Chapter 7 Instrumentation and Control Systems

7.1 Introduction

This chapter presents specific detailed design and performance information for the Instrumentation and Control (I&C) systems that are significant for plant operation and that are used throughout the plant. I&C Distributed Control and Information Systems (DCIS) are designated as either Safety-related DCIS (Q-DCIS) or Nonsafety-related DCIS (N-DCIS). A description of the system of classification is found in Section 3.2. The following subsections, tables, and figures provide a synopsis of the DCIS.

- Subsection 7.1.1 contains a brief description of the DCIS.
- Subsection 7.1.2 summarizes the Q-DCIS.
- Subsection 7.1.3 contains a detailed description of the Q-DCIS.
- Subsection 7.1.4 summarizes the N-DCIS.
- Subsection 7.1.5 contains a detailed description of the N-DCIS.
- Subsection 7.1.6 discusses DCIS conformance to regulatory requirements, guidelines, and industry codes and standards.
- Table 7.1-1 is a regulatory requirements applicability matrix.
- Table 7.1-2 is a section roadmap of an evaluation of IEEE Std. 603 specific criteria compliance.
- Figure 7.1-1 is a simplified network functional diagram of the DCIS.
- Figure 7.1-3 is a distributed power-sensor diversity diagram.
- Figure 7.1-4 is a hardware/software (architecture) diversity diagram.

7.1.1 Distributed Control and Information System

The DCIS is an arrangement of I&C networked components and individual systems that together provide:

- Digital processing and logic capability
- Remote and local data acquisition
- Datalinks and gateways between systems and components
- Operator monitoring and control interfaces
- Secure communications to external computer systems and networks
- Alarm management functions
- Communications between the systems

Figure 7.1-1 shows a simplified network functional diagram of the DCIS. The data communication systems embedded in the DCIS perform the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8.

The Q-DCIS and N-DCIS architectures, their relationships, and their acceptance criteria are further described throughout Section 7.1.

The Q-DCIS and N-DCIS functions are implemented with diverse power and sensors as indicated in Figure 7.1-3, and diverse hardware and software architectures as shown in Figure 7.1-4. These are discussed in Reference 7.1-4, the Licensing Topical Report (LTR), “ESBWR I&C Diversity and Defense-In-Depth Report,” NEDO-33251.

The Q-DCIS comprise the platforms that are defined in Table 7.1-1. The N-DCIS comprise the network segments that are defined in Table 7.1-1. These platforms or network segments comprise systems of integrated software and hardware elements. Software projects are developed for the various platforms or networks segments. The software development process is described in Appendix 7B.

7.1.2 Q-DCIS General Description Summary

The Q-DCIS, which performs the safety-related control and monitoring functions of the DCIS, is organized into four physically and electrically isolated divisions. The Q-DCIS uses three diverse hardware/software technological platforms that operate independently of each other:

- Reactor Trip and Isolation Function-Neutron Monitoring System (RTIF-NMS)
- Safety System Logic and Control/Engineered Safety Features (SSLC/ESF)
- The Independent Control Platform (ICP)

The ICP provides independent logic control of:

- The Anticipated Transient Without Scram mitigation and Standby Liquid Control (ATWS/SLC) functions.
- The vacuum breaker (VB) isolation function.
- The High Pressure Control Rod Drive (HP CRD) isolation bypass function.
- The Isolation Condenser System (ICS) DPV Isolation Function (IDIF).

The ICP platform is fundamentally and technologically diverse from the other two safety-related Q-DCIS hardware/software technology platforms; RTIF-NMS and SSLC/ESF. The ICP digital hardware platform is implemented in a system composed of custom programmable logic devices (CPLDs). And the ICP safety-related function is not changeable after initial configuration and setup. The ICP implementation that performs its safety-related control function does not execute, run, or use a cyclic real-time executive or operating system or any associated controller application program to perform its safety function. The ICP implementation that performs its safety-related control function does not incude a system clock as there is no cyclic real-time executive. The overall

ICP platform does include monitoring and diagnostics programs but these programs are independent from the implementation that performs the safety-related control function. The ICP implementation that performs the safety-related control functions are implemented in CPLDs and are relatively simple functions. The ICP functions are only required after the complete failure of RTIF-NMS, SSLC/ESF or other safety-related equipment functions.

The design objective with ICP implementation is to configure them to be nearly 100% testable. The currently available CPLD logic and associated digital circuit engineering design and configuration tools are software based. There is a possibility that system level or functional logic and control requirement errors exist or that the engineering design and configuration tools used to implement the CPLDs contain a latent defect. Identifying, dispositioning, and remediating both of these types of errors are addressed by the rigorous and structured system and software development lifecycle (SDLC) as described in Section 7B Software Development. The ICP platform does not execute, run, or use any active software to perform its safety-related control function, the functions implemented are simple, and it is designed to be nearly 100% testable. Therefore, the ICP digital hardware platform is highly immune to common-cause failure (CCF) with respect to its own software based engineering design and configuration tool, itself, as well as the other two Q-DCIS hardware/software technology platforms as well as the systems and functions implemented on them.

The Q-DCIS major cabinets are Reactor Trip and Isolation Function (RTIF) cabinet, Neutron Monitoring System (NMS) Function cabinet and the SSLC/ESF cabinet. These cabinets include the following systems and functions:

- RTIF Platform Systems and Functions
  - Reactor Protection System (RPS) (Refer to Subsection 7.2.1).
  - Main Steam Isolation Valve (MSIV) functions of the Leak Detection and Isolation System (LD&IS) (Refer to Subsection 7.3.3).
  - Suppression Pool Temperature Monitoring (SPTM) function of the Containment Monitoring System (CMS) (Refer to Subsection 7.2.3).
- NMS Functions:

  NMS is implemented using the same hardware/software platform as RTIF systems; NMS includes the following systems and functions:

  - Startup Range Neutron Monitor (SRNM) functions
  - Power Range Neutron Monitor (PRNM) functions that include:
    - Local Power Range Monitor (LPRM) functions
    - Average Power Range Monitor (APRM) functions
    - Oscillation Power Range Monitor (OPRM) functions

- Safety System Logic and Control/Engineered Safety Features (SSLC/ESF) Platform, Systems, and Functions
    - Emergency Core Cooling System (ECCS) functions that include:
        - Automatic Depressurization System (ADS) functions
        - Gravity-Driven Cooling System (GDCS) functions
        - Isolation Condenser System (ICS) functions
        - SLC system functions
    - LD&IS Functions (except the MSIV functions)
    - Control Room Habitability System (CRHS) functions
    - Safety-related information systems
- ICP Platform, Systems, and Functions
    - VB isolation function of the containment system (Refer to Subsection 7.3.6 for additional information).
    - ATWS/SLC functions (Refer to Subsection 7.4.1 and Subsection 7.8.1 for additional information).
    - HP CRD Isolation Bypass function (Refer to Section 4.6 as well as Subsections 7.1.2.8.8, 7.3.3, and 7.4.5 for additional information).
    - ICS DPV Isolation Function (Refer to Subsection 7.3.7 for additional information).

Space consideration may dictate locating the ICP hardware in separate cabinets.

The Q-DCIS major components include:

- Fiber-optic cable and hardwired networks
- System processors
- Non-micro-processor based logic (i.e. ICP)
- Remote multiplexer units (RMUs)
- Load drivers (discrete outputs)
- Communication interface modules (CIMs)
- Video display units (VDUs)
- Hard controls/indicators (for monitoring)
- Cabinets for housing devices such as power supplies

The Q-DCIS provides the interface functions for the RTIF, NMS, SSLC/ESF, and ICP protection systems. These functions include data acquisition, monitoring, communication, and control functions. As a safety-related system, Q-DCIS is qualified for the environments and conditions that

exist before, during, and following the abnormal events identified in Table 15.0-2. Each division of the Q-DCIS is electrically isolated from other Q-DCIS divisions and from the N-DCIS. Data communication is controlled between the Q-DCIS divisions and between the Q-DCIS and the N-DCIS. Communication between Q-DCIS divisions and between the Q-DCIS and the N-DCIS is via fiber-optic cable. Data communication between the Q-DCIS and the N-DCIS is managed by isolation devices, which are safety-related components within the Q-DCIS, via datalinks and N-DCIS gateways. The RTIF, NMS, SSLC/ESF, and ICP protection systems are designed so that no safety-related function depends on the existence or function of any nonsafety-related component, data, or communication channel. The ICP has no data communications interface to nonsafety-related components.

The Q-DCIS uses RMUs for data acquisition for the RTIF, NMS, and SSLC/ESF protection systems and for safety-related displays in the Main Control Room (MCR) and Remote Shutdown System (RSS). These data acquisition and network communication units are either distributed within the division or reside in specific chassis and are not dedicated to specific RTIF, NMS, or SSLC/ESF protection systems.

For added reliability and diversity, the architecture of the RTIF and NMS protection systems is different from the architecture of the SSLC/ESF protection system (refer to Figure 7.1-3 and Figure 7.1-4). These systems operate automatically under normal conditions, without operator input.

The RTIF and NMS status is monitored on the divisional Q-DCIS safety-related MCR and RSS VDUs that are connected to the SSLC/ESF (the N-DCIS VDUs also have the capability to independently monitor the RTIF and NMS statuses but only after isolation and with no capability to control the Q-DCIS). The RTIF and NMS process and status data are sent per division through the required safety-related isolation and via a one-way dedicated communication path for display on the corresponding divisional safety-related VDU. The RTIF, NMS, and SSLC/ESF operate independently of the VDUs. They continue to perform their safety-related functions if there is a failure of the VDU network. The VDUs have no capability to control the RTIF or the NMS. Safety-related VDUs are provided in the MCR and at the RSS panels and operate independently of one another. The safety-related VDUs provide data display capability for the RTIF, NMS, and SSLC/ESF safety-related systems but manual control capability only for the SSLC/ESF safety-related systems in the same division as the safety-related VDU, all in a Human Factors Engineering (HFE) approved format.

The divisional Q-DCIS components outside of the MCR are located in physically separate DCIS divisional rooms or compartments in the Reactor Building (RB) and Control Building (CB) that have fire barriers between them.

The divisional Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies (UPSs) dedicated to their division with battery backup (per division) for at least 72 hours. After 72 hours, the Q-DCIS can operate continuously on power from diesel

generators or from off-site power. (Refer to Chapter 8 for additional information about the power sources for the isolation load centers and safety-related uninterruptible alternating current (AC) power).

The Q-DCIS provides self-diagnostics that monitor communication, power, and processors to the replaceable card, module, or chassis level. Process diagnostics include system alarms and the capability to identify sensor failures. Process and self-diagnostic system alarms are provided to the MCR.

7.1.2.1 Q-DCIS Safety-Related Design Bases Summary

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Section 4. Safety System Designation including all sub-sections thereof; 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, and 4.12. IEEE Std. 603, Section 4 addresses, reading signals, performing signal conditioning, transmitting data signals and commands, performing safety-related logic independently, providing alarms, and isolating data communication.

The three Q-DCIS hardware/software technology platforms must be designed to conform to IEEE Std. 603 by meeting the requirements therein. Derived from IEEE Std. 603, the fundamental reliability of digital control systems is based in large part on four essential objective design principles of independence, data processing and communications with guaranteed determinancy or determinism, redundancy, and defense-in-depth and diversity (D3) as well as one subjective attribute of simplicity. The Q-DCIS design basis commitments needed to implement the IEEE Std. 603 requirements as well as addresses the four design principles and one subjective attribute are discussed individually below.

7.1.2.1.1 Independence Design Principle

Fundamentally this requirement relates to any of the individual safety-related divisions of the three Q-DCIS platforms. Each platform shall be able to perform its safety-related functions regardless of the operability or adverse impact potentially present in any aspect of the other three of four divisions of its specific Q-DCIS platform or any aspect of the other two Q-DCIS platforms across their four divisions. Also, any of the individual safety-related divisions of the three Q-DCIS platforms shall be able to perform its safety-related functions regardless of the operability or adverse impact of the N-DCIS via any nonsafety-related data communication. The ESBWR overall I&C and DCIS architecture and configuration design basis includes the requirement that there is very limited, selective, and closely managed communication from nonsafety-related N-DCIS to safety-related Q-DCIS and that this communication cannot involve any control capability. Furthermore, safety-related divisions can only be controlled by the displays and controls appropriate to that division. The only allowed interconnections between divisions will be limited to that needed to support two-out-of-four trip voting logic processing within each of the individual Q-DCIS platforms are:

- Trip status
- Bypass status of a division (also referred to as divisional bypass)
- Data communications or message authenticiation status

Independence is usually sub-divided into requirements for:

Physical Separation: The ESBWR Q-DCIS is divided into four independent divisions whose hardware is located in physically separate rooms and fire areas. If nonsafety-related equipment is in the same area, then it will be rated Seismic Category 2A (See IEEE Std. 603 sub-section 5.6.3.2 Equipment in Proximity). The ESBWR I&C and DCIS design is such that a physical assault (fire, smoke, etc.) on any one division will not adversely affect another division. The only allowed exceptions are the areas or spaces involving MCR and RSS both located outside containment and certain actuators located both inside and outside containment. The MCR and RSS require proximity to allow convenient operator control and monitoring but the divisional Q-DCIS hardware are placed in separate equipment cabinets and compartments that are otherwise immune to environmental common cause failures (CCF) like fires. The Q-DCIS equipment cabinets are located such that they are not affected by the design basis events they are designed to mitigate. The actuators located inside and outside containment require proximity because many ESBWR actuators have multiple initiators (squibs and solenoids). For these cases, wiring and fiber optic cables are in separate conduit and penetrations. The loss of the actuator will not cause the loss of associated divisional Q-DCIS. These statements address IEEE Std. 603 sub-section 5.6.2 Independence - Between Safety Systems and Effects of Design Basis Event.

- **Electrical Separation:** All data communication between safety-related divisions of the Q-DCIS in ESBWR will be via optical fiber. There are no electrically conductive paths between the divisions of Q-DCIS. All data communication between any Q-DCIS division and nonsafety-related components will be via optical fiber. There are no electrically conductive paths between Q-DCIS and N-DCIS. Additionally, the divisional Q-DCIS will be powered by separate, redundant, and uninterruptible power supplies that have no connection between divisions. Nonsafety-related electrical power supplies will not power any Q-DCIS and safety-related power supplies will not power any nonsafety-related components. These statements address IEEE Std. 603 sub-section 8.1 Electrical Power Sources.
- **Communication Separation:** In previous nuclear plant designs, the only "communication" between divisions was typically electrical signals from relays. The ESBWR DCIS has active data communication between safety-related divisions of Q-DCIS and from Q-DCIS to N-DCIS. Accordingly, the ESBWR DCIS design addresses data communications that can potentially adversely affect the divisional Q-DCIS's performance of its safety-related functions as is described below.

  ESBWR overall DCIS employs three types of safety-related data communication:

  - Within a Q-DCIS division needed to make the divisional safety-related functions work.

- Between Q-DCIS divisions needed to make the divisional safety-related functions work.
- Between Q-DCIS divisions and N-DCIS for monitoring, recording, alarming and nonsafety-related control purposes. Additionally in the case of SSLC/ESF only, the same path is used to send absolute time from the N-DCIS to SSLC/ESF via the appropriate N-CIMs. This type of data communication is never required to make the safety-related functions work.

All safety-related data communication independence concerns are addressed in both the three Q-DCIS platforms and additionally as an aspect of the administrative controls associated with physical security. All inter-divisional Q-DCIS and N-DCIS data communications carried on optical fibers are run in conduit and terminate in their applicable DCIS cabinets that are locked and whose door position is alarmed in the MCR. Additionally, the DCIS cabinets are located in locked rooms requiring badge access and associated aspects of administrative controls. These design basis features make it highly improbable that anyone can gain access (or silent access) to the DCIS cabinets or their associated wiring and cables. This addresses IEEE Std. 603 sub-section 5.9 - Control of Access. Further discussion will relate to the features in the hardware and software that preserve independence.

Note that data communications within a safety-related division is important for operability and must be suitably designed but it is not an independence concern. Failure or compromise of intra-divisional data communication is a single divisional failure for which all reactors must be designed and will be addressed in the as part of the determinacy design principle (see Subsection 7.1.2.1.2).

The ESBWR communication independence concerns can be localized to the data communication between divisions and to data communication between the safety-related divisions and the N-DCIS since these are the only paths than can compromise otherwise independent divisions. For the RTIF-NMS, SSLC/ESF and ICP Q-DCIS platforms, data communication between divisions is limited to that necessary to support the two-out-of-four trip voting logic used for trips/and control function initiations in all Q-DCIS platforms. Common to all Q-DCIS platforms is that these data communications are respectively limited to only bypass and trip status and message authentication information and to “one way” data communication. Additional design description concerning "one way" data communications is addressed for RTIF-NMS, SSLC/ESF, and ICP hardware/software platforms in Sections below. Additionally, common to the RTIF-NMS and SSLC/ESF Q-DCIS platforms is that all controller application processors will obtain their data communication through shared memory via data communications interface modules (CIMs). All CIMs are designated and implemented as safety-related equipment. The CIMs cannot "interrupt" the controller application processors nor do they require any controller application processor resources to perform their data communication function. Specifically, a controller application processor is programmed to always look in or write to a specific shared memory location. The controller application is either "burnt in" (RTIF-NMS) or under appropriate administrative control procedure, these include control of a

physical key needed for the keylock on the applicable chassis and control of the programming device. As a result of these design features, the controller application program cannot be changed in normal operation. The controller application code is also continuously surveilled for indication of any change. The safety-related data communication interfaces are also programmed to read and write to specific shared memory locations to supply or obtain the necessary data. CIMs that interface only between the three independent, separate, redundant, and diverse Q-DCIS are generically refered to as Q-CIMs. In normal operation, data is communicated "one way" or "uni-directional" in the direction from Q-DCIS to N-DCIS equipment. CIMs that interface between the Q-DCIS and the N-DCIS are Q-CIMs at the source and nonsafety-related N-CIMs or gateways on the receiving side.

The ESBWR DCIS does not perform safety-related control functions from nonsafety-related systems, components, and equipment. No "prioritization modules" or other embodiment of either intra-divisional safety-related or safety-related and nonsafety-related combinations of data are necessary to implement the required safety-related control functions.

7.1.2.1.1.1 RTIF-NMS Independence Design Principle

Two-out-of-four trip voting logic related data communication: This section specifically addresses IEEE Std. 603 sub-section 5.6.1 - independence between redundant portions of a safety-related system.

The RTIF-NMS Q-DCIS platform uses one way (transmit only) point-to-point optical fibers that are fail-safe such that loss of data communication is assumed to be a trip (specifically a trip of all parameters from that division). The transmitted messages are automatically received by a shared memory; the controller application processor is not interrupted by nor does it have to request the received message. The transmission data rates are at least 100 Mbits/Sec (100 MHz) such that the trip data are inserted into shared memory virtually instantaneously (i.e. much faster than the controller application processor cycle time). As previously described, no analog data are transmitted to support the two-out-of-four trip voting logic, only discrete per parameter trip status and system bypass status information is sent. The burnt in code of the controller application processor "instructs" the application to access a specific shared memory location (per trip parameter and bypass status); no other locations are accessed and the application code is continuously monitored for change. Since the controller application processor is only "looking" for discrete information in a specific memory location, the design is unaffected by conditions like buffer and memory overflow; memory is also part of the continuous self diagnostics of RTIF-NMS.

Assuming the division itself does not fail (which is covered by N-1 redundancy discussed in Subsection 7.1.2.1.3), given the above, the only credible way for a division or its data communication to adversely affect another division using two-out-of-four trip voting logic data communication would be to disconnect the incoming fiber and simulate a "no trip" signal. Physically disconnecting the fiber is both difficult (cabinet doors are locked in badge accessed normally

unmanned rooms and the RTIF-NMS cabinet doors will alarm in the control room if opened) and impossible to do silently since it will immediately cause a divisional trip and alarms in the receiving division (the alarms will occur even if the division is bypassed which is only possible from the MCR). Although point-to-point, the transmitted message includes authentication techniques. Specifically, transmission coding is modified code in which each data bit has at least one transition and occupies the same time. The transitions which signify 0 or 1 occur at the midpoint of a period. The existence of guaranteed transitions allows the signal to be self-clocking and also allows the receiver to automatically align correctly without communicating with the transmitter. The coding also makes it easy to determine that data communications have been lost or corrupted. Finally, the encoded message will include the identification of the transmitter and a checksum to enable further corruption checking. An incorrect identification on a specific incoming line will not be accepted and will be interpreted as a trip.

Nonsafety-related data communication: This section specifically addresses IEEE Std. 603 sub-section 5.6.3 - independence between safety-related systems and other systems.

The RTIF-NMS Q-DCIS platform is connected for data communication to the N-DCIS using a shared reflected memory data communication bus technology (sometimes referred to as "scramnet") arranged in a ring configuration. There are actually two "scramnet" rings, each redundant, that connect all RTIF-NMS Q-DCIS chassis within the division. Note that only one of the redundant "scramnet" rings includes any nonsafety-related components. The "scramnet" ring which connects only the safety-related components will be addressed in Subsection 7.1.2.1.2 which discusses determinacy.

The dual redundant "scramnet" rings are continuously circulating data between the physical and logical locations on the data communications bus in both a clockwise and counterclockwise direction. These bus locations are referred to as nodes. The "scramnet" data communication processors automatically investigate their node's shared memory addresses and forward their contents to the next node on the "scramnet" ring. The "scramnet" data communication processor in the downstream node will pull the data from the ring, load it into the same nodal memory location as the sending node (hence "reflective" memory) and simultaneously pull the receiving node's data and send it to the next downstream node. Each safety-related chassis on the "scramnet" rings uses safety-related hardware and software data communications RTIF-NMS Q-CIMs to insert any changed data from shared memory. Each nonsafety-related chassis on the "scramnet" rings uses N-CIMs to "pull" changed data from shared memory. The changed data are put into the shared memory by the controller application processor of the chassis. The data will be actively sent to all the series connected CIMs on the "scramnet" ring within micro-seconds to update all shared memory addresses. This "scramnet" ring data loading includes those addresses in the N-CIMs. Overall system timing issues will be addressed in Subsection 7.1.2.1.2 which discusses determinacy. The CIMs do not interrupt the Q-DCIS or N-DCIS controller application processors to ask for data. Monitoring and diagnostic as well as process data is automatically put into the shared

memory addresses. The "scramnet" data communication processors then load the data on the ring and transmit it to the up- and down- stream nodes. In normal operation, the N-CIMs on the ring are programmed to not send data nor will they have access to "sensitive" locations in the shared memory locations of the Q-DCIS components data communicating through the CIMs. This feature of the CIMs keeps N-DCIS information from Q-DCIS components. Additionally, the Q-DCIS controller application processors are programmed to not "look" in the N-CIM data addresses on the "scramnet" ring safety-related data.

Since the data arrive automatically in the N-DCIS components, at no time do they have to request data or affect a transmit-receive or "handshake" with the Q-DCIS components. In normal operation, N-CIM components are not capable of even communicating with the Q-DCIS controller application processors.

In the above statements "normal operation" will not allow nonsafety-related data communication to safety-related components but for setup and calibration such transmission is allowed. This calibration is possible following an appropriate administrative control procedure, which includes control of a physical key needed for the keylock on the applicable chassis which will render the division "inop"; because the design of these Q-DCIS platforms is fail-safe, the division will trip in "inop" unless the operator bypasses the division (only one division at a time can be physically and logically bypassed). The operator can review the downloaded, originally nonsafety-related information before the operator manually allows its acceptance; from then the downloaded information is monitored for change and at no time can this information affect the safety-related functions of the controller application processor. This addresses IEEE Std. 603 sub-section 5.7 capability for testing and calibration.

As previously described, the "scramnet" rings are much faster than the RTIF-NMS Q-DCIS platform controller application processor cycle times. Therefore, no absolute time information need to be sent to any RTIF-NMS Q-DCIS component for time stamping data. The four divisions of RTIF-NMS Q-DCIS run asynchronously and absolute time is not needed by the controller application programs. Because of the scramnet speed no time skew is incurred by time stamping the data at the N-CIMs/gateways which connect with the N-DCIS GENE network segment and network time.

The RTIF-NMS Q-DCIS platforms include extensive monitoring and diagnostics features including A/D conversion constants, memory, internal clocks, application code, power supplies and internal temperature. Although the design removes ways to adversely affect these features, the monitoring and diagnostics make it highly improbable that the systems can change from their validated and verified test status without alarm indication in the MCR. In summary, the N-CIM components can only influence their "scramnet" addresses if they violate their own software and attempt to write instead of read. Even if a "scramnet" memory address is affected, then it is not an address where the "burnt in" controller application program is instructed to look nor a memory address used by the Q-DCIS controller application program to perform its safety-related function.

7.1.2.1.1.2 SSLC/ESF Independence Design Principle

Unlike the RTIF-NMS Q-DCIS platforms, the SSLC/ESF uses Ethernet data communication networks to communicate with other divisions for two-out-of-four trip voting logic, with the N-CIMs for N-DCIS data communication, and within the division (determinacy of these networks is discussed in Subsection 7.1.2.1.2). All three of these Ethernet networks exist per division. All three of these Ethernet networks are separate and redundant. As with the different but analogous RTIF-NMS "scramnet" data communications rings, only the Ethernet networks between the divisions and interfacing with the N-CIMs are relevant to independence. Also analogous with RTIF-NMS, the SSLC/ESF cabinets are normally locked and the door position alarmed in the MCR; the cabinets are located in a normally unmanned room requiring badge access. The optical fiber cables supporting the networks will be very difficult to access physically and impossible to access silently.

The SSLC/ESF controller application processors are doubly buffered. Each of the triply modular redundant (TMR) controller application processors per division has its own data communication processor and uses shared memory between them. The controller application processor is never interrupted for any data communication. Additionally, the controller application processors are programmed such that data communications variables must be specifically identified as inputs or outputs (or both) and the application programs are thereafter monitored for change. In turn the data communications processor interfaces with the applicable SSLC/ESF Q-CIM card through another shared memory. These SSLC/ESF Q-CIM cards provide or accept data communications from the controller application processors by enforcing their identification of the variables and whether they are inputs or outputs. In addition, SSLC/ESF Q-CIM cards perform message authentication. For a shared network between divisions, robust message authentication is important and will determine if a message is accepted. A message persistently failing authentication is alarmed. For SSLC/ESF, message authentication includes transmitter and receiver identification, message sequence number, hash functions and cyclic redundancy checks. The message authentication resides always in the receiving division and does not depend in any way on the correct operation of the transmitting division. The network's monitoring and diagnostic functions will also alarm if a network fiber optic cable is disconnected. Note that even if the physical networks were somehow compromised and a new source with the correct transmitter address were added to the network, it is not credible that the correct message sequence number and hash functions would be maintained and transmitted to the receiving divisions. The authentication scheme will identify messages from incorrect sources and also whether a message from a correct source has been corrupted. Messages are acknowledged but authentication does not depend on the message source responding to the acknowledgement.

Two-out-of-four trip voting logic related data communication: this section specifically addresses IEEE Std. 603 sub-section 5.6.1 - independence between redundant portions of a safety-related system.

The redundant two-out-of-four trip voting logic SSLC/ESF networks are connected to each division via a separate data communication network using Q-CIMs. In the SSLC/ESF Q-DCIS platform, these Q-CIMs are also referred to as Q-CIM cards. The SSLC/ESF data communication implementation uses two Q-CIM cards and their respective ports per safety-related division. The two redundant SSLC/ESF data communications networks are configured to support both two-out-of-four trip voting logic and N-2. Adequate network functionality is retained even if two divisions are faulted or one of the redundant data communications networks is faulted. There are only four nodes (one per divisions) on each of the redundant networks and another signal source would be both alarmed and ignored. Although determinism is discussed in Subsection 7.1.2.1.2 the two-out-of-four trip voting logic data communication networks are so lightly loaded (only trip, bypass and authentication information is transmitted) that data loss or collisions are virtually eliminated. Unlike RTIF-NMS, the SSLC/ESF is fail “as-is” design such that there are no "default" ECCS control function initiations, however since data communication is "expected", the various divisions will alarm if transmissions are not received. For the receiving division to accept the "trip" and "bypass" status message, it must be properly addressed (sender and receiver), in the correct sequence, be properly identified via the hash function and uncorrupted before it will be passed through the data communications card and shared memories to the controller application processor. It should be noted that even in the very unlikely event that all the two-out-of-four trip voting logic data communication /networks were lost, each division retains the ability to monitor the plant and the manual capability to initiate the various ECCS functions.

Nonsafety-related data communication: this section specifically addresses IEEE Std. 603 sub-section 5.6.3 - independence between safety-related systems and other systems.

The SSLC/ESF data communications to the N-DCIS are also redundant and implemented on a different set of data communications cards and ports than intra-divisional and two-out-of-four trip voting logic data communications. As part of implementing this function, advantage is taken of internally setting the data communications card to "read" (from the controller application processor) only such that data communications are directed by the system to be "one way" or "uni-directional". The controller application processor programming tags these variables as "output" only such that they would have no adverse affect even if the SSLC/ESF Q-CIM card failed (which is also diagnosed and alarmed) No "inputs" are programmed into the application for the N-DCIS gateway connection. The application is unaffected by the N-DCIS data communications and the existence of the receiving N-DCIS gateways or the correctness or presence of the network absolute time signal. The only N-DCIS data communication exception is network time sent to the communications card for time stamping of data sent to N-DCIS and the safety related VDU displays. The Q-DCIS to N-DCIS communications medium is Ethernet and, although the time at which the Q-DCIS data arrive at the gateway is short (since there are only two nodes on the network), it is somewhat variable in the millisecond range. The resulting time skew can be eliminated by time stamping at the communication card origin; an accurate time stamp is important for the various non safety-related

ESBWR analyses and recording systems and time displays on the safety related VDUs indicate the displays are properly updating. The safety related communication cards prevent time from ever reaching the controller application processors (i.e. absolute time is not input to the shared memories) and time is never used for synchronization within the division or between divisions.

7.1.2.1.1.3 ICP Independence Design Principle

As described in Subsection 7.1.2, the ICP digital hardware platform is inherently simpler and more robust to adverse data communications and provision of independence because it does not execute, run, or use a cyclic real-time executive or operating system or any associated controller application program to perform its safety-related function. The ICP is not changeable after initial setup. The ICP does not use data communication multiplexing or networking so that all input/output (I/O) is via hard copper wire. The ICP also uses two-out-of-four trip voting logic and accept bypass inputs and this is done via "hard" (point-to-point) optical fibers. The ICP does not have direct data communication with N-DCIS and are located in locked cabinets whose door position is alarmed in the MCR to make tampering obvious.

Two-out-of-four trip voting logic data communication: this section specifically addresses IEEE Std. 603 sub-section 5.6.1 - independence between redundant portions of a safety-related system.

To perform two-out-of-four logic for ICP control function initiation, these Q-DCIS platforms use point-to-point optical fiber but, unlike programmed systems, data communications must be kept simple. Accordingly the ICP signal formats use one specific frequency for "1's" and another frequency for "0's"; no other frequencies are accepted and the scheme makes it easy to identify loss of data communication and alarm. The ICP receiver input gates that accept divisional trip signals are dedicated to the transmitter; there is no possibility that a transmitter could affect any other input gates than its own. As with RTIF-NMS, the only way to adversely affect a previously set up and tested ICP is by a simulating the trip signals. This action cannot be done without an alarm indication in the MCR.

Nonsafety-related data communication: this section specifically addresses IEEE Std. 603 sub-section 5.6.3 - independence between safety-related systems and other systems.

As described above, the ICP do not have direct links to N-DCIS, instead they are monitored by the RTIF Q-CIM in the associated RTIF division (i.e. intra-divisional data communication only). There is a micro-processor based monitoring and diagnostic application program in the ICP that looks at and reports on the status of various ICP internal gates. This micro-processor monitoring application program does not communicate with the logic gate based controller function and no control is possible over this link. The micro-processor based monitor sends the ICP status and diagnostic information to the RTIF Q-CIM which then passes the information on through the N-CIMs to the N-DCIS GENE network segment gateways to provide indication the in MCR as described in Subsection 7.1.2.1.1.1. The RTIF components do not communicate with the ICP. Any signals the ICP needs are available from within its division and are hard wired.

7.1.2.1.2 Determinant Data Processing and Communication (Determinism) Design Principle

Reliability, redundancy and independence in ESBWR DCIS can be achieved separately from timing considerations but there must be timing criteria that ensure that the DCIS operates fast enough to satisfy the automatic and manual operability requirements. Transients, design basis and beyond design basis events are analyzed in Chapter 15 and assume time criteria that the DCIS must meet to make the analyses accurate. The ESBWR DCIS design bases will use these requirements to determine the speed required of the Q-DCIS (and N-DCIS) controller application programs and required data communication management programs. Per BTP HICB-21, Q-DCIS computer timing will be shown to be consistent with the limiting response times and the characteristics of the computer hardware, software, and data communications systems and ESBWR DCIS design basis documents will describe system timing goals. Specifically per IEEE Std. 603 sub-section 4 - safety-related system design basis, item j, the ESBWR DCIS design basis documents will identify:

- 4.10.1) The point in time or plant conditions for which the protective actions of the safety-related system shall be initiated.
- 4.10.2) The point in time or plant conditions that define the proper completion of the safety-related function.
- 4.10.3) The point in time or the plant conditions that require automatic control of protective actions.
- 4.10.4) The point in time or the plant conditions that allow returning a safety-related system to normal.

