The median signal selection process of the algorithm is described in DCA Part 2, Tier 2, Section 7.2.10. The MCS performs quality and validation checks on the input process variable data. The MCS determines if the process value is "good." The operator has the ability to select a signal for control if the inputs are determined to be good. If four process values are good, the MCS will use the median value of all four inputs. If one of the inputs is "bad" because of a failure or bypass, a notification is sent to the operator workstation. The MCS selects the appropriate selection methodology for the number of remaining good signals for utilization. For a two-signal input, there are three possible configurations for a selection algorithm. When both inputs are good, the operator has the option to select which signal is used as an input to the process controller. When both signals are bad, the loop control is transferred to the operator for manual control. When one signal is good, then the process controller uses that signal.

For a three-input signal, a determination is made on the value of the three inputs: lowest, median, and highest. When three inputs are determined to be good, the median signal is transferred as the input to the control process. If one of the input signals is tagged as bad, then an average of the two remaining signals is used as the input to the control process. When two of the inputs are marked as bad, the one remaining good signal is used by the control process. When all signals are bad, the loop control is transferred to the operator for manual control, and the operator is alerted. For four input signals, if the MCS determines the four channel inputs are good, the MCS uses the median value of the four inputs. If one channel has been bypassed for maintenance, or if the channel has failed (i.e., has been marked as bad), the channel is disregarded by the signal select algorithm. The signals from the remaining three channels are then processed as described for three inputs. When two of the four signals are bad, the MCS will use the average value of the remaining two valid inputs. When a single value is good, the MCS uses the value of the single good input for control. When four signals are bad, the loop control is transferred to the operator for manual control, and the operator is alerted.

In addition, the NRC staff evaluated the I&C system design provisions to satisfy the requirements of Section 6.7 of IEEE Std. 603-1991 for when a channel is in maintenance bypass. The MPS safety-related variables are monitored by four redundant channels. The safety functions are actuated by two-out-of-four coincident logic. This logic assures that the required safety function remains operable in the event of a single random failure of a protection channel concurrent with a channel in maintenance bypass. This has been evaluated in Sections 7.1.2.4 and 7.1.3.4 of this report. While the sense and command features equipment for the MPS are in maintenance bypass, the safety system retains its ability to accomplish the safety function. As evaluated in Section 7.2.4.4 of this report, the sense and command features also continue to meet the single-failure requirements.

Based on the evaluations in Sections 7.1.2.4, 7.1.3.4, and 7.2.10.4 of this report and the median selection process described above, the NRC staff confirmed that the I&C system is designed such that the capability of a safety system to accomplish its safety function is retained even while the sense and command features equipment is in maintenance bypass. The staff also confirmed that during such operation, the sense and command features continue to meet the single-failure requirements in Section 5.1 of IEEE Std. 603-1991 according to the requirements for interaction between sense and command features and other systems in Section 6.3 of IEEE Std. 603-1991 based on the NRC staff's evaluations in Sections 7.2.4.4 and 7.2.10.4 of this report and the referenced TR-1015-18653.

7.2.10.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.10.6 Conclusions

The NRC staff concludes that the application provides information sufficient to demonstrate that non-safety-related system interactions with safety systems are limited and do not adversely affect the I&C safety systems. Based on the discussion above, the NRC staff concludes that the NuScale I&C design meets ASAI 40, as described in Section 7.1.6 of this report. Therefore, the NRC staff also concludes that the design of I&C systems satisfies the requirements in Section 6.3 of IEEE Std. 603-1991 related to interactions between the sense and command features and other systems.

7.2.11 Multi-unit Stations

7.2.11.1 Introduction

This section addresses the review of SSCs that are shared between nuclear power plant (NPP) units of multiunit stations (i.e., multiple NPP units located at the same site). GDC 5 in Appendix A to 10 CFR Part 50 and IEEE Std. 603-1991 allow this sharing, provided that it will not impair the performance of the required safety functions in all units.

The fundamental principles described in Section 7.1 of the DSRS inform the review of multiunit stations. In addition, if the application proposes multiunit shared displays and controls, the review should be coordinated with the organization responsible for reviewing human factors to confirm that shared user interfaces are sufficient to support the operator needs for each of the shared units. The review of any proposed sharing of electrical power in multiunit NPPs or proposed capability for manual connection for sharing of electrical power should be coordinated with the organization responsible for reviewing electrical engineering.

7.2.11.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 2.5, “Instrumentation and Control Systems,” and Section 2.6, “Neutron Monitoring System.”

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.11, “Multi-Unit Stations,” and DCA Part 2, Tier 2, Chapter 21, “Multi-Module Design Considerations.”

DCA Part 2, Tier 2, Section 7.2.11, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.2.11, in addition to text from the referenced TR-1015-18653. The disposition of ASAI 35, which relate to multi-unit stations, is described in Section 7.1.6 of this report.

ITAAC: The ITAAC related to common SSCs are described in Section 14.3.6 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.11, and DCA Part 2, Tier 2, Chapter 21.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.11, and DCA Tier 2, Chapter 21.

7.2.11.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.13, "Multi-Unit Stations," which states that the sharing of structures, systems, and components between units at multiunit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired.

- 10 CFR Part 50, Appendix A, GDC 5, "Sharing of Structures, Systems, and Components," states that SSCs important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.

The guidance in DSRS Section 7.2.11 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS sections. In addition, the following guidance document provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- I&C systems and components should conform to the application of the single-failure criterion in IEEE Std. 379-2000 as endorsed by RG 1.53, Revision 2.

7.2.11.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed DCA Part 2, Tier 2, Section 7.2.11, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to multiunit stations. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.11.3 and to address ASAI 35, which relates to multi-unit stations and that is discussed in greater detail in in Section 7.1.6 of this report.

<u>Shared I&C Systems across Multiple NuScale Power Modules</u>

DCA Part 2, Tier 2, Section 7.2.11, describes the multiunit station design. The I&C safety systems use the term "modules" instead of "units" to describe the individual NPMs. Section 7.2.11 also states that the NuScale power plant may include up to 12 individual NPMs. The modules have a separate MPS and NMS-excore to provide safety-related protective functions. The MPS and NMS-excore for the NPM do not share information with the other NPMs and are isolated from them.

