

7.0 Instrumentation and Controls

7.1 Introduction

Chapter 7 describes the instrumentation and controls (I&C) for the U.S. EPR systems. The description of the I&C systems includes system classifications, functional requirements and assignment, and system architecture. The information provided emphasizes those instruments and associated equipment that constitutes the safety systems as defined in IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-1998) (Reference 1), which meets or exceeds the requirements of IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-1991) (Reference 2).

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

This section describes the systems that comprise the U.S. EPR I&C architecture and the design features associated with these systems.

Figure 7.1-1—Chapter 7 Figure Legend is provided to illustrate the symbols used in the figures provided in this chapter.

Definitions

The terminology used in this chapter reflects those used in IEEE Std 603-1998 (Reference 1):

Actuated Equipment – the assembly of prime movers and driven equipment used to accomplish a protective function, such as solenoids, shutdown rods, and valves.

Actuation Device – a component or assembly of components that directly controls the motive power for actuated equipment.

Application Software – software that is developed using a set of engineering tools associated with a generic I&C platform and is specific to a particular set of functional requirements.

Beyond Design Basis Event (BDBE) – postulated event that are excluded from the deterministic design basis based on their low probability of occurrence. BDBEs are considered in the design of the plant based on specific regulatory requirements or guidance, or based on results from the probabilistic risk assessment.

Communication Module – A device that is used to transmit digital information from one device to another over one or several data communication links using a predetermined protocol.

Channel – an arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

Class 1E – the safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

Component Level – actuation or control of a single actuation device (component).

Credited - designation for a system that can perform a safety function, and is qualified and relied upon to do so.

Data Communication – a method of sharing information between devices that involves a set of rules, formats, encodings, specifications, and conventions for transmitting data over a communication path, known as a protocol.

Division – the designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

Design Basis Event (DBE) – postulated events used in the design to establish the acceptable requirements for the structures, systems, and components.

Function Processor – a device that contains hardware, system software, and application software that executes instrumentation and control functions.

Functional Unit – a set of assembled components within a system that perform specific functions to support overall system operation.

I&C Platform – a generic set of system hardware, system software, and engineering tools that can be configuration for a wide variety of instrumentation and control functions.

Hardwired I&C – operator controls and indicators that are connected with other I&C equipment using an analog signal path. This includes devices such as buttons, switches, analog indicators, or standalone digital indicators.

Hardwired Signal – a signal that does not use a data communications protocol.

Input/Output (I/O) Module – a module that converts signals from a hardwired to digital form (or vice versa).

Non-Credited – designation for a system that can perform a safety function, but is not qualified or relied upon to do so.

Optical link module – a device that converts an electrical signal to an optical signal.

Protective action – the initiation of a signal within the sense and command features or the operation of equipment within the execute features for the purpose of accomplishing a safety function.

Protection system – That part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features.

Safety function – one of the processes or conditions (e.g., emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a DBE.

Safety system – a system that is relied upon to remain functional during and following design events to maintain: (A) the integrity of the reactor coolant pressure boundary (RCPB), (B) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (C) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

Sensor – the portion of a channel that responds to changes in a plant variable or condition and converts the measured process variable into an electrical, optical or pneumatic signal.

System level – actuation or control of a sufficient number of components to achieve a desired function.

System Hardware – hardware associated with a generic I&C platform, including function processors, I/O modules, communication modules, subracks and other hardware devices associated with a generic I&C platform.

System software – refers to relevant software including an operating system, firmware, and runtime software that is integrated to form a generic I&C platform.

7.1.1 U.S. EPR I&C Architecture

7.1.1.1 Overview

The U.S. EPR implements a modern digital I&C design based on experience gained internationally from new plant designs and retrofits from existing plants with digital I&C equipment. The U.S. EPR I&C architecture implements these design features to optimize overall plant safety:

- Use of digital technology:

The I&C design maximizes the use of digital I&C platforms. Many features of digital I&C provide overall improvements in plant safety. These features include continuous online self-testing and diagnostics that allow early detection of failures and improved human-machine interfaces (HMI) using video display units that provide an integrated view of process systems status to the operators.

- Robust I&C architecture design:

The I&C architecture implements several design principles such as defense-in-depth, diversity, redundancy, independence and priority to optimize plant safety. These principles are applied so that the impact of failures is minimized and the required safety functions are executed when required.

- Automation of plant operation:

A high degree of automation is implemented to improve plant operation, reduce operator burden, and improve situational awareness during normal and accident conditions. For DBEs, safety functions required during the first 30 minutes are automated.

- State of the art design for human factors:

The I&C systems design is integrated with the human factors engineering (HFE) principles addressed in Chapter 18 for improved human reliability and overall plant safety.

The U.S. EPR I&C architecture is represented in Figure 7.1-2—U.S. EPR I&C Architecture. The overall I&C architecture is categorized into four levels:

- Level 3: business management systems – These consist of plant information management systems. Other than interfaces provided from Level 2, these systems are not within the scope of this document and are not shown on Figure 7.1-2.
- Level 2: unit supervision and control – These I&C systems are provided as an interface between the operator and the automation systems. Typical functions include monitoring plant processes and manual control of plant components.
- Level 1: system automation - These I&C systems acquire and process sensor information to perform automatic system control functions and transmit information for display to the operator. These systems also process manual commands to operate plant equipment.
- Level 0: process interface - These I&C systems act as the coupling between the physical process and the I&C systems. They include sensing components, actuation devices, and actuated equipment such as pressure sensors, thermocouples, switchgear, pumps and valves.

7.1.1.2 Use of TELEPERM XS in the U.S. EPR

TELEPERM XS (TXS) is a digital I&C platform that has been specifically designed and qualified for use in nuclear safety-related applications.

7.1.1.2.1 TXS Platform Design

The TXS platform is described in the Reactor Protection System Topical Report (EMF-2110(NP)(A) (Reference 3). Because of advances in technology and rapid obsolescence of components, the various modules described in EMF-2110(NP)(A)

(Reference 3) will be modified and upgraded over time, and new modules will be developed. However, the principles and methods described in EMF-2110(NP)(A) (Reference 3) and summarized below apply to the application of the TXS platform for the U.S. EPR.

- Platform design using four building blocks, which include:
 - System hardware.
 - System software.
 - Application software.
 - Engineering tools to configure the application.
- System hardware, system software, and engineering tools development processes that meet the quality requirements of 10 CFR 50.55a(a)(1) and GDC 1. This includes software verification and validation (V&V) methods.
- Processing principles that provide for system integrity, which include:
 - Real-time, static operating system.
 - Cyclic processing.
 - Interference free communications.
 - Self monitoring and diagnostics.
 - Fail-safe design.
- Control of access principles, including service unit (SU) maintenance interfaces.

The TXS product family also extends to other modules and components outside of those described in EMF-2110(NP)(A) (Reference 3). Examples include the priority module described in AV42 Topical Report (ANP-10273P) (Reference 4), and the qualified display system (QDS). The QDS is a video display unit designed for use in nuclear safety-related applications. Modules and components that are developed for use in I&C systems design shall be consistent with the requirements described in this chapter.

7.1.1.2.2 Application of the TXS Platform

TELEPERM XS Software Topical Report (ANP-10272) (Reference 5) describes the lifecycle processes for application software development used in safety-related applications of the TXS platform for the U.S. EPR, as well as software V&V processes. These phases are listed below along with the primary documentation generated at the end of each phase:

- Basic design phase;

- Functional requirements specification.
- Software requirement specification.
- Hardware requirement specification.
- Concept activity V&V summary report.
- Requirements activity V&V summary report.
- Detailed design phase;
 - Software design description.
 - Cabinet design and layout.
 - Code generation and documentation.
 - Software test plan.
 - Software test report.
 - Design activity V&V summary report.
 - Implementation activity V&V summary report.
- Manufacturing Phase.
- Testing Phase;
 - Factory acceptance test plan.
 - Factory acceptance test report.
 - Test activity V&V summary report.
- Installation and Commissioning Phases;
 - Site acceptance test plan.
 - Site acceptance test report.
 - Installation and checkout activity V&V summary report if required for any changes following testing phase.

7.1.1.3 Level 2 - Unit Supervision and Control

7.1.1.3.1 Safety Information and Control System

The safety information and control system (SICS) is provided as a safety-related HMI. The process information and control system (PICS) is normally used by the operator to

monitor and control process systems, and the SICS is used in the unlikely event that the PICS is not available. The SICS provides control and monitoring capabilities in both the main control room (MCR) and remote shutdown station (RSS).

This section describes the SICS with regards to I&C design. Details such as screen displays, levels of automation, and panel layout are designed using the HFE principles described in Chapter 18.

Classification

The SICS is classified as safety-related.

Functions

The functions of the SICS are specified for the MCR or the RSS.

The SICS performs these safety-related functions:

- Manual actuation of reactor trip (MCR and RSS).
- Manual actuation and control of engineered safety features (ESF) systems for accident mitigation (MCR).
- Manual control of systems to achieve and maintain safe shutdown (MCR and RSS).
- Display of Type A through Type C post-accident monitoring (PAM) variables (MCR).

The SICS performs these non-safety-related functions:

- Monitoring and control of essential non-safety-related systems to achieve and maintain hot-standby on a loss of PICS (MCR).
- Monitoring and control of systems to mitigate severe accidents (MCR).
- Backup safety parameter display system (SPDS) functions (MCR).
- Display high priority alarms (MCR).

Architecture

The SICS consists of safety-related portion and a non-safety-related portion to perform its functions.

Safety-Related Portion of SICS

Figure 7.1–3—Safety Information and Control System Architecture (Safety-Related Portion) provides a functional representation of the safety-related portion of the SICS.

The safety-related portion of the SICS is organized into four independent divisions located in separate Safeguards Buildings. HMI equipment is located in the MCR and RSS, and is physically separated.

The safety-related portion of the SICS consists of these functional units:

- Panel interfaces (PI)
- Qualified display systems (QDS).
- Service units.

PIs perform data processing functions and are provided to interface between the various level 1 systems and the HMI devices in the MCR or RSS. Control PIs process manual commands initiated from the HMI devices and information related to actuator status for display. Monitoring PIs only transfer information to the HMI devices for display to the operator. Hardwired connections to non-safety-related I&C systems may be used as required by the SICS human factors design and are isolated as described in Section 7.1.1.6.4.

Control QDSs provide the capability to initiate manual commands and display actuator-related information. Monitoring QDSs only provide information to the operator. The number and physical arrangement of QDSs provided in the MCR and RSS are determined based on functional and human factors requirements.

Hardwired I&C is used to provide information to the operator and provide the ability to actuate and control plant equipment. Hardwired I&C is connected to the PIs, various level 1 I&C systems, and the reactor trip devices.

Section 7.2 and Section 7.3 describe the methods used for manual actuation of reactor trip and engineered safety features. For other manual controls, the human factors principles described in Chapter 18 shall be used to select the type of HMI used.

SUs are provided for configuration and maintenance of the SICS. The PIs are serviced by the SUs of the SAS via the monitoring and service interface (MSI) of the SAS. The QDSs have dedicated SUs that are only connected to the QDS. The number and location of SUs is determined based on the number and layout of QDSs.

Non-Safety-Related Portion of SICS

Figure 7.1–4—Safety Information and Control System Architecture (Non-Safety-Related Portion) provides a functional representation of the non-safety-related portion of the SICS.

These functional units are implemented in the non-safety-related portion of the SICS:

- Gateways (GW).
- Qualified display systems (QDS).
- Service units.

GWs are provided to interface to the plant data network.

QDSs provided in divisions 2 and 3 to monitor and control other non-safety-related I&C systems via GWs on a loss of PICS.

QDSs are provided in divisions 1 and 4 to monitor and control equipment dedicated to mitigate severe accidents. These QDS utilize point to point data connections to transmit and receive information to the severe accident I&C (SA I&C).

The QDSs have dedicated SUs that are only connected to the QDS. The number and location of SUs is determined based on the number and layout of QDSs.

Hardwired I&C is also provided to monitor and control non-safety-related I&C systems. The human factors principles described in Chapter 18 are used to select the type of HMI used.

Equipment

The SICS is implemented with the TXS digital I&C platform and hardwired I&C equipment.

The PIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. The QDS consists of a computer, video display with touch screen capabilities, and input devices such as a keyboard and trackball. The hardwired I&C consists of conventional HMI devices such as buttons, switches, and analog and digital indicators that are hardwired from the various I&C systems. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

The equipment used in the safety-related portion of the SICS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the safety-related portion of the SICS is developed using the lifecycle processes described in Section 7.1.1.2.2.

Diversity Requirements

The SICS is credited in the defense-in-depth and diversity analysis described in Section 7.8.2. The manual reactor trip actuation is implemented from the SICS using a hardwired path that is not affected by a software common cause failure (CCF) of the SICS or PS.

Data Communications

These are a summary of the data communications implemented in the safety-related portion of the SICS:

- PS-SICS (Control) – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Control) – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- PS-SICS (Monitoring) – uni-directional (PS to SICS), point to point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Monitoring) – uni-directional (SAS to SICS), point to point data connections implemented with the TXS Profibus protocol.
- PI-QDS (Control) – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- PI-QDS (Monitoring) – uni-directional (PI to QDS), point to point data connections implemented with the TXS Ethernet protocol.
- PI-PI (Monitoring) – bi-directional, point to point data connections implemented with the TXS Profibus protocol. This network is provided to allow the display of redundant divisional information on a single QDS for optimization of the human factors design. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.
- SU-QDS – bi-directional, networked data connections implemented with the TXS Ethernet protocol. The SU is an auxiliary feature, and this network is non-safety-related network provided for servicing of the QDSs. These data connections use dedicated ports on the QDS separate from the PI-QDS connections. The system software provides for isolation between the safety-related and non-safety-related data. Software modifications cannot be performed with the QDS in operation. Access is authorized only with appropriate administrative controls. Fiber optic cable is provided for electrical isolation.

These are a summary of the data communications implemented in the non-safety-related portion of the SICS:

- SA I&C-SICS – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- GW-QDS – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network – bi-directional, networked communications.
- SU-QDS – bi-directional, networked data connections.

Power Supply

The safety-related portion of the SICS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the emergency diesel generators (EDG) in the case of a loss of offsite power (LOOP). In the event of a station blackout (SBO), the EUPS has the capability of receiving power from the station blackout diesel generators (SBODG).

The non-safety-related portion of the SICS is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during an LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.3.2 Process Information and Control System

The PICS is a modern, digital HMI. It allows the monitoring and control of process systems for the execution of required plant operations, including those required for abnormal and emergency situations. The PICS is provided in both the MCR and the RSS. View-only capabilities are provided in other areas of the plant as needed, including the technical support center (TSC) for support of emergency response operations.

This section describes the PICS with regards to I&C design. Details such as screen displays, levels of automation, and panel layout are designed using the HFE principles described in Chapter 18.

Classification

The PICS is classified as non-safety-related.

Functions

The PICS performs these functions:

- Monitoring and control of process systems during normal operation, including startup, power and shutdown operation.
- Monitor the status of the automatic reactor trip and ESF systems during abnormal events, including AOOs and postulated accidents.
- Manual reset of automatic reactor trip and ESF actuation functions.
- Non-credited means to monitor and control systems required to achieve and maintain safe shutdown.
- Manual component level control of safety-related process systems via the process automation system (PAS) and priority and actuator control system (PACS) diverse from the TXS based safety systems.
- Primary SPDS functions.

- Display of Type A-E PAM variables.
- Monitoring and control of systems required to mitigate severe accidents.
- Display bypassed and inoperable status of safety systems.
- Alarm management.
- Data archival.
- Interface to external I&C computers.
- Interface to external computers via a unidirectional firewall.

Architecture

Figure 7.1–5—Process Information and Control System Architecture provides a functional representation of the PICS.

The PICS consists of primarily of processing units (PU), external units (XU), operator workstations, plant overview panels (POP) and a firewall.

PUs are provided for data exchange between the plant data network and the terminal data network. The PUs perform functions such as data message validation, short term data storage, and alarm management. Redundant PUs are provided so that the PICS remains operational in case of a failure of a single PU.

PICS workstations with control and monitoring capabilities are located in the MCR and RSS. Normally, the operator displays in the RSS are in supervisory mode (view only) to prevent plant control until authorized in accordance with plant procedures. Operator displays are provided in other locations in the plant (e.g., TSC) as necessary. PICS workstations may be used for local control of specific plant systems with appropriate administrative controls.

The number of terminals per workstation, and number and location of the operator workstations is determined as a result of the human factors design process described in Chapter 18.

Plant overview panels are provided in the MCR, and other locations such as the TSC as desired. These are wide screen displays that are capable of providing continuously visible information to the operator.

XUs provide an interface to other computers from the PICS. Specialized monitoring systems may utilize dedicated computers that require an interface to the PICS for operator monitoring and management. A firewall is provided for unidirectional transfer of information from the XUs to Level 3 I&C systems. Remote access to the PICS is prohibited. Refer to Section 7.1.1.6.6 for more information on cybersecurity.

The PICS may include other functional units as necessary to carry out its functions. Examples are:

- Long term data storage units.
- Networked printers.
- Service equipment.

Equipment

The PICS is implemented with an industrial digital I&C and HMI platform.

The PUs consist of industrial computers. Operator workstations typically consist of computers, displays and input devices (i.e., computer mice and keyboards). The operator may use several monitors that share input devices. These monitors display different plant functions, and the display content is interchangeable. The POP is a set of large panels that display an overview of plant and system status. Equipment such as network switches and electrical and fiber optic cable are provided to support data communications.

The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. An alarm hierarchy with a color coding system is used to immediately alert the operator of the importance of the alarm based on the impact of the event to plant safety.

The PICS is used to control both safety-related and non-safety-related process systems. The PICS implements these measures to preclude spurious actuation of plant equipment:

- Operation of plant equipment is performed using a two step process. A single mouse click on a component is followed by a verification step requiring a second single mouse click, so a single inadvertent action by the operator does not result in a command signal.
- Touch screen displays are not used.

Qualification Requirements

There are no qualification requirements for the PICS equipment.

Quality Requirements

There are no quality requirements for the PICS equipment.

Diversity Requirements

The PICS is credited by the defense-in-depth and diversity analysis described in Section 7.8.2. These diversity requirements are established:

- The system hardware in the PICS is diverse from the TXS system hardware.
- The system software in the PICS is diverse from the TXS system software.

- The PICS displays are diverse from the SICS displays (QDS).

Data Communications

The PUs transmit data to and receive data from the Level 1 I&C systems via the plant data network. The PUs, operator workstations, POP, and XUs exchange data via the terminal data network. These networks implement periodic communications and message validation for robust data communications. Remote access of the PICS is not possible.

Power Supply

The PICS is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during an LOOP.

Refer to Chapter 8 for more information on electrical power systems.

7.1.1.4 Level 1 - System Automation

7.1.1.4.1 Protection System

The PS is an integrated digital reactor protection system (RPS) and ESF actuation system. The PS detects plant conditions that indicate the occurrence of AOO and postulated accidents, and it actuates the safety-related process systems required to mitigate the event.

Classification

The PS is classified as safety-related.

Functions

The PS performs these functions:

- Actuation of reactor trip.
- Actuation of ESF systems.
- Processing Type A-C PAM variables for display on the SICS.
- Interlocks.

Architecture

Figure 7.1–6—Protection System Architecture provides a functional representation of the PS.

The PS is organized into four redundant, independent divisions located in separate Safeguards Buildings. Each division contains two functionally independent

subsystems (A and B). These subsystems are used to implement functional diversity for reactor trip functions.

The PS consists of these functional units:

- Remote Acquisition Units (RAU).
- Rod Control Cluster Assembly Units (RCCAU).
- Acquisition and Processing Units (APU).
- Actuation Logic Units (ALU).
- MSIs.
- GWs.
- SUs.

Details on these functional units, along with details of the PS architecture are described in Digital Protection System Topical Report (ANP-10281) (Reference 6).

Equipment

The PS is implemented with the TXS digital I&C platform.

The RAUs, RCCAUs, APUs, ALUs, and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

The equipment used in the PS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the PS is developed using the lifecycle processes described in Section 7.1.1.2.2.

Diversity Requirements

There are no equipment diversity requirements for the PS.

Data Communications

The data communications for the PS are described in ANP-10281P (Reference 6).

Power Supply

The PS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of an LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

Refer to Chapter 8 for more information on the electrical power systems.

7.1.1.4.2 Safety Automation System

The SAS is Class 1E control system. The SAS performs automatic and selected manual control functions to perform safety-related controls during normal operations, mitigate the effects of abnormal operational occurrences and postulated accidents and to achieve and maintain safe shutdown.

The SAS only implements safety-related, credited control functions for safety systems. Non-safety-related or non-credited control functions for safety systems are performed by the PAS and PICS.

Classification

The SAS is classified as safety-related.

Functions

The SAS performs these functions:

- Automatic controls.
- Manual controls.
- Processing Type A-C PAM variables for display on the SICS.
- Interlocks.

Architecture

Figure 7.1–7—Safety Automation System Architecture provides a functional representation of the SAS.

The SAS is organized into four independent divisions located in separate Safeguards Buildings. SAS equipment may also be located in other safety-related structures as necessary.

The SAS consists of these functional units:

- Control Units (CU).
- MSIs.
- GWs.
- SUs.

The CUs execute the logic for the assigned automatic and manual control functions. Redundant CUs are provided within each division. They acquire hardwired inputs from sensors, the PS or the SICS via hardwired connections. Manual commands initiated from the SICS (QDS) or PICS are received via the MSI. Outputs from the CUs are sent to the PACS for signal prioritization and drive actuation. Data is sent from the CUs to the MSIs for display on SICS or PICS.

The MSIs provide a communication path between the SAS and other I&C systems via the GWs for both display of information and transfer of manual commands. The MSIs also provides a path to the SU for testing and maintenance of the CUs.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the SAS.

Equipment

The SAS is implemented with the TXS digital I&C platform.

The CUs and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

The equipment used in the SAS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the SAS is developed using the lifecycle processes described in Section 7.1.1.2.2.

Diversity Requirements

There are no equipment diversity requirements for the SAS.

Data Communications

These are summary of the data communications implemented in the SAS:

- CU-CU (A or B) – bi-directional, point to point data connections implemented with the TXS Profibus protocol. This network is provided to implement signal selection algorithms using redundant sensors for improved reliability in the control of safety-related processes. Separate connections are used for redundancies A and B. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.
- CU-MSI – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Control) – refer to Section 7.1.1.3.1.
- SAS-SICS (Monitoring) – refer to Section 7.1.1.3.1.
- MSI-GW – bi-directional, point to point data connections implemented with the TXS Ethernet protocol. This network is provided to allow monitoring and control of the SAS from the PICS. The design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.
- MSI-SU – non-safety-related, inter-divisional, bi-directional, point to point data connections implemented with the TXS Ethernet protocol. This network is provided for the servicing of the SAS. The design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.
- GW-Plant Data Network – non-safety-related, divisional, bi-directional, networked communications.

Power Supply

The SAS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of an LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

Refer to Chapter 8 for more information on the electrical power systems.

7.1.1.4.3 Priority and Actuator Control System

The PACS is a safety-related system that performs prioritization of signals from different I&C systems, drive actuation, and monitoring plant actuators.

Classification

The PACS is classified as safety-related.

Functions

The PACS supports the functions of other I&C systems by performing these:

- Prioritize actuation requests from the various Level 1 and Level 2 I&C systems.
- Essential equipment protection.
- Drive actuation.
- Drive monitoring.

Architecture

Figure 7.1–8—Priority and Actuator Control System Architecture provides a functional representation of the PACS.

The PACS is organized into four independent divisions located in separate Safeguards Buildings. PACS equipment may also be located in other safety-related structures as necessary.

The PACS is composed primarily of priority and actuator control (PAC) modules. A PAC module is provided for each actuator.

The PAC module receive actuation orders sent by the various I&C systems for prioritization. Signals are sent either via hardwired connections or a dedicated data connection to the PAS. Interfaces with actuation devices and actuated equipment (e.g., switchgear, torque and limit switches) are via hardwired connections. Priority between actuation requests from the various I&C systems is established by wiring the inputs using the priority principles described in Section 7.1.1.6.5.