Typically, the ESBWR RTIF and NMS timing requirements will be 10's of milliseconds and, because of the passive design ESBWR margins, the SSLC/ESF timing requirements will only need to be 100's of milliseconds. The ESBWR does not require any manual actions to mitigate transients and accidents since Q-DCIS is designed to automatically provide all design basis responses for the first 72 hours of those events.

Even with serious, beyond design basis events, there are no manual actions required for at least 30 minutes. Subsequent to the operator's decision to actuate a safety-related function, the video display unit (VDU) to final actuate response time of approximately one second (as determined by the HFE process) is easily accommodated by the response times of the overall loop of the manual action to controller to actuator (including the data communications) of the Q-DCIS.

As important as it is to establish timing requirements, it is equally important to design the DCIS such that the requirements are met consistently and always less than or equal to those requirements. This feature is defined as "determinacy" and is achieved when known PRECONDITIONS and INPUTS are provided and the output is predictable in the time frame of interest. For the Q-DCIS and N-DCIS logic this translates to using deterministic algorithms that behave predictably. The ESBWR algorithms, given a particular input, will always produce the same output, and the Q-DCIS platform will always pass through the same sequence of states. Deterministic algorithms are by far

the most studied and familiar kind of algorithm, as well as one of the most practical, since they can and have been run on real machines performing safety critical functions.

More specifically, ESBWR Q-DCIS platforms will be said to be "deterministic" if it reacts always in the same way according to the order (time stamps) of the events occurring at its input channels. Said differently, if event E1 occurs at T1 at the input I1 and event E2 occurs at T2 > T1 at the input I2, the consequence of E1 should be seen at the outer limit output of the system before the consequence of E2. In order to react in this way, all the events have to be "serialised" in a "scheduler" before their consequence is processed and seen in the corresponding output channel.

The Q-DCIS and N-DCIS platforms must:

- Measure a parameter.
- Compare the parameter to a trip setpoint.
- Use the trip decision in two-out-of-four trip voting logic to determine a scram/and control function initiation.
- Operate the final actuators.

Per BTP HICB-21, the ESBWR will establish a time budget for these tasks and appropriately design the hardware/software to achieve the desired result. The budget will specifically include the "skew" occurring when measurements are obtained at the instrument cycle time rate (for example it could "just miss" the low water level and not measure again for 10's of milliseconds). Also included will be the skew occurring in the two-out-of-four trip voting logic occurring because the four divisions are not synchronized. Note that skew is random but has an upper limit imposed by the hardware and data communications such that it does not cause a system to be non-deterministic. The system architecture may also include separate chassis to accomplish the above tasks and therefore data communication between chassis must be included in the time budget. Finally transducer and actuator response times must be accounted for.

Per BTP HICB-21, the ESBWR Q-DCIS and DPS (specific N-DCIS hardware/software controllers) platforms do not use the following in normal operation:

- Non-deterministic data communications (see Subsection 7.1.2.1.2.2 below)
- Non-deterministic computation
- Interrupts
- Multi-tasking
- Dynamic scheduling
- Event-driven designs

The ESBWR three Q-DCIS platforms design basis documents will describe the specification, design and testing processes used to provide determinism. These processes will be followed both for initial design changes as well as any subsequent changes. These Q-DCIS platforms use both

their monitoring and diagnostic capabilities and periodic surveillance testing through administrative controls to confirm operability, including clock tests and response time.

7.1.2.1.2.1 RTIF-NMS Determinism Design Principle

All of the controller application processors in RTIF-NMS platfrom run or use a cyclic real-time executive or operating system that include both the controller application program as well as monitoring and diagnostics programs. The cyclic real-time executive or operating system is clock (not absolute time) driven and not event driven. The RTIF-NMS platform does not incorporate "interrupts". The RTIF-NMS platform is monitored by both watchdog timers and the external technical specification monitor (TSM) to diagnose any application program loop failures to execute or " stalls". The TSM can also independently monitor other RTIF-NMS operability functions. The RTIF-NMS platform includes a fail-safe design that will trip on critical self diagnostic failures. The application program is "burnt in" and starts with the application of power without operator intervention. The RTIF-NMS platform application programming is not dependent on any external hardware. As previously described, the controller application processors use shared memory using RTIF-NMS Q-CIMs. Data communications functionality does not use controller application programming resources to ask for or transmit data. The controller application processors are dedicated to their respective task.

As previously described, the RTIF-NMS systems use two, redundant "scramnet" rings per division specific to RTIF and separately specific to NMS. One of the redundant "scramnet" rings is used for data communication through the N-CIMS to N-DCIS GENE network segment via the gateways. The other "scramnet" ring is connected via the RTIF-NMS Q-CIMs and dedicated to only the safety-related chassis. The various chassis have controller application program loop cycle times of 10's of milliseconds and the "scramnet" rings are capable of updating the reflective memories in each chassis in micro-seconds. The data produced and needed by the applications are transported at a rate that is two to three orders of magnitude faster than the controller application program cycle time. From a practical perspective, this response time is credibly deterministic. The two-out-of-four trip status and bypass status data communication between divisions is via point-to-point optical fiber. This data is written to shared memory address and is available for use by the controller application program virtually instantaneously. From a practical perspective, this response time is credibly deterministic.

Since the inter- chassis and inter- divisional data communications are virtually instantaneous, the ESBWR RTIF-NMS time budgets will concentrate on the controller applications programs running in the various chassis. These application programs and hardware will be designed to meet the budget and are feasible with currently known methods and representative equipment.

7.1.2.1.2.2 SSLC/ESF Determinism Design Principle

The SSLC/ESF uses triply redundant controller application processors per division within which all application logic is run, per division the triply redundant controller application processors are

synchronized with each other but not to absolute time nor with the triply redundant controller application processors in the other divisions. All of the controller application processors in SSLC/ESF run cyclic programs that include both the application and diagnostics and that do not incorporate interrupts. The cyclic application program is clock (not absolute time) driven and not event driven and monitored by both watchdog timers and the external technical specification monitor to diagnose stalls; the TSM can also independently monitor other SSLC/ESF operability functions. The application program is changeable only under an appropriate administrative control procedure. These include control of a physical key needed for the keylock on the applicable chassis and control of the programming device. Manual operation of the keylock will cause an alarm (after the alarmed cabinet doors are unlocked). After the tested application program is downloaded it will be monitored for change by self diagnostics. The application programs start with the application of power without operator intervention. It is not dependent on any external hardware. As previously described, the controller application processors use shared memory and do not use resources to ask for or transmit data to the SSLC/ESF Q-CIM cards. The cards perform data transmission and receipt and the controller application processors are dedicated to their task. The controller application processors receive and output data to triply redundant I/O cards in local and remote multiplexing cabinets. The I/O cards are "polled" by the application program (the application program is not interrupted). Therefore, the input/output data are deterministic at the polling rate.

Each of the three controller application processors uses a shared memory interface to its own data communications processor. The shared memory interface allows communication to and from the controller application processor without interrupts and therefore supports its cyclic application program. In turn, the data communications processors are connected to an internal triply redundant data communications bus through another pair of shared memory transmit and receive buffers. The triply redundant data communications bus is connected to all of the SSLC/ESF Q-CIM cards that support the network based communications. There are three such redundant networks each dedicated to a specific function; two-out-of-four logic, intra-divisional VDU communication, and communication to N-DCIS. Accordingly, there are six total communication ports per division. The redundant communication ports and cards operate independently to their redundant networks and do not provide a connection between those networks.

Each of the SSLC/ESF Q-CIM cards is connected to the triply redundant internal communication bus such that each has access to the three controller applications processors and their data communication processors. The SSLC/ESF Q-CIM card interfaces to the communication bus through three pair of transmit and receive shared memory buffers, one pair per controller application processor. Specifically, the internal SSLC/ESF data communication path to or from the application processors is:

- Application processor to/from
- Shared memory to/from

- Communications processor to/from
- Shared memory to/from
- Communications bus to/from
- Shared memory to/from
- SSLC/ESF Q-CIM card

Since the only "common" location between the SSLC/ESF Q-CIM cards is after the shared memory, any transmitted or received data are independent. A SSLC/ESF Q-CIM card failure on one network will not affect the other card or its data.

The shared memory buffers do not produce any significant time delay such that the cycle time of the controller application processors will govern determinism. In addition to the physical interface, a major SSLC/ESF Q-CIM card function is message authentication. In the SSLC/ESF design, independence requirements mean that the receiving division is solely responsible for determining if a received message is accurate and authentic. There is no dependence on the performance or existence of the transmitting division. The specific message path requires the SSLC/ESF Q-CIM card to accept a message, determine its authenticity and accuracy and pass it to the data communications processor on the controller application processor card. That data communications processor does further authentication and then puts the data into the shared memory buffer of the controller application processor. The controller application processor accesses the memory location to use the data in its application only if the data in the message has been identified as a "write" variable. As stated above, the application program, specifically including its read and write declarations, is not changeable in normal operation and it is continuously monitored for change. The SSLC/ESF Q-CIM card has an additional ability to disable its "write" (to the controller application processor) shared memory such that no data can be passed to the data communications bus and the controller applications processor.

In the ESBWR Q-DCIS SSLC/ESF implementation, each one of the redundant networks has an independent Q-CIM card that sends data to the controller application processor.

The SSLC/ESF uses a dedicated and dual redundant Ethernet network to support the two-out-of-four trip voting logic. Each Ethernet Network has only four nodes; one node per division. The data communication on each Ethernet network is limited to:

Since the only "common" location between the SSLC/ESF Q-CIM cards is after the shared memory, any transmitted or received data are independent. A SSLC/ESF Q-CIM card failure on one network will not affect the other card or its data.

The shared memory buffers do not produce any significant time delay such that the cycle time of the controller application processors will govern determinism. In addition to the physical interface, a major SSLC/ESF Q-CIM card function is message authentication. In the SSLC/ESF design, independence requirements mean that the receiving division is solely responsible for determining if

a received message is accurate and authentic. There is no dependence on the performance or existence of the transmitting division. The specific message path requires the SSLC/ESF Q-CIM card to accept a message, determine its authenticity and accuracy and pass it to the data communications processor on the controller application processor card. That data communications processor does further authentication and then puts the data into the shared memory buffer of the controller application processor. The controller application processor accesses the memory location to use the data in its application only if the data in the message has been identified as a "write" variable. As stated above, the application program, specifically including its read and write declarations, is not changeable in normal operation and it is continuously monitored for change. The SSLC/ESF Q-CIM card has an additional ability to disable its "write" (to the controller application processor) shared memory such that no data can be passed to the data communications bus and the controller applications processor.

In the ESBWR Q-DCIS SSLC/ESF implementation, each one of the redundant networks has an independent Q-CIM card that sends data to the controller application processor.

The SSLC/ESF uses a dedicated and dual redundant Ethernet network to support the two-out-of-four trip voting logic. Each Ethernet Network has only four nodes; one node per division. The data communication on each Ethernet network is limited to:

- Trip status per parameter
- Divisional sensors bypass status
- Message authentication

The two-out-of-four data communication links will operate at a speed of 100 Mbits/Sec at a minimum. Although Ethernet communication is not inherently deterministic, the inter-divisional (two-out-of-four) SSLC/ESF Q-DCIS network transmission rates and message sizes are small enough that the design produces a network loading of approximately 0% and thereby achieves functional data communications determinism. In this SSLC/ESF application, functional determinism is achieved with rates of two to four times per second. Even if multi millisecond delays and collisions happen, the two-out-of-four safety function will not be adversely affected.

Using the following assumptions:

- Ten times per second message rate
- Message size of 1024 bytes
- A return response acknowledge message requirement

an example calculation from industry practice and experience indicates that a per division probabilistic analysis results in greater than 0.9999999 probability that data will not be lost or delayed beyond one millisecond per transmission per 100 years. Since the data communication rates of SSLC/ESF are very low and only two divisions are needed to initiate ECCS control functions, determinism is functionally achieved. Continuing the example, the ten times per second

two-out-of-four data are included in the SSLC/ESF time budget but the very small network delay will not represent a significant delay to a controller application program running the two or four times per second.

SSLC/ESF data communication with N-DCIS has been previously described as dedicated, redundant and isolated by the separate SSLC/ESF Q-CIM cards which support "one way" or "uni-directional" data communication. There are no determinism requirements for data sent to N-DCIS other than such data communication should not adversely affect SSLC/ESF controller application processor resources. To achieve this independence, the controller application processors are not interrupt driven and are double shared memory buffered. Additionally, these SSLC/ESF Q-CIM cards are programmed not to write data to the SSLC/ESF internal data communications bus. The reading of controller application processor data to the shared memory buffers is included in the controller application processor time budget. The same data independence scheme also prevents the SSLC/ESF Q-CIM cards from sending time to the controller application processors nor will the time message be accepted since it is not needed by nor programmed as an input by the applications.

The SSLC/ESF platform uses a third dedicated, redundant network to provide intra-divisional data communication between SSLC/ESF platform, the safety-related VDUs, and the RTIF-NMS platform. These are separate and redundant Ethernet networks with only four nodes connecting the safety-related VDUs, RTIF, NMS, and SSLC/ESF. The safety-related VDUs are typically updated once per second and each display format only has a limited number of variables (as determined by human factors engineering). This set of conditions produces functional determinacy. Note that no manual operator action from the VDUs is needed for ESBWR response to design basis accidents. The VDUs are typically only used for monitoring. Manual operator action is by definition slow and limited to the estimated one second VDU update rate. This situation will not challenge the data communication links.

Another factor impacting response time determinism for the SSLC/ESF is the divisional data transmitted between its remote multiplexer units (RMUs) in the control building and reactor building. The input/output cards in the RMUs do not interrupt the controller application processors. The data are actively polled by the controller application processors on a specific cycle time. Therefore, the input/output data are deterministic at the controller application design polling rate. The time required to input and output data is included in the SSLC/ESF time budget.

7.1.2.1.2.3 ICP Determinism Design Principle

As described in Subsection 7.1.2, the ICP digital hardware platform is inherently simpler and more robust to adverse data communications and provision of deterministic data processing and communications because it does not execute, run, or use a cyclic real-time executive or operating system or any associated controller application program to perform its safety-related function. The ICP is not changeable after initial configuration and setup. Plant process conditions or status and

sensor (instrument) measurements are presented to the input gates and the data propagates (it is not "clocked") through the ICP at the rates the gate's material can support. The ICP implemented functions will have a time budget from sensor (instrument) inputs through logic gate decision making to actuator output. The end-to-end input through logic gate decision making to actuator output timing rates associated with the ICP functions required by the plant process safety-related control are very low or slow. The ICP platform's performance or response time of one to five seconds will be faster or occur with a shorter time duration than that required by the plant process it is controlling and is therefore acceptable. The resulting end-to-end input through logic gate decision making to actuator output rates will be tested. Once tested, there is no re-configuration possible to the unchangeable logic or input errors that could change the tested performance or response time rates. Based on these design features, the ICP is deterministic.

7.1.2.1.3 **Redundancy Design Principle**

The ESBWR Q-DCIS and the systems that it actuates are highly reliable. Redundancy is a design principle that addresses and mitigates single failures. Eliminating and mitigating single failures is one of many factors leading to high reliability. The ESBWR Q-DCIS specifically meets the requirements of IEEE Std. 603, sub-sections 5.1 - Single Failure Criterion and sub-section 5.6.3.3 - Effects of a Single Random Failure by providing safety-related functionality for design basis events even if a portion of the Q-DCIS has randomly failed or been damaged by that event or in the presence of spurious actuations caused by that event. The level of redundancy required by IEEE Std. 603 is such that the safety-related systems perform their safety-related functions with three out of four safety-related divisions available, in the presence of a single failure (therefore the term “N-1”). The ESBWR Q-DCIS is designed such that one of the four safety-related divisions may accidentally or deliberately be out of service and an additional random failure accepted and the remaining two divisions can provide all the required safety functions (therefore the term “N-2”). Therefore, one division of Q-DCIS can be deliberately out of service (usually for maintenance, repair or testing) then a design basis event can occur accompanied by a single random failure in the remaining Q-DCIS and the safety functions will be accomplished.

For the ESBWR, Q-DCIS redundancy is accomplished by providing four independent (See Subsection 7.1.2.1.1) and deterministic (Subsection 7.1.2.1.2) divisions that are separately and redundantly powered per each of the four safety-related divisions. Any two of the safety-related divisions can accomplish the safety functions. Although sensors (instruments) and actuators are not explicitly part of the Q-DCIS control system architecture, they are part of the mechanical systems within which they are located and therefore part of the overall plant process system. The ESBWR provides corresponding redundancy for the safety-related sensors and actuators for these associated plant process systems.

7.1.2.1.3.1 RTIF-NMS Redundancy Design Principle

The RTIF-NMS hardware/software platform is described in detail in Section 7.2. The safety-related systems implemented on the RTIF-NMS platforms have four physically, electrically and data communications separated divisions. Each division has a dedicated sensor or sensors per scram parameter. The sensors can be bypassed (i.e. not contribute to the two-out-of-four scram decision voting logic). Only one division can be bypassed at a time which is enforced by a "joystick" type bypass switch and logic. After the scram decision has been made, there is another two-out-of four final scram decision voting logic made for the final scram actuators (i.e. solenoids on the HCUs). The final scram decision can also be bypassed one division at a time. The actual scram logic is "any two like parameters that cross the setpoint will result in a scram". This scram logic remains operational or true no matter what combination of "sensor" or "logic" bypasses are implemented in the MCR.

The scram actuators are de-energized using two-out-of-four logic but electrically exist in only two divisions. This redundancy is acceptable because the safety-related systems implemented in RTIF-NMS are designed to be fail-safe and its power is redundant per division. The scheme will scram if any two divisions lose power, have critical self-diagnostic faults, communication failures or measured parameter crosses its setpoint threshold. This scheme satisfies the N-2 redundancy criterion. In the absence of a real scram requirement, the RTIF-NMS design will not scram on any single failure of the Q-DCIS. This means that RTIF-NMS will not be a credible transient initiator.

As previously described, the RTIF-NMS intra-divisional data communication between system components is carried on dual redundant “scramnet” rings and is implemented using optical fiber. The RTIF-NMS data communication to the safety-related VDUs hosted by SSLC/ESF is via dual redundant Ethernet networks and is implemented using optical fibers. The RTIF-NMS inter-divisional data communication used to support two-out-of-four voting is point-to-point, is implemented using optical fiber but is not redundant because of the fail-safe system design. In all cases loss of communication is alarmed.

7.1.2.1.3.2 SSLC/ESF Redundancy Design Principle

The SSLC/ESF hardware/software platform is described in detail in Section 7.3. The overall SSLC/ESF system design architecture is similar to RTIF-NMS in that there are four physically, electrically and data communications separated divisions. Each division has a dedicated sensor or sensors per ECCS or isolation parameter. The largest difference from RTIF-NMS is the nature of the SSLC/ESF actuators. Unlike active plants where all actuators are part of a mechanical division, the ESBWR actuators are safety-related but not solely or exclusively associated with a single division (i.e. divisionalized). For example, a squib initiated depressurization valve or IC/PCCS pool interconnect valve is safety-related but can be actuated by any of the four divisional squib initiators or divisional solenoids mounted on the valve. Typically, the arrangement is that three squib initiators/solenoids are actuated by three divisions and a fourth initiator/solenoid is actuated by

DPS. The divisional assignment of the initiators/solenoids is rotated though the various actuators to equalize SSLC/ESF computational and power loading. Since any SSLC/ESF division or DPS can actuate the valve, the safety function reliability is very high. The SSLC/ESF sense-command-actuate loop is made internally single failure proof by employing triply redundant controller application processors per division and ensuring that there are at least two output load drivers in series to the actuator where each load driver makes a two-out-of-three decision from the controller application processors' demand. This scheme and the fail "as-is" logic makes the individual ESBWR ECCS actuators reliable for both opening and inadvertent actuation.

As with RTIF-NMS, the SSLC/ESF sensors can be bypassed (i.e. not contribute to the two-out-of-four initiate or isolate decision). Only one division can be bypassed at a time which is enforced by a "joystick" type bypass switch and logic. The scheme will alarm if any divisions lose power, have critical self diagnostic faults, or experience communication failures. The scheme will initiate/isolate if, in any two divisions, any measured like parameter crosses its setpoint threshold. This scheme satisfies the N-2 redundancy criterion. The design will not initiate/isolate on any single failure of the Q-DCIS in the absence of a real initiate/isolate requirement. This means that SSLC/ESF will not be a credible transient initiator. The SSLC/ESF functions can be manually initiated at the system level by providing operator input to at least two of the four divisions. The SSLC/ESF individual components can be manually controlled from within a division with appropriate HFE safeguards.

The SSLC/ESF provides the data communications supporting the dedicated safety-related VDUs (shared with RTIF-NMS) in the MCR and RSS for systems monitoring and control by the operator. These VDUs represent the only way the corresponding divisions can be accessed and controlled by the operator. Although safety-related systems can be monitored, recorded, and alarmed by the N-DCIS, there is no possibility of nonsafety-related N-DCIS control of safety-related systems. There are always two or three redundant safety-related VDUs per division which operate independently such that a single failure in one will not result in a loss of safety-related divisional control by the operator. The networks that support the safety-related VDUs are dual redundant and loss of communication is alarmed.

As previously described, the data communication networks implemented using optical fibers that support two-out-of-four voting logic are dual redundant and loss of communications is alarmed. The hardwires, cables, and optical fibers that support the transport of input sensor signal (i.e. process parameter measurements) to the triply redundant controller application processors per division, are themselves triply redundant and alarmed. Similarly arranged hardwires, cables, and optical fibers also support the transmission of output actuation signals to the remote load drivers.

7.1.2.1.3.3 ICP Redundancy Design Principle

The ICP digital hardware platform and the four separate functions developed on it are described in Subsection 7.1.2.8. The ICP digital hardware platform does not use a cyclic real-time executive or

operating systems with an associated controller application processor. The ICP digital hardware platform is not changeable after initial setup. All of its inputs and outputs and control logic are hardwired. The ICP platform does not have internal redundancy since they provide a beyond design basis event backup control function in case the redundant safety-related function fails to operate. The ICP digital hardware platform architecture is similar to RTIF-NMS in that there are four physically, electrically and data communication separated divisions. Each division uses a dedicated sensor or sensors per function implemented. The ICP digital hardware functions are redundantly powered per division. The largest difference between the ICP digital hardware platform and either RTIF-NMS or SSLC/ESF platforms is the nature of the ICP actuators. Unlike active plants where all actuators are part of a mechanical division, the ESBWR actuators are safety-related but not divisionalized. For example, an IC isolation valve or SLC injection valve is safety-related but can be actuated by any of the squib initiators or solenoids mounted on the valve. These squib initiators and solenoids are designed to require two-out-of-four divisions of ICP to initiate the function. The scheme is always single failure proof to initiate the ICP function but not necessarily single failure proof to prevent inadvertent actuation. This is acceptable because inadvertent actuation of ICP functions does not cause large transients and because the ICP platform is, by the nature of its technology, inherently very reliable. For some functions like SLC injection, the ICPs will use two hardwired outputs in series to initiate. The design of the ICP is fail "as-is".

As with RTIF-NMS and SSLC/ESF, the ICP sensors can be bypassed (i.e. not contribute to the two-out-of-four initiate or isolate decision). Only one division can be bypassed at a time which is enforced by a "joystick" type bypass switch and logic. The scheme will alarm if any division lose power or suffer data communications failures. The scheme will initiate or isolate if, in any two divisions, any measured like parameter crosses its setpoint threshold. This scheme satisfies the N-2 redundancy criterion. The ICP functions can be manually initiated at the system level by providing operator input to at least two of the four divisions with the appropriate HFE safeguards.

The ICP functions can be monitored but not controlled by either the safety-related or nonsafety-related VDUs. They can be monitored, recorded, and alarmed by N-DCIS. All ICP function control inputs are hardwired. ICP functions do not use data communication networks to perform their safety-related functions. As previously described and similar to RTIF-NMS, the ICP point-to-point data communication implemented using optical fibers which supports the two-out-of-four ICP voting logic is not redundant but loss of communication is alarmed.

7.1.2.1.4 **Defense in Depth and Diversity (D3) Design Principle**

The overall ESBWR DCIS solution provides many features that address the design principle of defense in depth and diversity (D3) for important safety-related functions. This diversity is provided both within Q-DCIS on its the three diverse hardware/software platforms and externally to Q-DCIS within the nonsafety-related N-DCIS Diverse Protection System (DPS). Although the three diverse Q-DCIS hardware/software platforms meet all design bases requirements and it is highly

improbable that these platforms will fail, additional features are provided to mitigate against such failures, specifically software related common cause failures (CCFs). The DPS is a regulatory treatment of non- safety systems (RTNSS) and is located on the GENE N-DCIS network segment. The DPS is further discussed in Section 7.8.1 and in the LTR NEDO-33251 ESBWR I&C Defense-in-Depth and Diversity Report.

7.1.2.1.4.1 RTIF-NMS D3 Design Principle

The RTIF-NMS hardware/software platform provide the safety-related scram and MSIV isolation functions using four physically, electrically and data communication separated divisions as described in Section 7.2. Note that the RTIF-NMS hardware/software platform is diverse from those of the other two Q-DCIS platforms, SSLC/ESF and ICP. The simplest RTIF-NMS diversity feature is a manual scram and manual isolation that are each "software free" in that the manual pushbuttons in the MCR and RSS hardware panels directly interrupt the current in scram and MSIV solenoids. When initiated, the manual scram and MSIV isolation will operate independently of the status of the software or automatic logic platforms in RTIF-NMS.

The RTIF cabinets provide a backup scram should the scram solenoids on the HCUs fail in the energized condition such that they cannot be de-energized by the manual scram or automatic logic load drivers. This scheme uses relay logic to energize solenoid valves on the air header to the HCUs whenever an automatic or manual scram occurs. When the air header bleeds down, a hydraulically driven scram will occur.

Diversity for the scram function is also supplied by the ATWS/SLC ICP function and DPS platforms discussed in Subsection 7.1.2.1.4.3 and Section 7.8.1. Diversity for the MSIV isolation function is also supplied by the DPS. The safety-related ATWS/SLC ICP function and nonsafety-related DPS functions will operate independently to successfully shut down the reactor even given the complete failure of the RTIF platforms.

7.1.2.1.4.2 SSLC/ESF D3 Design Principle

The SSLC/ESF platform perform the ECCS functions and non- MSIV isolation functions. Through their safety-related VDUs, SSLC/ESF provides for both monitoring and manual control of the safety-related systems implemented on this platform. The safety-related VDUs are dedicated per division and can only control the systems within their associated division. There is no diversity within the SSLC/ESF platform. However, note that its hardware/software platform is diverse from those of the other two Q-DCIS platforms, RTIF-NMS and ICP. A common cause failure in the reactor trip system will not affect the isolation, ECCS and the monitoring systems. Conversely, a common cause failure in the SSLC/ESF platform will not prevent a reactor scram.

Diversity for some of the non-MSIV isolation functions and some of the ECCS functions are supplied by the ICS DPV Isolation Function (IDIF) implemented in ICP and DPS platforms as discussed in Subsection 7.1.2.1.4.3 and Section 7.8.1. Control of the safety-related systems is not

possible from the nonsafety-related VDUs. A common cause failure of the safety-related VDUs will not affect the SSLC/ESF to N-DCIS data communication which is implemented in a diverse manner. Therefore, monitoring and recording of the safety-related parameters by N-DCIS using its diverse VDUs remain functional.

7.1.2.1.4.3 ICP D3 Design Principle

The safety-related ICP digital hardware platform provide independent control logic to implement four key design features:

- Anticipated Transient Without Scram mitigation and Standby Liquid Control (ATWS/SLC) functions.
- Vacuum breaker (VB) Isolation Function (VBIF).
- High Pressure Control Rod Drive (HP CRD) isolation bypass function.
- Isolation Condenser System (ICS) DPV Isolation Function (IDIF).

As described in Subsection 7.1.2, The ICP digital hardware platform is diverse from those of the other two Q-DCIS hardware/software platforms, RTIF-NMS and SSLC/ESFP. The ICP platform does not use a cyclic real-time executive or operating system with associated controller application processor. The ICP platform is not changeable after setup and testing. The ICP digital hardware platform is highly immunne to a common-cause failures (CCFs) with respect to its own software based engineering design and configuration tool, itself, the other two Q-DCIS hardware/software technology control platforms. The ICP platform provide backup to the highly improbable failure of the other safety-related Q-DCIS hardware/software platforms and used to mitigate beyond design basis events. For example, ATWS/SLC is provided to mitigate against the failure of RTIF to scram the reactor. VBIF is provided to mitigate against the failure of the vacuum breakers to successfully reclose after design basis events. The HP CRD isolation bypass function is provided to mitigate against the failure of GDCS to depressurize and inject. IDIF is provided to mitigate against the failure of SSLC/ESF to isolate the ICs after depressurization. The simple and diverse nature of ICP platform and the functions implemented using it ensures these four key control actions occur even given a common cause failure of both RTIF-NMS and SSLC/ESF.

7.1.2.1.5 Simplicity Design Principle and Subjective Attribute

Given its requirements, application and purpose in the context of a nuclear power plant, the ESBWR DCIS architecture and design approach, benefits in terms of functional performance, reliability, usability, and quality based on the simple manner in which its constituent systems and components (i.e. hardware/software technology platforms) are arranged and assembled. Simplicity is a subjective attribute and hard to measure quantitatively. The ESBWR DCIS architecture and design approach was determined after reviewing the various nuclear regulatory requirements, applicable industry standards, established standard criteria for safety-related systems and industry design principles and practices specifically as well as GEH's internal product requirements and

controls development process requirements. Simplicity in overall design and process used in development is an objective and is "built in" by incorporating the following the design principles discussed below.

The safety-related systems are manually or automatically controlled by switches and VDUs of the same division. No nonsafety-related VDU or switch is able to control any safety-related component. Therefore "prioritization" modules are not needed and are not used. "Prioritization" modules involve mixing various combinations of safety-related and nonsafety-related inputs and their associated inter-dependent logic in order for it to produce its output and thereby perform its safety-related function. "Prioritization" modules are considered to be complex systems that may be difficult to fully understand and assess if they perform their safety-related function with adequate determinism and independence per the requirements of IEEE Std. 603. The ESBWR DCIS solution does not use "prioritization" modules.

The ESBWR DCIS does not perform any closed loop control over data communications networks. All safety-related and nonsafety-related controller application processors directly control the inputs and outputs needed for their function. This design approach supports determinism and minimizes inter-controller interfaces.

Providing for adequate design certification cyber security in the overall ESBWR DCIS solution involves several approaches to be robust. Design certification cyber security is built into the overall ESBWR DCIS architecture and design throughout its various access means, layers, network segments, diverse hardware/software technology platforms, system decomposition, function portioning assignment to specific components or equipment as well as a rigorous and structured systems and software development process. The systems and software lifecycle development (SDLC) process for the ESBWR DCIS soultion is governed by Section 7B Software Development.

This design and development approach forces the security concerns to be addressed early in the design process for the various concerned structures, systems, and components. Cyber security is least effective when it is an afterthough to the design and added on later.

The ESBWR RSS is designed as an auxiliary control room instead of a limited function control station. This design approach simplifies and re-uses the supporting HFE design methodology as well as operator procedure development and training.

The ESBWR DCIS controller application processors are assigned to and operate on only a few, plant process related systems. This design practice may not use the full available functional and performance capacity of the controllers. This design approach makes DCIS system and software development lifecycle phases and processes of; planning, requirements management and traceability, design, implementation, test, and installation as well as independent auditing simpler.

The ESBWR DCIS safety-related control systems do not share sensors (instruments) not even within the same division. Any network based communication between controllers or controllers and

VDUs is used only for operator monitoring and manual control, the networks do not serve a control function. This design approach supports determinism and simplicity.

The ESBWR DCIS and MCR is designed to eliminate copper wiring associated with the sense-command-actuate control loop. The design approach reduces other copper wiring associated with controls to the minimum level possible. This design approach simplifies the fire hazards, inadvertent actuation and related probabilistic risk analyses.

The ESBWR DCIS nonsafety-related reactor level control, reactor pressure control, control rod position control, feedwater temperature control and automation control systems are located in separate cabinets. Although these major reactor control systems are not implemented on diverse control systems, they are implemented on separate dual and triply redundant controllers. A hardware or application software failure will not simultaneously disable more than one function (e.g. the failure of the reactor level control system will not cause pressure control to be lost, a feedwater controller runaway transient will not be accompanied by a feedwater temperature controller runaway). This design approach simplifies plant performance and transient analyses.

The ESBWR DCIS safety-related and nonsafety-related control systems are single failure proof. This design requirement re-classifies certain transient events from anticipated operational occurrences to infrequent events. Infrequent events are non- contributors to fuel thermal limits contribution and reduce the challenge to soft duty guidelines. This design approach simplifies plant performance and transient analyses and related probabilistic risk analyses.