DCA Part 2, Tier 2, Section 21.2.3, "Shared System Interactions," states that the "shared systems that have potential for an adverse system interaction or an undesirable multimodule interaction were evaluated as summarized in Table 21-2 and Table 21-3." Table 21-3, "Shared System Interactions (Electrical and Instrumentation and Control Systems)," identifies three I&C systems that are shared across multiple NPMs: (1) the SDIS, (2) the PPS, and (3) the PCS. All three are non-safety-related I&C systems.

The NRC staff reviewed the I&C design described in the application to assure that safety-related SSCs are not shared between units in multiunit stations. The NRC staff confirmed that the I&C architecture and system design meet the regulatory requirements in Section 5.13 of IEEE Std. 603-1991 and the guidance in IEEE Std. 379-2000 with respect to the sharing of safety I&C systems among multiunit stations. Below is the evaluation of three I&C systems that are shared across multiple NPMs.

The SDIS processes data from the MPS and PPS but does not control equipment. The SDIS consists of two redundant hubs that provide display of PAM variables. An SDIS hub isolation is achieved by utilizing fiber optic cables and ports to assure the one-way direction of network data traffic. The SDIS is designed to meet the single-failure requirements such that the system continues to perform its functions in the event of a single failure. Certain component failures may affect the SDIS displays for MPS or PPS data for up to 12 NPMs and may include PCS displays depending on the failure mode, but the MPS and PPS data on the other division are unaffected. A loss of SDIS does not adversely affect safety-related NPM functions and is not a unique initiating event. The SDIS is available for 72 hours in DBEs, including a station blackout. If a total failure of the SDIS occurs, plant monitoring and control remain available from the MCR via the MCS and process control system displays. The NRC staff's evaluation of the shared SDIS to support the operator needs for each of the shared units is described in Section 7.2.13 of this report.

The PPS consists of two independent and redundant divisions and is designed to perform its function given a single failure. A single failure in one division will not interfere with the proper operation of the redundant PPS division. There are no connections between the PPS and NPM safety systems. A failure in the PPS does not result in a DBE and does not adversely affect safety-related NPM functions.

The systems controlled by the PCS are considered for failure in the scope of the safety analysis and affect areas such as the ultimate heat sink, which are controlled by plant technical specifications. The PCS does not directly affect the NPMs or have module-level portions, which are controlled by the module control system (separately considered for failure). Therefore, the NRC staff finds that a failure in the PCS would not directly affect the NPMs and result in a new DBE.

The PCS failure modes and effects analysis includes an analysis of internal PCS modes and failure modes represented by various SSCs that make up the described segment of the PCS and the effects of those failures on the NuScale power plant. The PCS does not interface directly with safety-related actuators, and PCS component failures do not adversely impact safety-related functions. Simultaneous failure of both PCS segment controllers (primary and secondary) is considered to be a CCF that results in the loss of the entire segment for the process. For certain worst-case segment failures, this could possibly result in the automatic shutdown of multiple NPMs but does not affect any safety-related NPM functions. The NRC staff's evaluation of the PCS segmentation is described in Section 7.0.4.3.2 of this report. The NRC staff's evaluation of the PCS redundancy is described in Section 7.1.3 of this report.

The NRC staff finds that the DBEs occurring in one module do not impair the ability of the I&C systems in another module to perform their required safety functions. The NRC staff confirmed that provisions are included in the SDIS, PPS, and PCS design to assure that single failures or transients within the I&C safety systems of one unit will not adversely affect or propagate to another unit and thereby prevent the shared systems from performing the safety functions credited for the other unit.

The evaluation of independence and redundancy is described in Section 7.1.2 and Section 7.1.3 of this report, respectively. The NRC staff finds that a single failure or transient within a

safety-related I&C system of one NPM does not adversely affect or propagate to another NPM. The safety-related I&C systems are module specific, and no safety systems share functions across multiple NPMs.

Electrical Power of the NuScale Power Modules

DCA Part 2, Tier 2, Section 7.2.11, states that the electrical power provided by the module-specific EDSS is not shared between NPMs. The common portion of the EDSS provides electrical power to shared plant SSCs and is evaluated in Section 8.3 of this report. Class 1E isolation is provided between the EDSS and MPS, and the isolation devices are classified as part of the safety system. Cross-tie capabilities between NPMs are not provided in the EDSS design.

The NRC staff confirmed that any proposed contingency or emergency plans for temporary sharing of systems (such as electrical power cross-ties) will not adversely affect the capability of the I&C safety systems to perform their safety functions.

7.2.11.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.11.6 Conclusions

The NRC staff finds that the application provided sufficient information to demonstrate that sharing of the SSCs, including I&C systems among multiple units will not impair performance of the credited safety functions in any unit. The NRC staff reviewed the application against ASAI 35 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets ASAI 35. On this basis, the NRC staff concludes that the design of I&C systems satisfies the guidance in IEEE Std. 379-2000 and the requirements of Section 5.13 of IEEE Std. 603-1991 and GDC 5 of Appendix A to 10 CFR Part 50.

7.2.12 Automatic and Manual Control

7.2.12.1 Introduction

This section addresses the review of automatic and manual initiation of protective actions to assure that the I&C safety systems automatically initiate and execute protective action for the range of conditions and performance specified in the safety analysis. In addition, the review of manual controls confirms that the controls will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary.

The NRC staff's evaluation includes coordinating with the organization responsible for the review of human factors to confirm that the functions controlled and the characteristics of the controls allow plant operators to take appropriate manual actions.

7.2.12.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.12, "Automatic and Manual Control."

DCA Part 2, Tier 2, Section 7.2.12, describes the means by which the automatic and manual features accomplish reactor trip and ESF actuation functions necessary to shut down and maintain the reactor in a safe condition.

DCA Part 2, Tier 2, Section 7.2.12, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.2.12, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 38 and 39, which relate to automatic and manual control, is described in Section 7.1.6 of this report.

TR-1015-18653, Sections 2.5.1, "Safety Function Module," and 2.5.4, "Equipment Interface Module," describe the HIPS platform design features to meet the automatic control requirements of IEEE Std. 603-1991, Sections 6.1 and 7.1.