Equipment

The PACS is implemented primarily with subracks, PAC modules and qualified isolation devices as needed. Fiber optic cable is used for the data connection between the PAS and the PACS.

The PAC module is described in ANP-10273P (Reference 4). The PAC modules may be modified and upgraded as needed, but shall exhibit these characteristics.

- Each PAC module consists of two parts: a safety part and an operational part.
- The safety part consists of logic implemented with firmware-only based devices (e.g., EEPROM), with no system software or application software.
- The inputs and outputs of the safety part are via hardwired connections.
- The logic of the safety part is fully testable and not subject to software common cause failure.
- The operational part is qualified as an associated circuit.

- The data communications from the PAS is only via the operational part.

Qualification Requirements

The equipment used in the PACS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the PAC modules is described in ANP-10273P (Reference 4).

Diversity Requirements

The PAC modules are diverse from the digital TXS function processors.

Data Communications

Non-safety-related, bidirectional, data connections are implemented between the operational part of the PAC modules and the PAS.

Power Supply

The PACS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of an LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

Refer to Chapter 8 for more information on the electrical power systems.

7.1.1.4.4 Severe Accident Instrumentation and Control

Classification

The SA I&C is classified as non-safety-related.

Functions

The SA I&C performs monitoring and control functions required for severe accident mitigation.

Architecture

Figure 7.1–9—Severe Accident I&C System Architecture provides a functional representation of the SA I&C.

The SA I&C is organized into four divisions located in separate Safeguards Buildings.

The SA I&C consists of these functional units:

- Control Units (CU).

- Drive Control Modules (DCM).
- MSIs.
- GWs.
- SUs.

The CU's perform data acquisition and control functions. Hardwired inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems. Hardwired outputs are sent to the DCMs or PACS for component actuation. DCMs are provided to interface to the non-safety-related actuated equipment used for severe accident mitigation.

The MSIs provide a communication path between the SA I&C and other I&C systems via the GWs for both display of information and transfer of manual commands. The MSIs also provides a path to the SU for testing and maintenance of the CUs.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the SA I&C.

Equipment

The SA I&C is implemented with the TXS digital I&C platform.

The CUs and MSIs generally consist of subracks, I/O modules, function processors, and communication modules, and optical link modules. SUs and GWs are non-safety related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

There are no qualification requirements for the SA I&C equipment.

Quality Requirements

There are no quality requirements for the SA I&C equipment.

Diversity Requirements

There are no diversity requirements for the SA I&C equipment.

Data Communications

These are a summary of the data communications implemented in the SA I&C:

- CU-MSI – bi-directional, point to point data connections implemented with the TXS Profibus protocol.

- MSI-GW – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- MSI-SU – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network – bi-directional, networked communications.

Power Supply

The SA I&C is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during an LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.5 Reactor Control, Surveillance and Limitation System

Classification

The reactor control, surveillance, and limitation system (RCSL) is classified as non-safety-related.

Functions

The RCSL performs these functions:

- Automatic reactor limitation functions.
- Automatic and manual reactor operational (control) functions.
- Core monitoring.

Architecture

Figure 7.1–10—Reactor Control, Surveillance, and Limitation System Architecture provides a functional representation of the RCSL.

The RCSL is organized into four divisions located in separate Safeguards Buildings.

The RCSL consists of these functional units:

- Acquisition Units (AU).
- Control Units (CU).
- Drive Units (DU).
- MSIs.
- GWs.

- SUs.

The AUs perform data acquisition functions. Hardwired inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems.

Redundant CUs acquire information from the AUs. The CUs implement signal selection algorithms for use in the control and limitation functions described in Section 7.7.1. Outputs from the CUs are sent to the DUs for actuation.

Redundant DUs are provided in both divisions 1 and 4. This configuration is chosen so that the control rods remain operable given a failure of a single CU. Hardwired outputs from the DUs are sent to the Control Rod Drive Control System (CRDCS) or to other I&C systems for actuation.

The MSIs provide a communication path between the RCSL and other I&C systems via the GWs for both display of information and transfer of manual commands. The MSIs also provides a path to the SU for testing and maintenance of the various functional units of the RCSL.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the RCSL.

Equipment

The RCSL is implemented with the TXS digital I&C platform.

The AUs, CUs, DUs and MSIs generally consist of subracks, I/O modules, function processors, and communication modules, and optical link modules. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

There are no qualification requirements for the RCSL equipment.

Quality Requirements

There are no quality requirements for the RCSL equipment.

Diversity Requirements

There are no diversity requirements for the RCSL equipment.

Data Communications

These are a summary of the data communications implemented in the RCSL:

- AU-CU – bi-directional, point to point data connections implemented with the TXS Profibus protocol.

- CU-DU – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- AU-MSI - bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- CU-MSI - bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- DU-MSI - bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- MSI-GW – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- MSI-SU – bi-directional, point to point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network – bi-directional, networked communications.

Power Supply

The RCSL is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during an LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.6 Process Automation System

The PAS is the main automation and control system for the plant. The PAS provides controls for both safety-related and non-safety-related equipment.

The PAS only implements non-safety-related or non-credited control functions for safety-related systems. The SAS is provided to perform safety-related, credited control functions for safety-related process systems.

Classification

The PAS is classified as non-safety-related.

Functions

The PAS performs these functions:

- Automatic risk reduction functions, including:
 - Mitigation of ATWS and software common cause failure.
 - Mitigation of SBO.

- Mitigation of other risk significant events.
- Automatic primary plant limitation functions.
- Automatic operational functions, including;
 - Equipment protection.
 - Closed loop controls.
- Manual control functions.
- Processing of information for display, including;
 - Type A-E PAM variables.
 - Process system instrumentation.
 - Alarms.

Architecture

The PAS is segregated into subsystems to account for differences in geographic location within the plant, and design and quality requirements. The PAS contains these subsystems:

- Nuclear island subsystem (NIS).
- Turbine island subsystem (TIS).
- Balance of plant subsystem (BPS).
- Diverse actuation subsystem (DAS).

For these descriptions, a statement regarding the PAS includes all four subsystems. Statements applicable to a particular subsystem refer specifically to that subsystem.

Nuclear Island Subsystem

Figure 7.1–11—Process Automation System Architecture (Nuclear Island Subsystem) provides a functional representation of the NIS.

The NIS is organized into four divisions located in separate Safeguards Buildings. NIS equipment may also be located in other structures in the Nuclear Island as necessary.

The NIS implements redundant CUs to perform its functions. The CUs acquire hardwired signals directly from field sensors or from other I&C systems. Outputs are sent to non-safety-related actuators directly or to the PACS for the actuation of safety-related actuators. The CUs interface with the PICS via the plant data network for manual commands and display of information.

Turbine Island Subsystem

Figure 7.1–12—Process Automation System Architecture (Turbine Island and Balance of Plant Subsystems) provides a functional representation of the TIS.

The TIS is located in the Turbine Switchgear building.

The TIS implements redundant CUs to perform its functions. The CUs acquire hardwired signals directly from field sensors or from other I&C systems. Outputs are sent to non-safety-related actuators. The CUs interface with the PICS via the plant data network for manual commands and display of information.

Balance of Plant Subsystem

Figure 7.1–12—Process Automation System Architecture (Turbine Island and Balance of Plant Subsystems) provides a functional representation of the BPS.

The BPS is located in the Turbine Switchgear building and other locations in the Balance of Plant as necessary.

The BPS implements redundant CUs to perform its functions. The CUs acquire hardwired signals directly from field sensors or from other I&C systems. Outputs are sent to non-safety-related actuators. The CUs interface with the PICS via the plant data network for manual commands and display of information.

Diverse Actuation Subsystem

Figure 7.1-12—Process Automation System Architecture (Diverse Actuation Subsystem) provides a functional representation of the DAS.

The DAS is organized into four redundant divisions located in separate Safeguards Buildings.

Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the PS as described in Section 7.1.1.6.4 and compared to a setpoint. Fiber optic data connections are provided to share trip requests, and two out of four voting is done in each DAU. Outputs are sent to the PACS via hardwired connections.

The DAUs interface with the PICS via the plant data network for the display of information.

Equipment

The PAS is implemented with an industrial digital I&C platform.

The PAS generally consists of subracks, I/O modules, function processors, and communication modules, and optical link modules. Fiber optic and copper cable is used for the various data and hardwired connections. Specialized components such as drive modules and interfaces to third party control systems may be used.

Qualification Requirements

There are no qualification requirements for the PAS equipment.

Quality Requirements

There are no quality requirements for the NIS, TIS, or BPS.

The DAS is designed, fabricated, erected, and tested under the augmented quality program described in Chapter 17.

To provide software quality, the application software used in the DAS is developed using the lifecycle processes described in Section 7.1.1.2.2.

Diversity Requirements

The PAS is credited by the defense-in-depth and diversity analysis described in Section 7.8.2. These diversity requirements apply to the PAS equipment:

- The system hardware in the PAS is diverse from the TXS system hardware.
- The system software in the PAS is diverse from the TXS system software.

Data Communications

The functional units in the PAS interface to the PICS via the plant data network.

The NIS implements point-to-point data connections between the CUs in each division to share signals to implement signal selection algorithms.

The DAS implements point-to-point data connections between the DAUs for voting purposes.

Other data connections may be implemented as required.

Power Supply

The various subsystems of the PAS have different power supplies.

The NIS and the DAS are powered from the 12hr UPS. The 12hr UPS provides backup power with 12-hour batteries and the SBODGs in the event of an LOOP.

The TIS and the BPS are powered from the non-Class 1E uninterruptible power supply (NUPS). The NUPS provides backup power with 2-hour batteries and the SBODGs in the event of an LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.7 Turbine Generator I&C

The turbine generator (TG) I&C system regulates the operation of the turbine-generator for power generation. It provides speed and load control, as well as control of TG auxiliaries.

Refer to Section 10.2 for further information on the TG I&C.

7.1.1.5 Level 0 - Process Interface

The process interface level includes components such as sensors, actuators, and switchgear.

The majority of the process interface equipment is included within the mechanical and electrical process systems that the I&C systems monitor and control. These systems are described in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10 and Chapter 11.

The systems listed in these sections are distinct I&C systems within the process interface level:

7.1.1.5.1 Control Rod Drive Control System

Classification

The CRDCS is primarily classified as non-safety-related. The trip contactors are safety-related.

Description

The CRDCS controls the actuation of the 89 RCCAs in the reactor vessel. The CRDCS accomplishes this task by providing current to the individual coils of the control rod drive mechanism (CRDM) to move its respective RCCA.

The CRDCS receives DC power from the NUPS to move and hold the CRDMs. The reactor trip breakers are upstream of the CRDCS. Refer to Section 8.3 for more information on the NUPS and the reactor trip breakers.

Within the CRDCS, the safety-related trip contactor modules interrupt power to the CRDMs when a trip signal is received from the PS. The trip contactors get a signal from each division of the PS and are arranged to implement two-out-of-four logic. The contactor modules are environmentally qualified, including seismic and EMI and RFI effects.

The RCSL transmits commands containing the direction of movement (i.e., withdrawal or insertion), speed of movement, and drop and hold information to the CRDCS. Withdrawal and insertion commands are used for reactor control functions. Drop orders are issues for a partial or full reactor trip in support of the reactor limitation functions. Refer to Section 7.7.1 for a description of the reactor control and limitation functions.

The non-safety-related components of the CRDCS are designed such that a seismic event does not result in damage that disables the safety function of the trip contactors.

Refer to Section 4.6.2 for more information on the reactivity control systems.

7.1.1.5.2 Incore Instrumentation System

Classification

The incore instrumentation system (ICIS) is classified as safety-related.

Description

Figure 4.4-8—Arrangement of Incore Instrumentation Components shows the arrangement of the various components within the core.

The ICIS measures certain in-vessel parameters. The ICIS consists of safety-related and non-safety-related equipment.

The ICIS consists of:

- Self-powered neutron detectors (SPND) (safety-related except for test equipment).
- Aeroball measurement system (AMS) (non-safety-related).
- Fixed core outlet thermocouple (COT) measurement system (safety-related).
- Reactor pressure vessel dome temperature (RPVDT) measurement system (non-safety-related).