The ESBWR N-DCIS solution will selectively employ non- native or commercial off-the-shelf "packaged" control systems and supporting digital systems, equipment, and devices (e.g. environmental monitoring systems). These systems are interfaced with the N-DCIS network segment only through cyber secure, managed network switches or gateways. This design approach simplifies achieving a high degree of cyber security assurance.

The ESBWR DCIS data communication is predominately implemented using optical fiber. This design approach simplifies; implementing data isolation techniques, minimizes conduit, tray, and raceway fill constraints in physical layout design, and fire analyses and related probabilistic risk analyses.

The ESBWR DCIS data communication links use remote multiplexing unit technology to the maximum extent possible. This design approach minimizes the use of copper wiring and simplifies voltage drop analyses and the need for mitigating designs and implementations (e.g. for the reactor trip system interfacing with the HCU).

7.1.2.2 **Q-DCIS Power Generation (Nonsafety-Related) Design Bases Summary**

The power generation design bases for the Q-DCIS are to transmit safety-related system data through qualified isolation devices to the N-DCIS (via datalinks and gateways) for historical trending, analysis, and alarm management functions.

7.1.2.3 Q-DCIS Safety Evaluation Summary

The Q-DCIS conforms to IEEE Std. 603 criteria for safety-related I&C systems.

The Q-DCIS is arranged into four divisions. The intra-divisional and safety-related to nonsafety-related fiber-optic cable communication paths are redundant to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. No failure of any single hardware component, in any one division, can lead to an inadvertent trip. Safety-related cabinets and chassis are powered by redundant safety-related UPS for both reliability and diagnostic capability. For communications between divisions of safety-related systems, there is no single communication or power failure that results in the loss of a safety-related function. A dual communication or power failure can result in the loss of a single division but not in the loss of a safety-related function.

Safety-related systems perform their safety-related functions with three out of four safety-related divisions available, in the presence of a single failure. For the ESBWR design basis, the term N-2 means that one of the four safety-related divisions may accidentally or deliberately be out of service; an additional random failure accepted and the remaining two divisions can provide all the required safety functions. In accordance with the ESBWR N-2 design basis, a two division failure which requires four communications or power failures, does not result in the loss of a safety-related function.

Table 7.1-1 identifies the DCIS systems and the associated regulatory requirements, guidelines, and codes and standards applied in accordance with the Standard Review Plan (SRP). The following subsection summarizes conformance of I&C systems to regulatory requirements, guidelines, and industry standards.

7.1.2.4 Q-DCIS Regulatory Requirements Conformance Summary

The Q-DCIS conforms to the applicable portions of:

- 10 CFR 50.34, 10 CFR 50.44, 10 CFR 50.49, 10 CFR 50.55, 10 CFR 50.62, 10 CFR 50.63, and 10 CFR 52.47.
- NUREGs 694, 718, 737, NUREG/CR-6083, and NUREG/CR-6303.
- IEEE Std. 7-4.3.2, 323, 344, 379, 338, 383, 384, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1050, and 1074.
- American National Standards Institute (ANSI)/Instrument Society of America (ISA) 67.02.01 and 67.04.01.
- General Design Criteria (GDC) 1, 2, 4, 10, 12, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 41, 43, 44, 63, and 64.
- Staff Requirements Memoranda (SRM) on Item II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) and Item II.T (Control Room Annunciator (Alarm)

Reliability) of SECY 93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs).

- Regulatory Guides (RGs) 1.22, 1.45, 1.47, 1.53, 1.62, 1.75, 1.89, 1.97, 1.100, 1.105, 1.118, 1.151, 1.152, 1.153, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, 1.204, and 1.209.
- Branch Technical Positions (BTPs) HICB-1, 8, 9, 10, 11, 12, 14, 16, 17, 18, 19, and 21.

7.1.2.5 Q-DCIS Testing and Inspection Requirements Summary

The Q-DCIS integrated hardware and software functions, including the network parameters and data status, are checked and tested together. The Analog-to-Digital (A/D) converters in the RMUs are the only components requiring periodic calibration checks. Key diagnostics include:

- The central processing unit (CPU) status check
- Parity checks, watchdog timer status
- Voltage level in controllers
- Data path integrity and data validation checks
- Data cycling time
- Processor clock time

7.1.2.6 Q-DCIS Operator Interface Requirements Summary

The Q-DCIS VDUs support operator monitoring and manual control of the safety-related systems. The VDUs present process and diagnostic alarm information. When one of the two power supplies or communications paths within a division fails, the division and VDU operation continue automatically, without operator intervention. Failures in three divisions are required before there is a loss of a safety-related function.

The Q-DCIS indications and alarms provided in the MCR, as a minimum, are:

- Q-DCIS MCR alarms for Division 1, 2, 3, and 4 trouble
- Q-DCIS MCR indications for Division 1, 2, 3, and 4 diagnostic displays

7.1.2.7 Q-DCIS Boundary Summary

There are no Q-DCIS components in the N-DCIS. The Q-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.2.8 Q-DCIS Major Systems Description Summary

The Q-DCIS systems and components include equipment for the Reactor Trip System (RTS), and Engineered Safety Features Actuation System (ESFAS). The RTS includes the RPS function, the SRNM and PRNM functions of the NMS, and the SPTM function of the CMS. The SSLC/ESF is the designated ESFAS. The automatic decision-making and trip logic functions associated with the safety-related RTS and ESFAS are accomplished by independent, separate, and diverse protection

logic platforms, each using four logic-processing divisions. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action through the associated actuation devices (for example, pilot solenoid valves, squib valves, and air operated valves). The Q-DCIS also includes the ICP platform and systems which include the ATWS/SLC functions, VB isolation function, HP CRD isolation bypass function, and ICS DPV isolation function.

7.1.2.8.1 **Reactor Protection System Description Summary**

The RPS implements the reactor trip functions. The RPS is the overall collection of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiates rapid insertion of control rods to shut down the reactor in situations that could result in unsafe reactor operations. This action prevents or limits fuel damage and system pressure excursions, minimizing the release of radioactive material.

The RPS also establishes appropriate logic for different reactor operating modes, provides monitoring and control signals to other systems, and actuates alarms.

The RPS overrides selected operator actions and process controls and is based on a fail-safe design philosophy. The RPS design provides reliable, single failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. This is accomplished through the combination of fail-safe and fault-tolerant equipment design, and a two-out-of-four voting logic algorithm.

The RTIF cabinets house the ICP platform systems, which include the ATWS/SLC functions, the VB isolation function, and the HP CRD isolation bypass function, the logics for the ATWS/SLC functions, VB isolation function, HP CRD isolation bypass function, and ICS DPV isolation function. Space consideration may dictate locating the ICP hardware in separate cabinets. The ICP uses diverse hardware from the other two Q-DCIS platforms; RTIF-NMS and SSLC/ESF. The ICP logic function design is fail "as-is". The RPS hardware/software platform is diverse from the SSLC/ESF hardware/software, from the ICP hardware platform, and from the Diverse Protection System (DPS) hardware/software platforms. The RPS and DPS sensors are diverse and RPS sensors are not shared with other Q-DCIS or N-DCIS systems.

7.1.2.8.2 **Neutron Monitoring System Description Summary**

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

- The SRNM system monitors thermal neutron flux levels from very low average power levels to a power level above 15% of rated power. Between 1% and 15% of rated power the monitoring

function overlaps the LPRM/APRM systems functions to assure continuous monitoring of thermal neutron flux levels. The SRNM channel is able to provide local power information up to 100% of rated power. The SRNM system generates trip signals to prevent fuel damage resulting from abnormal positive reactivity insertions under conditions that are not covered by the APRMs. The SRNMs generate trips on high neutron flux and high rate of increase in neutron flux (i.e., high startup rate or short reactor period).

- The PRNM system includes the LPRM, the APRM, and the OPRM functions. The outputs of the individual LPRMs are averaged to provide the average power level of the reactor core, and the OPRM System provides monitoring of neutron flux and core thermal hydraulic instabilities.
- The Automatic Fixed In-core Probe (AFIP) is a nonsafety-related component of the NMS system and does not provide information to the Q-DCIS. It calibrates the LPRM system by providing neutron flux information to 3D MONICORE.
- The Multi-Channel Rod Block Monitor (MRBM) is a nonsafety-related component of the NMS system and is completely isolated from the Q-DCIS by one-way communication through qualified safety-related isolation devices and via fiber-optic cable communication. It provides control rod blocks to the Rod Control and Information System (RC&IS) to prevent core thermal limit violations.

7.1.2.8.3 SSLC/ESF System Description Summary

The SSLC/ESF is the overall collection of instrument channels, trip logics, trip actuators, manual controls, and actuation logic circuitry that initiates protective action to mitigate the consequences of design basis events (DBEs). Input signals from redundant channels of safety-related instrumentation are used to make trip decisions and perform logic operations that result in accident mitigating actions. The SSLC/ESF provides the automatic decision-making and trip logic to actuate:

- The various ECCS
- Leak detection, containment isolation, and radioactivity release barrier defense
- Control room habitability

7.1.2.8.3.1 Emergency Core Cooling System Description Summary

The ECCS provides emergency core cooling for events that threaten reactor coolant inventory, such as a Loss-of-Coolant-Accident (LOCA). The ECCS comprises the ADS, the GDCS, the ICS, and the SLC system. The ECCS function is discussed further in Subsection 7.3.1.

7.1.2.8.3.1.1 Automatic Depressurization System Description Summary

The ADS resides within the Nuclear Boiler System (NBS) and comprises Safety Relief Valves (SRVs), Depressurization Valves (DPVs), and associated I&C. The ADS depressurizes the reactor to allow the low head GDCS to provide makeup coolant to the reactor. The ADS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.3.1.2 Gravity-Driven Cooling System Description Summary

Following the receipt of an actuation signal, the GDCS provides emergency core cooling when the reactor has been depressurized. The GDCS is capable of injecting large volumes of water into the Reactor Pressure Vessel (RPV) to keep the core covered for at least 72 hours following a LOCA. The GDCS also performs a deluge function that drains the GDCS pools to the lower drywell if a severe accident core melt sequence occurs. The GDCS deluge logic, which is nonsafety-related except for permissives to avoid inadvertent actuation, is separate and diverse from the Q-DCIS. The basic components of the GDCS are within the containment. The GDCS pools, piping, and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope. The GDCS I&C is designed to:

- Automatically initiate the GDCS to prevent fuel cladding temperatures from reaching their limits.
- Respond to a need for emergency core cooling following reactor depressurization.
- Be completely automatic in operation. Manual initiation of the GDCS is possible at any time providing protective permissive conditions have been satisfied.
- Prevent the inadvertent actuation of the deluge valves, thus preventing inadvertent draining of the GDCS pools.

7.1.2.8.3.1.3 Isolation Condenser System Description Summary

The ICS removes reactor decay heat following reactor shutdown and isolation. It also prevents unnecessary reactor depressurization and operation of the ECCS. The primary function of the ICS is to limit reactor pressure and prevent SRV operation following an isolation of the main steam lines. The ICS, together with the water stored in the RPV, provides sufficient reactor coolant volumes to avoid automatic depressurization caused by low reactor water level. The ICS passively removes excess sensible and core decay heat from the reactor, with minimal loss of coolant inventory from the reactor, when the normal heat removal systems are unavailable. The primary ICS logic resides in the SSLC/ESF platform of the Q-DCIS. Refer to Subsection 7.4.4 for additional information.

The ICS DPV isolation function control logic is implemented in the ICP. Refer to Subsection 7.3.7 for additional information.

The nonsafety-related ICS vent function control logic is implemented in the DPS. Refer to Subsection 7.8.1.1 for additional information.

7.1.2.8.3.1.4 Standby Liquid Control System Description Summary

The SLC system performs dual functions. In its ECCS mode, it provides additional coolant inventory to respond to a LOCA. It is also a backup method for bringing the nuclear reactor to subcriticality, by adding soluble poison, and then maintaining subcriticality as the reactor cools.

The SLC system bases are discussed in Subsection 7.4.1. The SLC logic resides in the SSLC/ESF and the ATWS/SLC portions of the Q-DCIS.

7.1.2.8.3.2 Leak Detection and Isolation System Description Summary

The LD&IS monitors leakage sources from the Reactor Coolant Pressure Boundary (RCPB). It automatically initiates closure of the appropriate valves to isolate the source of the leak if monitored system variables exceed preset limits. This limits coolant release from the RCPB and, therefore, the release of radioactive materials into the environment. Refer to Subsection 7.3.3 for additional information.

The MSIV isolation logic of the LD&IS is fail-safe and therefore performed as part of the RTIF logic platform. The non-MSIV isolation logic of the LD&IS is performed as part of the SSLC/ESF logic platform.

7.1.2.8.3.3 Control Room Habitability System Description Summary

The primary function of the CRHS is to provide a safe environment for the operators to control the nuclear reactor and its auxiliary systems. The CRHS monitors the Control Room Habitability Area (CRHA) inlet ventilation air and actuates logic to isolate and filter the CRHA on detection of hazardous environmental conditions. The CRHS logic resides in the SSLC/ESF portion of the Q-DCIS.

7.1.2.8.4 ATWS/SLC System Description Summary

The ATWS mitigation logic provides a diverse means of reducing power excursions from certain transients and a diverse means of emergency shutdown. The ATWS mitigation logic, which uses the soluble boron injection capability of the SLC system as a diverse means of negative reactivity insertion, is implemented using the ICP as safety-related logic (designated as ATWS/SLC), and is diverse from the RTIF-NMS platform and the SSLC/ESF platform and therefore not susceptible to a common-cause failure. The ATWS/SLC logic also provides a feedwater run-back signal to attenuate power excursions.

In the event that the control rods cannot provide sufficient negative reactivity insertion, the SLC system provides the capability of an orderly and safe shutdown by a diverse means. In addition to providing hot shutdown capability, the SLC is sized to counteract the positive reactivity that results from shutting down from rated power to a cold shutdown condition. The SLC system can be initiated manually, or automatically via the ATWS mitigation logic or the SSLC/ESF logic as an ECCS function. (Refer to Subsection 7.1.2.8.3.1.4.) The SLC logic resides on the SSLC/ESF and ATWS/SLC portions of the Q-DCIS.

The nonsafety-related ATWS mitigation logic is implemented in the DPS. Refer to Subsection 7.8.1.1.

7.1.2.8.5 Passive Containment Cooling System Description Summary

The Passive Containment Cooling System (PCCS) cools the containment following a rise in containment pressure and temperature without requiring any component actuation. The PCCS

does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation in the first 72 hours after a LOCA. For long-term effectiveness of the PCCS, the vent fans are manually initiated by operator action. Refer to Subsections 7.3.2 and 6.2.2 for additional information.

7.1.2.8.6 Containment Monitoring System Description Summary

The CMS provides the functions identified in Subsections 7.1.2.8.6.1 and 7.1.2.8.6.2. Refer to Subsection 7.5.2 for additional information.

7.1.2.8.6.1 Suppression Pool Temperature Monitoring Subsystem Description Summary

The safety-related SPTM function is part of the CMS and monitors suppression pool temperatures under all operating and accident conditions. Should the suppression pool temperature exceed established limits, SPTM provides input for both a reactor scram and for automatic initiation of the suppression pool cooling mode of the Fuel and Auxiliary Pools Cooling System (FAPCS) operation. Unless there are space constraints, the RTIF cabinet houses the equipment that performs the Suppression Pool Temperature Monitoring functions for the CMS discussed in Subsection 7.5.2.

7.1.2.8.6.2 Other Containment Monitoring Systems Description Summary

Other CMS functions, some of which are nonsafety-related, include monitoring several key containment parameters. These include fluid and radiation levels, pressures, temperatures, hydrogen/oxygen concentrations, and dew point/humidity values. These parameters are monitored during normal reactor operations and post-accident conditions to evaluate the containment integrity and other conditions. Abnormal measurements and indications initiate alarms in the MCR.

7.1.2.8.7 Vacuum Breaker Isolation Function

The safety-related VB isolation function prevents the loss of long-term containment integrity by automatically isolating an excessively leaking VB using a VB isolation valve. Unless there are space constraints, the RTIF cabinet houses the equipment that performs the VB isolation function. The VB isolation function is implemented using the ICP digital hardware platform, which is diverse from the RTIF-NMS and the SSLC/ESF hardware/software platforms.The ICP digital hardware platform is highly immunne to a common-cause failures (CCFs) with respect to its own software based engineering design and configuration tool, itself, the other two Q-DCIS hardware/software technology control platforms. Refer to Subsection 7.3.6 for additional information.

7.1.2.8.8 HP CRD Isolation Bypass Function

The safety-related HP CRD isolation bypass function automatically bypasses the HP CRD injection isolation (intended to prevent the over-pressurization of the containment and therefore loss of long-term containment integrity) to compensate for a failure of the GDCS to inject. Unless there are space constraints, the RTIF cabinet houses the equipment that performs the HP CRD isolation

bypass function. The HP CRD isolation bypass function is implemented using the ICP digital hardware platform, which is diverse from the RTIF-NMS and the SSLC/ESF hardware/software platforms. The ICP digital hardware platform is highly immune to a common-cause failures (CCFs) with respect to its own software based engineering design and configuration tool, itself, the other two Q-DCIS hardware/software technology control platforms. Refer to Section 4.6 as well as Subsections 7.3.3 and 7.4.5 for additional information.

7.1.2.8.9 ICS DPV Isolation Function

The ICS DPV isolation function ensures that, upon detection of DPV open position, there is no loss of long-term containment integrity. It is implemented in the ICP platform. Refer to Section 7.3.7 for additional information.

7.1.3 Q-DCIS Specifics

The Q-DCIS architecture, its relationships, and its acceptance criteria are described below. The Q-DCIS data communication systems are embedded in the DCIS, which performs the data communication functions that are part of or support the systems described in Sections 7.2 through 7.8. A simplified network functional diagram of the DCIS appears as Figure 7.1-1, which shows the elements of the Q-DCIS and the N-DCIS, and is a functional representation of the design.

7.1.3.1 Q-DCIS Design Bases

7.1.3.1.1 Q-DCIS Safety-Related Design Bases

The safety-related design bases applicable to the Q-DCIS are found in IEEE Std. 603, Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, and 4.12. These sections specify that the Q-DCIS:

- Reads signals from the safety-related instrumentation locally and through RMUs.
- Performs required signal conditioning, if this function is required, and then digitizes and formats the input signals into messages for transmission on the Q-DCIS network or data path.
- Transmits the data signals and commands onto the Q-DCIS network or data path for interface with other safety-related systems.
- Supports safety-related system monitoring and operator input to and from the MCR and RSS VDUs.
- Performs safety-related logic functions.
- Performs closed loop control and logic independently of the VDUs.
- Transmits the actuation signals to safety-related equipment via load drivers or contactors.
- Provides self-diagnostic and process alarm information to the operator.
- Isolates data communication to and from the N-DCIS.

7.1.3.1.2 Q-DCIS Power Generation (Nonsafety-Related) Design Bases

The power generation design basis for the Q-DCIS is to transmit plant parameters and other safety-related system data through qualified safety-related isolation devices to the N-DCIS for use by nonsafety-related system logic and displays for power generation.

7.1.3.1.3 Q-DCIS Setpoint Methodology

To determine setpoints and select appropriate I&C, the following are considered: range, accuracy, resolution, instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error. The response time of the instrument is assumed in the safety analysis and verified in plant-specific surveillance testing. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; the Q-DCIS equipment is micro-processor based with discrete setpoints that do not drift.

The actual settings are determined from operating experience or conservative analyses when specific instrument operating experience is not available. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of the safety-related action. At the same time, they are far enough from the analyzed trip values to ensure that appropriate margins are maintained between the actual settings and the analyzed values. The margin between the limiting safety-related system settings and the actual safety limits include consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components. Setpoints are established for the Q-DCIS systems in accordance with Reference 7.1-9.

7.1.3.2 Q-DCIS Description

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

The Q-DCIS contains multiple dual redundant fiber-optic cable networks for each of the four divisions. The networks connect the RMUs with:

- Divisional safety-related VDUs.
- RTIF and NMS Digital Trip Modules (DTMs).
- RTIF and NMS CIMs.

- SSLC/ESF CIMs.
- RTIF, NMS, and SSLC/ESF cabinets, located in the safety-related Q-DCIS equipment rooms in the RB and CB.
- The N-DCIS, through qualified safety-related isolation devices via datalinks and gateways.

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

An RMU is an assembly of divisional Input/Output (I/O) equipment, power supplies and any logic housed in one cabinet. The field and process sensors are hardwired to the divisional local RMUs in the RB and CB. At the input module of the field RMUs, the analog data are delivered to the analog input modules and discrete data are delivered to the digital input modules. The field sensors, actuators, and wiring belong to the process system to which they are attached and are not part of the Q-DCIS. Analog signal conditioning, A/D conversion, and digital signal conditioning such as filtering and voltage level conversion are performed at the input modules.

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

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

The Q-DCIS RMUs in the RB and safety-related logic cabinets in the CB are located in mild environments. The rooms containing this equipment are cooled by nonsafety-related Heating, Ventilation and Air Conditioning (HVAC) during normal operation when either offsite or diesel generator power is available. When no active cooling is available, such as when the system is operating on only battery power during a Station Blackout (SBO), the cooling is passive. The Q-DCIS components, including the fiber-optic cable network, are not located in containment or in high radiation areas. Signals from within these areas are hardwired by copper cable to the RMUs. Electromagnetic compatibility (EMC) of the RMUs and Q-DCIS equipment is ensured by conformance to the following program.

- The Q-DCIS components are designed to minimize susceptibility to and generation of electromagnetic interference (EMI) and radio frequency interference (RFI).
- The Q-DCIS components are subjected to tests for EMI, RFI, and surge conditions that conform to guidelines in RG 1.180.

- Grounding of RMU and Q-DCIS equipment follows the guidance given in IEEE Std. 518 and IEEE Std. 1050.

To minimize EMI effects, the Q-DCIS electrical equipment incorporates shielding and filtering. The equipment is mounted in grounded panels provided with isolated instrument grounds.

The four divisions of Q-DCIS are physically located in four separate quadrants of the Reactor Building and four separate equipment rooms in the Control Building. These locations represent separate fire areas. Within the Reactor Building, there are separate fire areas within a division. The intra division fire areas are used to separate the RMUs that contain the series-connected load drivers used to operate safety-related solenoids and squib valves. The same Reactor Building fire areas are used to separate the DPS RMUs that contain the series-connected multiple load drivers used to operate nonsafety-related solenoids and squib valves. The fire area separation for both the safety-related and nonsafety-related RMUs will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the Control Building Q-DCIS, N-DCIS, and DPS rooms are all separated into different fire areas.

7.1.3.2.1 Reactor Trip Systems

The Reactor Trip Systems include the RPS, the NMS, and SPTM functions.

7.1.3.2.1.1 Reactor Protection System

The safety-related RPS initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage and limits system pressure, thus minimizing the release of radioactive material. Refer to Subsection 7.2.1 for additional information.

7.1.3.2.1.2 Neutron Monitoring System

The safety-related NMS monitors the core thermal neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor when a condition necessitating a reactor scram is detected. Refer to Subsection 7.2.2 for additional information.

7.1.3.2.1.3 Suppression Pool Temperature Monitoring Subsystem

The safety-related SPTM function of the CMS monitors suppression pool temperatures under all operating and accident conditions. This subsystem operates continuously during reactor operation. If the suppression pool temperature exceeds established limits, SPTM provides input for a reactor scram and for automatic initiation of the suppression pool cooling mode of the FAPCS. Refer to Subsection 7.2.3 for additional information.

7.1.3.2.2 Safety System Logic and Control / Engineered Safety Features System

The SSLC/ESF system performs the control logic processing of the plant sensor data and manual control switch signals activating the functions of the LD&IS (non-MSIV), ECCS, and CRHS. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety-related action. Trip logic outputs to the actuation devices, such as pilot solenoid valves and squib valves, initiate the appropriate plant protection actions. Refer to Subsection 7.3.5 for additional information.

7.1.3.2.2.1 Emergency Core Cooling System

The safety-related ECCS is an engineered safety feature that mitigates LOCAs by automatically initiating:

- The ICS (Refer to Subsection 7.4.4)
- The ADS (Refer to Subsection 7.3.1.1)
- The GDCS (Refer to Subsection 7.3.1.2)
- The SLC system (Refer to Subsection 7.4.1)

7.1.3.2.2.2 (Deleted)

7.1.3.2.2.3 Leak Detection and Isolation System

The safety-related LD&IS monitors leakage sources from the RCPB. It automatically initiates closure of the appropriate valves to isolate the source of the leak if the monitored system variables exceed preset limits. This action limits the loss of coolant from the RCPB and the release of radioactive materials to the environment. Refer to Subsection 7.3.3 for additional information.

7.1.3.2.2.4 Control Room Habitability Systems

The safety-related CRHS provides a safe environment within the MCR that allows the operator(s) to:

- Control the nuclear reactor and its auxiliary systems during normal conditions
- Safely shut down the reactor
- Maintain the reactor in a safe condition during abnormal events and accidents

The CRHS includes CB shielding, area radiation monitoring and a CRHA Heating, Ventilation and Air Conditioning (HVAC) System. The CRHS provides emergency food and water storage; emergency kitchen and sanitary facilities; protection from and removal of airborne radioactive contaminants; and the capability to remove smoke. The CRHA envelope, ventilation inlet/return isolation dampers, redundant Emergency Filter Units (EFUs) in the emergency HVAC system, and associated controls are safety-related. Refer to Subsection 7.3.4 for more information.

7.1.3.2.2.5 (Deleted)

7.1.3.2.2.6 Passive Containment Cooling System

A description is included in Subsection 7.1.2.8.5 for completeness. Refer to Subsections 7.3.2 and 6.2.2 for additional information.

7.1.3.2.3 Safe Shutdown Systems

Safe shutdown systems include the SLC system and the RSS.

7.1.3.2.3.1 Standby Liquid Control System

The safety-related SLC system provides a diverse means to shut down the reactor from full power to a subcritical condition, and then maintains the reactor subcritical using soluble boron injection. The SLC system can be manually initiated or initiated automatically for ATWS mitigation. The SLC system is also initiated automatically in response to LOCAs as part of the ECCS. Refer to Subsections 7.1.2.8.3.1.4, 7.1.2.8.4, and 7.4.1 for additional information.

7.1.3.2.3.2 Remote Shutdown System

The RSS has two redundant and independent panels located in two different areas in the RB. If the MCR becomes uninhabitable, Division 1 and 2 safety-related parameters and nonsafety-related parameters displayed or controlled at a Q-DCIS, and N-DCIS MCR VDU can be monitored and controlled from either of the RSS panels. Refer to Subsection 7.4.2 for additional information.

7.1.3.2.4 Safety-Related Information Systems

Safety-related information systems include the Post-Accident Monitoring (PAM) instrumentation, the CMS instrumentation, and Process Radiation Monitoring System (PRMS) instrumentation.

7.1.3.2.4.1 Post-Accident Monitoring Instrumentation

The PAM instrumentation monitors variables and systems under accident conditions to ensure plant and personnel safety. An assessment of conformance to RG 1.97 is presented in Subsection 7.5.1.

7.1.3.2.4.2 Containment Monitoring System

The CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in containment under post-accident conditions. The CMS is designed to operate continuously during normal operation and is automatically put in service upon detection of LOCA conditions. Refer to Subsection 7.5.2 for additional information.

7.1.3.2.4.3 Process Radiation Monitoring System

Safety-related PRMS instrumentation monitors the following for radioactive materials: discharges from the ICS vent, and ventilation discharges. The nonsafety-related PRMS is discussed in Subsection 7.1.5.2.2.1. The MCR display, recording, and alarm capabilities are provided along with

controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 11.5.3 for additional information.

7.1.3.2.5 Interlock Logic

The interlock logic functions are embedded in the DCIS logic, so that a separate interlock system is not required. Refer to Section 7.6 for additional information.

7.1.3.2.6 Nuclear Boiler System Instrumentation

Redundant NBS safety-related instrumentation provides the following data for operator monitoring:

- RPV water level indicated in the MCR on displays associated with the different water level ranges.
- The reactor pressure indicated in the MCR and at four local instrument racks in the Reactor Building (RB).
- The discharge line temperatures of the SRVs viewed on safety-related video display units (VDUs) in the MCR. Any temperature exceeding the trip setting is used to indicate leakage of a SRV seat.
- RPV temperature is indicated in the MCR, and high bottom head to reactor coolant differential temperature is indicated in the MCR.
- Main steam flow rate is indicated in the MCR.

The NBS instrumentation also provides inputs to the safety-related actuation systems during normal, transient, and accident conditions. Refer to Sections 7.2 and 7.3 for additional information.

7.1.3.2.7 Data Communication Systems

The DCIS data communication functions are embedded within the Q-DCIS and the N-DCIS architectures. Safety-related Q-DCIS internal and external communication protocols are deterministic.

7.1.3.3 Q-DCIS Safety Evaluation

All communication between the Q-DCIS and the N-DCIS is through safety-related CIMs, via datalinks and fiber-optic cable. Fiber-optic cable is also used for:

- Limited communication between the Q-DCIS divisions (such as the two-out-of-four voting logic)
- Communication within a division
- Providing data to the VDU monitors
- Transferring VDU outputs corresponding to manual initiation actions

The dual redundant fiber-optic cable data networks described below replace the many conventional, long length, copper conductor cables of existing nuclear power plants. This reduces the cost and complexity of divisional cable runs that connect components of the plant protection

and safety-related systems such as the RPS, MSIV isolation logic functions, LD&IS containment isolation functions, SSLC/ESF, and safety-related VDUs. The fiber-optic cable provides transmission path immune from EMI for plant sensor data and safety-related system control signals.

7.1.3.3.1 Safety-Related Isolation

The use of fiber-optic cable provides complete electrical isolation between components and noise free communication pathways, but is not credited for either the safety-related isolation or the safety-related separation. The safety-related fiber-optic CIMs are the isolation devices, including data isolation, and convert signals between electricity and light on the safety-related side of the fiber-optic cable. These safety-related fiber-optic CIMs are powered by the division within which they are physically located. The safety-related fiber-optic CIMs, which provide the safety-related isolation and separation, are qualified safety-related components.

The IEEE Std. 603, Sections 5.6 and 6.3, isolation and separation (electrical, physical, data, and communications) occurs in the safety-related fiber-optic CIM (transmitter or receiver) where the signal is converted between electricity and light. Although IEEE Std. 383 is applicable to electrical cable, the fiber-optic cables are sheathed in material meeting the IEEE Std. 383 that addresses fire propagation mitigation.

The physical communication between safety-related systems and between safety-related and nonsafety-related systems is via fiber-optic cable. Within the safety-related system, the electrical to light interface (the CIM) is safety-related. There is no credible seismic event, design basis accident (DBA), etc. that could cause a failure of the isolation barrier between the safety-related or safety-related/nonsafety-related portions of the isolator (specifically, the components at each end of the fiber-optic cable). Although unlikely, the worst-case failure is loss of communication. Therefore, the design complies with IEEE Std. 603, Section 5.6.

In addition to the assured electrical isolation and separation, data/communication isolation enforces the design basis that no safety-related function depends on nonsafety-related communication. The safety-related Q-DCIS communications are governed by both hardware and software protocols. These protocols are governed by References 7.1-10 and 7.1-12 and control the transmission, acceptance, and authentication of data from outside the division so that these communications cannot adversely affect the operation or safety-related functions of that division. The communication protocols meet the design principles of the Q-DCIS CIMs as described in Subsection 7.1.3.3.2. Note that whether or not the CIM is operable or whether there is anything functional on the nonsafety-related side or other divisional safety-related side of the CIM, the operation of the safety-related system is not affected.

7.1.3.3.2 Communication Pathways (CIMs, Fiber-Optic Cable, Datalinks, and Nonsafety-Related Gateways)

Instances of nonsafety-related to safety-related communication (described below) are also via fiber-optic cable, datalinks, gateways, and through safety-related fiber-optic CIMs (in order to provide the required safety-related isolation, separation, and message authentication). The safety-related fiber-optic CIMs receiving data from the N-DCIS are qualified safety-related (Q-DCIS) components. Safety-related system functions do not depend on the correctness or even the existence of the safety-related/nonsafety-related communications. The loss of any communication in either direction only results in alarms and the potential loss of data between the Q-DCIS and the N-DCIS. Any single divisional data loss to N-DCIS does not affect power generation or safety. The loss of all safety-related data to N-DCIS can potentially affect power generation but only in a long-term situation, such as core thermal limits monitoring.

The Q-DCIS is arranged into four independent divisions. Other than the RPS and NMS point-to-point communication used for two-out-of-four voting logic, the intra-divisional and safety-related to nonsafety-related fiber-optic cable communication pathways are redundant in order to support reliability and to allow self-diagnostics to be communicated in the presence of a single failure. The RPS and NMS two-out-of-four voting logic communication redundancy is acceptable because loss of communication is interpreted as a trip from the sending division. Similarly, all safety-related cabinets and chassis are powered by redundant UPS for reliability and self-diagnostics. For all safety-related to safety-related communication, safety-related functions continue to be initiated and executed in the presence of any single or dual communication or power failure. A dual communication or power failure could result in the loss of a single independent division but not in the loss of a safety-related function. A dual-division failure, requiring four communications or power failures, does not result in the loss of a safety-related function.