TR-1015-18653, Sections 2.5.5, "Hard-Wired Module," and 4.5, "Hard-Wired Module," describe the HIPS platform design features to meet the manual control requirements of IEEE Std. 603-1991, Sections 6.2 and 7.2.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.12, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 8 through 13. The evaluation of the ITAAC is in Section 14.3.5 of this report.

Technical Specifications: The technical specifications associated with DCA Part 2, Tier 2, Section 7.2.12, are given in DCA Part 2, Tier 2, Chapter 16. Specifically, Technical Specifications, Section 3.3.1, 3.3.2, 3.3.3, 3.3.4, B.3.3.1, B.3.3.2, B.3.3.3, and B.3.3.4 address I&C automatic and manual actuation functions.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.12.

7.2.12.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Sections 6.1 and 7.1, "Automatic Control," and Sections 6.2 and 7.2, "Manual Control." Sections 6.1 and 7.1 provide requirements for the automatic initiation and control of all protective actions for both sense and command features as well as execute features. Section 6.2 requires, in part, that means be provided to manually initiate protective system actuation at the division level, with a minimal number of discrete operator manipulations. Similarly, Section 7.2 requires, in part, that any additional design features in the execute features necessary to accomplish manual controls shall not defeat single-failure protection and will support the capability of other safety-related manual controls.

The guidance in DSRS Section 7.2.12 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS sections. In addition, the following guidance document provides acceptance criteria that confirm that the above requirements have been adequately addressed:

- The I&C components and systems should conform to RG 1.62, Revision 1.

7.2.12.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed Section 7.2.12 of DCA Part 2, Tier 2 and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference address the required information relating to automatic and manual control. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.12.3 and to address ASAIs 38 and 39, which relate to automatic and manual control and that are discussed in greater detail in Section 7.1.6 of this report.

7.2.12.4.1 Automatic Control

The NRC staff determined that TR-1015-18653, Sections 3.6.3.1 and 3.6.4.1, along with the NuScale design demonstrating compliance with ASAI 38, provides reasonable assurance that Sections 6.1 and 7.1 of IEEE Std. 603-1991 are met.

Section 7.2.12.1 of DCA Part 2, Tier 2 states that the MPS automatically initiates the protective actions necessary to mitigate the effects of the DBEs identified in Table 7.1-1. The variables monitored by the MPS to initiate safety-related functions are identified in Table 7.1-2. The safety-related reactor trip and ESFAS functions of the MPS are listed in Table 7.1-3 and Table 7.1-4, respectively. The NRC staff finds that the I&C design provides the capability to automatically initiate and control all protective actions and provide information sufficient to confirm that the performance specifications are met. The staff also finds that the evaluation of the precision of the safety system is addressed to the extent that the setpoints, margins, errors, and response times factored into the analysis (as evaluated in Section 7.2.7 of this report) meet the requirements of Section 4.4 of IEEE Std. 603-1991.

The NRC staff also determined in the evaluation of TR-1015-18653, Section 3.5, and as described and evaluated in Section 7.1.4.4 of this report, that the NuScale design accounts for the response times for all I&C timing delays involved in an instrument channel from sensor to final actuation device, thus adequately addressing the fundamental design principle of predictability and repeatability.

7.2.12.4.2 Manual Control

In its evaluation, the NRC staff determined that TR-1015-18653, Sections 3.6.3.2 and 3.6.4.2, along with the NuScale design demonstrating compliance with ASAI 39, provides reasonable assurance that Sections 6.2 and 7.2 of IEEE Std. 603-1991 are met.

DCA Part 2, Tier 2, Section 7.2.12.2, states that the MPS conforms to RG 1.62, Revision 1, and is designed to manually initiate the protective actions listed in Table 7.1-4 at the divisional level. All protective actions have automatic controls; therefore, Section 4.5 of IEEE Std. 603-1991 is not applicable, and all hard-wired manual actuation switches input are downstream of the digital components within the MPS. Therefore, failure of the MPS automatic function does not prevent the manual initiation of the required protective action. In addition, a Division I and Division II set of manual switches are provided for manual initiation of protective actions and are connected to the HWM of the corresponding RTS and ESFAS division. Therefore, the manual control of the actuated component meets the single-failure criterion requirement.

The HFE program is evaluated in Chapter 18 of this report.

The NRC staff has evaluated that all manual controls have power available and that the equipment is appropriately qualified as evaluated in Section 7.2.3 of this report.

The I&C design describes that, if enabled by the operator using the enable nonsafety control switch, the capability for manual component-level control of ESF equipment is possible through discrete hard-wired inputs from the MCS to the HWM. These signals are then input to the APL circuit on the EIM. Any automatic or manual safety-related signal will override the non-safety-related signal and is prioritized within the APL. For beyond-DBEs and for some actuated equipment, a safety-related override switch can be used to prioritize a non-safety-related signal over an automatic signal.

7.2.12.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.12.6 Conclusions

The NRC staff concludes that the I&C design provides information sufficient to (1) demonstrate that I&C systems provide the capability to automatically initiate and control all protective actions for the range of conditions and performance specified in the safety analyses and (2) demonstrate that manual controls will be functional, accessible within the time constraints of operator responses, and available during plant conditions under which manual actions may be necessary. The NRC staff reviewed the application against ASAIs 38 and 39 in TR-1015-18653, Revision 2. The staff concludes that the NuScale I&C design meets the ASAI 38 and 39, as described in Section 7.1.6 of this report. On this basis, the staff finds that the design of I&C systems satisfies the manual control guidance in RG 1.62, Revision 1, and the automatic and manual control requirements in Sections 6.1, 6.2, 7.1, and 7.2 of IEEE Std. 603-1991.

7.2.13 Displays and Monitoring

7.2.13.1 Introduction

This section addresses the review of the display and monitoring systems, which provide information for (1) the safe operation of the plant during normal operation, AOOs, and PAs, (2) supporting manual initiation and control of safety systems, (3) the normal status and the bypassed and inoperable status of safety systems, and (4) satisfying the requirements of 10 CFR 50.34(f), which are sometimes identified as Three Mile Island (TMI) action plan items.

7.2.13.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 2.5.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Sections 7.0.4.4, “Safety Display and Indication System,” and 7.2.13, “Displays and Monitoring.”