There are 72 SPNDs that continuously measure the neutron flux at given positions in the core to provide information about the three-dimensional flux distribution. The AMS is used to calibrate the SPNDs at regular intervals. The SPNDs and AMS are described in detail in Incore Transient Methodology Topical Report (ANP-10287P) (Reference 7).

The COT continuously measures fuel assembly outlet temperature. The fixed thermocouples are placed in selected fuel assemblies that are located azimuthally and radially within the core. The core outlet temperature is used to determine the saturation margin (ΔT_{sat}) at the core exit and provide information about the radial temperature distribution in the core and average temperature in the reactor coolant system (RCS). There are a total of 36 COTs. The COTs are arranged with three thermocouples (two narrow range thermocouples and one wide range thermocouple) within each of the twelve SPND finger assemblies.

The RPVDT measurement system continuously measures the temperature within the reactor dome. The sensing elements are thermocouples, which are passive devices that do not use electrical power. RPVDT instrumentation provides temperature signals corresponding to the top-level, mid-level, and bottom-level measurement regions of the dome. The measurements of fluid temperature in the RPV dome provide

information to the operator during normal and emergency operations if they are available (although not required for post-accident monitoring).

The main functions of the dome thermocouples are to:

- Indicate a potential steam bubble.
- Indicate average dome temperature.
- Indicate temperature above RCCA plate to determine temperature difference across the plate.
- Indicate air temperature during RCS venting during startup.

7.1.1.5.3 Excore Instrumentation System

Classification

The excore instrumentation system (EIS) is classified as safety-related.

Description

The EIS monitors neutron flux during power and shutdown modes of operation. Because it is not possible to measure the entire operating range of reactor power with a single instrument, three ranges of detection are used.

- Power range – uses an uncompensated, boron lined ionization chamber detector.
- Intermediate range – uses a gamma compensated, boron lined ionization chamber detector.
- Source range – uses a boron lined proportional counter detector.

Figure 7.1–14—Measuring Ranges of Excore Instrumentation illustrates the coverage and overlaps of the excore detectors. These ranges provide coverage from shutdown conditions to about 200 percent reactor power. Overlaps in the measuring ranges are provided to allow operation of each range during transitions in power levels.

Figure 7.1–15—Excore Instrumentation Detector Locations illustrates the arrangement of the excore detectors.

There are eight power range detectors (PRD) that cover the upper three decades up to 200 percent reactor power. Two detectors are located in one of four radial locations around the core (45°, 135°, 225°, 315°). The two detectors at each location measure the center of the upper and lower portions of the core for monitoring and control of axial flux distributions.

Four intermediate range detectors (IRD) monitor a little more than seven decades up to at least 60 percent full power, with an overlapping of the source range by about 2.5 decades. They are located in the same radial locations as the PRDs.

Three source range detectors are provided at three radial locations around the core (0°, 90°, 270°). The source range monitors the lower six decades.

7.1.1.5.4 Boron Concentration Measurement System

Classification

The boron concentration measurement system (BCMS) is classified as safety-related.

Description

Figure 7.1–16—Boron Concentration Measurement System Arrangement illustrates the arrangement of the BCMS.

The BCMS measures the boron concentration in the CVCS. The measured boron concentration is further processed and used by the PS to mitigate the risk of homogeneous and heterogeneous dilution of the RCS. Each boron concentration signal generated by the four redundant measuring devices is processed in a separate division.

To measure boron concentration, an Americium-Beryllium neutron source is used. The neutron source is located adjacent to CVCS piping. Neutrons are counted on the other side of the pipe. The number of neutrons counted is indicative of the boron concentration of the CVCS. A temperature sensor is used to measure the temperature of the fluid and provide a correction factor to the measured boron concentration.

7.1.1.5.5 Radiation Monitoring System

Classification

The radiation monitoring system (RMS) is classified as safety-related.

Description

The RMS performs these functions:

- Post-accident radioactivity monitoring.
- Process radioactivity monitoring.
- Effluent radioactivity monitoring.
- Airborne radioactivity monitoring.
- Area radioactivity monitoring.

The RMS consists of various detectors and processing equipment throughout the plant. Refer to Section 7.3.1 for radiation monitors used in ESF actuation functions. For radiation monitors used for PAM, refer to Section 7.5.1. For other monitoring functions, refer to Chapter 11 and Chapter 12.

7.1.1.5.6 Hydrogen Monitoring System

Classification

The hydrogen monitoring system (HMS) is classified as safety-related.

Description

The HMS is described in Section 6.2.5.

7.1.1.5.7 Reactor Pressure Vessel Level Measurement System

Classification

The reactor pressure vessel level (RPVL) measurement system is classified as safety-related.

Description

Figure 4.4–8—Arrangement of Incore Instrumentation (Top View) shows the arrangement of the various components within the core.

Figure 4.4–10—Arrangement of Incore Instrumentation (Side View) illustrates the vertical arrangement of the RPVL measurement system.

The RPVL measurement system provides an indication to the operator of the water level in the reactor vessel for use in post-accident monitoring. The RPVL measurement instrumentation primarily consists of four probes containing three thermocouple sensors each for level measurement. Three thresholds are detected by the RPVL measurement instrumentation.

- Higher threshold located at the top of hot leg of the RCS.
- Lower threshold located at the bottom of hot leg of the RCS.
- Intermediate threshold located between the top and the bottom of hot leg of the RCS.

Sensing elements consist of heated and unheated thermocouples. The difference between the signals of the heated and unheated thermocouples is used to indicate coolant level in the RPV. If the difference of the thermovoltages between heated and unheated thermocouples exceeds a defined threshold, this would indicate that the water level is below the heated thermocouples.

7.1.1.5.8 Seismic Monitoring System

Classification

The seismic monitoring system is classified as non-safety-related.

Description

The seismic monitoring system is described in Section 3.7.4.

7.1.1.5.9 Loose Parts Monitoring System**Classification**

The loose parts monitoring system (LPMS) is classified as non-safety-related.

Description

The LPMS detects, locates, and analyzes detached or loosened parts and foreign bodies in the RCS and the secondary side of the steam generators during normal plant operation. By providing an early detection of loose parts, the probability of primary or secondary system component damage can be lessened and exposure to station personnel can be minimized.

Metallic loose parts excited by fluid streaming impact the inner wall of the pressurized boundary of the primary or secondary system. These impacts (also called bursts) generate structure borne noise, which can be detected by accelerometers attached to the outer surface of the monitored components. Signal conditioning equipment is used to provide the LPMS with reliable data. The signals are recorded and analyzed and common alarms are provided to the operators in the MCR upon violating predefined thresholds. Background noise generated by the plant is eliminated to the greatest extent possible to avoid faulty alarms or inaccurate measurements.

7.1.1.5.10 Vibration Monitoring System**Classification**

The vibration monitoring system (VMS) is classified as non-safety-related.

Description

The VMS monitors changes in the vibration behavior of the RPV and its internals, the primary system components, the main coolant pumps, and portions of the main steam line structures in the secondary system by monitoring the frequencies and amplitudes of service-induced component and fluid vibrations.

Changes in the vibration behavior of a structure or component is one of the most sensitive indicators of a change in the condition of the component such as reduction of screw bolt pretensions, reduction in the stiffness of core barrel hold-down springs, direct contact between primary components and the Containment Building, damage to main coolant pump bearings, and cracks in the main coolant pump shaft.

The system automatically performs measuring, analysis, and logging functions required for monitoring vibration, either at selectable intervals or upon operator command. Threshold violations caused by changes in frequency and amplitude are annunciated. In addition to component and fluid vibrations, process parameters such as temperature, pressure or flow rate, which have an influence on vibration behavior

are also acquired and then used to distinguish between service-induced and abnormal changes in vibration. This minimizes the probability of false diagnoses.

7.1.1.5.11 Fatigue Monitoring System

Classification

The fatigue monitoring system is classified as non-safety-related.

Description

The fatigue monitoring system is provided to record actual fatigue loading conditions on plant equipment. It measures various plant parameters such as temperature and pressure to calculate actual stress loads on major plant components. This allows the comparison of actual loads against design loading conditions, which provides plant operating personnel the information needed to adjust operations, maintenance, and inspection activities accordingly.

Thermocouples are used to measure actual component temperatures. System pressure is considered uniform and is received from existing sensors. The information is received, processed, stored and analyzed. Data is retrievable by operators and other plant personnel.

7.1.1.5.12 Leak Detection System

Classification

The leak detection system (LDS) is classified as non-safety-related.

Description

The LDS, in conjunction with other associated systems, promptly detects, quantifies, and localizes leakage from the RCPB and selected portions of the main steam system.

The LDS includes these components:

- Condensate mass flow measurement devices inside containment.
- Humidity and temperature sensors inside containment.
- Local humidity detection system for the main steam piping.

The leak-before-break approach for the U.S. EPR is described in Section 3.6.3. The RCPB leakage detection approach is described in Section 5.2.5.

The local humidity detection system measures local increases in relative humidity along appropriate portions of the MS lines inside of the containment to detect and localize leakages from the lines with a high degree of accuracy.

Alarms and indications associated with the LDS are available to the operators in the MCR.

7.1.1.6 I&C Architecture Design Principles

7.1.1.6.1 Defense-in-Depth

The U.S. EPR implements the following lines of defense to establish the defense-in-depth principle:

- Preventive line of defense.
- Main line of defense.
- Risk reduction line of defense.

These lines of defense are described in the Instrumentation and Controls Topical Report (ANP-10284) (Reference 8).

To implement the defense-in-depth principle, four primary functional categories are defined for proper operation of the plant. These categories are mapped to the various sections of this document.

- Safety I&C functions - used to prevent or mitigate DBEs:
 - Section 7.2 – Reactor trip functions.
 - Section 7.3 – ESF actuation and control functions.
 - Section 7.4 – Safe shutdown functions.
 - Section 7.5 – Safety-related information display functions.
 - Section 7.6 – Interlock functions.
 - Chapter 8 and Chapter 9 – Safety-related functions for auxiliary support features.
- Risk Reduction I&C functions – used to mitigate BDBEs:
 - Section 7.8 – Diverse I&C functions.
 - Chapter 8.4 – SBO mitigation functions.
 - Chapter 19 – Severe accident and other risk mitigation functions.
- Limitation I&C functions:
 - Section 7.7 – Control functions.
- Operational I&C functions:
 - Section 7.7 – Control functions.

Figure 7.1–17—Implementation of Defense-in-Depth illustrates the implementation of the defense-in-depth concept for the U.S. EPR.

7.1.1.6.2 Diversity

Figure 7.1–18—Implementation of the Diversity Principle illustrates the implementation of diversity for the U.S. EPR.

The U.S. EPR implements the following diversity features:

- Functional diversity.
- Platform diversity.

Functional diversity (defined as signal diversity in NUREG/CR-6303 (Reference 9)) utilizes different process variables to detect the effects of a design basis event and initiate a reactor trip. The PS provides separate subsystems within each division to implement functional diversity.

Platform diversity refers to the use of different I&C platforms to accomplish the same function. Platform diversity consists of the following diversity attributes from NUREG/CR-6303 (Reference 9):

- Software diversity (e.g. system software).
- Equipment diversity (e.g. system hardware).

These attributes are the primary means of establishing diversity between the TXS platform and the digital platform(s) used for the PICS and PAS. Diversity requirements for the PICS and PAS are described in Section 7.1.1.3.2 and Section 7.1.1.4.6, respectively.

Functional diversity (as defined by NUREG/CR-6303 (Reference 9)) is implemented within the various process systems described in other chapters of this document. Examples include diverse means for reactor shutdown (reactor trip or extra boration system), core heat removal (main steam relief train or main condenser), and coolant inventory control (chemical volume and control system or safety injection system).

Refer to ANP-10284 (Reference 8) for more information regarding diversity features of the U.S. EPR.

7.1.1.6.3 Redundancy

Redundancy is implemented throughout the I&C architecture to prevent a single failure from causing a loss of function. The level of redundancy assigned depends on the classification and functional requirements of the system. Table 7.1.2—Levels of Redundancy in I&C Architecture illustrates the redundancies assigned to the various I&C systems.

7.1.1.6.4 Independence

For safety I&C systems, independence is established so that a single failure does not result in the loss of the safety function.

The following measures are implemented for the safety I&C systems:

- Independence between redundant divisions.
- Independence from the effects of DBEs.
- Independence between the safety-related I&C systems and the non-safety-related I&C systems.