The safety-related fiber-optic CIMs (which are the isolation devices, as described above) within the Q-DCIS along with datalinks and gateways within the N-DCIS transmit safety-related data to the N-DCIS via fiber-optic cable. The gateways are specific to the communication link between the sending and receiving components. For example, the gateway between the SSLC/ESF and N-DCIS is different from the gateway between the RTIF-NMS and the N-DCIS. The sending sources are different even though the receivers are the same.

Safety-related software is as simple as possible so that Q-DCIS components have neither interrupts from nonsafety-related devices nor do they respond to nonsafety-related component queries for information. The Q-DCIS components simply put information on the safety-related (Q-DCIS) networks in a known format so that other safety-related devices can retrieve what is needed for their function. Self-diagnostics information is also put on the DCIS networks. The safety-related fiber-optic CIMs provide the safety-related isolation. The CIMs indiscriminately retrieve all of the divisional information from the safety-related (Q-DCIS) networks and send it one way to the N-DCIS

(via fiber-optic cable and a datalink or via a combination of fiber-optic cable, datalinks and nonsafety-related gateways). Time tags are described below.

7.1.3.3.3 **Nonsafety-Related Gateways**

The nonsafety-related gateways translate the information sent between the Q-DCIS (through the required isolation, via datalinks and fiber-optic cable) and the N-DCIS into a format that the other portion of the DCIS (either N-DCIS or Q-DCIS) can apply. The N-DCIS gateways package the safety-related information into the necessary message packets to support specific N-DCIS components for monitoring and alarm management purposes. The N-DCIS gateways also respond to interrupts and queries. Safety-related to nonsafety-related communication pathways that do not involve nonsafety-related gateways use safety-related fiber-optic CIMs (which provide the safety-related isolation), datalinks, and fiber-optic cable. Nonsafety-related gateways are not used when the N-DCIS (nonsafety-related receiver) is capable of receiving and extracting the data signal generated by the Q-DCIS (safety-related fiber-optic CIM) without the need for data conversion. One example of datalink communication between the Q-DCIS and the N-DCIS without the use of a nonsafety-related gateway is the communication from the NMS to the MRBM and automated thermal limit monitor (ATLM). The nonsafety-related gateways, handle the data translation/packaging interface, but do not serve to provide the required safety-related isolation for communications between the Q-DCIS and the N-DCIS. When nonsafety-related gateways are necessary they package the data for the various N-DCIS functions, respond to the N-DCIS requests for information and monitor communication link status. The safety-related isolation and separation for communications between the Q-DCIS and the N-DCIS is provided by the safety-related CIMs, as described above, regardless of whether a combination of datalinks and gateways is used or only a datalink is used.

7.1.3.3.4 **Communication from N-DCIS to Q-DCIS (DCIS Time tagging and NMS Calibration)**

The safety-related systems are designed to not depend on nonsafety-related communication to function, therefore, loss of communication is not a safety issue. Specifically, no process feedback signals are sent from the N-DCIS to the Q-DCIS. The only signals sent from nonsafety-related components to safety-related components are those involved in time tagging and the transmission of data for calibration of the safety-related NMS, which is only possible under the specific circumstances described below.

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

The only other instance of nonsafety-related to safety-related communication involves the calibration of the APRM and LPRM. LPRM and APRM calibration gain adjustment factors, which are calculated in the nonsafety-related plant computer functions (PCF) of the N-DCIS, are transmitted to the safety-related LPRM/APRM equipment through proper signal isolation (the safety-related fiber-optic CIMs). However, this data transmission can only be implemented and accepted by the safety-related equipment with the operator's acknowledgment. This transfer of data is similar to that used by retrofit Nuclear Measurement Analysis and Control (NUMAC) PRNM systems already licensed for some U.S. nuclear power plants, which is done manually and is rigorously controlled. Before the RTIF-NMS platform can accept new calibration data, even if it has been continuously sent by 3D MONICORE, the operator must use a keylock switch to make the particular chassis inoperable. If the operator has not additionally put the corresponding division in bypass, the inoperable is interpreted as an NMS trip. It is physically impossible to simultaneously bypass more than one division. Trips and bypasses are indicated in the MCR.

After the chassis has been made inoperable, the operator reviews the download received by the chassis being calibrated. Additionally, the operator can determine that a checkback signal interchange indicates that the RTIF-NMS platform has correctly received the 3D MONICORE data. If a checkback signal is utilized, it is initiated by the RTIF-NMS equipment and sent to 3D MONICORE. 3D MONICORE receives the checkback signal, verifies/validates that the information received by the RTIF-NMS equipment is what was sent, and then sends a signal back to the RTIF-NMS equipment confirming that the data was received accurately. There is no automatic/automated system response to a good or bad checkback signal. Only after the operator is satisfied that the calibration data are accurate and correct (through manual verification of the data or the use of a confirming electronic checkback signal) can the operator instruct the RTIF-NMS platform that it is acceptable to use the downloaded data. This process is equivalent, but more convenient and accurate, to carrying the calibration data to the RTIF-NMS platform then entering it manually. The manual process is still possible. After the download is accepted by the RTIF-NMS platform, the operator uses the keylock switch to make the instrument operable (removing it from the inoperable state) and then resets the bypass for the division.

7.1.3.3.5 **Dataflow, RMUs, Controller Cabinets, and VDUs**

Dataflow within each of the four divisions of the Q-DCIS is from the RMUs located in the CB, RB, and Fuel Building (FB) in areas appropriate to their division; there are no safety-related RMUs in any other building. Data such as that from transducers and switches is acquired by the RMUs, the signal appropriately conditioned, and sent via the redundant fiber-optic cable communication links (datalinks) along with diagnostic data to the RTIF, NMS and SSLC/ESF cabinets. The RTIF, NMS, and SSLC/ESF cabinets are distributed throughout the division to perform the logic required by the safety-related systems.

There are RTIF, NMS, and SSLC/ESF cabinets located in the MCR back panel area where there are four Q-DCIS rooms, one per division. The back panel area is where the inter-divisional communication is physically performed to support the two-out-of-four voting that initiates safety-related action. Additionally RTIF, NMS, and SSLC/ESF safety-related fiber-optic CIMs are used to operate the safety-related VDUs in that division and to provide isolation between the Q-DCIS and the N-DCIS. Finally, calculated outputs from the RTIF, NMS, and SSLC/ESF cabinets are sent via the redundant Q-DCIS communication system to the RMUs that provide outputs to the safety-related actuators (i.e., solenoids, explosive squib valves, etc.) via load drivers. Note that some may use point-to-point optical fiber or hardwiring to the final load drivers or final actuators if higher speeds are required.

There are at least two safety-related VDUs per division in the MCR. Divisions 1 and 2 have an additional VDU located on each RSS panel. The VDUs are used to monitor safety-related information from their connected division and are used to provide manual operator inputs to the safety-related (SSLC/ESF) logic. The VDUs provide access to a full range of plant parameters in accordance with the requirements of 10 CFR 50.34(f)(2)(iv)[I.D.2]. The VDUs are also used for divisional self-diagnostics and divisional alarms.

The four VDU divisions allow checking of the operational availability of each sense and command feature input sensor for the RTIF, NMS, and SSLC/ESF systems. This is accomplished by cross-checking between channels that bear a known relationship with each other.

7.1.3.3.6 Two-out-of-four Voting Logic

The interconnections between Divisions 1, 2, 3, and 4 are used for two-out-of-four voting logic. The interconnections are provided between safety-related fiber-optic CIMs through fiber-optic cable; there are no electrical connections between divisions. Fail-safe systems like the RPS or the NMS interpret loss of inter-divisional communication as a trip from that division. The trip counts toward the two-out-of-four voting logic initiations, unless the failed division is bypassed. Fail-as-is systems like the ECCS do not interpret loss of communications as a trip. The chances of a CIM card hardware failure in a manner that simultaneously sets all trip inputs to "trip" is negligible, the chances of a CIM card hardware failure in a manner that simultaneously sets all trip inputs to "trip" without an accompanying diagnostic is even smaller. The I&C design basis is N-2, therefore, safety-related systems are capable of performing all safety-related functions, with three out of four safety-related divisions available in the presence of a single failure.

The four redundant divisions of the Q-DCIS satisfy the single failure criterion of IEEE Std. 603, Section 5.1. They also satisfy the independence, testing, and repair requirements outlined in IEEE Std. 603, Sections 5.6, 5.7, and 6.5. The safety-related fiber-optic CIMs (transmitters/receivers), fiber-optic cable, and network that are part of the Q-DCIS within and between the four redundant divisions satisfy the separation and independence requirements of divisional equipment. The cable

routing separation meets the requirements of the SRP Subsection 9.5.1, "Fire Protection Programs."

7.1.3.3.7 Continuous On-line Diagnostics and Redundant Power Supplies

The DCIS performs continuous on-line diagnostic functions that monitor transmission path quality and integrity as well as the integrity of system components. Self-diagnostics extend down to the replaceable card or module level. Off-line tests with simulated input signals can also be used to verify the overall system integrity. Segments of Q-DCIS can be tested and calibrated while on-line when portions of safety-related logic are bypassed. These components and the dual redundant data communication pathways are repairable on-line. Because of the redundant power supplies and communication pathways, self-diagnostic alarms can be viewed in the MCR while a single or multiple failures exist. The Q-DCIS failures are indicated in the MCR.

The Q-DCIS components and cabinets have redundant power supplies that are supplied by redundant uninterruptible power feeds within each division. These power feeds support the Q-DCIS operation for 72 hours with neither diesel generator nor offsite power available. The loss of one power feed or power supply does not affect any safety-related system function.

The Q-DCIS includes the safety-related hardware and software for the RTIF, NMS, and SSLC/ESF protection functions and parallels the four-division design of those systems. No failure of any two divisions prevents a safety-related action, such as a detection or a trip, from being accomplished successfully. Component self-testing reconfigures the system to the approved safe state upon detection of uncorrectable errors. The capability for off-line test and calibration of the Q-DCIS components is designed into the system. An individual division can be disconnected for maintenance and calibration through the use of bypasses within the safety-related logic division without compromising the operations of the other divisions. Only one division can be bypassed at any one time and the existence of a bypass is indicated in the MCR.

7.1.3.3.8 Acceptance Criteria, Guidance, and Conformance

The regulatory acceptance criteria and guidance applicable to each of the Q-DCIS systems identified in the "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800 are stated in Table 7.1-1, "Regulatory Requirements Applicability Matrix." Sections 7.2 through 7.8 contain regulatory conformance discussions for each specific system. The degree of applicability and conformance, along with any clarification or justification for exceptions, is presented in the safety evaluation sections for each specific system.

7.1.3.4 Q-DCIS Testing and Inspection Requirements

The Q-DCIS uses three diverse safety-related platforms: RTIF-NMS (RPS, NMS, and the MSIV isolation function) and SSLC/ESF, and ICP.

The RTIF-NMS and SSLC/ESF platforms are accessible for testing purposes. Their continuous automatic on-line diagnostics detect data transmission errors and hardware failures at the

replaceable card or module level. On-line diagnostics for RTIF-NMS and SSLC/ESF are qualified as safety-related in conjunction with functional software qualification, and also meet the self-diagnostic characteristics for digital computer based protection systems recommended by IEEE Std. 7-4.3.2.

Both RTIF-NMS and SSLC/ESF have self-diagnostic features that check the validity of input signals. An analog input outside expected limits creates an alarm.

The RTIF-NMS hardware has watchdog timers for various processors and logic functions that monitor the execution of the software. If the software stops executing (suspending the self-diagnostics), its watchdog timer resets the affected processor or logic function. This results in a channel trip and alarm while the processor or logic function is resetting.

The SSLC/ESF platform is a Triple Modular Redundant (TMR) system, with three controller application processors. The controller application processors are monitored by individual watchdog timers that reset or fail a controller application processor depending on the severity of the problem. A single or double controller application processor failure causes alarms, but the division continues to function to provide the required automatic protective actions.

Both RTIF-NMS and SSLC/ESF are cyclically tested from the sensor input point to logic contact output. The self-diagnostic capabilities include power supply checks, micro-processor checks, system initialization, watchdog timers, memory integrity checks, I/O data integrity checks, communication bus interfaces checks, and checks on the application program (checksum). Cyclically monitored items include:

- Sensor inputs to the I/O for unacceptably high/low levels.
- Proper execution of application code/checksum verification of code integrity.
- Internal clocks.
- Functionality of input cards/modules, and their processor communication.
- Controller application processor communication with the output contact (SSLC/ESF platform).
- Inter-divisional point-to-point data communication in RTIF.
- Inter-divisional point-to-point data communication in NMS).
- Functionality of the output contact by momentarily reversing its state and confirming readiness to change state on demand (SSLC/ESF platform).
- Power supplies.

Subsequent to verification and validation (V&V) of software during factory and preoperational testing in accordance with approved test procedures, there is no mechanism for the RTIF-NMS or SSLC/ESF code, response time, or coded trip setpoints to inadvertently change. For user adjustable parameters a new checksum is calculated at the time acceptable changes are implemented. The new checksum is used from that point forward to validate the application

software. The trip setpoint parameters are continuously sent to the N-DCIS Technical Specifications Monitoring (TSM) for comparison of the setpoints to confirm consistency between divisions and the required values.

The ICP is similar to the RTIF-NMS and SSLC/ESF platforms in that it contains self-diagnostic capabilities, which are independent from the implementation that performs the safety-related control function, to ensure that the platform is functioning properly. The ICP self-diagnostics possess the capability to:

- Detect data transmission errors
- Detect hardware failures
- Check platform operability

The following describes the provisions made to allow periodic testing of safety-related platforms. Additional information on testing and inspection requirements for each system within the Q-DCIS is presented in specific subsections in Chapter 7.

Channel Check

The channel check is a qualitative assessment of channel behavior during operation. The on-line self-diagnostic features of the safety-related platforms, in conjunction with the TSM, accomplish the channel check requirements for detecting unacceptable deviations by automatic cyclic comparison of channel outputs. TSM provides a log of the results and sends out-of-limits alarms to the Alarm Management System (AMS). The TSM uses a hardware/software platform diverse from the safety-related platforms. The TSM functions are listed in Subsection 7.1.5.2.4.5.

If there are any self-diagnostic test results and indicating alarms, a summary report is available to the operator on demand.

Sensor and actuation logic channel monitoring capability are provided at the VDUs to enable manual validation of TSM report results.

Channel Functional Test

The channel functional test ensures that the entire sensor channel performs its intended function. The on-line self-diagnostic features of the safety-related platforms, in conjunction with the TSM, support the channel functional test requirements. The channel functional test can be conducted by manual injection of a simulated signal, one division at a time. The channel functional test confirms the channel through the DTM function is functioning correctly. The coincidence logic, involving more than one channel, and the final control elements are not activated in the channel functional test.

Logic System Functional Test

A LOGIC SYSTEM FUNCTIONAL TEST shall be a test of all logic components required for OPERABILITY of a logic circuit, from as close to the sensor as practicable up to, but not including,

the actuated device, to verify OPERABILITY. The LOGIC SYSTEM FUNCTIONAL TEST may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested.

Response Time Test

The determinism of the systems is verified by their response time test. The test is performed by a series of sequential, overlapping, or total steps to measure the entire response time. The watchdog timers monitor processor internal clocks and alarms for out-of-limit conditions and the completion of application code per logic processor or logic function cycle. Since the clocks set the response time, there is no mechanism for the response time to change without alarm or trip. All time delays incorporated into system logics are performed by software and the values are set during factory and preoperational testing in accordance with approved test procedures. Subsequent to final V&V of the code, there is no mechanism for the time delay values to inadvertently change.

The response time tests for the remaining portions of each sense, command and actuate loop (i.e. sensors, and final control elements/actuators) are performed separately from self-diagnostics and the TSM.

7.1.3.5 Q-DCIS Instrumentation and Control Requirements

The data transmission function delivers system data to nodes in the network, such as distributed logics of the Q-DCIS RMUs and specific safety-related logic system components, and in certain safety-related systems through dedicated data paths. The Q-DCIS thus provides the necessary integrated support for the distributed control logic functions of the RMUs and safety-related logic equipment. The data I/O and transmission functions do not require any manual operator intervention and have no operator controls.

The Q-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the interfacing systems. When one network of the dual network system fails, operation continues automatically without operator intervention. In the event that a channel failure occurs, the network alarms in the MCR indicate the failed component. The failed segment of the channel can be isolated from the operating segments and repaired on-line.

The following Q-DCIS displays and alarms, as a minimum, are provided in the MCR.

- MCR Alarms:
    - Division 1 Q-DCIS trouble
    - Division 2 Q-DCIS trouble
    - Division 3 Q-DCIS trouble
    - Division 4 Q-DCIS trouble

- MCR Indications:
    - Division 1 Q-DCIS diagnostic displays
    - Division 2 Q-DCIS diagnostic displays
    - Division 3 Q-DCIS diagnostic displays
    - Division 4 Q-DCIS diagnostic displays

7.1.3.6 Q-DCIS Boundaries

The Q-DCIS does not include N-DCIS components. The field sensors, actuators, and wiring belong to the process system to which they are attached and are not part of the Q-DCIS.

7.1.4 N-DCIS General Description Summary

The N-DCIS comprises the nonsafety-related portion of the DCIS. The N-DCIS components are redundant when they are needed to support power generation and are segmented into systems. Segmentation allows, but does not require, the systems to operate independently of each other. The N-DCIS major systems and functions are defined in Subsection 7.1.4.8.

The N-DCIS major components include:

- Fiber-optic cable and hardwired networks
- System controller application processors
- Workstations
- Dedicated network switches
- RMUs
- Gateways, datalinks, signal isolators, and I/O modules
- MCR consoles and display panels
- Fiber-optic modems and media converters
- Computer peripherals, such as printers and plotters

Although the N-DCIS is larger and more complex than the Q-DCIS, it is designed with a segmented architecture that allows the different portions of the system to operate independently of one another. Redundant automatic network switches manage the network so that during normal operation the segments appear seamless to the MCR operator; the network is designed to tolerate a single hardware failure (and many dual hardware failures) without loss of power generation capability or challenge to a safety-related system. The N-DCIS cannot control any Q-DCIS component. The N-DCIS accepts one-way communication from the Q-DCIS so that the safety-related information can be monitored, archived and indicated seamlessly with the N-DCIS data.

The N-DCIS performs control functions with logic processing modules using signals acquired by the RMUs. The N-DCIS logic processing can be found in the N-DCIS cabinets dedicated to specific

system logic functions, such as Steam Bypass and Pressure Control (SB&PC) System and the Turbine-Generator Control System (TGCS), and in cabinets where several system logic functions are combined. The N-DCIS logic is implemented in triple redundant control systems for core nonsafety-related key systems, such as the Feedwater Control System (FWCS), SB&PC System, and Plant Automation System (PAS). The N-DCIS logic is redundant for systems required for power generation, so that no single failure of an active DCIS component can cause or prevent a BOP trip or reactor scram.

The N-DCIS provides the control and monitoring operator interface on the N-DCIS nonsafety-related VDUs in the MCR and RSS panels. The VDUs operate independently of one another yet each can access any component in the N-DCIS. This gives the RSS panels the same control and monitoring capability as the displays in the MCR. The N-DCIS provides datalinks and gateways to allow vendor supplied or prepackaged ("foreign") control systems to be integrated into the DCIS. Examples include the Condensate Purification System (CPS) and the Area Radiation Monitoring System (ARMS).

The N-DCIS components that support power generation are provided with two or three sources of uninterruptible power with battery backup for at least two hours. For loss of offsite power events or after DCIS battery backup power is lost, the N-DCIS operates continuously from diesel generators.

The N-DCIS provides extensive self-diagnostics that monitor communication, power, and other failures to the replaceable card, module or chassis level. Process diagnostics include system alarms and the capability to identify sensor failures. All of the process and self-diagnostic system alarms are provided in the MCR.

7.1.4.1 N-DCIS Safety-Related Design Bases Summary

The N-DCIS does not perform or support the performance of any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.4.2 N-DCIS Nonsafety-Related Design Bases Summary

The nonsafety-related design bases for the N-DCIS include the following requirements to:

- Provide functional/operational independence of nonsafety-related components important to power generation.
- Perform closed loop control and system logic.
- Tolerate a single failure of an N-DCIS component without loss of power generation capability or challenge to a safety-related system.
- Receive selected signals from the Q-DCIS and send them to nonsafety-related devices.
- Collect and archive data for transient analysis, data trending, sequence of events recording, display of Safety Parameter Display System (SPDS) and accident monitoring information, and managing the annunciation of alarm conditions in the MCR.

- Provide secure data communication to all authorized external systems, including the technical support center (TSC), the emergency operating facility (EOF), and the emergency response data system (ERDS).
- Provide gateway interfaces to control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier.
- Perform various PCF that include calculations, displays, and alarms.
- Provide for report generation.
- Provide for a Plant Configuration Database (PCD).

7.1.4.3 N-DCIS Safety Evaluation Summary

The N-DCIS is used as the primary control, monitoring, and data communication system with power production applications. The N-DCIS is not required for safety-related purposes, nor is its operability required during or after any DBE. The system is required to operate in the normal plant environment and is relied on for data communications and power production applications. The N-DCIS provides an isolated alternate path for safety-related data to be presented to the plant operators. The N-DCIS network that supports the dual/triple, fault-tolerant digital controllers and communication scheme is diverse from the Q-DCIS network design in both hardware and software.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. RMUs are located throughout the plant and auxiliary buildings. Computer equipment and peripherals are located mainly in the CB (MCR and Back Panel areas), Radwaste Building, TSC, EOF, and other auxiliary buildings.

The N-DCIS panels and components are designed to maintain structural integrity, during and after a DBE, and do not prevent any safety-related equipment in their area from performing its safety-related function.

Table 7.1-1 identifies the Q-DCIS systems and N-DCIS segments and the associated codes and standards applied, in accordance with the SRP. The following subsection summarizes N-DCIS conformance to regulatory requirements, guidelines, and industry standards.

7.1.4.4 N-DCIS Regulatory Requirements Conformance Summary

As shown in Table 7.1-1 or described in Subsection 7.1.6 the N-DCIS meets applicable portions of:

- 10 CFR 50.34(f)(2)(iii)[I.D.1]
- 10 CFR 50.34(f)(2)(iv)[I.D.2]
- 10 CFR 50.34(f)(2)(v)[I.D.3]
- 10 CFR 50.34(f)(2)(xv)[II.E.4.4]
- 10 CFR 50.34(f)(2)(xvii)[II.F.1]
- 10 CFR 50.34(f)(2)(xviii)[II.F.2]

- 10 CFR 50.34(f)(2)(xix)[II.F.3]
- 10 CFR 50.34(f)(2)(xxi)[II.K.1.22]
- 10 CFR 50.34(f)(2)(xxiv)[II.K.3.23]
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3]
- 10 CFR 50.49
- 10 CFR 50.55a(a)(1)
- 10 CFR 50.62
- 10 CFR 52.47(a)(21)
- 10 CFR 52.47(b)(1)
- 10 CFR 52.47
- IEEE Std. 7-4.3.2, 338, 497, 518, 603, 828, 829, 830, 1008, 1012, 1028, 1050, 1074
- ISA 67.02.01 (RG 1.151) and 67.04.01 (RG 1.105)
- GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64
- SRM on Item II.Q and Item II.T of SECY 93-087
- RGs 1.89, 1.97, 1.100, 1.105, 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173, 1.180, and 1.209
- BTPs HICB-1, 10, 16, and 19

7.1.4.5 N-DCIS Testing and Inspection Requirements Summary

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS elements are performed before fuel loading and startup testing to ensure that the system functions as designed and that actual system performance is within specified criteria.

The N-DCIS controllers, displays, monitoring and input and output communication interfaces function continuously during normal power operation. Abnormal operation of these components can be detected during plant operation. In addition, the controllers are equipped with on-line diagnostic capabilities to identify and isolate failure of I/O signals, buses, power supplies, processors, and inter-processor communications. These on-line diagnostics can be performed without interrupting the normal operation of the N-DCIS.

7.1.4.6 N-DCIS Operator Interface Requirements Summary

The N-DCIS VDUs allow operator control and monitoring of the N-DCIS systems. However, they allow only monitoring of safety-related system data, through appropriate isolation. The VDUs are also segmented so that the network segments can be monitored and controlled independently. During normal operation the segments are not apparent to the operators. The N-DCIS supplies

alarm and annunciation information to the operator and on the wide display panel for important plant information.

7.1.4.7 N-DCIS System Boundaries

The N-DCIS includes no Q-DCIS components. The N-DCIS does not include the sensors or the sensor wiring to the RMUs or the RMU output wiring to the actuators.

7.1.4.8 N-DCIS Major Systems Description Summary

The N-DCIS systems and components are nonsafety-related entities of the DCIS. The N-DCIS major system summary descriptions follow.

7.1.4.8.1 GENE Systems Description Summary

The GENE network segment is a single channel of workstations, triple redundant controllers, and dual redundant controllers, that execute the following functions:

- Workstations:
  - 3D MONICORE
  - SPDS
- Dual Redundant Controllers:
  - RC&IS (includes Rod Server Processing Channel [RSPC], Rod Action and Position Information [RAPI], File Control Module [FCM], Signal interface unit [SIU]).
  - ATLM.
  - Rod Worth Minimizer (RWM).
- Triple Redundant Controllers:
  - DPS

7.1.4.8.2 Plant Investment Protection Systems (Train A and Train B) Description Summary

The Plant Investment Protection (PIP) network segment comprises two channels (A and B) of dual redundant controllers that execute the following functions:

- Control Rod Drive (CRD) System
- Reactor Water Cleanup and Shutdown Cooling (RWCU/SDC) System
- FAPCS
- Nonsafety-related RSS
- Reactor Component Cooling Water System (RCCWS)
- Plant Service Water System (PSWS)
- PSWS cooling towers

- Nuclear Island Chilled Water System (NICWS)
- Drywell cooling nonsafety-related electrical systems
- Instrument Air System (IAS)
- Nonsafety-related Post-Accident Monitoring (PAM) systems
- Nonsafety-related LD&IS systems
- PCCS Ventilation Fans
- Ancillary and standby diesel generators
- 6.9 KV plant electrical power system
- Low voltage electrical system
- Nonsafety-related UPS

The N-DCIS segments in PIP A and PIP B allow for operator control and monitoring from the MCR nonsafety-related VDUs and the RSS VDUs. The A and B segments can operate independently of one another.

During loss of offsite power events, the N-DCIS for PIP A and PIP B is powered by its respective nonsafety-related batteries for two hours and then by diesel generators and can therefore operate without offsite power.

7.1.4.8.3 **Balance Of Plant Systems Description Summary**

The balance of plant (BOP) network segments is a single channel of triple redundant and dual redundant controllers that execute the following functions:

- Triple Redundant Controllers:
    - Steam Bypass and Pressure Control (SB&PC)
    - Feedwater Control System
    - Feedwater Temperature Control System
    - Turbine-Generator Control System
- Dual Redundant Controllers
    - Turbine auxiliary.
    - Generator auxiliary controller.
    - Electrical system main transformer/Unit Auxiliary Transformer (UAT) controller.
    - Main condenser controller.
    - Electrical system Reserve Auxiliary Transformer (RAT) controller.
    - Normal heat sink controller.

- Condensate/Feedwater (FW)/drains/extraction controller, including extraction and level control.
- Water systems controller.
- Service air/containment inerting/floor drains controller.
- Miscellaneous HVAC controller.

Segments in the BOP systems allow for operator control and monitoring from the MCR nonsafety-related VDUs.

7.1.4.8.4 **Plant Computer Functions Description Summary**

The PCF provide:

- Performance monitoring and control (PMC) functions, prediction calculations, visual display control, point log and alarm processing, surveillance test support, and automation.
- Core thermal power/flow calculations.
- The plant Alarm Management System (AMS) that alerts the operator to process deviations and equipment/instrument malfunctions.
- Fire Protection System (FPS) data through datalinks and gateways.
- The Historian function, that stores data for later analysis and trending.
- Control of the main mimic on the MCR Wide Display Panel (WDP).
- Support functions for printers and the secure data communications to the TSC, EOF, ERDS, and potential links to the Simulator.
- On-line procedures (OLP) to guide the operator during normal and abnormal operations, and to verify and record compliance.
- Transient recording.
- Nonsafety-related PAM displays.
- Report generators to allow the operator, technician, or engineer to create historical or real time reports for performance analysis and maintenance activities.
- The Plant Configuration Database (PCD) to document, manage, and configure components of the N-DCIS.
- Gateways to vendor-supplied nonsafety-related systems such as seismic, meteorological, and radiation monitoring.
- Nonsafety-related process and area radiation monitoring.

PCF information display and control capability are provided by nonsafety-related VDUs in the MCR and RSS panels.

7.1.4.8.5 Nonsegment-Based Equipment

Equipment shared among segments are listed below:

- Nonsafety-related VDU/ Main Control Room Panel (MCRP) (the N-DCIS VDUs are connected to specific network segments to assure that the segment can be independently monitored and controlled should other segments fail; in the absence of such failures the VDUs are shared among the segments).
- Gateways.
- Datalinks.
- Safety Parameter Display System (SPDS) logic.

7.1.5 N-DCIS Specifics

The N-DCIS data communication systems are embedded in the DCIS that performs the data communication functions that are part of and support the nonsafety-related systems described in Sections 7.2 through 7.8 and support the Q-DCIS to N-DCIS communications for the safety-related systems described in Sections 7.2 through 7.8. A simplified network functional diagram of the DCIS appears as Figure 7.1-1, and indicates the elements of the N-DCIS and the Q-DCIS.

The N-DCIS architecture, its relationships, and its acceptance criteria are further described in this subsection.

7.1.5.1 N-DCIS Design Bases

7.1.5.1.1 N-DCIS Safety-Related Design Bases

The N-DCIS does not perform or ensure any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

7.1.5.1.2 N-DCIS Nonsafety-Related Design Bases

The N-DCIS is used as the primary control, monitoring, and data communication system for power production applications. The design bases for the N-DCIS include the requirements to:

- Segment the N-DCIS display and control of the two PIP Systems (A&B) and the BOP systems so they can operate independently of one another.
- Segment the major reactor control systems (FWCS, SB&PC System, TGCS and PAS) so they can operate independently of one another and from the DPS.
- Perform closed loop control and system logic independently of the MCR VDUs and Ethernet networks. Operability of the RSS panels, and their VDUs is independent of the operation or existence of the MCR displays.
- Ensure that no single failure of an N-DCIS component affects power generation.

- Provide a communication path for nonsafety-related data gathered and distributed throughout the plant, including datalink interfaces to control systems. The communication paths are redundant and include both the "native" control systems and "foreign" vendor supplied or prepackaged control systems (condensate purification, offgas, radwaste, area radiation monitoring, and meteorological monitoring, for example).
- Reliably transfer to or from the plant areas, in digital format, analog or binary information that has been collected and digitized from nonsafety-related RMUs. The signals to the RMUs include contact closures and other sensors or process activation signals communicated via transmitters, generated elsewhere for the control of remote devices such as pumps, valves or solenoids.
- Receive selected safety-related signals from the Q-DCIS through qualified safety-related isolation devices and datalinks to gateway devices or workstations and then transmit the signals to nonsafety-related VDUs and other nonsafety-related systems for control, monitoring and alarming purposes.
- Replace a majority of conventional, long-length, copper-conductor cables that connect components of the nonsafety-related plant I&C systems with fiber-optic cable data networks to reduce cost and complexity.
- Provide an electrically noise-free transmission path for plant sensor data and control signals.
- Collect and archive data for transient analysis and data trending, sequence of events recording, display of SPDS and RG 1.97 information in the MCR, processing, and annunciation of alarm conditions to plant operational staff.
- Perform various PCF including PMC by providing Nuclear Steam Supply System (NSSS) performance and prediction calculations, visual display control, point log and alarm processing, surveillance test support, automation and the BOP performance calculations.
- Provide a permanent record and historical perspective for plant operating activities and abnormal events.
- Provide a secure communications interface with external computer and monitoring systems (one-way communication, no control capabilities). This includes the Plant Simulator (for training and for development and analysis of operational techniques), TSC, EOF, and the ERDS.
- Provide key-locked control equipment cabinet doors including door position switches. Electronic protection of control systems including password protection is provided in accordance with Reference 7.1-8.
- Provide reactor core performance information.
- Provide a SPDS of critical plant operating parameters. The parameters include reactor power, RPV water level, temperatures, pressures, flows, and the status of pumps and valves. The SPDS allows the MCR operators to follow the plant emergency operating procedures (EOPs) to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown

conditions and maintain containment integrity as required by 10 CFR 50.34(f)(2)(iv)[I.D.2]. Specific SPDS displays are available in the MCR and SPDS parameters are available on the main plant mimic on the MCR WDP.