The SDIS provides HSI for the MPS and PPS to monitor and display PAM variables and provides the capability for control inputs and status information.

DCA Part 2, Tier 2, Section 7.2.13, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.2.13, in addition to text from

the referenced TR-1015-18653. The disposition of ASAIs 27, 28, 29, and 30, which relate to displays and monitoring, is described in Section 7.1.6 of this report.

TR-1015-18653, Sections 2.5.2, "Bypass or Trip Operation," and 4.7, "Monitoring and Indication," describe the internal HIPS platform signal processing and bypass features to meet the requirements of IEEE Std. 603-1991, Section 5.8.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.13, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Items 22 through 25. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.13.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.13.

7.2.13.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.8, "Information Displays." Section 5.8 provides requirements for displays used for manually controlled actions, system status indication, including indication of bypasses, and location of information displays.

- 10 CFR 50.34(f)(2)(iv) requires a plant safety parameter display console that will show operators a minimum set of parameters defining the safety status of the plant, will be capable of displaying a full range of important plant parameters and data trends on demand, and will be capable of indicating when process limits are being approached or exceeded.

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

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

- 10 CFR 50.34(f)(2)(xii) requires, in part, that AFWS flow indication be provided in the control room.

- 10 CFR 50.34(f)(2)(xvii) requires instrumentation in the control room to measure, record, and read out (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential accident release points. Instrumentation must provide for continuous sampling of radioactive iodine and particulates in gaseous effluents from all potential accident release points and for onsite capability to analyze and measure these samples.

- 10 CFR 50.34(f)(2)(xviii) requires, in part, that instruments be provided in the control room to provide an unambiguous indication of inadequate core cooling, such as primary coolant saturation meters in PWRs, and a suitable combination of signals

from indicators of coolant level in the reactor vessel and in-core thermocouples in PWRs.

- 10 CFR 50.34(f)(2)(xix) requires instrumentation adequate for use in monitoring plant conditions following an accident that includes core damage.

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

- 10 CFR Part 50, Appendix A, GDC 13.

- 10 CFR Part 50, Appendix A, GDC 19.

The guidance in DSRS Section 7.2.13 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- RG 1.97, Revision 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," endorses IEEE Std. 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," with identified exceptions and clarifications.

- RG 1.47, Revision 1.

- The SRM on SECY-93-087, Item II.T, "Control Room Annunciator Alarm Reliability," provides general guidance on the alarm system interface with operator workstations.

7.2.13.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.13, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference address the required information relating to displays and monitoring. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.13.3 and to address ASAIs 27, 28, 29, and 30, which relate to displays and monitoring and that are discussed in greater detail in Section 7.1.6 of this report

7.2.13.4.1 Compliance with IEEE Std. 603-1991, Section 5.8.1

In its evaluation, the NRC staff determined that TR-1015-18653, Section 3.6.2.8.1, along with the NuScale design demonstrating compliance with ASAI 27, provides reasonable assurance that Section 5.8.1, "Displays for Manually Controlled Actions," of IEEE Std. 603-1991 is met. DCA Part 2, Tier 2, Section 7.1.1.2.1, states, "All required protective actions by the MPS are automatic. There are no credited manual actuations required for the MPS to accomplish its safety functions." DCA Part 2, Tier 2, Table 7.1-7, "Summary of Type A, B, C, D, and E

Variables," and DCA Part 2, Tier 2, Section 7.2.13.1, states, "There are no credited manual actions required to mitigate DBEs, and there are no Type A post-accident monitoring variables. There are no safety-related information displays in the MCR."

Based on the above, the NRC staff has reasonable assurance that the I&C systems demonstrate compliance with ASAI 27, as described in Section 7.1.6 of this report, and with the requirements of Section 5.8.1 of IEEE Std. 603-1991.

7.2.13.4.2 Compliance with IEEE Std. 603-1991, Section 5.8.2

In its evaluation, the NRC staff determined that TR-1015-18653, Section 3.6.2.8.2, along with the NuScale design demonstrating compliance with ASAI 28, provides reasonable assurance that Section 5.8.2, "System Status Indication," of IEEE Std. 603-1991 is met.

(1) Identification of Main Control Room Indications

In Chapter 18 of this report, the NRC staff evaluated whether the MCR indications required by 10 CFR 50.34(f)(2) are included in the application's MCR design and confirmed that the applicant's task analysis, in part, identifies all controls, alarms, and displays needed in the MCR to manage the plant safety functions.

(2) Identification of Remote Shutdown Station Indications

DCA Part 2, Tier 2, Section 7.2.13.3, states that there is an identical set of MCS and PCS displays in the RSS provided for the operator to monitor the plant operation if evacuation of the MCR is required. SDIS displays are not provided in the RSS, as there is no manual control of safety-related equipment allowed from the RSS. In DCA Part 2, Tier 2, Section 7.2.12.2, and Figure 7.1-1j reflect that an alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches in the RSS.

(3) Identification of Accident Monitoring Variables

As indicated in Section 7.2.13.4.1 above, there are no PAM Type A variables for the NuScale design. DCA Part 2, Tier 2, Table 7.1-7, provides a list of Type B, C, D, and E variables. DCA Part 2, Tier 2, Section 7.1.1.2.2, provides the approach and basis for the development of the PAM variable selections, which are maintained in Table 7.1-7.

DCA Part 2, Tier 2, Section 7.1.1.2.2, states that the PAM instrumentation includes the required functions, range, and accuracy for each variable monitored. The selection of each type of variable follows the guidance in Section 4 of IEEE Std. 497-2002, as modified by RG 1.97, Revision 4.

The NRC staff verified that Type B, C, D, and E variables conform to the performance, design, and qualification criteria in Sections 5 through 9 of IEEE Std. 497-2002, as modified by RG 1.97, Revision 4.

In addition to the guidance in IEEE Std. 497-2002, the following attributes should also be reviewed:

- The ranges for radiation instrumentation are evaluated in Chapters 11 and 12 of this report.

- To the extent practicable, the same instruments should be used for accident monitoring as are used for normal operations of the plant. This is evaluated in Chapter 18 of this report.

- Accident monitoring equipment identified as Type B or C is environmentally qualified as required by 10 CFR 50.49 and seismically qualified in accordance with RG 1.100, Revision 3, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants," and is evaluated in Sections 3.10, 3.11, and 7.2.2 of this report.