Independence of Redundant Safety Divisions

Figure 7.1–19—Independence Between Redundant Safety Divisions illustrates the implementation of inter-divisional independence.

The SICS, PS, SAS and PACS each consists of four independent divisions. Independence between redundant divisions is maintained using the following:

- Physical separation.
- Electrical isolation.
- Communications independence.

Independent divisions are located in each of the four physically separated Safeguards Buildings. Safety I&C systems may be implemented in other safety-related structures, where redundant divisions are adequately separated.

Electrical isolation is required for hardwired and data connections, and is provided through the use of qualified isolation devices and fiber optic cable.

The SICS, PS, and SAS implement interdivisional communications to support the system functional requirements. Communications independence is provided by the following features of the TXS platform:

- Communications modules are provided separate from the function processors performing the safety function.
- Communications are implemented with separate send and receive data channels.
- Asynchronous, cyclic operation of the function processors and communications modules.

In addition, only predefined messages are accepted by the receiving function processor, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Refer to Section 2.9 of Reference 3 for more information on the principles of communications independence.

Independence from the Effects of Design Basis Events

The TXS equipment used in the safety-related I&C systems is qualified to withstand the effects of DBEs.

Independence between the Safety I&C Systems and Non-Safety I&C Systems

Figure 7.1–20—Independence Between Safety and Non-Safety I&C illustrates the implementation of independence between safety-related and non-safety-related I&C systems.

Independence between safety-related and non-safety-related I&C systems is provided using these principles:

- Physical separation.
- Electrical isolation.
- Communications independence.

The safety-related I&C systems are physically separated from non-safety-related I&C systems.

Electrical isolation is provided for both hardwired and data communications between safety-related and non-safety-related I&C. For hardwired signals, qualified isolation devices are used with the safety-related I&C systems for signals to and from the non-safety-related I&C. Fiber optic cable is used for data connections between safety-related and non-safety-related I&C.

Communications independence is provided between the safety-related I&C systems and the non-safety-related I&C systems via the MSIs. Connections to the SUs are also via the MSI.

These features of the MSIs provide for communications independence:

- Communication modules separate from the function processors for the purpose of handling communications to the GWs.
- Communications between the function processors and communications modules are implemented with separate send and receive data channels.
- The function processors and communications modules operate cyclically and asynchronous to each other.

In addition, only predefined messages are accepted by the MSI, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Refer to Section 2.9 of Reference 3 for more information on the principles of communications independence for the TXS platform.

Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related part of the PAC module. Connections between the non-safety-related and safety-related part of the PAC module are hardwired. The non-safety-related part is qualified as an associated circuit.

The safety-related I&C systems are implemented in four independent divisions. The safety-related I&C systems retain their ability to perform their function given a single failure of a common element to both the safety-related and non-safety-related systems concurrent with another single failure. The control systems implement signal selection algorithms and redundancy to minimize the possibility of a single failure that results in a design basis event that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and accommodate failures.

7.1.1.6.5 Priority

The U.S. EPR I&C design allows for multiple I&C systems to send requests to a given actuator. To make certain that each individual actuator executes the proper action for the given plant condition, priority management rules are provided. The four primary functional categories provide the basis for priority management of the U.S. EPR I&C architecture.

The order of priority for automatic functions is listed from highest to lowest:

- Safety-related I&C functions (safety-related):
 - Actuation functions.
 - Control functions.
- Risk reduction I&C functions (non-safety-related).
- Limitation I&C functions (non-safety-related).
- Operational I&C functions (non-safety-related):
 - Equipment protection functions.
 - Automatic control.
 - Manual control.

The PACS manages priority for safety-related components. For non-safety-related components, priority is managed in the application software of the Level 1 I&C systems.

7.1.1.6.6 Cyber Security

The U.S. EPR I&C design provides features for cyber security. These include:

- Communications independence measures implemented between the non-safety-related I&C and safety-related I&C.
- SUs for the safety-related I&C systems are not connected to non-safety-related I&C networks.
- No direct connections from external networks to the safety-related I&C systems.
- Connections between non-safety-related I&C networks and external plant networks are via a unidirectional firewall. Remote access to the I&C systems is prohibited. No other interface points are provided.

The I&C systems comprise a level of defense for cybersecurity. Figure 7.1–21—Levels of Defense of Cybersecurity illustrates these concepts.

External levels of defense and other features that provide for cyber security are addressed as part of the overall security plan, which is described in Section 13.6.

7.1.2 Identification of Safety Criteria

Table 7.1–2—I&C System Requirements Matrix, shows the I&C system requirements matrix which details the regulatory requirements for the I&C systems of the U.S. EPR.

The U.S. EPR is designed in accordance with IEEE Std 603-1998 (Reference 1). ANP-10281P (Reference 6) describes how IEEE Std 603-1998 (Reference 1) meets or exceeds the requirements established in IEEE Std 603-1991 (Reference 2).

These I&C systems are within the scope of the protection system as defined in IEEE Std 603-1998 (Reference 1):

- Protection system.
- Incore instrumentation system.
- Excore instrumentation system.
- Boron concentration measurement system.
- Radiation monitoring system.
- Process instrumentation (refer to Section 7.2 and Section 7.3 for details).

The scope of the safety systems, as defined in IEEE Std 603-1998 (Reference 1) are those I&C systems that are classified as safety-related and the safety-related trip contactors.

7.1.2.1 Compliance to 10 CFR Parts 50 and 52**7.1.2.1.1 10 CFR 50.55a(a)(1) – Quality Standards and Records for Systems Important to Safety**

The applicable I&C systems listed in Table 7.1–2 shall be designed to meet the requirements of 10 CFR 50.55a(a)(1). This is provided by compliance with Clause 5.3 (quality) of IEEE Std 603-1998 (Reference 1).

7.1.2.1.2 10 CFR 50.55a(h)(2) – Protection Systems

The applicable I&C systems listed in Table 7.1–2 are designed to meet the requirements 10 CFR 50.55a(h)(2). This is provided by compliance with IEEE Std 603-1998 (Reference 1), which meets or exceeds the requirements established by IEEE Std 603-1991 (Reference 2).

7.1.2.1.3 10 CFR 50.55a(h)(3) – Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.55a(h)(3). This is provided by compliance with conformance to IEEE Std 603-1998 (Reference 1), which meets or exceeds the requirements established by IEEE Std 603-1991 (Reference 2).

7.1.2.1.4 10 CFR 50.34(f)(2)(v) – Bypass and Inoperable Status Indication

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(v). This is provided by compliance to Clause 5.8.2 (system status indication) and Clause 5.8.3 (indication of bypasses) of IEEE Std 603-1998 (Reference 1). Refer to Section 7.5.2.1.1 for more information regarding bypassed and inoperable status.

7.1.2.1.5 10 CFR 50.34(f)(2)(xi) – Direct Indication of Relief and Safety Valve Position

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xi). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.6 10 CFR 50.34(f)(2)(xii) – Auxiliary Feedwater System Automatic Initiation and Flow Indication

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xii). Section 7.3.1.2.2 describes the automatic and manual initiation of the emergency feedwater (EFW) system. Section 7.5.2.1.1 describes the EFW flow indication.

7.1.2.1.7 10 CFR 50.34(f)(2)(xiv) – Containment Isolation Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xiv). Section 7.3.1.2.9 describes the containment isolation function, including reset of the function. Section 6.2.4 describes the containment isolation system.

7.1.2.1.8 10 CFR 50.34(f)(2)(xvii) – Accident Monitoring Instrumentation

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xvii). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.9 10 CFR 50.34(f)(2)(xviii) – Instrumentation for the Detection of Inadequate Core Cooling

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xviii). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.10 10 CFR 50.34(f)(2)(xix) – Instruments for Monitoring Plant Conditions Following Core Damage

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xix). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.11 10 CFR 50.34(f)(2)(xx) – Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xx). The pressurizer level sensors are acquired by the PS for the functions described in Section 7.2.1.2.12 and Section 7.3.1.2.10. The pilot valves for the pressurizer safety relief valves (PSRV) are controlled by the PS and PACS as described in Section 7.3.1.2.13. The PS and PACS are powered by the EUPS as described in Section 7.1.1.4.1 and Section 7.1.1.4.3. The PSRVs are described in Section 5.2. The EUPS is described in Section 8.3. Refer to Section 7.5.2 for more information.

7.1.2.1.12 10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients without Scram

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 10 CFR 50.62. Refer to Section 7.8.2.1.3 for more information.

7.1.2.2 Compliance to 10 CFR Part 50, Appendix A GDC

Compliance statements in this section are specific to the I&C systems. Refer to Section 3.1.1 for compliance to the GDC for the U.S. EPR.

7.1.2.2.1 GDC 1 – Quality Standards and Records

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements of GDC 1. This is provided by compliance with Clause 5.3 (quality) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.2 GDC 2 – Design Bases for Protection against Natural Phenomena

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements for GDC 2. The applicable I&C systems are located within the four Safeguards Buildings and other safety-related structures as necessary. The design of

these structures is described in Chapter 3. Compliance with Clause 5.4 (equipment qualification) of IEEE Std 603-1998 (Reference 1) demonstrates that the applicable I&C systems remain operable during and following seismic events.

7.1.2.2.3 GDC 4 – Environmental and Dynamic Effects of Design Bases

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements for GDC 4. This is provided by compliance with Clause 5.4 (equipment qualification) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.4 GDC 10 – Reactor Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 10. Section 7.7 describes control and limitation functions that regulate the operation of the reactor and limit the effects of AOOs. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in U.S. EPR Instrument Setpoint Methodology (ANP-10275P) (Reference 11).

7.1.2.2.5 GDC 13 – Instrumentation and Control

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 13. Refer to the I&C systems description in Section 7.1.1 for more information.

7.1.2.2.6 GDC 15 – Reactor Coolant System Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 15. Section 7.7 describes control and limitation functions that regulate the operation of the RCS and limit the effects of AOOs. Section 7.2 and Section 7.3 describe the I&C related protective actions credited in the RCS overpressure analysis described in Section 5.2.2. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11).

7.1.2.2.7 GDC 16 – Containment Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 16. Section 7.3.1.2.9 describes the containment isolation function. Section 6.2.4 describes the containment isolation system. Section 7.3.12.2.1 describes the safety injection actuation function. This actuates the safety injection system, which provides for long term heat removal from the containment and is described in Section 6.3.

7.1.2.2.8 GDC 19 – Control Room

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 19. Section 7.1.1.3.1 and Section 7.1.1.3.2 describe the capabilities of the SICS and PICS with regards to the capability for safe operation of the plant from the MCR during normal and accident conditions. Section 7.3.1.2.16 describes the MCR air

conditioning isolation and filtering function to limit radiation levels in the MCR. Section 7.1.1.3.1 and Section 7.1.1.3.2 describe the capabilities of the SICS and PICS to achieve both hot and cold shutdown conditions from the RSS.

7.1.2.2.9 GDC 20 – Protection System Functions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 20. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11).

7.1.2.2.10 GDC 21 – Protection System Reliability and Testability

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 21. This is provided by compliance with IEEE Std 603-1998 (Reference 1). Specifically, compliance with Clause 5.1 (single-failure criterion), Clauses 5.7 and 6.5 (capability for testing and calibration), and Clauses 6.7 and 7.5 (maintenance bypass) demonstrates the capability for testing the applicable I&C systems during operation.

7.1.2.2.11 GDC 22 – Protection System Independence

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 22. This is provided by compliance with Clause 5.6 (independence) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.12 GDC 23 – Protection System Failure Modes

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 23. The failure modes and effects analysis (FMEA) for the applicable I&C systems are described in Section 7.2.2.2 and Section 7.3.2.2.

7.1.2.2.13 GDC 24 – Separation of Protection and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 24. This is provided by compliance with IEEE Std 603-1998 (Reference 1). Specifically, compliance with Clause 5.1 (single-failure criterion), Clause 5.6 (physical, electrical, and communications independence), Clauses 6.3 and 6.6 (control protection interaction), Clause 5.12 (auxiliary features), and Clause 8 (power sources) limit the interconnections to assure that safety is not significantly impaired. Section 7.7 describes design features of the controls systems that minimize and limit challenges to the PS due to controls system failures. Worst-case credible failures of the plant control systems are postulated in the analysis of off-design operational transients and accidents described in Chapter 15.