- Provide the MCR overview displays, navigational/top level displays, and system level displays.
- Provide TSC and EOF displays.
- Provide an AMS designed to alert the operator to an alarm condition, informing the operator of its priority, guiding the operator's response, and confirming whether the response was effective.
- Display normal, abnormal and EOPs on operator or other workstations where display of operating procedures is permitted.
- Warn the operator to document that a Technical Specification limit, such as a limiting condition for operation (LCO), is being approached or violated when such conditions are detectable.
- Provide a 3D MONICORE system interface with the operator and with other systems (refer to Subsection 7.1.5.2.4.8 for additional information about 3D MONICORE).
- Provide time tagging of all measured points to facilitate transient recording and analysis (TRA), sequence of events recording, and first out determination.
- Provide real-time core thermal power and flow calculations.
- Provide on-line diagnostics and monitoring of plant individual thermal heat cycle components, normalized to current plant conditions.
- Provide hard copy reports of current and historical plant operating data with pre-defined and custom formats to suit the needs of operations, maintenance, and engineering.
- Provide overall configuration management functions for the N-DCIS PCD.
- Provide manual and automatic DPS Selected Control Rod Run-in (SCRRI) initiation and Select Rod Insert (SRI).
- Provide the Alternate Rod Insertion (ARI) initiation signal.
- Initiate Fine Motion Control Rod Drive (FMCRD) and Emergency Rod Insertion (ERI) condition signals.
- Acquire process measurement and equipment status signals from the process sensors and discrete monitors of the plant's nonsafety-related systems.
- Perform signal conditioning and A/D conversion for continuous process (analog) signals and perform signal conditioning and change-of-state detection for discrete signals.
- Provide data message formatting and data transmission from remote locations in the plant to the MCR through fiber-optic cable and hardwired network connections.

- Receive command and control signals from the redundant controllers in the MCR area, and transmit the signals from the MCR area to remote locations in the plant where the N-DCIS distributes the signals to the final actuating devices.
- Provide datalink interfaces to all control and logic processing equipment supplied by parties other than the primary N-DCIS equipment supplier.
- Provide data support functions through a secure communications interface with the TSC, EOF, and the ERDS.
- Provide operator aids from the PCF, such as safety parameter displays, transient data recording, analysis, archiving, alarm processing, and sequence of events processing.

7.1.5.1.3 N-DCIS Setpoint Methodology

To select I&C and to determine setpoints, the design considers instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability. Adequate margin between limits and instrument setpoints is provided to allow for instrument error. The amount of instrument error is determined by test and experience. The setpoint is selected based on a known error; most of this error is in the transducer to the measurement channel and A/D converters of the RMU. The remaining equipment is micro-processor based with discrete setpoints that do not drift. The recommended test frequency is greater for instrumentation that demonstrates a stronger tendency to drift.

Ideally, the actual settings are determined by operating experience. However, in cases where operating experience is not available, settings are determined by conservative analysis. The settings are far enough from the values expected in normal operation to preclude inadvertent initiation of certain actions and far enough from the analyzed values to ensure that appropriate margins are maintained between the actual settings and analyzed values. The margin between the limiting system settings and the actual limits includes consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components.

7.1.5.2 N-DCIS Description

The N-DCIS is segmented into parts that can work independently of one another if failures occur. The segments are not visible to the operator during normal operation. The N-DCIS uses hardware and software platforms that are diverse from the Q-DCIS. The N-DCIS network is dual redundant and at least redundantly powered so no single failure of an active component can affect power generation.

The individual N-DCIS segments are the:

- GENE network

- PIP A network
- PIP B network
- BOP network
- PCF network

Managed network switches are redundant per segment and provide monitoring and control of the N-DCIS networks while transmitting data and alarms, recording and displaying information and operator control information between segments and components. Managed network switches monitor and transmit data acquisition and control messages and displays associated with that segment. Each managed network switch has the capability to monitor and control unexpected and excessive traffic on its respective N-DCIS network segment. Each network switch can have up to several hundred "nodes" and several "uplink" ports that are connected to the other switches; all connections to these switches are through the fiber-optic cable network. Fiber-optic cables used for nonsafety-related applications are sheathed in material meeting IEEE Std. 383 that addresses fire propagation mitigation.

The switches allow the various controllers, data acquisition and displays associated with a segment to communicate with each other by almost instantaneous virtual connections that end when the communication is finished. The switches' "backbone" capacity determines how many simultaneous two-way connections can be made, but the capability is higher than actually required.

These managed switches have security features that include identification of legal addresses, the capability to ignore or not uplink (to other segments) unexpected connections or their traffic, and the capability to alarm network traffic. Only when a switch determines that an information data packet is destined for a node on another switch is the information put on an uplink to another switch. The network switches learn and maintain their own forwarding tables containing a list of all the nodes and hosts on their respective network segment. When a network switch receives a data communication packet, it forwards only that particular data packet to the segment to which that receiving host is connected. This mechanism prevents data traffic between devices on the network from affecting devices on other segments of the network.

The uplink ports on the switches are connected together radially and in a data communication ring because multiple interconnections increase reliability. Specifically, the switches use a "spanning tree protocol" to automatically enable and disable ports so there is one path from the nodes of one switch to another. Should a path become disabled, the switches automatically reconfigure to establish another path through the remaining switches and fiber-optic cable paths. Reconfiguration requires no operator input and is usually accomplished in seconds.

Each switch "node" (workstation, display, and controller) is connected to redundant switches of the segment. These connections support normal plant operation. The switches have Mean Time Between Failure (MTBF) of greater than 100,000 hours. Each switch has redundant power feeds

and can work from either power source. The switches and connected controllers support extensive component and data self-diagnostics, and failures are indicated.

The above text and Figure 7.1-1 show that the N-DCIS is not a single network. It is redundant and segmented to support the DCIS with high reliability. A single failure of one of the redundant switches in a segment or multiple failures that involve no more than one switch per segment has no effect on plant operation or data. The failure is indicated and can be repaired on-line. In the highly unlikely event of both switches of a segment simultaneously failing, that particular segment is lost. However, the remaining segments are unaffected and individual nodes connected to the failed switches can continue to function. The remaining switches then automatically reconfigure their uplink ports such that the remaining segments automatically find available data paths between each other.

The major N-DCIS functions are segmented as defined in Subsection 7.1.4.8.

7.1.5.2.1 Nonsafety-Related Shutdown Systems

Descriptions of nonsafety-related shutdown systems follow.

7.1.5.2.1.1 Remote Shutdown System

Each RSS panel has the ability to operate all of the nonsafety-related PIP equipment and the BOP equipment, either automatically or manually. Refer to Subsection 7.4.2 for additional information.

7.1.5.2.1.2 Reactor Water Cleanup/Shutdown Cooling System

The nonsafety-related RWCU/SDC system maintains reactor water purity during operation. It also provides normal shutdown cooling by taking suction from the RPV, pumping the flow through heat exchangers, and returning the cooled water to the vessel through the feedwater line. The system is segmented and allows the PIP Train A and B components to operate independently. Refer to Subsection 7.4.3 for additional information.

7.1.5.2.1.3 Fuel and Auxiliary Pools Cooling System

The nonsafety-related FAPCS maintains the fuel pool, spent fuel pool, suppression pool, auxiliary pools, and GDCS pools, by pumping pool water through heat exchangers and a water treatment unit (equipped with pre-filters and demineralizers) into two 100% cooling and cleaning trains. It also maintains suppression pool temperatures and cleanliness during operation. The FAPCS can also initiate a low pressure coolant injection (LPCI) mode following an accident and after the reactor has been depressurized to provide reactor makeup water for accident recovery. In this mode the FAPCS pump takes suction from the suppression pool and pumps it into the RPV through RWCU/SDC Loop B and Feedwater Loop A. The system is segmented and allows PIP Train A and B components to operate independently. Refer to Subsection 9.1.3 for additional information.

7.1.5.2.1.4 Control Rod Drive System

The nonsafety-related CRD system maintains the hydraulic control unit (HCU) accumulators at the pressure required to assure a successful scram, provides cooling water flow to the FMCRDs and provides various high-pressure purge flows. The CRD system also provides a HP CRD injection mode capable of supplying inventory to the RPV at elevated pressures. While HP CRD injection is isolated upon a low level indication from the GDCS pools or drywell high pressure coincident with drywell high level, the isolation is bypassed by a failure of the GDCS to successfully inject (a scenario which is beyond design basis). The system is segmented and allows PIP Train A and B components to operate independently. Refer to Section 4.6 as well as Subsections 7.1.2.8.8, 7.3.3, and 7.4.5 for additional information.

7.1.5.2.2 Nonsafety-Related Information Systems

Nonsafety-related information is provided by PRMS and ARMS.

7.1.5.2.2.1 Process Radiation Monitoring System

Nonsafety-related PRMS instrumentation monitors the main steam lines, the drywell, ventilation and stack discharges and liquid and gaseous effluent streams that might contain radioactive materials. The safety-related PRMS is discussed in Subsection 7.1.3.2.4.3. MCR display, recording, and alarm capabilities are provided along with controls that provide automatic trip inputs to the respective systems to prevent further radiation release. Refer to Subsection 11.5.3 for additional information.

7.1.5.2.2.2 Area Radiation Monitoring System

Nonsafety-related ARMS instrumentation continuously monitors the gamma radiation levels within designated areas of the plant. It provides early warning to operating personnel when predetermined dose rates are exceeded. Refer to Subsection 7.5.4 for additional information.

7.1.5.2.3 Control Systems

Descriptions of nonsafety-related control systems follow.

7.1.5.2.3.1 Nuclear Boiler System Instrumentation

Nonsafety-related NBS instrumentation provides indication of reactor coolant and vessel temperatures, RPV water level, and RPV pressure. Refer to Subsection 7.7.1 for additional information.

7.1.5.2.3.2 Rod Control and Information System

The nonsafety-related RC&IS is able to control reactor power level by controlling the movement of the control rods in the reactor core during manual, semi-automated, and automated modes of plant operations. The ATLM automatically enforces fuel operating thermal limits minimum critical power

ratio (MCPR) and maximum linear heat generation rate (MLHGR) when reactor power is above the ATLM enable setpoint. Refer to Subsection 7.7.2 for additional information.

7.1.5.2.3.3 Feedwater Control System

The nonsafety-related FWCS has two sets of highly reliable and triple redundant controllers. The feedwater level controller automatically and manually regulates the flow of feedwater into the RPV. It maintains a predetermined water level for all modes of reactor operation, including heatup and cooldown. The feedwater temperature controller allows reactor power maneuvering without moving control rods. Refer to Subsection 7.7.3 for additional information.

7.1.5.2.3.4 Plant Automation System

The nonsafety-related PAS:

- Provides automatic startup/shutdown algorithms and controls.
- Regulates reactivity during criticality control.
- Provides heat up and pressurization control.
- Regulates reactor power.
- Provides automatic power generation control during power operation. Refer to Subsection 7.7.4 for additional information.

The PAS is the plant-wide automation scheme implemented by the N-DCIS. The PAS coordinates the action of multiple systems using system-level controllers (with the capability to perform system-level automation) to automate the operation, maintenance, testing, and inspection functions. It uses Automated Program Functions (APF) to coordinate the Automatic Power Regulator (APR) and the Power Generation and Control Subsystem (PGCS).

The PAS provides the capability for supervisory control of the entire plant by supplying setpoint commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate. Safety-related systems are never controlled or tasked by the PAS. The automation system covers the tasks involved in criticality, heat-up and pressurization, turbine roll and synchronization, and plant power control.

The APR and PGCS automatically run the plant, with operator supervision from cold non-critical conditions to 100% rated temperature, pressure, and power, and back to cold non-critical conditions.

The PAS establishes several broad automation sequences:

- Pre-startup check
- Approach to criticality and reactor pressurization
- Turbine-generator startup, increase to rated speed and synchronization
- Power operations (increase turbine load to rated power)

- One button shut down

Prior to initiating any automation sequence including the turbine-generator startup, increase to rated speed and synchronization, prerequisite and continually operating equipment must be in a satisfactory pre-defined condition. There is a complete list of prerequisite conditions for each system. Some plant systems are never shut down, even during refueling outages and their operating conditions are independent of plant power.

7.1.5.2.3.5 Turbine Generator Control System

Functions of the TGCS include:

- Turbine speed/acceleration control (including ability to navigate 100% load rejection/ turbine island mode).
- Turbine over-speed protection.
- Turbine control interface with SB&PC System.
- Turbine load control.
- Turbine valve testing.
- Interfacing with the condensate/feedwater system.
- Related surveillance tests, checks, and inspections.
- Automatic response to alarm conditions, system faults, and plant transients.
- Related generator control functions.
- Related turbine generator (TG) auxiliary support control functions.

7.1.5.2.3.6 Steam Bypass and Pressure Control System

A highly reliable and triple redundant nonsafety-related SB&PC System controls reactor pressure during plant startup, power generation, and the shutdown modes of operation. This is accomplished through control of the Turbine Control Valves (TCVs) or Turbine Bypass Valves (TBVs) so susceptibility to reactor trip, turbine generator trip, main steam isolation and safety relief valve opening is minimized. Refer to Subsection 7.7.5 for additional information.

7.1.5.2.3.7 Neutron Monitoring System - Nonsafety-related Systems

The nonsafety-related AFIP provides a signal proportional to the axial thermal neutron flux distribution at the radial core locations of the LPRM detectors. The signal facilitates automated, precise, reliable calculation of the LPRM gains. The signal also provides axial power measurement data for three dimensional core power distribution determinations. The nonsafety-related MRBM logic issues a control rod block demand to the RC&IS logic to prevent fuel damage. It assures that the MCPR and MLHGR do not violate fuel thermal limits. Refer to Subsection 7.7.6 for additional information.

7.1.5.2.3.8 Containment Inerting System

The nonsafety-related Containment Inerting System (CIS) establishes and maintains an inert atmosphere within containment. It operates during all plant operating modes, except during plant shutdown for refueling or equipment maintenance and during limited periods of time to permit access for inspection at low reactor power. Refer to Subsection 6.2.5.2 for additional information.

7.1.5.2.3.9 Diverse Instrumentation and Control Systems

Diverse I&C is provided to address BTP HICB-19 on defense-in-depth and diversity in digital computer-based I&C systems. This is in addition to the ATWS mitigation features, which provide alternate control rod insertion, boron injection, and feedwater runback. The nonsafety-related diverse I&C functions are implemented in the DPS. The DPS functions are implemented in a highly reliable triple redundant control system whose sensors, hardware and software are diverse from their counterparts on any of the safety-related I&C platforms.

The following diverse actuation functions are provided by the DPS:

- A set of protection logics that provide a diverse means to scram the reactor via control rod insertion using sensors, hardware and software that are separate from and independent of the primary RPS.
- A set of initiation logics that provide a diverse means to initiate certain ESF functions using sensors, hardware and software that are separate from and independent of the primary ESF systems.
- A set of redundant ARI signals that initiate associated logics (such as the FMCRD Run-in) and insertion of control rods through an alternate means by opening the three sets of ARI valves of the CRD system.

The DPS provides both manual and automatic initiation of the above functions. Refer to Subsection 7.8.1 for additional information.

7.1.5.2.3.10 Selected Control Rod Run-In / Select Rod Insert

The DPS processes the signals described by Subsection 7.8.1 to develop the automatic SRI and SCRRI command signals. The SRI and SCRRI can also be initiated manually from the MCR. The redundant N-DCIS SCRRI command signals are sent to the RC&IS in which each of the dual rod action and position information (RAPI) channels performs a two-out-of-three vote and initiates RAPI channel logic associated with accomplishing the SCRRI function. When activated, the SCRRI function inserts control rods using the FMCRD motors to pre-defined positions to reduce reactor thermal power to a target power level. This logic is implemented in a highly reliable redundant control system. The SCRRI command signal is also used in the ERI control logic of the N-DCIS, as discussed in Subsection 7.1.5.2.3.12.

The redundant SRI command signals are sent to the nonsafety-related scram timing test panel. This panel is electrically isolated from the divisional panels that contain the switches in the 120 volts alternating current (VAC) return from each HCU scram solenoid. When commanded to open (using two-out-of-three voting logic) for either a full DPS scram, a single HCU scram timing test or for pre-defined rod groups (SRI) the affected HCUs scram their associated control rods. Because the scram timing switches are in the HCU scram solenoid 120 VAC return, the RPS load drivers are in the solenoid 120 VAC supply, and the switches and solenoids are in a "series" circuit, there is no credible failure of the scram timing panel that can prevent or affect an RPS scram.

7.1.5.2.3.11 Alternate Rod Insertion

The N-DCIS performs two-out-of-three voting of the redundant ARI signals from the DPS to become the N-DCIS ARI initiation signal. Each of the RC&IS dual RAPI channels performs two-out-of-three voting of the redundant ARI initiation signals and initiates the RAPI channel logic associated with accomplishing the FMCRD Run-in logic.

When activated, ARI hydraulically inserts all operable control rods by depressurizing the scram air header to open the HCU scram valves. This logic is implemented in a highly reliable redundant control system.

As a backup means for the hydraulic scram function of the CRD system, the ARI command signal is also used in the ERI logic of the N-DCIS to insert all operable control rods to the full-in position using the FMCRD motors, as discussed in Subsection 7.1.5.2.3.12.

7.1.5.2.3.12 Emergency Rod Insertion

The N-DCIS combines the SCRRI/SRI command signal and ARI command signal by an "OR" function to become an FMCRD emergency insertion signal. Redundant FMCRD emergency insertion signals are sent to the ERI Control Panels (ERICPs) of the RC&IS for two-out-of-three voting. Associated emergency insertion condition signals in the ERICPs provide inputs to the induction motor controllers of the RC&IS.

For the SCRRI or ARI and FMCRD Run-in logic of the RC&IS equipment to be initiated, the ERI signals to the induction motor controllers must be concurrent with the RAPI logic SCRRI/SRI command related signal or ARI related command signals to the induction motor controllers. This logic is implemented in a highly reliable redundant control system.

7.1.5.2.4 Plant Computer Functions

All PCF are an integral part of the HFE process (Refer to Chapter 18). The allocation of functions (AOF) accommodates human capabilities and limitations, fault detection and recovery capabilities are provided, and an acceptable operator workload is not exceeded. Additionally, PCF (like the plant controllers) are powered with UPS so that they are available to the operator for as long as the N-DCIS is powered.

The PCF increase the efficiency of plant performance by:

- Performing the functions and calculations necessary for the effective evaluation of nuclear power plant operation.
- Providing a permanent record and historical perspective for plant operating activities and abnormal events.
- Providing analysis, evaluation, and recommendation capabilities for startup, normal operation, and plant shutdown.
- Providing the capability to monitor plant performance through presentation of video displays in the MCR and elsewhere throughout the plant and providing the ability to directly control certain nonsafety-related plant equipment through on-screen technology.
- Providing secure data communication with all external computer and monitoring systems (for example, one-way communication, no control capabilities) including the TSC, EOF, and ERDS.
- Performing core thermal power and core coolant flow rate calculations from reactor heat balances. Iterative computational methods are used to establish a compatible relationship between the core coolant flow rate and core power distribution. The results are subsequently interpreted in the NSSS performance module as power in specified axial segments for each fuel bundle in the core.

The calculations performed by the N-DCIS include process validation and conversion, combination of points, NSSS performance calculations, and the BOP performance calculations.

The Performance Monitoring and Control Subsystem (PMCS) provides the NSSS performance and prediction calculations, visual display control, point log, and alarm processing and BOP performance calculations.

7.1.5.2.4.1 Safety Parameter Display System

The SPDS provides critical plant operating parameters such as reactor power, RPV water level, temperatures, pressures, flows, and status of pumps and valves. The SPDS system allows the MCR operators to follow plant EOPs to shut down the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions, and maintain containment integrity as required by 10 CFR 50.34(f)(2)(iv)[I.D.2]. Specific SPDS parameters are available in the MCR and on the WDP plant mimic.

7.1.5.2.4.2 MCR Displays

The MCR panel equipment is part of the MCR Panels (MCRP) System. Information for the displays is presented with the following functional configuration arrangement:

- Level 0 is the integrated overview display.
- Level 1 is the navigational/top level display.

- Level 2 is the system level display.
- The integrated overview display (sometimes called the main plant mimic) is provided on the WDP.
- The fixed position portion of the WDP provides critical plant operating information, such as reactor power, RPV water level, temperatures, pressures, flows, status of major equipment, and availability of safety-related systems. This information remains in its fixed location for all reactor operating conditions. There are other, variable portions of the integrated overview display that change formats to provide information appropriate to a plant operating mode such as refueling, startup power operations, or accidents. The dynamic display elements of the fixed-position displays are driven by dedicated micro-processor based controllers that are independent of the N-DCIS.
- The large variable display portion of the WDP can indicate any display format available on a nonsafety-related VDU; the plant operator initiates the chosen format.
- Appropriately isolated safety-related information is available for display on the nonsafety-related integrated overview display and various nonsafety-related VDUs.
- The PCF provide navigational or top level displays which include:
    - Main menu
    - Safety parameters
    - PAM (RG 1.97) variables
    - PGCS parameters
    - Power generation control
    - OLP
    - Technical specification monitor/RPS monitor
    - 3D MONICORE
    - Historian function
    - TRA
    - Thermal performance monitor and diagnostic (TPM&D)
    - Report generator
    - Bypass and inoperable status indication (BISI)
    - System level displays (Piping and Instrumentation Diagrams [P&IDs], alarms)

The PCF control displays provide direct control and parameter monitoring of nonsafety-related equipment and systems through the use of the VDUs and various input devices, which are part of the MCR panels.

The RC&IS dedicated operator interface provides control and monitoring of the RC&IS and is described in Subsection 7.7.2.

7.1.5.2.4.3 Alarm Management System

The plant AMS is accessible via the MCR VDUs and RSS VDUs, and indirectly at the TSC and EOF.

The plant AMS is designed to alert the operator to a deviation from normal conditions. It informs the operator of the deviation's priority, guides the operator's response, and confirms whether or not the response was effective.

To fulfill these basic functions, the system must:

- Detect and, in some cases, predict the occurrence of changes in the plant
- Alert users to changes significant to the current operating situation, such that:
    - Only operationally relevant changes are indicated.
    - The demands imposed on users' attention to recognize the changes are aggregated and considered with the demands of other concurrent control room tasks.
    - Operators are alerted to additional plant information needed to understand and respond to changes.

To accomplish the above, the AMS design bases are to:

- Alert the operators to off-normal conditions which require them to take action.
- Reduce the number of alarms to be consistent with the total operator workload.
- Guide the operators to the appropriate response (linking alarms to alarm response procedures).
- Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions.
- Minimize distraction and unnecessary workload placed on the operators by the alarm system – especially during transient and accident conditions.
- Satisfy the dark panel concept: no alarm signal is shown to the operator under normal operating conditions.
- Determine system level alarms based on function and task analysis.
- Include the means to provide the operator with information in different views including sorting, filtering, and grouping of alarms.
- Generate basic alarms and high-level composite alarms. The generated alarms are subject to potential filtering, alarm suppression, and alarm prioritization techniques. The plant Historian maintains an alarm log whether or not alarms are presented to the operator. Alarms are then presented in the MCR either audibly (annunciator), visually (display), or both.

- Create temporary operator-defined alarms and associated alarm setpoints.
- Integrate with other information systems, such as the OLP and TSM, to facilitate operator tasks; the AMS and TSM provide the suggested operator response to the various alarm and monitoring function events.

7.1.5.2.4.4 On-Line Procedures

OLP provide for:

- Display of normal, abnormal, and emergency operating procedures on operator or other workstations.
- Display of operating procedures in logic, flowchart, and text formats.
- Hardcopy output of operating procedures from all workstation locations with the displayed format and content, considering potential alternative uses for study guides, and procedure maintenance.
- Maintenance (that is, addition, deletion, and modification) of operating procedures.
- Manual, semi-automated (selected procedures), or fully automated (selected procedures) implementation of operating procedures from the operator or other workstations.
- Display of information on the use of controls from operator or other workstations.
- Continuous update of the display of parameters, to include embedded dynamic indication status (normal, warning, and alarm conditions), necessary for the plant operator to monitor or perform operating procedure steps.
- Operator confirmation of procedures in the MCR without resorting to written documentation.
- The ability to log operator actions.
- Indication of procedural steps that require manual logging.
- Validation of each operating procedure using the plant simulator.

7.1.5.2.4.5 Technical Specification Monitor

The TSM is a nonsafety-related function located on the GENE network segment. The TSM has no signals of it's own. The TSM receives both safety-related and nonsafety-related data from other systems. All safety-related data used by TSM is isolated at the source and transmitted by "one way" or unidirectional data links. There is no data communication or control functionality from TSM to other safety-related or nonsafety-related control systems. The TSM monitors both safety-related (e.g. RPS, SSLC/ESF) and non safety-related (e.g. DPS, SB&PC) systems. Monitoring by the TSM of these different systems are sub functions of TSM.

The TSM, when conditions are detectable, performs the following:

- Monitors, displays, and alarms all three safety-related platforms.

- Warns the operator when a technical specification limit, such as a LCO, is being approached.
- Warns the operator when the LCOs are being violated.
- Determines the approach to an LCO based on equipment status information, core limits, and margins and other data.
- Indicates appropriate action(s) to avoid violating the LCOs.
- Acquires and processes available information to determine the approach to and existence of an LCO.
- Automatically acquires required information.
- Determines, given available information, any automatic testing that could affect the LCOs.
- Indicates the action needed to recover from an LCO.
- Provides a log of LCO violations.
- Acquires or calculates as necessary, reactor and core parameters required for monitoring LCOs, such as thermal limit margins, power distribution, and heat generation rates.
- Shows the results of calculations of reactor and core parameters on operator displays.
- Supports technical specification surveillance testing.
- Provides manual input capability for LCOs and maintenance, calibration, and test data that cannot be monitored automatically by the TSM function.
- Sends alarms to the AMS, which provides for an acknowledgment function for alarm conditions.
- Shows the operator the availability status of the RPS and safety-related systems based on information from those systems' continuous self-diagnostic checks.
- For the Reactor Protection System Monitoring (RPSM) as a sub-function;
    - Monitors support services (for example, voltages, cooling water, oil pressure and levels) that can affect the availability of the RPS and other safety-related systems.
    - Monitors the availability of the initiating equipment (sensors and control systems) and the implementing equipment (for example, pumps, and valves).
    - Monitors the availability of primary and backup sources of services.
    - Monitors process parameters (reactor pressure, water storage tank levels, and environmental conditions) that can affect the successful operation of the RPS or other safety-related systems.

7.1.5.2.4.6 **Report Generator**

The Report Generator is a report definition and execution utility program that allows the user to create reports within the PCF. It produces required custom output reports in the MCR and indirectly to the TSC, and EOF.

The data sources for the Report Generator include any measured or calculated data stored either in the Historian or in a real-time database (measured and calculated points) that enables the report program to locate and retrieve data for pre-configured reports used by operators, engineers and maintenance personnel.

The Report Generator can process algorithms to support plant-wide equipment logs and reports.

7.1.5.2.4.7 Plant Configuration Database

The PCD provides overall configuration and management functions for the N-DCIS at a PCF engineering workstation.

7.1.5.2.4.8 3D MONICORE

3D MONICORE provides core performance information. It has two major components, the Monitor and the Predictor. Both components use a three-dimensional core model code as the main calculation engine. 3D MONICORE provides the logic in the input preparation file that interfaces with the core model code that calculates the key reactor state information such as axial and radial power, moderator void and core flow distributions. From these calculations, other parameters such as the magnitude and location of minimum margin to thermal limits (such as MCPR, peak fuel rod linear powers and average planar heat generation rates), fuel exposure and operating envelope data can be determined.

The 3D MONICORE Monitor periodically tracks current reactor parameters automatically with live plant data. Typically, the tracking interval is once per hour. Additionally, the 3D MONICORE system can be updated automatically by the PAS or ATLMs, or manually by the operator.

The 3D MONICORE Predictor runs upon user request on live data overlaid with user input. It predicts core parameters for steady or transient reactor states other than the present one. This allows the user to study the effects of different rod patterns, core flows and fuel burnups before performing reactor maneuvers to support plant operation.

For accuracy improvement, 3D MONICORE has several adaptation modes, which use in-core neutron flux measurements and AFIP data to calculate nodal fit coefficients that can be input to later Monitor and Predictor cases. The choice of mode depends on the method used to adapt the results of the core model code to in-core detector measurements.

The 3D MONICORE function automatically provides data to other systems including the ATLM and RC&IS. The 3D MONICORE function provides APRM/LPRM calibration data to the PRNM, but only when the equipment is under specific rigorous administrative and manual control (for further information see Subsection 7.1.3.3.4, "Communication from N-DCIS to Q-DCIS [DCIS Time tagging and NMS calibration]"). The data needed by these systems are detailed in their respective system specifications.

7.1.5.2.4.9 Historian

The Historian is the repository for all measured and calculated point data for the plant. It receives input from sources of point data, stores this data and presents it to the report generator, the display driver, and other applications needing historical point data. The Historian:

- Stores point data, plant operating activities, and abnormal event sequences, along with their time tags, for retrieval and analysis.
- Stores third-party generated data, such as 3D MONICORE data, in a format compatible with the display and report system.
- Stores values of RG 1.97 variables for current trending or later analysis.
- Provides on-line data storage capability dependent on plant history and events that are nominally for one fuel cycle. The system warns the system operator about remaining disk storage space, giving the operator time for download to an off-line archiving device. The preferred archiving device uses optical disks.

7.1.5.2.4.10 Transient Recording and Analysis and Sequence of Events Recording

The N-DCIS clock provides the capability to time tag all cabinets' data on the N-DCIS, including Q-DCIS data sent to the N-DCIS (through properly isolated nonsafety-related gateways) at the millisecond level for TRA and the sequence of events recording. Time tagging is accomplished as closely as possible to the origin of the data. The required resolution of time tagging is based on the speed of the monitored process variable, the origin of the data (N-DCIS or Q-DCIS), and the available technology.

The capability of first-out determination and event analysis is provided by the combination of TRA, sequence of events, and the Historian.

Time tagging utilizes a pair of redundant, nonsafety-related, GPS synchronized clocks to synchronize stored data. These N-DCIS clocks provide the network time to all N-DCIS components.

The TRA utilities include reports of current point and historical point data. The TRA utilities can be used to analyze plant events and to support plant startup tests.

Analysis functions are either triggered by plant events or performed periodically based on the wall clock (for example hourly, shift, daily logs and reports).

7.1.5.2.4.11 Core Thermal Power and Core Flow Calculation

Real-time core thermal power from critical to 100% of rated power is calculated continuously. The calculation is supported by multiple, validated parameter measurements and eliminates "constants," previously used for some heat balance inputs, so bias in the calculation is eliminated. At low thermal power levels, the low flow control valve (LFCV) feedwater flow measurement increases accuracy. The core flow is calculated by the heat balance core flow methodology using the core inlet temperature measurement as input to determine core inlet enthalpy.

7.1.5.2.4.12 Thermal Performance Monitor and Diagnostic

The TPM&D provides an on-line diagnostic and monitoring program for the thermal heat cycle. It calculates the deviations of the calculated performance of individual system components from the actual measured performance when the plant is above the threshold power. The trends of the performance data can be used by utility personnel to identify components contributing to thermal efficiency loss.

The TPM&D is a plant model that is normalized to current plant conditions such as reactor power, core flow, reactor pressure and circulating water temperature. The output of the model is a detailed calculation (for example, flows, enthalpies, pressures, and temperatures) of the plant individual heat cycle components with predicted (design basis) and actual performance parameters under that condition. These actual and predicted parameters are compared, and their differences are calculated. An example is an equivalent system parameter such as normalized heat exchanger cleanliness.

7.1.5.2.5 N-DCIS Hardware

The flow of data in the N-DCIS is similar to that in the Q-DCIS. Data are acquired in the nonsafety-related RMUs, sent to nonsafety-related controllers, and then to workstations and displays for monitoring, alarming and recording purposes. The N-DCIS has the following major equipment.

- RMUs located throughout plant buildings such as the RB, CB, FB, Circulating Water System (CIRC) pump house, switchyard, Electrical Building (EB), Turbine Building (TB), and Radwaste Building (RW). The N-DCIS RMUs acquire and output the same signal types as the Q-DCIS RMUs but are nonsafety-related. The RMUs are connected directly to the controller cabinets appropriate to the segment and located in the back panel areas of the CB. The links are by redundant fiber-optic cable.
- Controller cabinets housing the dual/triple redundant control processors, which process the control logic of nonsafety-related NSSS and most BOP systems. The controller processor cabinets receive plant process data multiplexed at the RMUs and transmitted to the controller application processor. The controller application processors then transmit the resulting data to the RMUs where their output signals are used for control of nonsafety-related actuators. The controller application processors also provide data to the MCR VDUs for operator interface displays or plant-level applications. Note that closed loop control takes place within a network segment and within a controller cabinet and its connected RMUs such that this control is not dependent on signals routed from another network switch segment nor dependent on the operation of the N-DCIS networks.
- Network switch cabinets containing the redundant, managed switches for Ethernet switching and providing segmentation, and connection between the N-DCIS components connected to the redundant high-speed fiber-optic cable networks.