The regulation in 10 CFR 50.34(f)(2)(xix) requires instrumentation for use in monitoring plant conditions following an accident that includes core damage. This is evaluated in Section 7.2.13.4.6 of this report.

The NRC staff coordinated the review with the organization responsible for reviewing PRA and severe accidents in identifying the necessary instrumentation. The staff considered the following attributes:

- The variables monitored and the range and accuracy of instrumentation provided to monitor these variables should comply with the severe accident analysis submitted pursuant to 10 CFR 52.47(a)(23).

- The instrumentation provided for monitoring severe accident conditions should be designed to operate in the severe accident environment for which it is intended and over the time span for which it is needed.

- To the extent practicable, the same instruments should be used for accident monitoring as are used for normal operations of the plant. In cases in which a single display may indicate the reading of more than one instrument, the underlying purpose of this recommendation is met if the same variable and same display are used for accident monitoring even though the sensors providing the signal are different.

The NRC staff has reasonable assurance that the system status indications in the MCR and RSS demonstrate compliance with ASAI 28, as described in Section 7.1.6 of this report, and to the requirements of Section 5.8.2 of IEEE Std. 603-1991.

7.2.13.4.3 Compliance with IEEE Std. 603-1991, Section 5.8.3

In its evaluation, the NRC staff determined that TR-1015-18653, Section 3.6.2.8.3, along with the NuScale design demonstrating compliance with ASAI 29, provides reasonable assurance that Section 5.8.3, "Indication of Bypasses," of IEEE Std. 603-1991 is met.

DCA Part 2, Tier 2, Section 7.2.4.4.1, evaluates how the HIPS platform bypass status information is used to automatically actuate the bypass indication for bypassed or inoperable conditions, when required. Additionally, DCA Part 2, Tier 2, Section 7.2.13.4, states that the capability to manually activate the bypass indication in the control room is provided by the MCS.

The NRC staff has reasonable assurance that the indication of bypasses in the NuScale I&C systems demonstrate compliance with ASAI 29, as described in Section 7.1.6 of this report, and with the requirements of Section 5.8.3 of IEEE Std. 603-1991.

7.2.13.4.4 Compliance with IEEE Std. 603-1991, Section 5.8.4

In its evaluation, the NRC staff determined that TR-1015-18653, Section 3.6.2.8.4, along with the NuScale design demonstrating compliance with ASAI 30, provides reasonable assurance that Section 5.8.4, “Location,” of IEEE Std. 603-1991 is met.

DCA Part 2, Tier 2, Section 7.2.13.2, states that the SDIS displays are in a separate location in the MCR from those used during normal plant operations. The SDIS displays the PAM variables to the operator during both normal plant operation and postaccident conditions. DCA Part 2, Tier 2, Section 7.2.12.2, states that the MPS provides outputs of monitored variables to two redundant divisions of the MCR SDIS displays for accident monitoring and to aid in manual operations. MCS HSI displays in the MCR are also used to support manual controls.

The NRC staff has reasonable assurance that the location of indications in the NuScale I&C systems demonstrate compliance with ASAI 30, as described in Section 7.1.6 of this report, and with the requirements of Section 5.8.4 of IEEE Std. 603-1991.

7.2.13.4.5 Annunciator Systems

DCA Part 2, Tier 2, Section 7.2.13.2, states that status information is non-safety-related related. As such, it is transmitted to the MCR for indication and recording from the MPS using the SDIS and MCS. The PPS uses the PCS in conjunction with the SDIS. Four types of MPS and PPS status information are provided: (1) process variable values and setpoints, (2) logic status, (3) equipment status, and (4) actuation device status.

The operator is alerted to deviations from normal operating conditions using any combination of these four variable types through the use of alarms and annunciators. The task analysis process that was used to identify the controls, alarms, and displays needed in the MCR to manage the plant safety functions and remote shutdown capability are evaluated in Section 18.7.2 of this report.

The SRM to SECY-93-087, Item II.T, identifies the following three design concepts:

(1) Hierarchical access to alarms—The HFE design principles are described in NUREG-0700, “Human System Interface Design Review Guidelines,” Revision 2, and is evaluated in Section 18.7 of this report. No additional reviews of this concept are needed as part of the Chapter 7 SER.

(2) Isolation of the non-safety alarm system - DCA Part 2, Tier 2, Section 7.0.2, states that the SDIS is classified as non-safety-related related; therefore, the SDIS must be isolated from interfacing Class 1E circuits. The requirement for electrical independence to comply with IEEE Std. 603-1991, Section 5.6, is evaluated in Section 7.1.2.4.2 of this report.

(3) Alarms for manually controlled actions - As shown in Section 7.2.13.4.1 above, there are no PAM Type A variables for the NuScale design and all required protective actions by the MPS are automatic.

The NRC staff finds that the NuScale annunciator system design is consistent with a the SRM to SECY-93-087, Item II.T.

7.2.13.4.6 Three Mile Island Action Items

The TMI action plan items for I&C systems important to safety are evaluated below:

- 10 CFR 50.34(f)(2)(iv), “Plant Safety Parameter Display Console” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the SDIS complies with 10 CFR 50.34(f)(2)(iv) by providing the capability to display the Type B and Type C variables identified in Table 7.1-7 over anticipated ranges for normal operation, for AOOs, and for PA conditions.

- 10 CFR 50.34(f)(2)(v), “Bypass and Inoperable Status Indication” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the bypassed and operable status indication of safety interlocks is automatically provided in the control room and satisfies the requirements of 10 CFR 50.34(f)(2)(v) and RG 1.47.

- 10 CFR 50.34(f)(2)(xi), “Direct Indication of Relief and Safety Valve Position” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the reactor safety valve position indication is processed by the MPS and then sent to the SDIS and the MCS for display in the MCR. The reactor safety valve position indication is seismically qualified to seismic Category I requirements and meets the requirements of 10 CFR 50.34(f)(2)(xi).

- 10 CFR 50.34(f)(2)(xii), “AFWS Automatic Initiation and Flow Indication” – DCA Part 2, Tier 2, Section 7.1.1.1, states that 10 CFR 50.34(f)(2)(xii) is not applicable to the NuScale design, as evaluated in Section 1.9 of this report and shown in Table 1.9-5.