7.1.2.2.14 GDC 25 – Protection System Requirements for Reactivity Control Malfunctions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 24. Section 7.2 and Section 7.3 describe the protective actions credited in the

accident analysis described in Chapter 15 for malfunctions of the reactivity control systems.

7.1.2.2.15 GDC 28 – Reactivity Limits

The applicable I&C systems listed in Table 7.1–2 are designed to meet the requirements for GDC 28. Section 7.7 describes the control systems for the U.S. EPR. Section 7.2 and Section 7.3 describe the protective actions implemented in the PS to mitigate the effects of AOOs and postulated accidents. Section 5.2.2 describes the overpressure analyses of the RCS, and Chapter 15 describes the safety analyses given malfunctions of control systems.

7.1.2.2.16 GDC 29 – Protection against Anticipated Operational Occurrences

The applicable I&C systems listed in Table 7.1–2 are designed to meet the requirements for GDC 29. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11).

7.1.2.2.17 GDC 33 – Reactor Coolant Makeup

The applicable I&C systems listed in Table 7.1–2 are designed to meet the requirements for GDC 33. Reactor coolant makeup is provided by the chemical volume and control system (CVCS) and the safety injection system (SIS). Refer to Section 9.3.4 and Section 6.3 for more information about the CVCS and SIS, respectively. Section 7.7 describes the pressurizer level control function that provides for reactor coolant makeup using the CVCS. Section 7.3 describes the actuation of the SIS, which provides for a safety-related source of borated water for makeup for small breaks in the RCPB. The I&C systems that perform the various functions, including information on power supplies, are described in Section 7.1.1.

7.1.2.2.18 GDC 34 – Residual Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 34. The SIS performs the residual heat removal function, and is described in Section 6.3. Section 7.4 describes the use of SIS to achieve and maintain safe shutdown following an accident. Section 7.6 describes the interlocks associated with the SIS. Section 7.7 describes the use of SIS to remove decay heat during normal shutdown periods. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.19 GDC 35 – Emergency Core Cooling

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 35. The SIS performs the emergency core cooling function, and is described in Section 6.3. Section 7.3 describes the actuation of the SIS to provide abundant core cooling. Section 7.6 describes the interlocks associated with the SIS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.20 GDC 38 – Containment Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 38. The SIS performs containment heat removal function, and is described in Section 6.3. Section 7.3 describes the actuation of the SIS. Section 7.6 describes the interlocks associated with the SIS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.21 GDC 41 – Containment Atmosphere Cleanup

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 41. The combustible gas control system (CGCS) performs the containment atmosphere cleanup function, and is described in Section 6.2.5.

7.1.2.2.22 GDC 44 – Cooling Water

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 44. The essential service water system (ESWS) and component cooling water system (CCWS) are provided to transfer heat from the plant to the ultimate heat sink. These systems are described in Section 9.2.1 and Section 9.2.2, respectively. Section 7.3 describes the actuation of the SIS, which starts the CCWS and ESWS. Section 7.4 describes the use of the CCWS and ESWS to achieve and maintain safe shutdown. Section 7.6 describes the interlocks associated with the CCWS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.3 Conformance to Staff Requirements Memoranda

7.1.2.3.1 SRM to SECY 93-087 II.Q – Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of the SRM to SECY 93-087 II.Q (Reference 10), with the exception of providing system level actuation of critical safety functions. The diversity and defense-in-depth (D3) methodology for the U.S. EPR is described in ANP-10284 (Reference 8). Section 7.1.1.4.6 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8.1.2 describes the functional requirements for the DAS. The D3 analysis is described in Section 7.8.2.2.

The SRM to SECY 93-087 II.Q (Reference 10) states that a set of displays and controls shall be provided in the MCR for the purpose of system level actuation of critical safety functions that are diverse from the safety I&C systems affected by a postulated CCF.

The U.S. EPR provides diverse displays and controls for component level actuation of critical safety functions via the PICS, NIS, and PACS. This approach is justified because the DAS, with appropriate subsequent operator action, provides sufficient functionality to achieve an acceptable plant response for each event analyzed in Chapter 15. Specifically, the DAS provides automatic actuation of these critical safety functions (using credited systems) when required due to abnormal plant conditions:

- Reactivity control – automatic reactor trip.
- Core heat removal – automatic actuation of the EFW system.
- Reactor coolant inventory – automatic actuation of SIS.
- Containment isolation – automatic actuation of containment isolation.
- Containment integrity - automatic actuation of SIS. The SIS provides for heat removal from the containment via the RHR heat exchangers.

The other system required to perform the critical safety functions is the operation of the main steam relief train (MSRT). Each MSRT contains two valves per steam generator that are opened to bleed steam, providing for core heat removal. The MSRT are also opened to assist in depressurizing the plant for the operation of the SIS. The operation of these valves at the component level is considered to be sufficient to perform the critical safety function.

The adequacy of the automatic functions of the DAS shall be verified as part of the plant procedures program described in Section 13.5. The adequacy of the controls and displays shall be verified in accordance with the human factors V&V program described in Section 18.10.

7.1.2.3.2 SRM to SECY 93-087 II.T – Control Room Annunciator (Alarm) Reliability

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of the SRM to SECY 93-087 II.T (Reference 10). Conformance is provided by these design features:

- Redundant PUs are provided for the transmittal of alarms to the operator workstations in the MCR.
- Multiple workstations are provided in the MCR. Each workstation has the same capabilities with regards to monitoring and control of plant systems.

7.1.2.4 Conformance to Regulatory Guides

7.1.2.4.1 RG 1.22 – Periodic Testing of Protection System Actuation Functions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance RG 1.22. The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.4.2 RG 1.47 – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance RG 1.47. The PICS automatically indicates the bypassed and inoperable status of the safety systems in the MCR. The bypassed and inoperable status of electrical auxiliary support features are described in Section 8.3.

7.1.2.4.3 RG 1.53 – Application of the Single-Failure Criterion to Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.53, which endorses IEEE Std 379-2000 (Reference 11). The redundancy and independence of the applicable I&C systems is described in Section 7.1.1.6.3 and Section 7.1.1.6.4. The FMEA for the PS functions are described in Section 7.2.2.2 and Section 7.3.2.2.

7.1.2.4.4 RG 1.62 – Manual Initiation of Protective Actions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.62. The means for manual initiation of protective functions are described in Section 7.2 and Section 7.3.

7.1.2.4.5 RG 1.75 – Criteria for Independence of Electrical Safety Systems

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.75, which endorses IEEE Std 384-1992 (Reference 12) with modifications. The design features that provide for independence are described in Section 7.1.1.6.4.

7.1.2.4.6 RG 1.97 – Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.97, which endorses IEEE Std 497-2002 (Reference 13) with modifications. Accident monitoring instrumentation is described in Section 7.5.1.2.

7.1.2.4.7 RG 1.105 – Setpoints for Safety-Related Instrumentation

The setpoints for the applicable I&C systems listed in Table 7.1-2 shall be developed using the guidance of RG 1.105, with the exception of those differences described in Instrument Setpoint Topical Report (ANP-10275P) (Reference 14). The setpoint methodology described in ANP-10275P (Reference 14) implements the guidance of Setpoints for Nuclear Safety Related Instrumentation (ANSI/ISA-67.04.01-2006) (Reference 15) which accounts for recent industry advances in setpoint methodologies. ANP-10275P (Reference 14) provides justification for its use as an acceptable method for calculating setpoints.

7.1.2.4.8 RG 1.118 – Periodic Testing of Electric Power and Protection Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.118, which endorses IEEE Std 338-1987 (Reference 16) with modifications. The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.4.9 RG 1.151 – Instrument Sensing Lines

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.151, which endorses ISA-S67.02-1980 (Reference 17) with modifications. The design features of the controls systems that minimize and limit challenges to the PS

failures of a single sensing line common to both protection and control functions are described in Section 7.7. The redundancy and independence of the PS that maintain functionality in the event of a single sensor failure are described in Section 7.1, Section 7.2 and Section 7.3.

7.1.2.4.10 RG 1.152 – Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.152, which endorses IEEE 7-4.3.2-2003 (Reference 18). Conformance to IEEE 7-4.3.2-2003 (Reference 18) is described in Section 7.1.2.6 with the compliance of IEEE 603-1998 (Reference 1).

RG 1.152 also provides additional guidance for cyber security. Conformance to the cyber security elements of RG 1.152 (Regulatory Positions 2.1 through 2.5) are addressed in Section 13.6 as part of the security plan. The standard TXS platform (hardware and operating system) was designed several years prior to the issuance of Revision 2 to RG 1.152. Aspects of the TXS platform design that address the nuclear safety aspects of communication independence, safety to non-safety system isolation and interference-free communication are equally applicable to cyber security. Some elements of the development activities are not explicitly addressed as cyber security activities in EMF-2110(NP)(A) (Reference 3) and the associated NRC safety evaluation report. The development process, including cyber security controls, for TXS application software for U.S. projects is described in ANP-10272 (Reference 5). The cyber security controls for TXS application software development fully meets the intent of Regulatory Positions C.2.1 through C.2.5.

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

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.168, except for the differences described in ANP-10272 (Reference 5) with regards of the use of alternate V&V methods. The methods used for software V&V are described and justified in ANP-10272 (Reference 5).

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

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.169, with the exception that a configuration control board is not used. The methods used for software configuration management plans are described and justified in ANP-10272 (Reference 5).

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

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.170. Refer to ANP-10272 (Reference 5) for a description of the software test documentation.

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

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.171. Refer to ANP-10272 (Reference 5) for a description of software unit testing.

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

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.172. Refer to ANP-10272 (Reference 5) for a description of software requirement specifications.

7.1.2.4.16 RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.173. Refer to ANP-10272 (Reference 5) for a description of software requirement specifications.

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

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.180. The equipment qualification program, which includes EMI/RFI qualification, is described in Section 3.11.

7.1.2.4.18 RG 1.189 – Fire Protection for Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.189. The design of the SICS, PICS, and the RSS are described in Section 7.1.1.3.1, Section 7.1.1.3.2 and Section 7.4.1.3.2. These systems provided the capability to achieve hot and cold shutdown from the RSS in case of a fire. Fiber optic cable is extensively used for communications to the Level 1 I&C systems to reduce the risk of fires and hot shorts. The fire analysis for the U.S. EPR is described in Chapter 9.

7.1.2.4.19 RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.204, which endorses IEEE Std 1050-1996 (Reference 19) and IEEE Std C62.23-1995 (Reference 20). Refer to Section 8.3 for more information on lightning and surge protection for the U.S. EPR.

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

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.209, which endorses IEEE 323-2003 (Reference 21) with modifications. The equipment qualification program is described in Section 3.11.

7.1.2.5 Conformance to Branch Technical Positions**7.1.2.5.1 BTP 7-1 – Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System**

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-1 (Reference 22), with the exception that the applicable RHR valves are not automatically shut upon re-pressurization of the RCS. The RHR suction valve interlocks and a justification for this approach are described in Section 7.6.1.2.1.

7.1.2.5.2 BTP 7-2 – Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-2 (Reference 23). The interlocks associated with the safety injection accumulators are described in Section 7.6.1.1.2.

7.1.2.5.3 BTP 7-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service

The applicable I&C systems listed in Table 7.1-2 are designed to meet the intent of the guidance of BTP 7-3 (Reference 24). Upon a loss of a RCP, a three-loop signal is automatically generated and is used to modify the calculation of various reactor trips described in Section 7.2 to account for the changes in flow rate. This performs the same effect as modifying the setpoint.

7.1.2.5.4 BTP 7-4 – Guidance on Design Criteria for Auxiliary Feedwater Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-4 (Reference 25). Section 7.3 describes the actuation of the EFW system and the FMEA of the PS. Section 10.4.9.3 describes the capability of the EFW system and to withstand a postulated line break, an active single failure, and an LOOP.

7.1.2.5.5 BTP 7-5 – Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-5 (Reference 26). Section 7.7 describes the control and limitation functions that regulate reactor operation. Section 15.4 describes the assumptions and analysis for reactivity and power distribution anomalies.