- Workstation cabinets, depending on the application, supporting redundant or single workstations that, in turn support the VDUs. The workstations are used for dedicated logic functions where the use of a controller application processor is not appropriate, such as for the Historian, core thermal power or alarm management.
- The N-DCIS datalinks and gateways providing the N-DCIS communication with the Q-DCIS, vendor-supplied controllers, secure communication with the TSC/EOF/ERDS, and other nonsafety-related packaged systems such as area radiation monitoring.
- Cabinets housing vendor-supplied control or monitoring systems such as seismic monitoring, area radiation monitoring, and integrated leak rate testing.
- Gateway cabinets that collect selected safety-related signals through isolated divisional interfaces for archiving and for nonsafety-related control and monitoring purposes. These gateways or workstations are interconnected by fiber-optic cable to support the electrical isolation requirements between the Q-DCIS and the N-DCIS components. The nonsafety-related (N-DCIS) systems have no control-related inputs to the safety-related (Q-DCIS) systems. For further details on gateways, their communication, and transmission of time tagging signals see Subsection 7.1.3.3.
- The MCR consoles and their MCR monitoring and control equipment are the main operator interfaces with the various plant processes. Examples are flat panels, soft controls, hard controls, party phones, meters, alarms, silence/acknowledge pushbuttons, recorders, main generator synchronizing inset, Private Branch Exchange (PBX), radio handsets, keyboards/trackballs.
- The display panels' components and functions that include alarm display, wide display panel, flat panel displays, Closed Circuit Television (CCTV) monitors, large variable display, and the components' associated micro- processors.
- Signal isolators for RMU internal buses and the redundant fiber-optic cable links in the field.
- I/O modules providing interfaces between process sensors/actuators.
- Fiber-optic modems and media converters transmitting and receiving data through the redundant fiber-optic cable links in the field to the redundant controller application processors.
- Computer peripherals, such as printers and plotters, providing output data capabilities.

7.1.5.2.6 **N-DCIS Functions**

The N-DCIS is not required to be operable during or after any DBE. The N-DCIS provides distribution and controls data communication networks that support the monitoring and control of interfacing nonsafety-related plant I&C systems. The N-DCIS also processes data from safety-related systems that are originally acquired by the Q-DCIS. Such data are transmitted through qualified safety-related isolation devices via datalinks and fiber-optic cable to provide the required isolation between the Q-DCIS and the N-DCIS.

Safety-related and nonsafety-related data, once acquired, are available for monitoring, alarming, and recording. Data can be organized for displays and reports. There are no "dedicated" data. For example, data for RG 1.97, SPDS, alarms, a specific system, or for the wide display panel are not restricted to those applications. Data from all sources can be combined as needed.

N-DCIS controllers perform closed loop control and system automatic logic independently of operator inputs from the control room N-DCIS VDUs. RSS panels operate independently of the MCR displays.

The system includes electrical devices and circuitry such as RMUs, controller application processors, network switches, data communication paths, and interfaces. These connect field sensors, display devices, controllers, power supplies, and actuators, which are part of the nonsafety-related systems. The N-DCIS also includes associated data acquisition and communications software that supports its data distribution and control function. The N-DCIS replaces most conventional, long-length, copper-conductor cables with a dual or triple redundant, fiber-optic cable, data network. The fiber-optic cable data network reduces the cost and complexity of cable runs and provides an electrically noise-free transmission path for plant sensor data and nonsafety-related control signals.

Triple redundant controllers and data acquisition systems are used for the DPS, FWCS, SB&PC System, TGCS and PAS. As a minimum, dual redundant controllers and data acquisition are used for all power generation functions including non-control functions (such as 3D MONICORE) that support power generation and core thermal power and flow calculations. The nonsafety-related data from sensors are multiplexed at nonsafety-related RMUs and then transferred through the N-DCIS data network to components of the N-DCIS. Selected signals from the nonsafety-related instrumentation are transmitted to the N-DCIS input cabinets through dedicated hardwired connections for faster transmission rates of signals, such as SB&PC System to TGCS control. Similarly, output signals to actuators and controls that require faster transmission rates, such as manual turbine trip signals, also use dedicated hardwired connections. The RMUs and the data communication network for such nonsafety-related data processing and transmission are part of the N-DCIS.

Divisionally separated redundant isolated digital gateways provide one-way communications from safety-related systems to the N-DCIS. The electrical and data isolation functions are part of the Q-DCIS, and the gateway functions (data conversion and packaging) are part of the N-DCIS. The communications from nonsafety-related systems to the Q-DCIS are limited to communication from the 3D MONICORE function of the N-DCIS to the PRNM (LPRM and APRM) function of the NMS and time tagging. For further detail on this communication and transmission of time tagging signals see Subsection 7.1.3.3.

The local N-DCIS RMUs perform signal conditioning and A/D signal conversion for continuous process signals. They also perform signal conditioning and change-of-state detection for discrete

signals such as contact closures and openings. The RMU function performs both I/O signal-processing functions. The RMU formats the acquired signals into data messages and transmits the data through the data network to N-DCIS components for logic processing. The RMU with a system logic function receives logic commands, such as trip commands and control signals, from the data network N-DCIS controller application processors. The RMU then provides terminal points for distributing the signals to the final actuating devices of the nonsafety-related systems.

Operator interfaces for control and display are realized through multiple, non-dedicated VDUs, each of which is connected to the segmented network switches.

The on-line diagnostic functions of the N-DCIS monitor transmission path quality and integrity. The dual redundant data communication paths are repairable on-line if one path fails. The N-DCIS failures are indicated in the MCR. Periodic surveillance, using off-line tests with simulated input signals, verifies the overall system integrity.

The N-DCIS networks and components are distributed throughout the plant and are powered by redundant internal power supplies fed from two 120 VAC UPS. Systems, such as the DPS, TGCS, FWCS, SB&PC System, and PAS, are triple redundant and are powered by three nonsafety-related UPS load groups.

7.1.5.3 **N-DCIS Safety Evaluation**

The N-DCIS is classified as nonsafety-related. Its operability is not required during or after any DBE. The N-DCIS is required to operate in the normal plant environment and is significant for power production applications. The N-DCIS does not perform any safety-related functions as a part of its design; however the N-DCIS does provide an isolated alternate path for safety-related data from Q-DCIS to N-DCIS that is presented in the MCR. The N-DCIS network that supports the dual/triple, fault-tolerant controllers of the process control systems provides for high speed transfer of data different from Q-DCIS and thus provides diversity in design.

The N-DCIS equipment is located throughout the plant and is subject to the environment of each area. Specifically:

- RMUs are located throughout the plant and auxiliary buildings; and
- Computer equipment and peripherals are located in:
    - The CB in the MCR
    - Back Panel areas in the MCR
    - The EOF
    - Radwaste Building
    - TSC
    - Fuel Building
    - Fuel Building roof area

- Alternate building designations specific to the plant design

Most of the N-DCIS controller cabinets are located in two different rooms of the Control Building that are in separate fire areas. These rooms include the DPS equipment rooms and any of the Q-DCIS Control Building equipment rooms. The RMUs that support the N-DCIS controllers are located in most buildings of the power plant. Where the controllers support PIP A and PIP B systems, the controllers and RMUs are located in different fire areas. The DPS controllers are located in fire areas separate from the N-DCIS and Q-DCIS equipment rooms and the four DPS RMUs are located in the Reactor Building. Two of the four RMUs are located in fire areas (quadrants) of the Reactor Building separate from the other two RMUs. The two RMUs of each pair are located in separate fire areas to separate the DPS RMUs that contain the series connected multiple load drivers used to operate solenoids and squib valves and will prevent inadvertent actuations affecting safe shutdown whether from hot shorts or fires in a single fire area. Finally, the input signals/sensors that provide DPS backup scram, isolation and ECCS functions, and the DPS squib/solenoid valve outputs are arranged such that half of the inputs/outputs are on each pair of RMUs so that a single event cannot cause loss of more than two of the signals needed for the two-out-of-four logic for all DPS (output) actuation.

The N-DCIS panels and components are designed to retain their structural integrity during and after DBEs so that proximate safety-related equipment is not prevented from performing its safety-related function.

Table 7.1-1 identifies the N-DCIS elements and the associated regulatory requirements, guidelines, and codes and standards applied. The N-DCIS major subsystems are summarized in Subsection 7.1.4.8. The following subsections address I&C systems conformance to regulatory requirements, guidelines, and industry standards.

General DCIS conformance to regulatory requirements, guidelines, and industry standards is also addressed in Subsection 7.1.6.

7.1.5.3.1 Code of Federal Regulations

10 CFR 50.34(f)(2)(iii)[I.D.1], Human factors engineering principles applied to control room design:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(iv)[I.D.2], Plant safety parameter display requirements:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and operable automatic status indication of safety systems:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xv)[II.E.4.4], Containment purge/venting system response time and isolation requirements under accident conditions:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident monitoring instrumentation and control room display requirements:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate core cooling instrumentation and control room indication requirements:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xix)[II.F.3], Post- core damage accident plant condition monitoring requirements:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary heat removal systems functional requirements under conditions when main feedwater system is not operable:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Reactor vessel water level measurement requirement under normal post-accident conditions:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of inplant radiation and airborne radioactivity requirements under a broad range of routine and accident conditions:

- Conformance: The N-DCIS design conforms to these requirements.

10 CFR 50.43(e), Innovative means of accomplishing safety functions:

- Conformance: When innovative means are used in the I&C design it complies with 10 CFR 50.43(e).

10 CFR 50.49, Environmental qualifications of electric equipment important to safety for nuclear power plants:

- Conformance: The N-DCIS design conforms to these requirements. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

10 CFR 50.62, Requirements for reduction of risk from Anticipated Transients Without Scram (ATWS) events for light-water-cooled nuclear power plants:

- Conformance: The design has ATWS mitigation functions, as described in Subsection 7.8.1.1.

10 CFR 50.55a(a)(1), Quality standards for systems important to safety, and 10 CFR 50.55a(h) Protection and safety systems compliance with IEEE Std. 603:

- Conformance: The N-DCIS design complies with the above requirements.

10 CFR 52.47, Contents of applications; technical information, level of design information:

- Conformance: The level of detail provided within the design control document (DCD) conforms to this requirement.

10 CFR 52.47(a)(21), Resolution of unresolved and generic (medium- and high-priority) safety issues identified in NUREG-0933:

- Conformance: The N-DCIS is nonsafety-related. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(25), Interface requirements for portions of the plant not within scope of certified design application:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(b)(1), ITAAC in design certification application:

- Conformance: Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for the N-DCIS are identified in Tier 1.

10 CFR 52.47(c)(2), Innovative means to accomplish safety function design completeness requirements per 10 CFR 50.43(e):

- Conformance: The I&C design may use innovative means for accomplishing safety functions.

7.1.5.3.2 General Design Criteria

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, and 64:

- Conformance: The N-DCIS design conforms to these GDCs. Refer to Subsections 3.1.1, 3.1.2, 3.1.3, 3.1.4, and 3.1.6 for a general discussion of each GDC.

7.1.5.3.3 Staff Requirements Memoranda

SRM on Item II.Q of SECY 93-087:

- Conformance: SRM on Item II.Q of SECY 93-087 states that if a postulated common mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

The N-DCIS provides diverse functionality via the DPS and associated interface systems. The nonsafety-related portions of the systems that conform to this guidance are further discussed in Section 7.8 and in Reference 7.1-4.

SRM on Item II.T of SECY 93-087:

- Conformance: The N-DCIS AMS follows guidance in the above document for redundancy, independence, and separation so that the "alarm system" is considered redundant, has its own redundant controller application processors and uses signals from distributed and redundant controllers. Alarm points are sent through a dual network to redundant controller application processors that have dual power feeds. The alarm processors are dedicated, redundant, and conservatively sized. The alarms can be displayed on multiple independent VDUs, each with dual power supplies. Alarms are driven by redundant data links to the AMS. There is one horn and one voice speaker. Test buttons test the horn and the lights.

7.1.5.3.4 Regulatory Guides

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.97.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: See Sections 3.9 (Mechanical Systems and Components) and 3.10 (Seismic and Dynamic Qualification of Mechanical and Electrical Equipment).

RG 1.151, Instrument Sensing Lines:

- Conformance: RG 1.151 is not applicable to the N-DCIS. The N-DCIS receives signals from nonsafety-related sensors in various systems in the plant that are supplied by instrument sensing lines, but the N-DCIS itself does not contain instrument sensing lines.
- For details on conformance to the Regulatory Guides listed in Subsection 7.1.4.4, refer to Subsection 7.1.6.4.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.170.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.171.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: The N-DCIS design conforms to RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: The N-DCIS design conforms to RG 1.180. See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

RG 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: See Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification).

7.1.5.3.5 **Branch Technical Positions**

BTP HICB-1, Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System:

- Conformance: The N-DCIS conforms to BTP HICB-1.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97:

- Conformance: N-DCIS conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52:

- Conformance: The level of detail in this subsection (7.1.5) conforms to BTP HICB-16.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems:

- Conformance: The nonsafety-related portions of the systems that conform to BTP HICB-19 are discussed in Section 7.8 and in Reference 7.1-4.

From the foregoing analyses, it is concluded that the N-DCIS meets its regulatory and industry design bases.

7.1.5.4 N-DCIS Testing and Inspection Requirements

Channel check, channel functional test, logic system functional test, channel calibration, and response time test are required for N-DCIS systems in support of technical specification surveillance requirements. The N-DCIS on-line diagnostic features described below support the technical specification surveillance requirements.

The N-DCIS controllers, displays, monitoring and I/O communication interfaces continuously function during normal power operation. Abnormal operation of these components is detected and indicated. The N-DCIS controllers are equipped with on-line diagnostic capabilities for cyclically monitoring the operability of I/O signals, buses, power supplies, processors, and inter-processor communications. On-line diagnostics are performed without interrupting the normal operation of the N-DCIS.

The N-DCIS components and critical components of interfacing systems are tested to ensure that the specified performance requirements are satisfied. Factory, construction, and preoperational testing of the N-DCIS is performed before fuel loading and startup testing to ensure that the system functions as designed and that tested system performance is within specified criteria.

The N-DCIS interfaces with the TSM for automatic cyclic comparison of channel outputs and monitoring of unacceptable deviations. The TSM provides a log of the results, and sends out-of-limits alarms to the AMS.

The N-DCIS uses diverse platforms for implementing nonsafety-related nuclear functions for 3D MONICORE, RC&IS, AFIP, MRBM, ATLM, and RWM. Self-diagnostic routines with alarms ensure operability.

- 3D MONICORE monitors the reactor core, by accepting signals from the AFIP and the LPRMs. The LPRMs are calibrated with respect to the AFIP signals. Failed sensor inputs are rejected so that they do not contribute to calculations. Subsection 7.1.5.2.4.8 provides a functional description of 3D MONICORE. There are two active redundant workstations, but only one is manually selected by the operator at any time to periodically send fuel thermal limits information to the two redundant ATLMs. The same information is also sent to the TSM to support channel check and channel functional test surveillances.
- The MRBM and the AFIP are subsystems of the NMS. AFIP signals are routed to the 3D MONICORE for calibrating the LPRM. Subsection 7.7.6.2.1 provides a functional description of

the AFIP. The MRBM sends rod block signals to RC&IS to ensure that fuel thermal safety limits are not violated. Subsections 7.7.6.2.2 and 7.7.2.2.7.4 respectively provide a functional description of the MRBM and the rod block function.

- The ATLM and the RWM have two redundant channels that are subsystems of RC&IS, which ensures consistency between specific control rod pattern restrictions and the actual pattern of the rods in the reactor. Subsection 7.7.2 provides a functional description, and Figure 7.7-2 shows a block diagram of RC&IS.
- The ATLMs receive data from 3D MONICORE through message-authenticated data links. They interchange data and generate alarms on disagreements. They send rod block signals to RC&IS to prevent violation of fuel operating thermal limits. Subsection 7.7.2.2.7.7 provides a functional description of the ATLM. ATLM failure automatically generates a rod block and an alarm. Only one ATLM can be bypassed at a time, thus there is always an active ATLM in service. Additionally, automated plant operation is not possible without both ATLMs being in service.
- Fuel thermal limits and rod block signals from the ATLMs and the MRBM are periodically sent to the TSM to support Channel Check and Channel Functional Test surveillances.

As described above, the 3D MONICORE and ATLMs send fuel thermal limit information to the TSM to support channel check and channel functional test surveillances. The data downloads from the two systems are synchronized. The TSM conducts a check to compare the values, and generates alarms if the values are not comparable within acceptable limits.

Once per shift, in steady state operation, an automatic check of rod block capability is generated by the ATLM to close rod block contacts to RC&IS (this signal can also be sent by operator VDU command). The TSM detects the rod block command and generates an alarm. This routine tests the functionality of the output contacts for rod block, and will execute only after checking and confirming that the nuclear parameters as seen by 3D MONICORE are in steady-state.

Additional surveillance tests associated with RC&IS ensure control rod operability and control rod pattern control. The control rod separation switches are also checked for functionality during a refueling outage, along with individual scram time testing on all the rods. A physical coupling and decoupling of the control rod is carried out to actuate the corresponding separation switches and validate the rod block functionality.

7.1.5.5 N-DCIS Instrumentation and Control Requirements

7.1.5.5.1 Uninterruptible Nonsafety-Related AC Power Supply

The N-DCIS components and cabinets that are key to power generation are supplied with either dual redundant or triple redundant power supplies and power feeds. The sources of this power are three independent UPS inverters, supported by AC power under normal operating conditions. If off-site power fails and the diesel generators fail, the N-DCIS inverters receive power from three independent battery systems. These AC power feeds are well regulated and supply 120 ±10%

VAC, 60 Hz. Inverter operation, frequency, voltages, currents, and battery and charger operation are monitored and indicated. The N-DCIS panel is designed so that the loss of one power supply or incoming power source does not affect the N-DCIS or its functional or plant operation.

7.1.5.5.2 Lighting and Service Power System

The Lighting and Service Power System (LSPS) supplies 120 VAC power to the N-DCIS for lighting and maintenance equipment. This includes internal cabinet lighting and convenience outlets.

7.1.5.6 N-DCIS Major System Interfaces

The N-DCIS has interfaces with the I&C and electrical nonsafety-related plant systems. Safety-related system information acquired by the Q-DCIS is available to the N-DCIS through qualified safety-related isolation devices (CIMs) that are part of the Q-DCIS. System interfaces with nonsafety-related systems, or portions of systems, and systems acquiring Q-DCIS data through the isolation devices, datalinks, and gateways include:

- ARMS
- Auxiliary Boiler System (ABS)
- Condensate and Feedwater System (C&FS)
- Chilled Water System (CWS)
- CIRC
- Condensate Storage and Transfer System
- CIS
- CMS
- Control Building HVAC System (CBVS)
- CPS
- CRD system
- Direct Current (DC) Power Supply System
- DPS
- Drywell Cooling System (DCS)
- Electric Power Distribution System (EPDS)
- Electrical Building HVAC (EBVS)
- Equipment and Floor Drain System
- Extraction System
- FAPCS
- FPS

- Fuel Building HVAC System (FBVS)
- Fuel Transfer System (FTS)
- FWCS
- GDCS
- Generator
- Generator Lube and Seal Oil System (GLSOS)
- Heater Drain and Vent System (HDVS)
- High Pressure Nitrogen Supply System (HPNSS)
- Hydrogen Gas Control System (HGCS)
- Hydrogen water chemistry
- IAS
- ICS
- LD&IS
- Lighting and Servicing Power Supply
- Liquid Waste Management System (LWMS)
- Low Voltage Distribution System
- Main condenser and auxiliaries
- Main turbine
- Makeup Water System
- Medium Voltage Distribution System
- Meteorological observation station
- Moisture Separator Reheater System
- NBS
- NMS
- Offgas System (OGS)
- Oil Storage and Transfer System
- Oxygen Injection System (OIS)
- PAS
- PCCS
- PRMS
- PSWS

- Process Sampling System (PSS)
- Q-DCIS
- Radwaste Building HVAC System (RWVS)
- RC&IS
- Reactor Building HVAC System (RBVS)
- RCCWS
- RWCU/SDC
- RPS
- RSS
- The SB&PC System
- Service Air System (SAS)
- Service Building HVAC
- Service Water Building HVAC
- SLC system
- Solid Waste Management System
- SSLC/ESF
- Standby on-site AC power supply
- Stator Cooling Water System (SCWS)
- Turbine Auxiliary Steam System (TASS)
- Turbine Building Cooling Water System
- Turbine Building HVAC System (TBVS)
- Turbine Bypass System (TBS)
- TGCS
- Turbine Gland Seal System
- Turbine Lube Oil System (TLOS)
- Turbine Main Steam System (TMSS)
- Uninterruptible AC Power Supply System
- Yard Miscellaneous Drain System
- Zinc Injection System (ZNIS), an optional system

7.1.6 General DCIS Conformance to Regulatory Requirements, Guidelines and Industry Codes and Standards

Table 7-1 of NUREG-0800 lists the Code of Federal Regulations (CFR), GDC, SRM, RGs, and Instrumentation and Controls Branch Technical Positions (BTP) that provide acceptance criteria or guidelines for each subsection of Chapter 7. Additional acceptance criteria or guidelines are delineated in the (NUREG-0800) SRP Chapter 7 sections.

The specific regulatory acceptance criteria and guideline requirements applicable to each of these systems (safety-related or nonsafety-related but significant for plant operation) identified in the SRP are tabulated in Table 7.1-1. The regulatory requirements and guidelines applicability matrix for Table 7.1-1 is followed in Sections 7.2 through 7.8 by a regulatory conformance discussion for each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the safety evaluation sections for each specific system. Justification for requirements and guidelines not addressed in the ESBWR design are delineated in Tables 1.9-7, 1.9-20, and 1A-1. General Q-DCIS and N-DCIS conformance is discussed in the following subsections.

7.1.6.1 Code of Federal Regulations

10 CFR 50.34(f), Conformance to Three Mile Island (TMI) Action Plan Requirements:

- TMI-related requirements are generically addressed in Appendix 1A. Applicable TMI-related requirements are identified for the systems in Table 7.1-1. The applicable systems are designed to conform. Those TMI-related requirements that are not applicable are not included in Table 7.1-1. The relevant TMI-related requirements that are resolved by the ESBWR Q-DCIS and N-DCIS design are identified as follows:
  - II.K.3.18 - ADS Actuation. ADS is designed for automatic operation.
  - II.K.3.21 - Automatic Restart of LPCS and LPCI. There are no automatic restart requirements based on the ECCS design.
- The TMI action items applicable to the I&C systems are:
  - 10 CFR 50.34(f)(2)(iii)[I.D.1], Human factors engineering principles applied to control room design.
  - 10 CFR 50.34(f)(2)(iv)[I.D.2], Plant safety parameter display requirements, (see Subsection 7.1.5.2.4.1).
  - 10 CFR 50.34(f)(2)(v)[I.D.3], Bypass and operable automatic status indication of safety systems.
  - 10 CFR 50.34(f)(2)(viii)[II.B.3], Capability to obtain and analyze samples from the reactor coolant system and containment.
  - 10 CFR 50.34(f)(2)(x)[II.D.1], Reactor coolant system relief and safety valves test program requirements.

- 10 CFR 50.34(f)(2)(xi)[II.D.3], Reactor coolant system relief and safety valves position (open or closed) indication requirements.
- 10 CFR 50.34(f)(2)(xv)[II.E.4.4], Containment purge/venting system response time and isolation requirements under accident conditions.
- 10 CFR 50.34(f)(2)(xvii)[II.F.1], Accident monitoring instrumentation and control room display requirements.
- 10 CFR 50.34(f)(2)(xviii)[II.F.2], Inadequate core cooling instrumentation and control room indication requirements.
- 10 CFR 50.34(f)(2)(xiv)[II.E.4.2], Containment isolation systems requirements.
- 10 CFR 50.34(f)(2)(xix)[II.F.3], Post- core damage accident plant condition monitoring requirements.
- 10 CFR 50.34(f)(2)(xxi)[II.K.1.22], Auxiliary heat removal systems functional requirements under conditions when main feedwater system is not operable.
- 10 CFR 50.34(f)(2)(xxiii)[II.K.2.10], Anticipatory reactor protection system trip requirements under conditions of loss of main feedwater and on turbine trip.
- 10 CFR 50.34(f)(1)(v)[II.K.3.13], High pressure coolant injection (HPCI) and reactor core isolation cooling (RCIC) initiation levels.
- 10 CFR 50.34(f)(1)(x)[II.K.3.28], Automatic Depressurization System, associated equipment and instrumentation functioning.
- 10 CFR 50.34(f)(2)(xxiv)[II.K.3.23], Reactor vessel water level measurement requirement under normal post-accident conditions.
- 10 CFR 50.34(f)(2)(xxvii)[III.D.3.3], Monitoring of inplant radiation and airborne radioactivity requirements under a broad range of routine and accident conditions.
- 10 CFR 50.34(f)(2)(xxviii)[III.D.3.4], Control room habitability design requirements due to pathways for radiation and radioactivity under accident conditions.

10 CFR 50.43(e), Innovative means of accomplishing safety functions:

- Conformance: When innovative means are used in the I&C design it complies with 10 CFR 50.43(e).

10 CFR 50.44(c)(4), Monitoring requirements for oxygen in containments that use an inerted atmosphere for combustible gas control:

- Conformance: The SSLC/ESF and CMS design conforms to this requirement.

10 CFR 50.49, Environmental qualifications of electric equipment important to safety for nuclear power plants:

- Conformance: The Q-DCIS systems are designed to meet the equipment qualification requirements set forth in 10 CFR 50.49. Details are discussed in Section 3.11

10 CFR 50.55a(a)(1), Quality standards for systems important to safety:

- Conformance: The Q-DCIS and N-DCIS designs conform to this requirement for the use of the applicable standards.

10 CFR 50.55a(h), Protection and safety systems compliance with IEEE Std. 603:

- Conformance: The Q-DCIS design conforms to IEEE Std. 603.

10 CFR 50.62, Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants:

- Conformance: The Q-DCIS and N-DCIS design has ATWS mitigation functions, as described in Section 7.8.

10 CFR 50.63, Loss of all alternating current power:

- Conformance: The Q-DCIS design conforms to these standards, as described in Sections 7.2, 7.3, and 7.4.

10 CFR 52.47, Contents of applications; technical information, level of design information:

- Conformance: The level of detail provided within the DCD conforms to this requirement.

10 CFR 52.47(a)(21), Resolution of unresolved and generic (medium- and high-priority) safety issues identified in NUREG-0933:

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(25), Interface requirements for portions of the plant not within scope of certified design application:

- Conformance: There are no interface requirements for this section.

10 CFR 52.47(b)(1), ITAAC in design certification application:

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(c)(2), Innovative means to accomplish safety function design completeness requirements per 10 CFR 50.43(e):

- Conformance: The I&C design may use innovative means for accomplishing safety functions.

7.1.6.2 General Design Criteria

In accordance with Table 7.1-1, the following GDC are addressed for the Q-DCIS:

GDC 1, 2, 4, 10, 12, 13, 15, 16, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 41, 43, 44, 63, and 64.

- Conformance: The Q-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

GDC 1, 2, 4, 12, 13, 19, 24, 25, 26, 27, 28, 29, 33, 38, 41, 42, 43, 63, and 64.

- Conformance: The N-DCIS design complies with these GDC. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.8.

7.1.6.3 Staff Requirements Memoranda

SRM on Item II.Q of SECY 93-087:

- Conformance: To minimize exposure to common-mode failures, the digital I&C systems are designed for high reliability, with the application of quality assurance requirements as specified in 10 CFR 50.55a(a)(1). Additionally, the digital I&C is designed applying principles of defense-in-depth and diversity defense against common mode failures. Section 7.8 includes the description of the diverse I&C systems that specifically addresses the requirements of this SRM.

SRM on Item II.T of SECY 93-087:

- Conformance: The AMS follows guidance in the above document for redundancy, independence, and separation because the "alarm system" is considered redundant. Alarm points are sent through dual networks to redundant data communication processors on dual power supplies. The AMS alarm processors are dedicated. The alarms are displayed on multiple independent VDUs that each have dual power supplies. The alarm tiles, or their equivalent, are driven by redundant datalinks (with dual power). There are redundant alarm processors. There are no alarms that require manually controlled actions for safety-related systems to accomplish their function. Thus the requirements for safety-related equipment and circuits are not applicable.

7.1.6.4 Regulatory Guides

A discussion of the general conformance of the I&C equipment to RGs is provided below.

RG 1.22, Periodic Testing of Protection System Actuation Functions:

- Conformance: Safety-related systems have provision for periodic testing. Proper functioning of analog sensors is verified by channel cross-comparison and is done continuously by the PCF. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the guidance

of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.8.

RG 1.45, Reactor Coolant Pressure Boundary Leakage Detection Systems:

- Conformance: Provisions are made to detect and monitor identified and unidentified leakage of reactor coolant consistent with the guidance of this RG.

RG 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems:

- Conformance: Bypass indications are designed to satisfy the guidance of IEEE Std. 603, Paragraph 5.8.3, and RG 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

Bypass indications use isolation devices that preclude adverse electrical effect of the bypass indication circuits on the plant safety-related system.

RG 1.53, Application of the Single Failure Criterion to Safety Systems:

- Conformance: The safety-related systems are organized into four physically and electrically-isolated divisions that use the principles of independence and redundancy for the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally, the design meets N-2 conditions. Analyses complying with IEEE Std. 379 will be used to confirm the safety-related systems designs' conformance to the single failure criterion.

RG 1.62, Manual Initiation of Protective Actions:

- Conformance: The applicable I&C systems are designed to comply with RG 1.62. Specific conformance of the I&C systems is addressed in Sections 7.2 through 7.4.

RG 1.75, Criteria for Independence of Electrical Safety Systems:

- Conformance: The safety-related system designs conform to RG 1.75 as described in Subsections 8.3.1.3 and 8.3.1.4.

RG 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants:

- Conformance: The safety-related system design conforms to RG 1.89.

RG 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants:

- Conformance: The Q-DCIS and N-DCIS are designed to meet the guidance of RG 1.97. Details of design implementation are discussed in Section 7.5.

RG 1.100, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants:

- Conformance: The Q-DCIS systems are designed to meet the guidance set forth in RG 1.100. See Section 3.9 (Mechanical Systems and Components) and 3.10 (Seismic and Dynamic Qualification of Mechanical and Electrical Equipment).

RG 1.105, Setpoints for Safety-Related Instrumentation:

- Conformance: The Q-DCIS and N-DCIS are consistent with the guidance of RG 1.105. The applicable analytical or design basis limit (technical specification limit), as well as the nominal trip setpoint (instrument setpoint) and any "as-found tolerance," and "as left tolerance" are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy safety-related requirements and plant availability objectives.

RG 1.118, Periodic Testing of Electric Power and Protection Systems:

- Conformance: The I&C systems are consistent with the guidance of RG 1.118.

RG 1.151, Instrument Sensing Lines:

- Conformance: The instrument sensing lines are designed to satisfy the guidance of RG 1.151. These lines are used to perform safety-related and nonsafety-related functions. There are four redundant, separate sets of instrument lines, each having safety-related instruments associated with one of the four electrical safety-related divisions. The RPS logic requires any two-out-of-four unbypassed, like parameter trip signals to scram. If a division is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with triple fault-tolerant digital controllers (FTDC) that use sensors separate from the safety-related sensors. Therefore, the systems are designed to meet N-2 conditions so that no single failure or two-division failure results in a plant condition requiring protective action and at the same time, prevents the remaining redundant protection divisions from providing the protective action. Sections of endorsed standard ISA-67.02.01 on design practices for tubing, vents, and drains also apply to nonsafety-related instrumentation.

RG 1.152, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants:

- Conformance: The guidelines of RG 1.152 are a basis for design procedures established for programmable digital equipment. As the principle RG for digital computers in safety-related systems in nuclear power plants, it endorses and refers to IEEE Std. 603 for specific criteria details. This RG also contains discussions on digital I&C equipment common mode failure issues. A design error in the software in redundant divisions of a safety-related system could lead to common cause or common mode failure of the safety-related system function. Therefore, a form of diversity is necessary that provides additional assurance beyond that which is provided by the design and quality assurance (QA) programs that incorporate software QA and V&V. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense-in-depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that

actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity.

The following sections are noted in IEEE Std. 7-4.3.2 as specifically addressed by the NRC in RG 1.152:

- Annex B, “Diversity Requirements Determination.” This annex provides a methodology for determining the need for diversity. RG 1.152 does not endorse Annex B.
- Annex C, “Dedication of existing commercial computers.”
- Annex E, “Communication Independence.” The NRC does not endorse Annex E.
- Annex F, “Computer reliability.” The NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. The NRC acceptance is based on deterministic criteria.
- Safety I&C System compliance with IEEE Std. 7-4.3.2

Additionally, RG 1.152 includes guidance applicable to the Q-DCIS. Compliance is summarized as follows:

- Defense against software common mode failures: GEH has evaluated BTP HICB-19 guidelines including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common mode failures. The four echelons are control systems, reactor trip system, Engineered Safety Features Actuation System (ESFAS), and monitoring and indicator functions. To address the guidelines of BTP HICB-19 on defense-in-depth and diversity and defense against common mode failures, the DPS backs up the primary safety-related I&C system protection functions. The DPS is implemented with hardware and software that is separate, independent, and diverse from the primary safety-related I&C protection systems (RTIF, NMS, and SSLC/ESF). The DPS is implemented in addition to the ATWS/SLC system function. A detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8.
- Software development process: The software development process of the Q-DCIS (including control systems key to plant operation) follows the guidelines of BTP HICB-14. Software development process plans for the DCIS design implementation include the Software Management Plan (SMP), Software Development Plan (SDP), Software Verification and Validation Plan (SVVP), Software Configuration Management Plan (SCMP), Software Safety Plan (SSP), as required by guidance in BTP HICB-14 and are described in Appendix 7B. Actual detailed hardware and software design implementation follows the guidelines specified by these plans as part of the design acceptance criteria process.