- 10 CFR 50.34(f)(2)(xvii), “Accident Monitoring Instrumentation” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the SDIS provides the capability to monitor containment pressure, containment water level, and the reactor containment atmosphere for radioactivity released from PAs. The MCS provides the recording function for the containment parameters. Consistent with 10 CFR 50.34(f)(2)(xvii)(c) and 10 CFR 50.44(c)(4), the process sampling system includes oxygen and hydrogen analyzers to monitor the containment environment and is evaluated in Section 6.2.5 of this report. These monitors are non-safety-related instruments that continuously monitor oxygen and hydrogen concentrations in containment during operation and are capable of monitoring during beyond-design-basis conditions. Consistent with 10 CFR 50.34(f)(2)(xvii)(E), the PCS displays and records in the MCR information on noble gas effluent release points for the NuScale plant.

- 10 CFR 50.34(f)(2)(xviii), “Instrumentation for the Detection of Inadequate Core Cooling” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the following variables satisfy the requirements of 10 CFR 50.34(f)(2)(xviii): core exit temperatures, wide-range reactor coolant system pressure, degrees of subcooling, wide-range reactor coolant system hot temperature, RPV water level, and containment water level.

- 10 CFR 50.34(f)(2)(xix), “Instruments for Monitoring Plant Conditions Following Core Damage” – DCA Part 2, Tier 2, Section 7.2.13.6, states that the MCR indication is provided to measure, record, and read out containment pressure, containment water level, and noble gas effluents at the potential accident release points to satisfy the requirements of 10 CFR 50.34(f)(2)(xix).

- Exemption from 10 CFR 50.34(f)(2)(xx), “Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves” – In 10 CFR 50.34(f)(2)(xx), the NRC specifies power provisions for pressurizer relief valves, block valves, and level indicators. In DCA Part 2, Tier 2, Table 1.9-5 and Section 7.1.1.1 state that 10 CFR 50.34(f)(2)(xx) is not applicable to the NuScale design. Part 7 of the DCA discusses the exemption to 10 CFR 50.34(f)(2)(xx). The NuScale design does not rely on pressurizer level indication to achieve and maintain natural circulation in a loss of electrical power condition. In the NuScale power plant design, following the loss of electrical power, the passive DHRS is able to achieve and maintain natural circulation

cooling of the RCS without electrical power. Specifically, natural circulation cooling is achieved and maintained without reliance on pressurizer level indication. Therefore, the NRC staff finds that the pressurizer level instrumentation is not necessary to maintain natural circulation cooling. DCA Part 2, Tier 2, Section 7.2.13.6, states that the pressurizer level indication is powered with highly reliable dc power from the EDSS rather than Class 1E power. Based on the staff's evaluation in Section 5.4.6 of this report, the staff finds that Class 1E electrical power for pressurizer level indication and controls for pressurizer relief and block valves is not required.

Based on the above discussion, the NRC staff finds that the NuScale design meets the requirements of 10 CFR 50.34(f)(2).

7.2.13.4.7 Other Information Systems

DCA Part 2, Tier 2, Section 7.2.13.7, states that the MCS and PCS provide monitoring data via one-way communication interfaces to the plant network, which provides data recording, trending, and historical retention that can be called up by the emergency operations facility stations and technical support center (TSC) engineering workstations. The plant network provides the required plant data to offsite emergency response facilities; the TSC is located separately from the operator workstations in the MCR. The adequacy of the independence of these systems is reviewed and evaluated in Section 7.1.2.4.3 of this report. Functional performance and other design aspects of the TSC and the offsite emergency operations facility are the subject of other chapters of the application and are not reviewed in connection with Chapter 7.

7.2.13.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.13.6 Conclusions

Based on the discussion above, the NRC staff finds that the application provides information sufficient to (1) demonstrate that I&C display and monitoring systems provide the necessary information for the safe operation of the plant during normal operation, AOOs, and PAs as described in the safety analyses, (2) demonstrate that I&C displays and monitoring systems will provide the necessary information for manual initiation and control of safety systems, and (3) provide normal status and the bypassed and inoperable status of safety systems. The NRC staff reviewed the application against ASAIs 27, 28, 29, and 30 listed in TR-1015-18653, Revision 2. The NRC staff concludes that the I&C design meets these ASAIs. On this basis, the NRC staff finds that the design of I&C display and monitoring systems satisfies the reliability, availability, and accuracy guidance in RG 1.47, Revision 1, and RG 1.97, Revision 4, and the requirements of 10 CFR Part 50, Appendix A, GDC 13, GDC 19, and IEEE Std. 603-1991, Section 5.8.

7.2.14 Human Factors Considerations

7.2.14.1 Introduction

This section addresses the review of the HFE principles and criteria applied to the selection and design of the displays and controls. Human performance design objectives should be described and related to the plant safety criteria. Recognized human factors standards should be employed to support the described human performance design objectives. The adequacy of the human factors aspects of the control room design and the appropriate application of human

factors principles should be confirmed with the organization responsible for reviewing Chapter 18 of the application.

7.2.14.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Section 3.15, "Human Factors Engineering."

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.14, "Human Factors Considerations," which is summarized in the following discussion.

DCA Part 2, Tier 2, Section 7.2.14, incorporates by reference TR-1015-18653, Revision 2. The applicant provided DCA application-specific information in Section 7.2.14, in addition to text from the referenced TR-1015-18653, consisting of the human factors considerations for the MPS, PPS, and SDIS. The disposition of ASAI 36, which relates to human factors considerations, is described in Section 7.1.6 of this report.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.14, are given in DCA Tier 1, Section 2.5, Table 2.5-7, Item 26, and Section 3.15, Table 3.15-1, Items 1 and 2. The evaluation of Chapter 7 ITAAC is in Section 14.3.5 of this report. The evaluation of Chapter 18 ITAAC is in Section 14.3.9 of this report.

Technical Specifications: There are no technical specifications associated with DCA Part 2, Tier 2, Section 7.2.14.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.14.

7.2.14.3 Regulatory Basis

In 10 CFR 50.55a(h), the NRC requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Section 5.14, "Human Factors Considerations." Section 5.14 requires, in part, that human factors be considered throughout the design process.