7.1.2.5.6 BTP 7-8 – Guidance for Application of Regulatory Guide 1.22

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-8 (Reference 27). Section 7.2.2.3.5 and Section 7.3.2.3.6 describes the continuous self testing measures and design for periodic testing. The PS and PACS provide the capability to periodically test actuated equipment at the intervals required by the technical specifications for the process systems in described Chapter 16.

7.1.2.5.7 BTP 7-9 – Guidance on Requirements for Reactor Protection System Anticipatory Trips

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-9 (Reference 28). The reactor trips implemented in the PS meet the requirements of IEEE 603-1998 (Reference 1). The RCSL performs non-safety-related, non-credited partial trips and an anticipatory full reactor trips on a complete loss of feed. Refer to Section 7.7 for further information.

7.1.2.5.8 BTP 7-10 – Guidance on Application of Regulatory Guide 1.97

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-10 (Reference 29). Accident monitoring instrumentation is described in Section 7.5.1.2.

7.1.2.5.9 BTP 7-11 – Guidance on Application and Qualification of Isolation Devices

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of BTP 7-11 (Reference 30). The equipment and means provided for isolation are described in Section 7.1.1.

7.1.2.5.10 BTP 7-12 – Guidance on Establishing and Maintaining Instrument Setpoints

The setpoints for the applicable I&C systems listed in Table 7.1-2 shall be developed using the guidance of BTP 7-12 (Reference 27). The setpoint methodology is described in ANP-10275P (Reference 31).

7.1.2.5.11 BTP 7-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

The applicable I&C systems listed in Table 7.1-2 implement the guidance of BTP 7-13 (Reference 32). The method for cross-calibration of PS resistance temperature detectors (RTD) is provided in Siemens Topical Report EMF-2341P (Reference 31).

7.1.2.5.12 BTP 7-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 shall be developed using the software development and V&V processes described in ANP-10272 (Reference 5).

Conformance with BTP HICB 7-14 (Revision 4 of NUREG 0800, “Standard Review Plan”) is described in ANP-10272 (Reference 5). The topical report identifies specific differences and provides appropriate justification. BTP HICB-14 was used, since it was the version of the guidance in effect at the time the topical report was submitted for approval. AREVA NP provided additional information on alignment with BTP HICB-14 during the review of the topical report. Both BTP HICB-14 (Revision 4, June 1997) and BTP 7-14 (Reference 33) are based on the same regulations, RGs, and endorsed IEEE Standards. As such, acceptance of the topical report, based on these common regulatory requirements, is sufficient to address conformance with BTP 7-14. The software quality assurance plan, software safety plan, software verification and

validation plan, software configuration management plan required by ANP-10272 (Reference 5) are designed to make sure proper implementation of the TXS application software development activities and the proper production of the required design output documents.

7.1.2.5.13 BTP 7-17 – Guidance on Self-Test and Surveillance Test Provisions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-17 (Reference 34). The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.5.14 BTP 7-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-18 (Reference 35). The system hardware, software, and engineering tools used in the PS, SAS and SICS are qualified in accordance with the processes described in Reference 3. Application software is developed using the processes described in ANP-10272 (Reference 5).

7.1.2.5.15 BTP 7-19 – Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-19 (Reference 36), with the exception of providing system level actuation of critical safety functions. The diversity and defense-in-depth (D3) methodology for the U.S. EPR is described in Section 7.1.1.6 and ANP-10284 (Reference 8). Section 7.1.1.4.6 describes the DAS, including architecture, quality and diversity requirements and power supplies. Section 7.8.1.2 describes the functional requirements for the DAS. The D3 analysis is described in Section 7.8.2.2.

Refer to Section 7.1.2.3.1 for a description on the methods that address Point 4 of BTP 7-19 (Reference 36).

7.1.2.5.16 BTP 7-21 – Guidance on Digital Computer Real-Time Performance

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-21 (Reference 37). The design features that provide for real-time, deterministic behavior of the SICS, PS, and SAS are described in EMF-2110(NP)(A) (Reference 3). Acceptable response times for protective actions are described in Section 15.0.

7.1.2.6 Compliance to IEEE Std 603-1998

This section describes compliance to IEEE Std 603-1998 (Reference 1). IEEE Std 603-1998 meets or exceeds the requirements of IEEE Std 603-1991 (Reference 2). By demonstrating compliance to IEEE Std 603-1998, compliance to 10 CFR 50.55a(h) is satisfied.

Where applicable, compliance to a Clauses of IEEE Std 603-1998 (Reference 1) is supplemented with conformance statements to IEEE Std 7-4.3.2-2003 (Reference 18) to address the digital safety systems (SICS, PS, SAS).

The Clauses of IEEE Std 603-1998 (Reference 1) are listed in this section. However, the primary focus of the description in this section is on the systems aspect of compliance. For information that is related primarily to functional requirements, references to other sections of this document are provided.

The scope of the sense and command features includes these systems:

- Safety information and control system.
- Protection system.
- Safety automation system.
- Priority and actuator control system.
- Incore instrumentation system.
- Excore instrumentation system.
- Boron concentration measurement system.
- Radiation monitoring system.
- Process instrumentation (refer to Section 7.2 and 7.3 for details).

The execute features consist of:

- The trip breakers (part of the NUPS).
- The trip contactors (part of the CRDCS).
- Class 1E actuation devices (i.e. switchgear) (part of the Class 1E electrical distribution systems).
- Actuated equipment (part of the process systems).

7.1.2.6.1 Design Basis: Design Basis Events and Corresponding Protective Actions (Clauses 4.a and 4.b)

Compliance to Clauses 4.a and 4.b is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.2 Design Basis: Permissive Conditions (Clause 4.c)

Compliance to Clause 4.c is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.3 Design Basis: Monitored Variables (Clause 4.d)

Compliance to Clause 4.d is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.4 Design Basis: Manual Actions (Clause 4.e)

Manual actions credited in the accident analysis are described in Section 15.0.0. The protective actions and variables used to initiate those actions are described in Section 7.2.2 and Section 7.3.2. Manual actions are executed by the operators from the MCR. The MCR air conditioning regulates the environmental conditions in the MCR to provide an adequate environment for operator actions during normal, abnormal, and accident conditions. The MCR air conditioning system is described in Section 9.4.1. The radiological analysis of the MCR during accident conditions is provided in Section 15.0.3.

7.1.2.6.5 Design Basis: Spatially Dependent Variables (Clause 4.f)

Compliance to Clause 4.f is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.6 Design Basis: Range of Operating Conditions (Clause 4.g)

The safety systems are qualified in accordance with the program described in Section 3.11. This qualification includes:

- Environmental effects (e.g. temperature, humidity).
- Seismic effects.
- EMI/RFI effects.

The safety systems are powered by Class 1E power supplies, including the EUPS and Class 1E power supply system (EPSS). The safety systems are designed to remain functional within the range of voltage and frequency provided. The EPSS and EUPS are described in Section 8.3.

7.1.2.6.7 Design Basis: Protection Against Natural Phenomena and Unusual Events (Clause 4.h)

The safety systems are designed to perform their required functions in the presence of natural phenomena and unusual events, which include seismic events, tornadoes and internal flooding. Refer to Chapter 3 for further information on these events. This is accomplished through the principles of independence described in Section 7.1.1 and equipment qualification described in Section 3.11.

7.1.2.6.8 Design Basis: Reliability Methods (Clause 4.i)

Two methods are used to evaluate the reliability of the safety systems. A FMEA is performed for the PS, and provides a qualitative means of evaluating the reliability of the system.

The probabilistic risk assessment (PRA) is used as a quantitative means for performing reliability analysis. The PRA is described in Chapter 19.

7.1.2.6.9 Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j)

Compliance to Clause 4.j is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.10 Design Basis: Equipment Protection Provisions (Clause 4.k)

The I&C systems provide the capability to implement equipment protection of the safety process systems. Equipment protection can be implemented as an operational I&C function or a safety I&C function. The categorization is derived from process system requirements. Safety I&C functions have priority over operational I&C functions as described in Section 7.1.1.6. Refer to Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10 and Chapter 11 on descriptions of the process systems.

7.1.2.6.11 Design Basis: Special Design Basis (Clause 4.l)

A software CCF of the safety systems is considered in the design. The D3 principles described in Section 7.1.1.6 provide sufficient means to mitigate a software CCF. Section 7.8 describes the D3 analysis.

7.1.2.6.12 Single Failure Criterion (Clause 5.1)

The safety systems meet the requirements of Clause 5.1 of IEEE Std 603-1998 (Reference 1).

The safety systems are arranged in four independent divisions, located in four physically separated Safeguards Buildings. The PS acquires redundant sensors and generally implements 2/4 voting logic to accommodate single failures. This approach also prevents a single failure from resulting in a spurious actuation of process safety-related systems.

Independence is provided so that the redundancy of the safety systems is not defeated due to a single failure. The independence measures provided are described in Section 7.1.1.6.4.

A FMEA for the protective functions executed by the PS is described in Section 7.2.2 and Section 7.3.2. Demonstration of the single failure criterion for the execute features is provided with the description of the process systems in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10 and Chapter 11.

7.1.2.6.13 Completion of Protective Action (Clauses 5.2 and 7.3)

The safety systems meet the requirements of Clause 5.2 of IEEE Std 603-1998 (Reference 1). When initiated by a safety system, protective actions proceed to completion. Return to normal operation requires deliberate operator intervention.

Once opened by the PS, the reactor trip breakers remain open until the reactor trip signal has cleared and they are able to be manually closed. The reactor trip signal is only cleared when the initiating plant variable returns to within an acceptable range.

Refer to Section 7.3.2.2 for a description of completion of protection action for ESF actuation functions.

The execute features within the U.S. EPR are designed so that once initiated, the protective actions continue until completion.

7.1.2.6.14 Quality (Clause 5.3)

The safety systems meet the requirements of Clause 5.3 of IEEE Std 603-1998 (Reference 1). The safety systems are within the scope of the U.S. EPR quality assurance program (QAP) described in Section 17.5. The TXS hardware quality is described in EMF-2110(NP)(A) (Reference 3).

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2-2003. This guidance addresses software quality processes for the use of digital technology in safety systems.

TXS system software is developed in accordance with the processes described in EMF-2110 (NP)(A) (Reference 3).

The application software of the digital safety systems conform to the guidance of IEEE Std 7-4.3.2-2003 (Reference 18), with these exceptions:

- Alternate V&V methods are used. These methods are described and justified in ANP-10272 (Reference 5).
- A configuration control board is not used. The justification for this approach is provided in ANP-10272 (Reference 5).

The application software is developed in accordance with the software development and V&V processes that are summarized in Section 7.1.1.2 and described in detail in ANP-10272 (Reference 5). These processes provide an acceptable method of software development to meet the quality requirements of IEEE Std 603-1998 (Reference 1).

7.1.2.6.15 Equipment Qualification (Clause 5.4)

The safety systems shall meet the requirements of Clause 5.4 of IEEE Std 603-1998 (Reference 1). The equipment used shall be qualified using appropriate methods under the program described in Section 3.11.

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2 (Reference 18). Integrated system testing (including factory acceptance testing and site acceptance testing) is performed as part of the TXS development process described in Section 7.1.1.2 to verify that the performance requirements of the safety functions have been met.

7.1.2.6.16 System Integrity (Clause 5.5)

The safety systems meet the requirements of Clause 5.5 of IEEE Std 603-1998 (Reference 1), and the guidance of Clause 5.5 of IEEE Std 7-4.3.2-2003 (Reference 18).

The systems are designed to perform their functions as described in the design basis. Equipment qualification is performed so that the safety systems perform their function under the range of conditions required for operation. The SICS, PS, SAS and PACS are implemented in four divisions located in physically separated Safeguards Buildings with electrical and communications independence measures.

The PS implements a fail-safe design. The reactor trip breakers are de-energized to trip, so that a reactor trip occurs on a loss of power. ESF actuations are energized to actuate, so a loss of power results in a fail as-is condition.

For digital safety systems, these provide for system integrity:

- Design for computer integrity.
- Design for test and calibration.
- Fault detection and diagnostics.

The processing principles of the TXS platform described in Section 7.1.1.2 provide for real-time, deterministic operation of the safety systems. The processing is independent of changes in process variable and other external effects.