- Equipment qualification, self-diagnostics, independence, and reliability: IEEE Std. 603 states that these requirements are applicable to safety-related I&C system equipment. The Q-DCIS meets the requirements of IEEE Std. 603, and the above requirements in areas applicable to digital computer-based equipment.
- Security: The security guidelines included in RG 1.152 are evaluated and incorporated as appropriate and necessary in the DCIS design, both on plant hardware security measures and software security measures. The software development process plans for the DCIS design implementation include the Cyber Security Program Plan.

RG 1.153, Criteria for Safety Systems:

- Conformance: Safety-related systems are designed to satisfy the requirements of IEEE Std. 603, as endorsed by RG 1.153.

RG 1.168, Verification, Validation, Reviews, and Audits For Digital Computer Software Used In Safety Systems of Nuclear Power Plants:

- Conformance: This RG endorses IEEE Std. 1012, IEEE Standard for SVVPs, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety-related systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and SVVP and thus comply with RG 1.168.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: RG 1.169 endorses IEEE Std. 828, IEEE Standard for SCMPs, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety-related systems. Safety-related systems use the guidance in these standards, as discussed in Reference 7.1-10, to develop portions of the overall SDP and SCMP and thus comply with RG 1.169.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems Of Nuclear Power Plants:

- Conformance: The guidance contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provides an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety-related system software subject to the provisions in this guide. Safety-related systems use the guidance in these standards to develop portions of the overall SDP and STP and thus comply with RG 1.170.

RG 1.171, Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants:

- Conformance: RG 1.171 endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. Safety-related systems use the guidance in this standard to develop, as discussed in Reference 7.1-10, portions of the overall SDP and, thus, comply with RG 1.171.

RG 1.172, Software Requirements Specifications For Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: RG 1.172 endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practices for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety-related applications; however, it does provide guidance on the development of software requirements specifications that exhibit characteristics important for developing safety-related system software. This is consistent with the goal of ensuring high-integrity software in reactor safety-related systems. Safety-related systems use the guidance in this standard, as described in the References 7.1-10 and 7.1-12, to develop portions of the overall SDP and STP and thus comply with RG 1.172.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants:

- Conformance: RG 1.173 endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard is used in conjunction with guidance from other appropriate RGs, standards, and software engineering literature. Safety-related systems use the guidance in this standard, as described in References 7.1-10 and 7.1-12, to develop portions of the overall SDP and thus comply with RG 1.173.

RG 1.180, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems:

- Conformance: Electrical and electronic components in the I&C safety-related systems are qualified for anticipated levels of EMI at their as-installed locations. EMC of I&C equipment is verified through factory testing and site-specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against the following:

- EMI
- RFI
- Electrostatic discharge
- Electrical surge

EMI qualifications, including methods of evaluating EMI operating envelopes, follow the requirements defined in Section 3.11.3.1. Q-DCIS equipment is qualified to perform continuously within specified ranges even when exposed to EMI environmental limits at the hardware mounting location. To that end, EMI qualifications for safety-related systems meet the proposed requirements of RG 1.180, Rev 1 “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in safety-related Instrumentation and Control Systems.”

RG 1.204, Guidelines for Lightning Protection of Nuclear Power Plants:

- Conformance: The surge withstanding capability of the safety-related I&C design conforms with IEEE Std. 1050. See Subsection 8A.1.2 for detailed information about the lightning protection system and conformance to RG 1.204.

RG 1.209, Guidelines For Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants:

- Conformance: The safety-related system design conforms to RG 1.209.

7.1.6.5 Branch Technical Positions

BTPs that are applicable to the DCIS systems are identified relative to the I&C systems in Table 7.1-1. BTPs that are not applicable to the I&C design are identified in Table 1.9-7. BTPs are guidance documents; the DCIS is generally designed to conform to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.1 through 7.8.

The following BTPs are not applicable to the ESBWR design:

BTP HICB-3, Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service. Reactor coolant pumps are not used in the design and Position B.1 does not apply.

BTP HICB-6, Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode. No recirculation pumps and ECCS pumps are used in the design.

BTP HICB-13, Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors. RTDs are not used in safety-related applications.

The following BTPs are applicable:

BTP HICB-1, Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System. The GDCS and PIP A/B segment of N-DCIS design conforms to BTP HICB-1.

BTP HICB-8, Guidance for Application of Regulatory Guide 1.22. The Q-DCIS is fully functional during reactor operation and is tested in conjunction with the SSLC/ESF. Therefore, the Q-DCIS design conforms to BTP HICB-8. The DPVs, SRVs, and squib valves are not tested during reactor operation.

BTP HICB-9, Guidance on Requirements for Reactor Protection System Anticipatory Trips. The Q-DCIS conforms to BTP HICB-9.

BTP HICB-10, Guidance on Application of Regulatory Guide 1.97. The Q-DCIS and N-DCIS design conforms to BTP HICB-10. Details of design implementation are discussed in Section 7.5.

BTP HICB-11, Guidance on Application and Qualification of Isolation Devices. The Q-DCIS design conforms to BTP HICB-11.

BTP HICB-12, Guidance on Establishing and Maintaining Instrument Setpoints. The Q-DCIS design conforms to BTP HICB-12.

BTP HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems. Refer to Subsection 7.1.2.4, References 7.1-10 and 7.1-12 discussions. The Q-DCIS design conforms to BTP HICB-14.

The Q-DCIS and N-DCIS follow a development process that is in accordance with BTP HICB-14. As part of the Certification activity, the software development process plans require NRC review and approval.

Safety-related I&C systems (RTIF, NMS and SSLC/ESF) use computers for their logic functions. A description of the Q-DCIS design, together with the description of the DPS is included in Section 7.8, and specifically addresses the issues of defense-in-depth and diversity and defense against common mode failures.

BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52. BTP HICB-16 is applicable to all sections of Chapter 7 of the Design Control Document and all sections conform to it.

BTP HICB-16 states that the application should:

- Describe the resolution of unresolved and generic safety issues applicable to the I&C systems.
- Describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system.
- Identify and describe the validation of innovative means of accomplishing I&C system safety-related functions.

Applications that propose the use of computers for systems with safety-related uses should describe the computer system development process. Applications that propose the use of computers for RTS and ESFAS functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The I&C design has no unresolved or generic safety-related issues. The I&C related issues are either not applicable to safety-related I&C systems or are addressed by the safety-related I&C design. Within the scope of the DCD submitted for certification application, there are no interface requirements described here that fall into this category.

The design uses the voluminous data available from operating plants and from the testing and licensing efforts performed to license the predecessor designs and individual plants. The I&C design does not use innovative means for accomplishing safety functions.

BTP HICB-17, Guidance on Self-Test and Surveillance Test Provisions. Refer to Subsection 7.2.1.3.5 and Subsection 7.3.4.3 discussions. The Q-DCIS design conforms to BTP HICB-17.

BTP HICB-18, Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems. The Q-DCIS design conforms to BTP HICB-18.

BTP HICB-19, Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087). The Q-DCIS, DPS and associated N-DCIS interfacing systems design conform to BTP HICB-19. The implementation of an additional diverse instrumentation and control system is described in Section 7.8.

BTP HICB-21, Guidance on Digital Computer Real-Time Performance. The Q-DCIS design conforms to BTP HICB-21.

7.1.6.6 Industry Standards

The safety evaluation subsections throughout Chapter 7 address the RGs identified by the SRP. The IEEE standards that are endorsed by RGs are not addressed separately.

Some codes or standards that are not mentioned in the SRP are used in specific system applications. These are identified in the system description and the corresponding reference section. In accordance with the SRP format, the following IEEE standards applicable to the I&C equipment are addressed in other chapters.

IEEE Std. 323, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.” Safety-related systems are designed to meet the requirements of IEEE Std. 323. Environmental qualification is addressed in Section 3.11.

IEEE Std. 344, “Recommended Practices for Seismic Qualification of Safety-related Equipment for Nuclear Power Generating Stations.” Safety-related I&C equipment is classified as Seismic

Category I and designed to withstand the effects of the safe shutdown earthquake (SSE). It remains functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE Std. 344 as indicated in Section 3.10.

IEEE Std. 379, “IEEE Standard for the Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems.” The three Q-DCIS platforms, RTIF-NMS, SSLC/ESF, and ICP are organized into four physically and electrically isolated divisions that use principles of redundancy and independence to conform to the single failure criterion.

IEEE Std. 383, “IEEE Standard for Type Test of Safety-related Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations.” Electric cable conforms to this standard. Fiber-optic cable insulation/covering/jacketing also conforms to the requirements for flame tests in IEEE Std. 383.

IEEE Std. 384, “IEEE Standard Criteria for Independence of Safety-related Equipment and Circuits.” See the discussion of RG 1.75 in Subsection 7.1.6.4.

IEEE Std. 497, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.” Accident monitoring instrumentation is discussed in Section 7.5.

IEEE Std. 518, “IEEE Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources.” The design conforms to IEEE Std. 518.

IEEE Std. 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.” Conformance to IEEE Std. 603 is discussed in Subsection 7.1.6.6.1.

IEEE Std. 1050, “IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations.” The design conforms to IEEE Std. 1050.

7.1.6.6.1 IEEE Std. 603 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

The scope of IEEE Std. 603 includes safety-related I&C systems that are described in Sections 7.1 through 7.8. IEEE Std. 603 does not directly apply to nonsafety-related systems, other than to require independence between nonsafety-related systems and safety-related systems. IEEE Std. 603 provides design criteria for safety systems. ESBWR divides safety systems into two parts: the Q-DCIS platforms, and the subsystems that contain the sensors and actuators used by the Q-DCIS platforms. This section describes how the IEEE Std. 603 criteria are allocated to the different Q-DCIS platforms and subsystems. For convenience, some of these requirements may also be adopted as design bases for some nonsafety-related I&C components and systems such as for accident monitoring instrumentation, in accordance with RG 1.97. Compliance with the requirements of IEEE Std. 603 is also identified as compliance with the requirements and guidance contained within the federal regulations, GDC, SRM, and RGs, as described throughout Section 7.1. The safety-related I&C design comprises the Q-DCIS which includes the equipment in

the RTIF (which may include ICP unless space consideration dictates locating the ICP hardware in separate cabinets), NMS, and SSLC/ESF cabinets. The design conforms to IEEE Std. 603. ITAACs are provided for the major attributes for compliance with IEEE Std. 603 and are not intended to limit the scope of compliance.

When the IEEE Std. 603 design criteria are applied to platforms relying on the use of software to perform their safety-related functions, additional criteria from IEEE Std. 7-4.3.2, which augments the IEEE Std. 603 criteria, also apply to the platform as described under the applicable IEEE Std. 603 criterion. The evaluation of Q-DCIS platforms for compliance with IEEE Std. 603 and IEEE Std. 7-4.3.2 criteria includes the examination of the effects that the associated sensors and actuators have on the performance of the safety-related function.

In accordance with the software development process described in Appendix 7B and the defense-in-depth and diversity strategy described in Section 7.8, the protection systems are executed as software projects on particular Q-DCIS platforms. The software projects are named RTIF, NMS, SSLC/ESF, VBIF, ATWS/SLC, HP CRD, and ICS DPV isolation function.

Table 7B-1 shows the relationship between the Q-DCIS platforms and their corresponding software projects. As shown, the RTIF-NMS platform has two software projects: RTIF and NMS. The SSLC/ESF platform has one software project: SSLC/ESF. The Independent Control Platform has four software projects: VBIF, ATWS/SLC, HP CRD, and ICS DPV isolation function.

7.1.6.6.1.1 Safety System Designation (IEEE Std. 603, Section 4, et al)

IEEE Std. 603, Section 4, requires that a specific basis be established for the design of each safety-related system. The designs of the Q-DCIS platforms are based on the abnormal events in Table 15.0-2.

Criterion 4.1 requires identification of the DBEs applicable to each mode of operation of the plant along with the initial conditions and allowable limits of plant conditions for each such event. Table 1.3-1 defines the reactor system design characteristics. Tables 15.0-3, 15.0-4, 15.0-5, and 15.0-6 define the safety-related analysis acceptance criteria for the anticipated operational occurrence (AOOs), infrequent events, special events, and accidents. Table 15.1-2 defines the ESBWR operating modes for the entire operating envelope. Table 15.1-3 defines the ESBWR abnormal events with applicable operating modes. Table 15.2-1 defines the input parameters, initial conditions, and assumptions for AOO events and infrequent events. Table 15.5-2 defines the initial conditions and bounding limits for ATWS events. Credited systems, interlocks, and functions for each DBE are described in Sections 15.2, 15.3, 15.4, and 15.5. Additional details about the specific safety-related or nonsafety-related interfacing system design bases, interlocks, and functions are found in Sections 4.6, 5.2, 5.4, 6.2, 6.3, 8.3, 9.1, 9.3, 9.4, 10.2, 10.3, and 10.4. Information provided for each design basis item enables the detailed design of the system to be carried out. Safety-related system design basis descriptions are included in the various sections of this chapter as indicated below.

- Reactor Trip System
  - RPS (Subsection 7.2.1)
  - NMS (Subsection 7.2.2)
  - Suppression Pool Temperature Monitoring (Subsection 7.2.3)
- SSLC/ESF (Subsection 7.3.5)
  - ECCS (Subsection 7.3.1)
    - ADS (Subsection 7.3.1.1)
    - GDCS (Subsection 7.3.1.2)
    - ICS (Subsection 7.4.4)
    - SLC system (Subsection 7.4.1)
- PCCS (Subsection 7.3.2).
- LD&IS non-MSIV functions (Subsection 7.3.3) (MSIV functions of the LD&IS are located in the RTIF cabinets).
- CRHS (Subsection 7.3.4).
- RSS (Subsection 7.4.2).
- RWCU/SDC (Subsection 7.4.3).
- PAM system (Subsection 7.5.1).
- CMS (Subsection 7.5.2).
- PRMS (Subsection 7.5.3).
- ATWS/SLC (Subsection 7.8.1).
- CRHS (Subsection 7.5.2).
- VB isolation function (Subsection 7.3.6).
- HP CRD (Subsection 7.4.5).
- ICS DPV isolation function (Subsection 7.3.7).

Criterion 4.2 requires identification of the safety-related functions and corresponding protective actions of the execute features for each event evaluated in the Nuclear Safety Operational Analysis (NSOA). Table 15.1-5 defines the execute systems required to respond to each event. Table 15.1-6 defines the automatic safety-related instrument trips in response to each event. Additionally, safety-related design bases for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.3 requires identification of the permissive conditions for each operating bypass capability that is to be provided. Additionally, the permissive conditions for each operating bypass for each

system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

Criterion 4.4 requires identification of the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. The minimum list of such variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that are associated with each event are discussed in the relevant subsection describing the event as defined in Table 15.1-7.

Criterion 4.5 requires identification of (1) the points in time and the plant conditions during which manual control is allowed, (2) the justification for permitting initiation or control subsequent to initiation solely by manual means, (3) the range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations are performed, and (4) the variables identified by Criterion 4.4 that are displayed for the operator to use in taking manual action, for each action identified by Criterion 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18.

Criterion 4.6 requires identification of the minimum number and locations of sensors required for protective purposes for those variables identified by Criterion 4.4 that have spatial dependence. The minimum list of variables and combinations of variables to be monitored is determined as part of the HFE design process described in Chapter 18. The variables and combinations of variables that have spatial dependence are described within each applicable subsection of this chapter.

Criterion 4.7 requires identification of the range of transient and steady-state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the safety system performs. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Section 3.11. Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Design Environmental Criteria.

Criterion 4.8 requires identification of the conditions having the potential for functional degradation of safety system performance and for which provisions are incorporated to retain the capability for performing the safety functions. Safety-related mechanical equipment and electrical equipment (which comprises electrical power and instrumentation and controls equipment) is qualified in accordance with the equipment qualification program described in Sections 3.9 through 3.11.

Environmental conditions for the zones where qualified equipment is located are calculated for normal, AOO, test, accident and post-accident conditions and are documented in Appendix 3H, Equipment Qualification Environmental Design Conditions.

Criterion 4.9 requires identification of the methods to be used to determine that the reliability of each safety system design is appropriate and any qualitative or quantitative reliability goals that may be imposed on the system design. The ESBWR Design Reliability Assurance Program (D-RAP) is a program utilized during detailed design and specific equipment selection phases to assure that the important ESBWR reliability assumptions of the Probabilistic Risk Assessment (PRA) are addressed throughout the plant life. The D-RAP is described in Section 17.4.

Criterion 4.10 requires identification of the critical points in time or the plant conditions, after the onset of a design basis event, including: (1) the point in time or plant conditions for which the protective actions of the safety system are initiated, (2) the point in time or plant conditions that define the proper completion of the safety function, (3) the point in time or the plant conditions that require automatic control of protective actions, and (4) the point in time or the plant conditions that allow returning a safety system to normal. The relevant points in time and plant conditions associated with each event, except for the allowable conditions for returning a plant to normal, are discussed in the relevant subsection describing the event as defined in Table 15.1-7. The allowable conditions for returning a plant to normal (i.e., return to service conditions) will be developed as part of the procedure development process described in Section 18.9.

Criterion 4.11 requires identification of the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The safety-related systems are designed to accomplish their safety-related functions in accordance with the single failure criterion, IEEE Std. 603, Section 5.1. Failure Modes and Effects Analyses (FMEAs) are performed on the safety-related system final design to ensure that no equipment protective provisions preclude correctly performing any safety-related function.

Criterion 4.12 requires identification of any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria). The design bases for each subsystem (including bases for diversity, interlocks, regulatory agency criteria) are identified within each applicable subsection of this chapter.

7.1.6.6.1.2 Single Failure Criterion (IEEE Std. 603, Section 5.1)

The safety-related system designs are organized into four physically and electrically isolated divisions that use the principle of independence and redundancy to conform to the single failure criterion as defined by IEEE Std. 379, Section 4, and IEEE Std. 603, Section 5.1; additionally the design meets N-2 conditions (see Subsection 7.1.3.3.6).

The safety-related control systems include sufficient redundancy and independence to fulfill their intended safety function even when degraded by any single credible failure. The RTIF - NMS, SSLC/ESF, and ICP implement the single failure criterion of IEEE Std. 603 Section 5.1 using four

independent and redundant divisions, which are provided in two-out-of-four trip logic. This ensures no single failure of or within any division prevents the system from performing its safety function or causing either an inadvertent reactor scram or an ECCS actuation. Redundancy begins with the sensors monitoring the variables and continues through the signal processing, output devices, and actuators.

Independence is implemented as described in Subsections 7.1.6.6.1.7 and 7.1.6.6.1.20.

Failure Modes and Effects Analyses (FMEAs) complying with IEEE Std. 379 are used to confirm the safety-related system designs' conformance to the single failure criterion.

The FMEA is consistent with the failure modes detectable by the self-diagnostic features of the hardware/software platforms and those detected by periodic surveillance.

Equipment is provided in accordance with a prescribed quality assurance program as described in Subsection 7.1.6.6.1.4.

7.1.6.6.1.3 Completion of Protective Action (IEEE Std. 603, Sections 5.2 and 7.3)

After initiation by either automatic or manual means, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2. They go to completion by using one of the following: seal-in logic, non-resettable squib valves, manually reset valves, diverse functions, or a combination of logic, valves and functions. Deliberate operator action is required to reset the safety-related systems. Additionally, completion of protective actions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.4 Quality (IEEE Std. 603, Section 5.3)

The Quality criterion requires that the Q-DCIS be consistent with minimum maintenance requirements and low failure rates and be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Q-DCIS meets this requirement through the application of the ESBWR Quality Assurance Program described in Chapter 17.

IEEE Std. 7-4.3.2 has additional quality assurance requirements related to software. Refer to LTRs "ESBWR - Software Management Program Manual" (Reference 7.1-12) and "ESBWR - Software Quality Assurance Program Manual" (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software quality assurance requirements.

- IEEE Std. 7-4.3.2, Criterion 5.3.1, Software Development. The quality of software development activities is assured in accordance with the Software Quality Assurance Plan (SQAP).
- IEEE Std. 7-4.3.2, Criterion 5.3.2, Software Tools. Software tools are controlled in accordance with the Software Configuration Management Plan (SCMP).

- IEEE Std. 7-4.3.2, Criterion 5.3.3, Verification and Validation (V&V). Software V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.4, Independent V&V. Software Independent V&V is performed in accordance with the Software V&V Plan (SVVP).
- IEEE Std. 7-4.3.2, Criterion 5.3.5, Software Configuration Management. Software configuration is controlled in accordance with the Software Configuration Management Plan (SCMP).
- IEEE Std. 7-4.3.2, Criterion 5.3.6, Software Project Risk Management: Software project risk management is managed in accordance with the Software Management Plan (SMP).

Safety-related equipment is provided under the GEH 10 CFR 50, Appendix B Quality Assurance Program. The NRC accepted GEH Quality Assurance Program with its implementing procedures, constitutes the Quality Assurance system that is applied to the Q-DCIS design. It satisfies the requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; and 3) ISO 9001. Safety-related I&C systems employing digital computers, software, firmware, and software tools conform to the quality requirements in IEEE Std. 7-4.3.2 as described in References 7.1-10 and 7.1-12.

7.1.6.6.1.5 Equipment Qualification (IEEE Std. 603, Section 5.4)

The Equipment Qualification criterion requires the referencing platform to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that the safety-related system is capable of meeting the performance requirements specified in the design basis. The Q-DCIS meets the Equipment Qualification requirements through the application of the Equipment Qualification program that is described in Sections 3.9 through 3.11. Refer to Table 3.11-1 for a list of electrical and mechanical equipment and conformance criteria for Equipment Qualification.

IEEE Std. 7-4.3.2 has additional Equipment Qualification requirements related to Structures, Systems, or Components (SSCs) using software. Refer to LTRs "ESBWR - Software Management Program Manual" (Reference 7.1-12) and "ESBWR - Software Quality Assurance Program Manual" (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software equipment qualification requirements.

- IEEE Std. 7-4.3.2, Criterion 5.4.2, Qualification of existing commercial computers: The commercial computer qualification testing is performed in accordance with the commercial-off-the-shelf dedication process in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.4.1, Computer System Testing: The referencing platform qualification testing is performed with the referencing system functioning with software and diagnostics that are representative of those used in actual operation in accordance with the Software Test Plan.

7.1.6.6.1.6 System Integrity (IEEE Std. 603, Section 5.5)

The System Integrity criterion requires that the referencing platform's features be adequate to ensure completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment enumerated in the design basis. The Q-DCIS meets this requirement through the application of the Equipment Qualification program described in Sections 3.9 through 3.11, and Subsection 7.1.6.6.1.5.

IEEE Std. 7-4.3.2 has additional system integrity requirements related to SSC using software. Refer to LTRs "ESBWR - Software Management Program Manual" (Reference 7.1-12) and "ESBWR - Software Quality Assurance Program Manual" (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 criteria related to the following hardware and software system integrity requirements:

- IEEE Std. 7-4.3.2, Criterion 5.5.1, Design for computer integrity: The referencing system is designed to perform its safety-related function when subjected to design basis conditions.
- IEEE Std. 7-4.3.2, Criterion 5.5.2, Design for test and calibration: The referencing system is designed to perform its safety-related function when undergoing test and calibration in accordance with the Software Development Plan.
- IEEE Std. 7-4.3.2, Criterion 5.5.3, Fault detection and self-diagnostics: Fault detection and self-diagnostics (as performed by platform self-test features) do not adversely affect the capability of the referencing system to perform its safety-related functions.

The Q-DCIS systems are required to accomplish their safety-related functions under the range of conditions enumerated in the design bases. Other areas addressed as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety-related analysis, as part of BTP HICB-14 requirements), failure to a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The Q-DCIS meets the integrity requirements described in IEEE Std. 603, Section 5.5. The RTIF - NMS platform functions fail to the tripped state. The SSLC/ESF platform and the independent control platform fail to a state where the actuated component remains "as-is" to prevent a control system induced LOCA. Hardware and software failures detected by self-diagnostics cause a trip signal to be generated in the RPS division in which the failure occurs and no trip signal is generated if the failure occurs in a SSLC/ESF or independent control platform division. Single failures of hardware and software do not inhibit manual initiation of protective functions.

7.1.6.6.1.7 Independence (IEEE Std. 603, Section 5.6)

The required independence between redundant portions of a safety-related system, between safety-related systems and the effects of DBEs, and between safety-related systems and other systems is defined. Three aspects of independence are addressed in each case: physical

independence, electrical independence, and communication independence. The Q-DCIS design meets these requirements.

Each division is sufficiently independent from the other divisions so that no one division is dependent on information, timing data, or communication from any other division to initiate a safety-related trip signal. The failure of a single division does not prevent the initiation of a safety-related trip. Each safety-related logic evaluates the data from its own division's sensors and continuously broadcasts the result of its evaluation to the other divisions as either a "trip" or "no trip" signal.

A safety-related trip is initiated whenever any two divisions sense conditions that require a safety-related trip. Each division receives input data from its own separate set of sensors connected to the same process source and separately transmits trip signals to the other divisions. The trip actuators go to their trip state whenever they receive concurrent, like parameter trip signals from any two safety-related logic transmissions. The signal isolators are qualified to withstand all credible faults, such as short circuits or high voltage (HV), so that faults cannot propagate and degrade the performance of any safety-related control function.

Physical Independence

The Q-DCIS systems have four redundant and independent divisions that are physically independent and separated and that have independent electrical power sources applied to them. Except where fiber-optic cable is used, there are no common switches shared by the four divisions. The sensors used for each of the four divisions, are independent and physically separated from one another. Wiring and electrical components are physically separated via isolation barriers or spacing. Refer to Subsection 7.1.3.3.1.

Electrical Independence

Independence between safety-related systems is achieved through equipment qualification and isolation. Safety-related systems are separated and independent from nonsafety-related systems. When system interfacing is required, electrical isolation is provided via isolation devices (qualified per IEEE Std. 384) and by the use of fiber-optic cables.

Communication Independence

Communication between redundant safety channels is limited (e.g., to trip bypass status and message authentication signals) and is through isolation devices. In accordance with IEEE Std. 379, communication between redundant divisions or between safety-related control systems and nonsafety-related control systems is electrically isolated and one-way. (Refer to Subsection 7.1.3.3.) In addition, loss of communication or communication upsets are contained within a single channel and cannot inhibit the ability of redundant channels to perform their functions. Optical couplers and fiber-optic cable provide the route for communications.

Communication between safety-related systems and nonsafety-related systems is carried out via fiber-optic cable through the required qualified safety-related signal isolation devices (i.e., CIMs), and data pathways such as datalinks and gateways. Communication from nonsafety-related systems to safety-related systems is prohibited, with the exception of time tagging and NMS calibration data. Additional discussion on this subject is included in Subsection 7.1.3.3. The RTIF, NMS, and SSLC/ESF protection functions have priority over data transmissions, so that data transmissions do not interfere with the RTIF, NMS, or SSLC/ESF protection functions.

7.1.6.6.1.8 Capability for Testing and Calibration (IEEE Std. 603, Section 5.7)

The capability for testing and calibration of safety-related system equipment is provided during power operation and duplicates the performance of the safety-related function as closely as practicable, as discussed in Sections 7.2 through 7.8. Tests are capable of being performed in overlapping segments when testing one safety-related function. Maintenance bypasses of individual functions are provided in the safety-related system channels to enable testing during power operation. For example, the safety-related functions of each safety-related division can be tested on-line with the tested division bypassed from the two-out-of-four voting trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors. The Q-DCIS meets the requirements outlined in this section. Refer to Subsections 7.1.3.3.6, 7.1.3.3.7, 7.1.3.4 and 7.1.3.5.

Safety-related sensors are designed with the capability for test and calibration during reactor operation. Additionally, exceptions for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.9 Information Displays (IEEE Std. 603, Section 5.8)

The Information Displays criterion requires that information displays for the referencing platform be designed to be accessible to the operators, display variables for manually controlled actions, display system status information, provide indication of bypasses, and display post-accident monitoring variables in accordance with the HFE process. The Q-DCIS information displays, including displays for manually controlled actions, meet this requirement by the application of the HFE design process described in Chapter 18. This process includes the steps to ensure compliance with regulatory requirements. The information display design conforms to the guidance offered in RG 1.47 for bypassed and inoperable status indication.

System Status Indication: The safety-related and nonsafety-related I&C systems are provided with system status information that meets the requirements of IEEE Std. 603, Section 5.8. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are displayed to the operator upon request. For safety-related systems, this information is available for each division. Certain information, key to plant operation and status monitoring, is permanently displayed on the large WDP in the MCR. Alarm and annunciation indications are also available in the MCR in accordance with system design requirements. Information available within a

division, including post-accident monitoring information, can be viewed on safety-related VDUs associated with that division. The same divisional information and nonsafety-related information can be viewed on the nonsafety-related VDUs and WDP.

Indication of Bypasses: For safety-related system protection functions, bypass status is continuously displayed to the operator.

Locations of Displays: Displays in the MCR are either on the main control console or on the large WDP visible and accessible to the operator. The man-machine interface system design includes design requirements and specifications for the classification of locations of displays in the MCR. More detailed descriptions of requirements for the locations of displays are included in Chapter 18.

7.1.6.6.1.10 Control of Access (IEEE Std. 603, Section 5.9)

Administrative control is used to implement access control to vital areas of the plant, including the MCR. Physical security and electronic security devices are provided to ensure only authorized and qualified plant personnel are allowed to have access to the Q-DCIS cabinets and consoles. Physical security is described in Section 13.6. In addition to the plant physical security, the Q-DCIS equipment has its own access control devices. Q-DCIS cabinets have doors with keylocks and position switches. Q-DCIS components within the cabinets have keylock switches that are used to control access to special functions (such as, the inoperable/operable switch).

Keys, passwords, and other security devices (following the guidance of RG 1.152) are used to control access to specific rooms; open specific equipment cabinets; obtain permission to access specific electronic instruments for calibration, testing, and setpoint changes; and, gain access to safety-related system software and data. Safety-related software is not routinely changed at the plant site.

Opening a Q-DCIS cabinet door produces an alarm in the MCR.

There is no control function access to safety-related system equipment and control through the network from nonsafety-related system equipment. Computer-related access controls and authorization are part of the cyber security program plan, which is described in the LTRs, "ESBWR Cyber Security Program Plan," NEDO-33295, (Non-Proprietary); and "ESBWR Cyber Security Program Plan," NEDE-33295-P, (Proprietary), (Reference 7.1-8).

7.1.6.6.1.11 Repair (IEEE Std. 603, Section 5.10)

The Q-DCIS systems provide timely recognition of location, replacement, repair, and adjustment of malfunctioning equipment. Periodic self-diagnostic functions locate the failure to the component level. Through individual division bypassing, the failed component is replaced or repaired on line without affecting the safety-related system protection function. During repairs the trip logic is two-out-of-three so that the single failure criterion is still met.

7.1.6.6.1.12 Identification (IEEE Std. 603, Section 5.11)

The Q-DCIS system equipment conforms to the identification requirements specified in IEEE Std. 603, Section 5.11. Color-coding is used as one of the major methods of identification. Safety-related equipment is distinctly marked in each redundant division of a safety-related system. Hardware component or equipment units have an identification label or nameplate. See Subsection 8.3.1.3 for additional details. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management formalizes system component and software identification.

IEEE Std. 7-4.3.2 has additional identification requirements related to SSC using software. Refer to LTRs “ESBWR - Software Management Program Manual” (Reference 7.1-12) and “ESBWR - Software Quality Assurance Program Manual” (Reference 7.1-10) for a description of the software plans that control the additional IEEE Std. 7-4.3.2 requirement for the identification and retrieval of software identification using software maintenance tools.

7.1.6.6.1.13 Auxiliary Features (IEEE Std. 603, Section 5.12)

Safety-related I&C system auxiliary supporting features conform to IEEE Std. 603, Section 5.12 where applicable and maintain the supported safety-related system performance at an acceptable level.

The Q-DCIS is supported by four divisions of safety-related uninterruptible power as described in Subsection 8.3.2. DC batteries supply power if there is a loss of off-site and on-site AC power.

HVAC, whether active or passive is a key auxiliary supporting system that maintains the necessary environmental conditions for both the safety-related and nonsafety-related I&C equipment. Under normal operating conditions when offsite power is available or when diesel generators are running, HVAC systems control the temperature and humidity of I&C equipment. Under a loss of power condition, including SBO, batteries provide continuous safety-related I&C operation for 72 hours, and continued operation of the nonsafety-related I&C equipment for two hours. However, during a loss of power condition, active HVAC is not available to the safety-related CB or RB equipment, except in the CRHA as noted below.

The Q-DCIS and its safety-related battery-operated support equipment remain powered and the heat generated is removed passively (except by small chassis mounted fans); the Q-DCIS and support equipment is qualified to the worst case anticipated temperature rise. Battery-backed N-DCIS equipment is only powered for two hours if offsite and diesel generator power is lost; during that interval the batteries supplying the N-DCIS also power nonsafety-related HVAC in the CRHA. If the nonsafety-related redundant HVAC is not available, safety-related temperature sensors with two-out-of-four logic trip the control room power that feeds pre-defined components of the nonsafety-related I&C and other pre-defined nonsafety-related heat loads. The safety-related I&C that remains operable is qualified for the resulting temperature rise with passive heat removal. This scheme protects the equipment and maximizes operator comfort. Additional description of the

HVAC design, including the use of room coolers powered by the ancillary diesel generators is included in Subsection 9.4.1 and Appendix 19A.