There are no specific DSRS acceptance criteria in this section.

7.2.14.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the NRC staff reviewed and approved TR-1015-18653, Revision 2. Human factors considerations is an application-specific activity; therefore, no evaluation was done and ASAI 36 was established to confirm full compliance with this regulatory requirement in the DCA. The NRC staff reviewed DCA Part 2, Tier 2, Section 7.2.14, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information incorporated by reference in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference address the required information relating to human factors considerations. Therefore, based on the safety conclusion specified by the SE for TR-1015-18653, along with the application-specific information in DCA Part 2, Tier 2, Section 7.2.14, the NRC staff concludes that the design meets ASAI 36, which is discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.2.14.3 and ASAI 36.

NUREG-0711 provides guidance for establishing a program for the application of HFE to systems, equipment, and facilities of nuclear power generating stations. NUREG-0711 contains the review criteria referenced in SRP Chapter 18 and is evaluated in Chapter 18 of this report. No additional reviews of HFE are performed as part of Chapter 7.

7.2.14.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.14.6 Conclusions

The staff reviewed the application against ASAI 36, listed in TR-1015-18653, Revision 2. The NRC staff concludes that the NuScale I&C design meets ASAI 36.

Based on the discussion above, the NRC staff finds that the human factors considerations for the design of NuScale I&C systems satisfy the requirements in Section 5.14 of IEEE Std. 603-1991.

7.2.15 Capability for Test and Calibration

7.2.15.1 Introduction

This section addresses the review of the capability for test and calibration of the safety systems. The periodic testing consists of surveillance testing required by technical specifications, including functional tests and checks, calibration verification, and time response measurements, to verify that I&C safety systems perform their safety functions as credited in the safety analysis. The review of test and calibration provisions should be coordinated with the organization responsible for reviewing technical specifications.

7.2.15.2 Summary of Application

DCA Part 2, Tier 1: DCA Part 2, Tier 1 information associated with this section is found in DCA Part 2, Tier 1, Sections 2.5 and 2.6.

DCA Part 2, Tier 2: DCA Part 2, Tier 2 information associated with this section is found in DCA Part 2, Tier 2, Section 7.2.15, "Capability for Test and Calibration."

DCA Part 2, Tier 2, Section 7.2.15, incorporates by reference TR-1015-18653, Revision 2. The applicant provides DCA application-specific information in Section 7.2.15, in addition to text from the referenced TR-1015-18653. The disposition of ASAIs 4, 24, 25, 26, 32, 47, 49, 50, and 51, which relate to the capability of test and calibration, is described in Section 7.1.6 of this report.

TR-1015-18653, Section 8.0, "Testing and Diagnostics," describes the calibration and testing of the HIPS platform to meet the capability for test and calibration requirements of IEEE Std. 603-1991, Sections 5.7 and 6.5.

ITAAC: The ITAAC associated with DCA Part 2, Tier 2, Section 7.2.15, are given in DCA Part 2, Tier 1, Section 2.5, Table 2.5-7, Item 24. The evaluation of ITAAC is in Section 14.3.5 of this report.

Technical Specifications: The technical specifications associated with DCA Tier 2, Section 7.2.15, are given in DCA Part 2, Tier 2, Chapter 16, "Technical Specifications." Specifically, Technical Specifications, Section 3.3.1, 3.3.2, 3.3.3, 3.3.4, B.3.3.1, B.3.3.2, B.3.3.3, and B.3.3.4 address test and calibration.

Technical Reports: There are no technical reports associated with DCA Part 2, Tier 2, Section 7.2.15.

7.2.15.3 Regulatory Basis

The following NRC regulations contain the relevant requirements for this review:

- 10 CFR 50.55a(h) requires compliance with IEEE Std. 603-1991 including the correction sheet, dated January 30, 1995, which is incorporated by reference in 10 CFR 50.55a(a)(2). This standard includes Sections 5.7 and 6.5, "Capability for Test and Calibration." These sections require the capability for test and calibration of safety system equipment, while retaining the capability of the safety systems to accomplish their safety functions.

- 10 CFR 50.36(c)(3) states that surveillance requirements relate to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within SLs, and that LCOs will be met.

- 10 CFR Part 50, Appendix A, GDC 21.

The guidance in DSRS Section 7.2.15 lists the acceptance criteria adequate to meet the above requirements, as well as review interfaces with other DSRS sections. In addition, the following guidance documents provide acceptance criteria that confirm that the above requirements have been adequately addressed:

- Digital I&C safety systems and components should conform to the guidance related to capability for test and calibration in Sections 5.7, 5.5.2, and 5.5.3 of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3.

- The design should conform to the guidance of RG 1.22, Revision 0.

- I&C components and systems should conform to RG 1.118, Revision 3, which endorses IEEE Std. 338-1987.

7.2.15.4 Technical Evaluation

As documented in the NRC staff's evaluation of the HIPS platform (ADAMS Accession No. ML17116A097), the staff reviewed and approved TR-1015-18653, Revision 2. The staff reviewed DCA Part 2, Tier 2, Section 7.2.15, and checked the referenced TR-1015-18653 to assure that the combination of the information in TR-1015-18653 and the information incorporated by reference in the DCA appropriately represents the complete scope of information relating to this review topic. The NRC staff's review confirmed that the information in the application and the information incorporated by reference in the application address the required information relating to the capability for test and calibration. The following describes the NRC staff's evaluation of the information provided by the applicant to satisfy the regulations in SE Section 7.2.15.3 and to address aspects of ASAIs 14, 24, 25, 26, 32, 47, 49, 50, and 51 that relate to capability for test and calibration. These ASAIs are discussed in greater detail in Section 7.1.6 of this report.

The following contains the NRC staff's evaluation of the information provided by the applicant against the regulations in SE Section 7.2.15.3 and ASAIs cited above.