7.1.6.6.1.14 Multi-Unit Stations (IEEE Std. 603, Section 5.13)

The multi-unit station criteria do not apply to the standard single unit plant design submitted for NRC certification.

7.1.6.6.1.15 Human Factors Considerations (IEEE Std. 603, Section 5.14)

The I&C system design includes a HFE design process that is consistent with the requirements outlined in NUREG-0711, “Human Factors Engineering Program Review Model.” The HFE process defines a comprehensive, iterative design approach for the development of a human-centered control and information infrastructure and is described in Chapter 18.

7.1.6.6.1.16 Reliability (IEEE Std. 603, Section 5.15)

The degree of redundancy, diversity, testability, and quality of the safety-related I&C design achieves the necessary functional reliability. Safety-related equipment is provided under GEH's 10 CFR 50 Appendix B Quality Assurance Program. The BTP HICB-14 and IEEE 7-4.3.2 (as endorsed by RG 1.152) guidance followed for software development processes achieves reliable software design and implementation. The Design Reliability Assurance Program (D-RAP) described in Section 17.4 confirms that any quantitative or qualitative reliability goals established for the protection systems have been met. To achieve defense against common mode failure, the design includes defense-in-depth and diversity measures including the incorporation of the DPS described in Section 7.8. Reference 7.1-4 provides specific information on the redundancy and diversity used in safety-related I&C systems. The Q-DCIS is included in the consideration of the probabilistic risk assessment (PRA). (Refer to Chapter 19.)

7.1.6.6.1.17 Automatic Control (IEEE Std. 603, Sections 6.1 and 7.1)

The ESBWR automatic protection actions are implemented through two-out-of-four voting logic whenever one or more process variables reach their actuation setpoint. Variables are monitored and measured by each of the RTIF - NMS, SSLC/ESF, and ICP divisions.

Plant-specific setpoint analyses determine the protection systems' instrument setpoints using the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that the combination of characteristics of the instruments such as range, accuracy and resolution provide the required high probability that the analytical limits in Chapter 15 analyses are not exceeded for the safety-related control system components and systems of the safety-related I&C. The response times of the I&C systems are assumed in the safety-related analyses and verified by plant specific surveillance testing or system analyses. The Q-DCIS application software, hardware processing rates, and internal and external communication

system design ensures that the real-time performance of the safety-related control systems is deterministic.

7.1.6.6.1.18 Manual Control (IEEE Std. 603, Sections 6.2 and 7.2)

Each protective action can be manually initiated at the system level, in conformance to RG 1.62, and at the division level in conformance to IEEE Std. 603, Sections 6.2 and 7.2. The manual initiation satisfies divisional rules for independence and separation. Two manual actions, each in a separate division, are required in order to satisfy the two-out-of-two system logic or the two-out-of-four division logic that initiates a reactor trip in the RPS and ESF functions in the SSLC/ESF systems.

The operator can manually initiate the ESF and ICP functions by performing the appropriate action in two-out-of-four divisions; thus, satisfying the two-out-of-two system initiation logic. The ESF functions that use squib valves use a redundant two-step arm and fire sequence. This prevents single failures from firing or from inhibiting the firing of the squib valves. The squib valves are the GDCS pool injection valves, the suppression pool injection valves, the GDCS deluge valves, the ADS DPV, and the SLC injection valves. To manually initiate the GDCS short-term and long-term injection systems, a low-pressure signal must be present in the RPV. This prevents inadvertent manual initiation of the system during normal reactor operation.

The operator can manually initiate reactor emergency shutdown, reactor trip, with control rods by using any of three different methods using redundant or diverse controls. The manual reactor trip occurs independently of the automatic trip logic and sensor status.

The two manual scram switches, the Reactor Mode Switch, and the four divisional manual trip switches (per protective system) are located in the MCR and are easily accessible to the operator.

The two MCR manual scram switches, the RSS manual scram switches share no equipment with the automatic controls and require no software for their operation, and the DPS manual scram switches share a minimum of equipment with the automatic controls. The MCR and RSS manual scram switches are directly connected to the power feed for the load drivers that are, in turn, connected directly to the scram pilot valve solenoids. The DPS can manually scram by controlling both the HCU scram solenoid valves (by interrupting the current in the 120 VAC return from the solenoid) and the ARI scram air header dump valves.

After manual initiation, the protective actions go to completion in conformance to IEEE Std. 603, Section 5.2 as described in Subsection 7.1.6.6.1.3. The manual initiation of a protective action performs actions carried out by automatic initiation.

In the Q-DCIS design, protective actions are automatic. There are also no manual actions necessary to maintain safe conditions after the completion of protective actions for 72 hours after a DBE.

The manual controls are designed so that the information provided, display content and location are taken into consideration for operator access and action in the MCR. Further information about the design of manual controls and HFE considerations, as well as plant manual operation procedure requirements, are included in Chapter 18. Additionally, manual controls for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.19 Interaction Between the Sense and Command Features and Other Systems (IEEE Std. 603, Section 6.3)

The Q-DCIS protection systems are separate and independent from the nonsafety-related control systems, in accordance with GDC 24. Any failure of nonsafety-related systems does not affect safety-related protection systems or prevent them from performing their safety-related functions. If one safety-related division fails, any nonsafety-related control system can be isolated from the failure by using data validation techniques to select a valid control input from the three other remaining divisions. The communication path broadcasts one way - from the protection system to the N-DCIS. A failure of communication does not affect the protection function. Therefore, providing additional redundancy to isolate the protection system from communication failure is not required and not applied. For further detail on communication between the Q-DCIS and the N-DCIS (including transmission of time tagging signals) see Subsection 7.1.3.3.

Sensors used by safety-related I&C systems are not shared with nonsafety-related control systems. Calculated safety-related signals such as APRMs can be used, after isolation, by nonsafety-related control systems.

7.1.6.6.1.20 Derivation of System Inputs (IEEE Std. 603, Section 6.4)

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. An example of an indirect measurement is the loss of feedwater flow in the RPS scram logics. The loss of the feedwater flow variable is represented by the loss of the power generation bus signal. When the power to the feedwater pump motor is lost, the feedwater flow is also immediately lost. The use of loss of power generation bus signals to represent the loss of feedwater flow signal meets the requirements of the safety-related analysis of Chapter 15, because it is the only credible way that all feedwater flow can be lost. Additionally, derivation of system inputs for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.21 Capability for Testing and Calibration (IEEE Std. 603, Section 6.5)

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that have a known relationship with each other and that have read-outs available, or by introducing and varying a substitute input to the sensor of the same nature as the measured variable. The four-division

RTIF-NMS, SSLC/ESF, and independent control platform logic provides at least two valid divisions for crosschecking of monitored variables. The third division also has the capability to be available for crosschecking, depending on the maintenance bypass status. When one division is placed into maintenance bypass mode, the condition is indicated in the MCR and the division logic automatically becomes a two-out-of-three voting scheme. Most sensors and actuators are provisioned for actual testing and calibration during power operation with the exceptions described in Sections 7.2 through 7.8. See Subsections 7.1.3.3.5, 7.1.3.3.6, 7.1.3.3.7, and 7.1.3.5 for additional details.

In the Q-DCIS design a 24 month calibration periodicity is implemented to ensure accuracy and integrity of signal development, transmission and processing. Digital I&C equipment utilized in the I&C design is qualified for the environment in which it is located so that it retains its calibration during the post-accident time period. Additionally, capability for testing and calibration for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.22 Operating Bypasses (IEEE Std. 603, Sections 6.6 and 7.4)

Operating bypasses are implemented in the Q-DCIS. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. The requirements of IEEE Std. 603 are met by the safety-related I&C operating bypass design. Specific descriptions of safety-related system operating bypasses are included in Subsections 7.2.1.5 and 7.3.5.2. Operating bypasses are automatically removed as described in Subsections 7.2.1.5 and 7.3.5.2. Additionally, operating bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.23 Maintenance Bypass (IEEE Std. 603, Sections 6.7 and 7.5)

Maintenance bypass capability is incorporated in the design of the Q-DCIS. This permits equipment maintenance, testing, and repair of one individual division with the plant operating and without initiating any protection functions. The single failure criterion is met under this bypass condition. Although it is possible to bypass only one division at a time, the Q-DCIS design is able to supply its safety-related functions even with a two-division failure. Maintenance bypass is indicated in the MCR. Maintenance bypass for safety-related I&C systems is applied through a joystick bypass switch with exclusive logic that allows only one division, out of four, to be bypassed at any given time. Maintenance bypasses are initiated manually by the plant operator per administrative control. Additionally, maintenance bypasses for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.24 Setpoints (IEEE Std. 603, Section 6.8)

For automatic protective devices, safety-related setpoints and setpoints having significant safety functions for the Technical Specification requires limiting safety system settings are determined by

the methodology described in Reference 7.1-9. The GEH setpoint methodology uses plant-specific setpoint analyses to ensure that an instruments' range, accuracy, and resolution meet the performance requirements assumed in the safety-related analyses in Chapter 15 for the safety-related control system components and systems. This methodology meets the requirements of IEEE Std. 603, Section 6.8. The response times of the I&C systems assumed in the safety-related analyses are verified by plant specific surveillance testing or system analyses.

7.1.6.6.1.25 Electrical Power Sources (IEEE Std. 603, Section 8.1)

The Q-DCIS protection system cabinets and components are supported by two independent power sources. Each division of safety-related I&C is powered by two UPS that can supply 120 VAC from either offsite power, diesel generator power, or safety-related batteries (for 72 hours). Either of the two power sources allows Q-DCIS operation. These power sources comply with IEEE 603 as described in Subsection 7.1.6.6.1. See Subsection 7.1.3.3.7 for additional description. Descriptions of safety-related system power sources are included in Chapter 8.

7.1.6.6.1.26 Non-electrical Power Sources (IEEE Std. 603, Section 8.2)

If a non-electrical power source is required for a safety function, then the source of the power is classified as safety-related and complies with IEEE 603 as described in Subsection 7.1.6.6.1. Additionally, non-electrical power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.27 Maintenance Bypass (IEEE Std. 603, Section 8.3)

The Q-DCIS components are powered by redundant, independent, and separated uninterruptible power supplies appropriate to their division with battery backup (per division) for at least 72 hours. The UPS have a manual maintenance switch and either supply (per division) can operate its Q-DCIS division. Using the inverter's manual bypass and shutting down either the associated batteries, chargers or inverters technically makes the division inoperable but, in fact the division remains fully functional, losing only the ability to operate for 72 hours should offsite or diesel power be lost (it operates for approximately 36 hours under those circumstances). Operation of the Q-DCIS when one of its power supplies is in maintenance bypass is appropriately indicated. In the very unlikely event that an entire division is without power the failsafe RTIF-NMS platform interprets the condition as a trip (unless bypassed) and neither the SSLC/ESF platform nor the ICP assumes a trip. Because only two divisions are necessary to satisfy the safety requirements, no functionality is lost. The condition of a division without power triggers an alarm. Refer to the discussion of GDC 18 in Subsection 8.3.1.2.1 for maintenance provisions of safety-related power supplies. Further discussion of the safety-related power supplies is provided throughout Chapter 8.

A single non-electrical redundant power source (e.g., one of two parallel accumulators, one of two squibs) may be taken to “maintenance bypass” (i.e., isolated) without adversely impacting the safety function of any system.

For those non-electrical power sources having a degree of redundancy of one, taking it to maintenance bypass does not adversely impact the reliability of any safety-related system to perform its safety functions. Additionally, manual bypassing of power sources for each system are discussed in the Safety Evaluation section for each applicable system as part of conformance to 10 CFR 50.55 a(h).

7.1.6.6.1.28 Cyber Security (IEEE Std. 7-4.3.2)

The security measures included in RG 1.152 are evaluated and incorporated in the Q-DCIS design and include plant hardware and software security measures. The software development process plans are developed with the security measures.

The comprehensive ESBWR Cyber Security Program Plan (Reference 7.1-8) includes methods for identifying security risks and outlines appropriate procedures. The plant ensures that hardware, controls, and data networks comprising the control network cannot be disrupted, interrupted, or negatively affected by unauthorized users or external systems. Reference 7.1-8 documents the design commitments, which meet the applicable guidance of RG 1.152, Section C.2, and Positions 2.1 through 2.9.

Inspections, tests, analyses, and acceptance criteria (ITAAC) associated with the cyber security program plan are provided in Tier 1 together with the SDP.

7.1.7 COL Information

None.

7.1.8 References

7.1-1 (Deleted)

7.1-2 (Deleted)

7.1-3 (Deleted)

7.1-4 GE Hitachi Nuclear Energy, "ESBWR I&C Diversity and Defense-In-Depth Report." NEDO-33251, Class I (Non-proprietary), Revision3, September 2010.

7.1-5 (Deleted)

7.1-6 (Deleted)

7.1-7 (Deleted)

7.1-8 GE Hitachi Nuclear Energy, "ESBWR Cyber Security Program Plan," NEDE-33295P, Class III (Proprietary), Revision 2, September 2010, and NEDO-33295, Class I (Non-Proprietary), Revision 2, September 2010.

7.1-9 GE Hitachi Nuclear Energy, "GEH ESBWR Setpoint Methodology," NEDE-33304P, Class III (Proprietary), Revision 4, May 2010, and NEDO-33304, Class II (Non-proprietary), Revision 4, May 2010.

7.1-10 GE Hitachi Nuclear Energy, "ESBWR - Software Quality Assurance Program Manual," NEDE-33245P, Class III (Proprietary), Revision 5, February 2010, and NEDO-33245, Class I (Non-Proprietary), Revision 5, February 2010.

7.1-11 (Deleted)

7.1-12 GE Hitachi Nuclear Energy, "ESBWR - Software Management Program Manual," NEDE-33226P, Class III (Proprietary), Revision 5, February 2010, and NEDO-33226, Class I (Non-proprietary), Revision 5, February 2010.

7.1-13 (Deleted)

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 1 of 10)

	Q-DCIS																					N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																		
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
10 CFR																									
50.34(f)(1)(v) [II.K.3.13]								X				X	X	X											
50.34(f)(1)(x) [II.K.3.28]												X													
50.34(f)(2)(iii) [I.D.1]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.34(f)(2)(iv) [I.D.2]																						X			
50.34(f)(2)(v) [I.D.3]	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				X
50.34(f)(2)(viii) [II.B.3]								X			X														
50.34(f)(2)(x) [II.D.1]								X			X														
50.34(f)(2)(xi) [II.D.3]								X				X													
50.34(f)(2)(xiv) [II.E.4.2]	X		X					X	X																
50.34(f)(2)(xv) [II.E.4.4]								X	X															X	

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 2 of 10)

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM)(6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4)(6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
50.34(f)(2)(xvii) [II.F.1]								X		X	X													X
50.34(f)(2)(xviii) [II.F.2]								X				X												X
50.34(f)(2)(xix) [II.F.3]								X		X	X	X												X
50.34(f)(2)(xxi) [II.K.1.22]	X	X						X						X							X			
50.34(f)(2)(xxiii) [II.K.2.10]		X						X						X										
50.34(f)(2)(xxiv) [II.K.3.23]																								X
50.34(f)(2)(xxvii) [III.D.3.3]								X		X	X													X
50.34(f)(2)(xxviii) [III.D.3.4]								X		X						X								
50.43(e)(11)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
50.44(c)(4)								X			X													
50.49	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 3 of 10)

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
50.55a(a)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
50.55a(h)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
50.62							X	X											X				X	X	X	
50.63	X	X	X			X		X	X				X	X		X									
52.47(a)(21)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(b)(1)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(a)(25)	N/A																									
52.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
52.47(c)(2)(11)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
GENERAL DESIGN CRITERIA																										
1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 4 of 10)

	Q-DCIS																					N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform				Network Segments			
	RTIF						NMS																		
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
10	X	X					X																		
12	X	X					X															X			
13	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
15	X		X					X	X			X													
16	X		X					X	X									X			X				
19	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
20	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
21	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
23	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
24	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 5 of 10)

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform				Network Segments			
	RTIF						NMS																		
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
25	X	X					X														X			
26	X	X				X	X												X		X			
27	X	X				X	X												X		X			
28																	X				X			
29	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X			
30								X	X			X													
33								X				X	X	X							X		X		
34								X						X							X				
35								X				X	X	X	X				X		X				
37								X				X	X	X	X				X		X				
38																						X			
41								X			X												X		

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 6 of 10)

	Q-DCIS																					N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																		
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
42																								X	
43								X			X													X	
44														X											
63								X																	X
64								X		X	X														X
Staff Requirements Memoranda on SECY 93-087																									
II.Q	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
II.T								X														X			X
Regulatory Guides (RG)																									
1.22	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.45								X	X	X	X														
1.47	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 7 of 10)

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
1.53	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.62	X	X	X					X	X			X	X	X		X		X	X	X	X				
1.75	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.89	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																								
1.97(10)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.100	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																								
1.105	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.118	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.151 (8)		X		X	X	X			X		X	X	X	X	X				X	X			X	X	
1.152(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.153	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.168(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 8 of 10)

	Q-DCIS																				N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform									Independent Control Platform				Network Segments			
	RTIF						NMS																	
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
1.169(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.170(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.171(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.172(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.173(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
1.180(9)	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
1.204	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
1.209	Refer to Table 3.11-1 (Electrical and Mechanical Equipment for Environmental Qualification)																							
Branch Technical Positions (BTP)																								
BTP HICB-3	N/A																							
BTP HICB-6	N/A																							
BTP HICB-8	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 9 of 10)

	Q-DCIS																					N-DCIS			
	RTIF - NMS Platform							SSLC/ESF Platform										Independent Control Platform				Network Segments			
	RTIF						NMS																		
Applicable Criteria Guidelines: SRP NUREG-0800, Section 7.1	RTIF	RPS	LD&IS (MSIV Only)(6)	CMS (includes SPTM) (6)	NBS(6)	CRD(6)	NMS	SSLC/ESF(3)	LD&IS (non-MSIV)(1)(6)	PRMS	CMS(6)	NBS (includes ADS)(6)	GDCS	ICS	SLC(6)	CBVS(2)	CRD(5)(6)	VBIF	ATWS/SLC(4) (6)	HP CRD Isolation Bypass Function	ICS DPV Isolation Function	GENE	PIP A/B	BOP	PCF
BTP HICB-9	X	X				X																			
BTP HICB-10(10)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-12	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-13	N/A																								
BTP HICB-14(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-16	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
BTP HICB-17(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				
BTP HICB-18(7)	X	X					X	X										X	X	X	X				
BTP HICB-19(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	
BTP HICB-21(7)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X				

Table 7.1-1 I&C Regulatory Requirements Applicability Matrix (Sheet 10 of 10)

Notes:

1. LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.
2. CBVS includes the CRHS and Control Room Habitability Area HVAC Subsystem (CRHAVS) and EFUs.
3. SSLC/ESF includes RSS, MCRP and safety-related VDUs.
4. Includes the NBS sensors associated with ATWS/SLC.
5. SSLC/ESF platform column for CRD includes safety-related sensors associated with control rod separation detection.
6. The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to Sections 7.2, 7.3, 7.4, and 7.5 for detailed descriptions of the system functions.
7. These criteria are addressed with digital computer-related functions of the Q-DCIS and N-DCIS.
8. Sections of the ISA standard that are not specific to safety-related systems, but provide guidance on design practices for tubing, vents and drains apply to the systems associated with the N-DCIS network segments.
9. Hardware associated with the N-DCIS network segments uses industrial methods for EMI/EMF/RFI/EMC compliance.
10. The ESBWR I&C conforms to RG 1.97 and applies the guidance in IEEE std. 497. RG 1.97 endorses IEEE Std. 497 (with clarifications and exceptions stated in RG 1.97) and the use of the HFE development process to determine the human actions during and following accident scenarios. Specific instruments credited for RG 1.97 compliance are determined as part of the HFE development process as discussed in Section 7.5.
11. The use of other innovative means as described in 10 CFR 52.47(c)(2) in the design of the three Q-DCIS platforms (RTIF-NMS, SSCL/ESF and ICP) may occur as part of the development process. If it does, then the software projects executed per the software development process described in Appendix 7B will conform to the requirements of 10 CFR 50.43(e).

Table 7.1-2 I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference (Sheet 1 of 5)

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM			
		RTIF						NMS													
IEEE Std. 603 Section	Functions [1]	RTIF	RPS	LD&IS (MSIV Only) [6]	CMS (includes SPTM) [6]	NBS [6]	CRD [6]	NMS [3]	SSLC/ESF [4]	LD&IS (Non-MSIV) [2],[6]	PRMS	CMS [6]	NBS (includes ADS) [6]	GDCS	ICS	SLC [6]	CBVS [7]	CRD [6]	VBIF	ATWS / SLC [5],[6],[7]	HP CRD Isolation Bypass Function	ICS DPV Isolation Function
4.1	Design basis events	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.2	Safety-related functions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1 7.5.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.3	Permissive conditions for operating bypasses	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.4	Monitored variables, and associated analytical limits	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.5	Minimum criteria for manual actions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.6	Spatially dependent variables	7.1.6.6.1.1	7.1.6.6.1.1 7.2.1.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.2.3.3.1	7.1.6.6.1.1 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.2.2.3.1	7.1.6.6.1.1 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.1 7.3.3.3.1	7.1.6.6.1.1 7.5.3.3.1	7.1.6.6.1.1 7.5.2.3.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.1.2.3.1	7.1.6.6.1.1 7.4.4.3.1	7.1.6.6.1.1 7.4.1.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1 7.3.6.3.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.7	Range of transient and steady-state conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.8	Adverse environmental conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.9	Reliability methods	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.10	Abnormal Event critical times / conditions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
4.11	Equipment protective provisions	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1

Table 7.1-2 I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference (Sheet 2 of 5)

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM			
		RTIF						NMS													
IEEE Std. 603 Section	Functions [1]	RTIF	RPS	LD&IS (MSIV Only) [6]	CMS (includes SPTM) [6]	NBS [6]	CRD [6]	NMS [3]	SSLC/ESF [4]	LD&IS (Non-MSIV) [2],[6]	PRMS	CMS [6]	NBS (includes ADS) [6]	GDCS	ICS	SLC [6]	CBVS [7]	CRD [6]	VBIF	ATWS / SLC [5],[6],[7]	HP CRD Isolation Bypass Function	ICS DPV Isolation Function
4.12	Special design basis	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1	7.1.6.6.1.1
5.1	Single failure criterion	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2	7.1.6.6.1.2
5.2	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3
5.3	Quality	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4	7.1.6.6.1.4
5.4	Equipment qualification	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5	7.1.6.6.1.5
5.5	System Integrity	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6	7.1.6.6.1.6
5.6	Independence	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7	7.1.6.6.1.7
5.7	Capability for test and calibration	7.1.6.6.1.8	7.1.6.6.1.8 7.2.1.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.2.3.3.1	7.1.6.6.1.8 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.2.2.3.1	7.1.6.6.1.8 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.8 7.3.3.3.1	7.1.6.6.1.8 7.5.3.3.1	7.1.6.6.1.8 7.5.2.3.1	7.1.6.6.1.8	7.1.6.6.1.8 7.3.1.2.3.1	7.1.6.6.1.8 7.4.4.3.1	7.1.6.6.1.8 7.4.1.3.1	7.1.6.6.1.8	7.1.6.6.1.8	7.1.6.6.1.8 7.3.6.3.1	7.1.6.6.1.8	7.1.6.6.1.8	7.1.6.6.1.8 7.3.7.4
5.8	Information displays	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9	7.1.6.6.1.9
5.9	Control of Access	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10	7.1.6.6.1.10
5.10.	Repair	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11	7.1.6.6.1.11
5.11	Identification	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12	7.1.6.6.1.12
5.12	Auxiliary features	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13	7.1.6.6.1.13
5.13	Multi-unit stations	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14	7.1.6.6.1.14
5.14	Human factors considerations	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15	7.1.6.6.1.15
5.15	Reliability	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16	7.1.6.6.1.16

Table 7.1-2 I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference (Sheet 3 of 5)

		Q-DCIS																				
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM			
		RTIF						NMS														
IEEE Std. 603 Section	Functions [1]	RTIF	RPS	LD&IS (MSIV Only) [6]	CMS (includes SPTM) [6]	NBS [6]	CRD [6]	NMS [3]	SSLC/ESF [4]	LD&IS (Non-MSIV) [2],[6]	PRMS	CMS [6]	NBS (includes ADS) [6]	GDCS	ICS	SLC [6]	CBVS [7]	CRD [6]	VBIF	ATWS / SLC [5],[6],[7]	HP CRD Isolation Bypass Function	ICS DPV Isolation Function
6.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17
6.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.7.3.1
6.3	Interaction between the sense and command features and other systems	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19	7.1.6.6.1.19
6.4	Derivation of system inputs	7.1.6.6.1.20	7.1.6.6.1.20 7.2.1.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.2.2.3.1	7.1.6.6.1.20 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.2.2.3.1	7.1.6.6.1.20 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.20 7.3.3.3.1	7.1.6.6.1.20 7.5.3.3.1	7.1.6.6.1.20 7.5.2.3.1	7.1.6.6.1.20	7.1.6.6.1.20 7.3.1.2.3.1	7.1.6.6.1.20 7.4.4.3.1	7.1.6.6.1.20 7.4.1.3.1	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20 7.3.6.3.1	7.1.6.6.1.20	7.1.6.6.1.20	7.1.6.6.1.20 7.3.7.3.1
6.5	Capability for testing and calibration	7.1.6.6.1.21	7.1.6.6.1.21 7.2.1.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.2.2.3.1	7.1.6.6.1.21 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.2.2.3.1	7.1.6.6.1.21 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.21 7.3.3.3.1	7.1.6.6.1.21 7.5.3.3.1	7.1.6.6.1.21 7.5.2.3.1	7.1.6.6.1.21	7.1.6.6.1.21 7.3.1.2.3.1	7.1.6.6.1.21 7.4.4.3.1	7.1.6.6.1.21 7.4.1.3.1	7.1.6.6.1.21	7.1.6.6.1.21	7.1.6.6.1.21 7.3.6.3.1	7.1.6.6.1.21	7.1.6.6.1.21	7.1.6.6.1.21 7.3.7.3.1
6.6	Operating bypasses	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.7.3.1
6.7	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.7.3.1
6.8	Setpoints	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24	7.1.6.6.1.24
7.1	Automatic Control	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17	7.1.6.6.1.17

Table 7.1-2 I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference (Sheet 4 of 5)

		Q-DCIS																			
		RTIF - NMS PLATFORM							SSLC/ESF PLATFORM										INDEPENDENT CONTROL PLATFORM			
		RTIF						NMS													
IEEE Std. 603 Section	Functions [1]	RTIF	RPS	LD&IS (MSIV Only) [6]	CMS (includes SPTM) [6]	NBS [6]	CRD [6]	NMS [3]	SSLC/ESF [4]	LD&IS (Non-MSIV) [2],[6]	PRMS	CMS [6]	NBS (includes ADS) [6]	GDCS	ICS	SLC [6]	CBVS [7]	CRD [6]	VBIF	ATWS / SLC [5],[6],[7]	HP CRD Isolation Bypass Function	ICS DPV Isolation Function
7.2	Manual control	7.1.6.6.1.18	7.1.6.6.1.18 7.2.1.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.2.3.3.1	7.1.6.6.1.18 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.2.2.3.1	7.1.6.6.1.18 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.18 7.3.3.3.1	7.1.6.6.1.18 7.5.3.3.1	7.1.6.6.1.18 7.5.2.3.1	7.1.6.6.1.18	7.1.6.6.1.18 7.3.1.2.3.1	7.1.6.6.1.18 7.4.4.3.1	7.1.6.6.1.18 7.4.1.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.6.3.1	7.1.6.6.1.18	7.1.6.6.1.18	7.1.6.6.1.18 7.3.7.3.1
7.3	Completion of protective action	7.1.6.6.1.3	7.1.6.6.1.3 7.2.1.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.2.3.3.1	7.1.6.6.1.3 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.2.2.3.1	7.1.6.6.1.3 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.3 7.3.3.3.1	7.1.6.6.1.3 7.5.3.3.1	7.1.6.6.1.3 7.5.2.3.1	7.1.6.6.1.3	7.1.6.6.1.3 7.3.1.2.3.1	7.1.6.6.1.3 7.4.4.3.1	7.1.6.6.1.3 7.4.1.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.6.3.1	7.1.6.6.1.3	7.1.6.6.1.3	7.1.6.6.1.3 7.3.7.3.1
7.4	Operating bypass	7.1.6.6.1.22	7.1.6.6.1.22 7.2.1.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.2.3.3.1	7.1.6.6.1.22 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.2.2.3.1	7.1.6.6.1.22 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.22 7.3.3.3.1	7.1.6.6.1.22 7.5.3.3.1	7.1.6.6.1.22 7.5.2.3.1	7.1.6.6.1.22	7.1.6.6.1.22 7.3.1.2.3.1	7.1.6.6.1.22 7.4.4.3.1	7.1.6.6.1.22 7.4.1.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.6.3.1	7.1.6.6.1.22	7.1.6.6.1.22	7.1.6.6.1.22 7.3.7.3.1
7.5	Maintenance bypass	7.1.6.6.1.23	7.1.6.6.1.23 7.2.1.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.2.3.3.1	7.1.6.6.1.23 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.2.2.3.1	7.1.6.6.1.23 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.23 7.3.3.3.1	7.1.6.6.1.23 7.5.3.3.1	7.1.6.6.1.23 7.5.2.3.1	7.1.6.6.1.23	7.1.6.6.1.23 7.3.1.2.3.1	7.1.6.6.1.23 7.4.4.3.1	7.1.6.6.1.23 7.4.1.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.6.3.1	7.1.6.6.1.23	7.1.6.6.1.23	7.1.6.6.1.23 7.3.7.3.1
8.1	Electrical power sources	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25	7.1.6.6.1.25
8.2	Non-electrical power sources	7.1.6.6.1.26	7.1.6.6.1.26 7.2.1.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.2.3.3.1	7.1.6.6.1.26 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.2.2.3.1	7.1.6.6.1.26 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.26 7.3.3.3.1	7.1.6.6.1.26 7.5.3.3.1	7.1.6.6.1.26 7.5.2.3.1	7.1.6.6.1.26	7.1.6.6.1.26 7.3.1.2.3.1	7.1.6.6.1.26 7.4.4.3.1	7.1.6.6.1.26 7.4.1.3.1	7.1.6.6.1.26	7.1.6.6.1.26	7.1.6.6.1.26 7.3.6.3.1	7.1.6.6.1.26	7.1.6.6.1.26	7.1.6.6.1.26 7.3.7.3.1
8.3	Maintenance Bypass	7.1.6.6.1.27	7.1.6.6.1.27 7.2.1.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.2.3.3.1	7.1.6.6.1.27 7.2.1.3.1 7.3.1.2.3.1 7.3.3.3.1 7.3.5.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.2.2.3.1	7.1.6.6.1.27 7.3.5.3.1 7.4.2.3.1	7.1.6.6.1.27 7.3.3.3.1	7.1.6.6.1.27 7.5.3.3.1	7.1.6.6.1.27 7.5.2.3.1	7.1.6.6.1.27	7.1.6.6.1.27 7.3.1.2.3.1	7.1.6.6.1.27 7.4.4.3.1	7.1.6.6.1.27 7.4.1.3.1	7.1.6.6.1.27	7.1.6.6.1.27	7.1.6.6.1.27 7.3.6.3.1	7.1.6.6.1.27	7.1.6.6.1.27	7.1.6.6.1.27 7.3.7.3.1

Table 7.1-2 I&C Systems - IEEE Std. 603 Criteria Compliance Cross-Reference (Sheet 5 of 5)

Notes:

1. The IEEE Std. 603 criteria apply to the safety-related portions of the systems identified in this table.
2. LD&IS (non-MSIV) controls the safety-related actuators (for the isolation valves and dampers) associated with the following nonsafety-related systems: RWCU/SDC, FAPCS, EFDS, CIS, CWS, CMS, HPNSS, RBVS, and FBVS. RWCU/SDC provides safety-related sensor inputs to LD&IS (non-MSIV). The regulatory requirements associated with these actuators and sensors are addressed as part of LD&IS.
3. NMS has Q and N parts. The Q parts are SRNM, LPRM, APRM, and OPRM. The N parts are AFIP and MRBM.
4. SSLC/ESF includes the RSS, MCRP, and safety-related VDUs.
5. Includes the NBS sensors associate with ATWS/SLC.
6. The following safety-related systems have logic implemented on multiple platforms in support of their protective functions: CMS, CRD, LD&IS, NBS and SLC. Refer to Section 7.2, Section 7.3, Section 7.4, and Section 7.5 for detailed descriptions of the system functions.
7. CBVS includes the CRHS and CRHAVS subsystems and EFUs.

Figure 7.1-1 SBWR DCIS Simplified Network and Functional Diagram