DCA Part 2, Tier 2, Section 7.2.15, states the following:

> *The testing and calibration functions of the MPS and NMS are designed to meet Sections 5.7 and 6.5 of IEEE Std. 603-1991, Section 5.7 of IEEE Std. 7-4.3.2-2003, and conform to the guidance in RG 1.22, Revision 0, RG 1.118, Revision 3, and RG 1.47, Revision 1.*
>
> *The information in this section satisfies the application specific information requirements in TR-1015-18653-P-A listed in Table 7.0-2 for ASAI numbers 14, 24, 25, 26, 32, 47, 49, 50, and 51.*

DCA Part 2, Tier 2, Section 7.2.15.2, describes how the I&C system design supports the types of testing required by the technical specifications. Section 7.2.15.1 states the following:

> *The MPS and NMS are designed with the capability for calibration and surveillance testing, including channel checks, calibration verification, and time response measurements, as required by the technical specifications to verify that I&C safety systems perform required safety functions.*

The system design supports the compensatory actions required by technical specifications when LCOs are not met. The design allows for tripping or bypass of individual functions in each safety system channel. Operating and maintenance bypasses is evaluated in Section 7.2.4 of this report.

According to the DSRS, the extent of test and calibration capability provided bears heavily on whether the design meets the single-failure criterion. Any failure that is not detectable must be considered concurrently with any random postulated, detectable single failure. The single-failure criterion for the NuScale I&C design is evaluated in Section 7.1.3 of this report.

DCA Part 2, Tier 2, Section 7.2.15, describes how the periodic testing duplicates, as closely as practical, the overall performance of the safety system credited in the safety analysis. The tests confirm operability of both the automatic and manual circuitry. DCA Part 2, Tier 2, Section 7.2.15.2 states, "The MPS and NMS allow SSCs to be tested while retaining the capability to accomplish required safety functions." DCA Part 2, Tier 2, Section 7.2.15, explains that the testing from the sensor inputs of the MPS through to the actuated equipment is accomplished through a series of overlapping sequential tests. Most of the testing may be accomplished during power operation. However, the APL circuit on the EIM of the MPS, the manual switches in the MCR, and the non-safety-related controls that provide input to the APL cannot be tested at power. Where testing the equipment could potentially affect plant operation or damage equipment, provisions are made to test the equipment when the NPM is shut down. The APL consists of discrete components and directly causes actuation of field components that cause the reactor to shut down or adversely affect operation. The APL is a very simple circuit and has acceptable reliability to be tested when the reactor is shut down. The manual trip and actuate switches in the MCR cannot be tested at power and require an outage. These switches are standby, low-demand components such that testing during every refueling outage is acceptable to maintain sufficient system reliability. Also, test procedures do not involve disconnecting wires or installation of jumpers for at-power testing.

DCA Part 2, Tier 2, Section 7.2.15.2, states that the MPS provides a means for checking the operational availability of the sense and command feature input sensors relied on for a safety function during reactor operation. The following methods are used to achieve this:

- perturbing the monitored variable;
- cross-checking between channels that have a known relationship (i.e., channel check); and
- introducing and varying a substitute input to the sensor.

The NRC staff confirmed that the applicable provisions in IEEE Std. 7-4.3.2-2003 and the guidance stated below are addressed as shown in DCA Part 2, Tier 2, Section 7.2.15. The test and calibration functions do not adversely affect the ability of the computer to perform its safety function, consistent with Section 5.5.2 of IEEE Std. 7-4.3.2-2003.

The NRC staff confirmed that the use of self-diagnostics does not replace the capability for test and calibration as required by Sections 5.7 and 6.5 of IEEE Std. 603-1991. Diagnostic data for the separation group and division of the MPS are provided to the MWS of the division. The MWS is located close to the equipment to facilitate troubleshooting activities. The interface between the MPS gateway and the MWS is an optically isolated, one-way diagnostic interface. Diagnostics data are communicated via the MIB. This is a physically separate communications path from the safety data path, ensuring that the diagnostics functionality is independent of the safety functionality. Further evaluation of how the MWS avoids having an adverse influence on the MPS's performance of its safety functions can be found in Section 7.1.2 of this report.

The amount of resources (e.g., cycle time, processing capacity) assigned to self-supervision should be appropriately balanced to assure that the safety function and performance of the I&C systems are not affected. This was evaluated in the NRC staff's SE of TR-1015-18653.

The MPS is an FPGA-based system. Traditional watchdog timers do not provide the same protection for FPGA-based systems as they do in microprocessor-based systems. The MPS addresses the need for aliveness via the self-testing features of the MPS modules (e.g., SFM). Examples of these features include the use of BIST in the FPGA logic and CRC checks (as described in Section 8 of the reviewed and approved TR-1015-18653), and other tests in each type of module (as appropriate) that verify their normal operation.

The NRC staff's evaluation of the Technical Specification Surveillance Requirements associated with the Module Protection System, Reactor Trip System Logic and Actuation, and Engineered Safety Features Actuation System Logic and Actuation are evaluated in Chapter 16 of this report.

7.2.15.5 COL Information Items

There are no COL information items listed in DCA Part 2, Tier 2, Table 1.8-2, for this area of review.

7.2.15.6 Conclusions

Based on its review of the information provided in DCA Part 2, Tier 2, Section 7.2.15, the NRC staff concludes that the application provides information sufficient to (1) demonstrate that I&C components and systems are capable of being tested and calibrated while retaining their capability to accomplish their safety functions, both manually and automatically, (2) demonstrate that, for digital-based I&C systems, test and calibration functions (including any self-diagnostic functions) do not adversely affect the ability of the computer to perform its safety function, (3) demonstrate that, for designs using RTDs, appropriate analyses are included in the application for cross-calibration of RTDs. The NRC staff reviewed the application against ASAIs 14, 24, 25, 26, 32, 47, 49, 50, and 51 listed in TR-1015-18653, Revision 2. The NRC

staff concludes that the NuScale I&C design satisfies the aspects of ASAIs 14, 24, 25, 26, 32, 47, 49, 50, and 51 that relate to capability for test and calibration, and that are discussed in greater detail in Section 7.1.6 of this report. On this basis, the NRC staff concludes that the design of I&C systems satisfies the guidance related to capability for test and calibration in Sections 5.5.2 and 5.5.3 of IEEE Std. 7-4.3.2-2003; the guidance in RG 1.22, Revision 0, and RG 1.118, Revision 3; and the requirements in GDC 21 of Appendix A to 10 CFR Part 50 and IEEE Std. 603-1991, Section 5.7.