The TXS platform is designed for in-service testing and calibration, as well as inherent fault detection and diagnostics. These include features such as message error checks and a watchdog timer circuit. Refer to IEEE Std 603-1998 (Reference 1) for further information.

7.1.2.6.17 Independence (Clause 5.6)

The safety systems meet the independence requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2 (Reference 18).

The features that provide for independence are described in Section 7.1.1.6.4.

7.1.2.6.18 Capability for Testing and Calibration (Clause 5.7)

The safety systems meet the requirements of Clause 5.7 of IEEE Std 603-1998 (Reference 1). Refer to Section 7.2.2 and Section 7.3.2 for information regarding the capability for testing and calibration.

7.1.2.6.19 Information Displays (Clause 5.8)

The safety systems meet the requirements of Clause 5.8 of IEEE Std 603-1998 (Reference 1). Displays and control are provided by the SICS for those manual actions described in Section 15.0.0. The displays meet the requirements of IEEE 497-2002. Refer to Section 7.2, Section 7.3 and Section 7.5 for further information.

The safety systems provide to the PICS their bypassed and inoperable status. This allows the operator to identify the specific bypassed functions and determine the state of actuation logic.

The arrangement of displays and controls shall be determined using the HFE principles described in Chapter 18.

7.1.2.6.20 Control of Access (Clause 5.9)

The safety systems meet the requirements of Clause 5.9 of IEEE Std 603-1998 (Reference 1).

Access to the cabinets of the SICS, PS, SAS and PACS are provided via doors that are normally closed and locked. Door positions are monitored allowing operators the ability to investigate unexpected opening of cabinet doors. Cabinets are also located in physically separate equipment rooms within the four Safeguards Buildings and can only be accessed by authorized personnel.

Access to software of the digital safety systems is limited to the SU. The SU and the safety systems have multiple features to control access and prevent unauthorized changes to software including:

- Authorized personnel may only access the SU.
- Access to the SU is password protected.
- Access is provided to the safety computers via the MSI.
- The Class 1E MSI, which serves as a communication isolation point between a division of PS or SAS and the SU, prevents unauthorized communication from entering the division and affecting the safety processors.

The computer terminals for the SUs are located in the I&C service center (I&C SC). Additional control of access measures are provided in Reference 3.

The SICS equipment is located in the MCR and RSS. Both rooms are controlled security areas. Refer to Section 7.1.1 for a description of access controls for the QDS.

7.1.2.6.21 Repair (Clause 5.10)

The safety systems meet the requirements of Clause 5.10 of IEEE Std 603-1998 (Reference 1).

Safety systems built upon the TXS platform contain self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities. Details on the self-test diagnostic capabilities are provided in EMF-2110(NP)(A) (Reference 3).

The PACS contains self-diagnostic test features to alert plant personnel of a fault within one of the PACS components. More information on self-diagnostic capabilities within PACS components is presented in ANP-10273P (Reference 4).

7.1.2.6.22 Identification (Clause 5.11)

The safety systems meet the identification requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18).

Redundant divisions of each safety system are distinctively marked. Equipment within a cabinet that belongs to the same train as the cabinet marking does not contain additional identification. However, equipment within a cabinet that is not the same train as the cabinet marking is marked to show its different train assignment. Equipment within the safety system cabinets that is too small to carry an identification plate are housed in larger equipment clearly marked as part of a single redundant division of that safety system. Versions of hardware are marked accordingly. Configuration management is used for maintaining identification of safety-related software.

7.1.2.6.23 Auxiliary Features (Clause 5.12)

The safety systems meet the requirements of Clause 5.12 of IEEE Std 603-1998 (Reference 1).

The safety systems include the scope of auxiliary supporting features, which are described in Chapter 8 and Chapter 9. These systems include EUPS, EPSS, and safety-related HVAC systems throughout the plant.

Other auxiliary features that are not required to be operable for the safety systems to perform their functions (e.g. SU) are designed to meet criteria that does not degrade the safety functionality of the safety systems below an acceptable level.

7.1.2.6.24 Multi-Unit Stations (Clause 5.13)

The safety systems meet the requirements of Clause 5.13 of IEEE Std 603-1998 (Reference 1).

The U.S. EPR is design as a single-unit plant. If multiple units are constructed at the same site, safety systems are not shared between sites.

7.1.2.6.25 Human Factors Considerations (Clause 5.14)

The safety systems meet the requirements of Clause 5.14 of IEEE Std 603-1998 (Reference 1).

Human factors are considered throughout the design of the safety systems in accordance with the HFE principles described in Chapter 18.

7.1.2.6.26 Reliability (Clause 5.15)

The safety systems meet the reliability requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18).

The safety systems are designed to accomplish their safety functions in a reliable manner to support overall plant availability. High reliability is provided through various features including:

- Highly redundant architecture.
- Reliable equipment.
- Independent subsystems within each division of the PS to implement functional diversity.
- Continuous online fault detection and accommodation abilities.
- High quality software design process.
- Strong operating experience of the TXS platform.

The safety systems (including software) are analyzed as part of the PRA, which is described in Chapter 19.

7.1.2.6.27 Common Cause Failure Criteria (Clause 5.16)

The safety systems meet the requirements of Clause 5.16 of IEEE Std 603-1998 (Reference 1).

The U.S. EPR architecture is designed so that plant parameters are maintained within acceptable limits established for each DBE in the presence of a single, credible common cause failure. The defense-in-depth and diversity principles that minimize the probability of a CCF and mitigate the consequences of a CCF are described in Section 7.1.1.6.1 and ANP-10284 (Reference 8). The D3 analysis is provided in Section 7.8.

7.1.2.6.28 Automatic Control (Clauses 6.1 and 7.1)

The safety systems meet the requirements of Clauses 6.1 and 7.1 of IEEE Std 603-1998 (Reference 1).

The various Level 0 systems provide signals representing the state of the process systems to the Level 1 safety systems.

The PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of DBEs. The PS automatically initiates appropriate safety functions whenever a measured variable exceeds a predefined setpoint.

The SAS is designed to perform ESF control functions and automated safety-related closed loop control functions once the safety-related process systems have been initiated by the PS.

The PACS is designed to automatically prioritize signals issued to safety-related actuators and monitor drive and actuator status for the execute features. The priority principles are described in Section 7.1.1.6.5.

The execute features within the U.S. EPR receive and act upon automatic control signals from the safety systems. Reactor trip output signals from the PS result in an opening of the reactor trip devices. Output signals for ESF actuation from the PS are sent to the PACS. The ESF control signals from the SAS are also sent to the PACS. The PACS prioritizes the signals from the PS and SAS and produces an output signal to the execute features.

7.1.2.6.29 Manual Control (Clauses 6.2 and 7.2)

The safety systems meet the requirements of Clauses 6.2 and 7.2 of IEEE Std 603-1998 (Reference 1).

Manual actuation of protective actions is possible from the SICS. The means provided minimize the amount of discrete operator manipulations, and depend on a minimum of equipment. Refer to Section 7.2 and Section 7.3 for the methods provided to initiate these functions.

Controls and indications are provided for those manual actions credited in the accident analyses described in Section 15.0.0. The controls are described in Section 7.2, Section 7.3 and Section 7.4. Type A variables are selected using the process described in Section 7.5.

The SICS provides the means to achieve and maintain safe shutdown following a DBE. This capability is provided through appropriate controls and indications. Refer to Section 7.4 and Section 7.5 for further information safe shutdown.

The execute features within the U.S. EPR are capable of receiving and acting upon manual control signals from the sense and command features. Manual control of equipment within the execute features is provided by the SICS and the PICS. Manual control of the execute features has a lower priority than the automatic actuation and control signals from the PS and SAS, consistent with the priority rules provided in Section 7.1.1.6.5.

7.1.2.6.30 Interaction between the Sense and Command Features and Other Systems (Clause 6.3)

The safety systems meet the requirements of Clause 6.3 of IEEE Std 603-1998 (Reference 1).

Sensors are shared between the safety and non-safety I&C systems for the execution of different functions (e.g., control, protection, diverse actuation, etc.). The sharing of sensors minimizes the amount of penetrations required in the various components in the RCS. This reduces the probability of small breaks in the RCPB and also reduces the amount of required piping.

These measures are provided that minimize the impact of a single, credible failure:

- The control systems (PAS, RCSL) are implemented using redundant controllers.

- The control systems (PAS, RCSL) implement signal selection algorithms that accommodate a single sensor failure. Refer to Section 7.7 for more information.
- The PS and SAS are implemented in four, independent divisions.
- The PS generally implements 2/4 voting. A single failed sensor does not result in a spurious action of safety-related equipment. Refer to Section 7.2 and Section 7.3 for more information.
- The SAS implements signal selection algorithms for critical control loops that accommodate a single sensor failure. Refer to Section 7.3 for more information.
- The DAS generally implements 2/4 voting. A single failed sensor does not result in a spurious action of the safety-related equipment. Refer to Section 7.8 for more information.
- Independence between the safety-related and non-safety-related systems. The independence measures provided are described in Section 7.1.1.6.4.

7.1.2.6.31 Derivation of System Inputs (Clause 6.4)

The safety systems meet the requirements of Clause 6.4 of IEEE Std 603-1998 (Reference 1).

The signals used in the sense and command features are direct measures of the desired variable in the design basis. The variables used for the inputs to the PS are described in Section 7.2 and Section 7.3.

The U.S. EPR implements an evolutionary means of reactor protection by acquiring a three-dimensional measurement of reactor flux through the use of the SPNDs. The SPNDs provide the inputs to the high linear power density (HLPD) reactor trip and low departure from nucleate boiling ratio (DNBR) reactor trip described in Section 7.2. The use of actual incore parameters in protection functions reduces the uncertainty associated with previous methods.

7.1.2.6.32 Capability for Testing and Calibration (Clause 6.5)

The safety systems meet the requirements of Clause 6.5 of IEEE Std 603-1998 (Reference 1).

Sensors are tested at intervals described in Chapter 16. The methods of testing including:

- Perturbing the monitored variable.
- Provide a substitute input to the sensor (e.g. calibrated source for a pressure sensor).
- Cross checking channels that have known relationships.

Operational availability during an accident may be verified using one of the above methods, or by specifying the time period it retains its calibration.

7.1.2.6.33 Operating Bypass (Clauses 6.6 and 7.4)

The safety systems meet the requirements of Clause 6.6 and 7.4 of IEEE Std 603-1998 (Reference 1).

Operating bypasses are implemented using permissive signals from the PS. If the plant conditions associated with allowing operational bypasses are not met, the PS automatically prevents the activation of the operating bypass.

When an operating bypass is in effect, indication of this condition is provided to the MCR. If plant conditions change during activation of an operating bypass, and the operating bypass is no longer permissible, in general the PS automatically removes the appropriate active operating bypass.

Low temperature overpressure protection (LTOP) of the RCS is normally bypassed using P17 when at power. During shutdown operations, LTOP protection is enabled when P17 is manually validated by the operator once the conditions for P17 are satisfied. This is a controlled evolution governed by plant operating procedures. This is consistent with the guidance provided in BTP 5-2 (Reference 38), industry precedent, and meets the intent of Clause 6.6 of IEEE Std 603-1998 (Reference 1). Refer to Section 5.2 for more information about LTOP.

Refer to Section 7.2 and Section 7.3 for further information on permissives and the operating bypasses of the protective functions.

7.1.2.6.34 Maintenance Bypass (Clauses 6.7 and 7.5)

The safety systems meet the requirements of Clause 6.7 of IEEE Std 603-1998 (Reference 1).

The safety systems are designed to permit channel bypass for maintenance, testing, or repair. Individual function computers of the SICS, PS and SAS can be placed into testing and diagnostic modes via the SU. The function computer being tested automatically changes its outputs to the associated I/O modules to test status, and communication from the unit under test is disregarded by the remainder of the system. This bypass is accomplished during power operation without causing initiation of a protective function, and single failure criterion are still met as the protection functions associated with the function computer in test status are duplicated in other redundant computers within the PS and SAS.

Sufficient redundancy and administrative controls that manage reduction of redundancy exist within each system to maintain acceptable reliability when a portion of the execute features is placed in bypass.

7.1.2.6.35 Sense and Command Features: Setpoints (Clause 6.8)

The safety systems meet the requirements of Clause 6.8 of IEEE Std 603-1998 (Reference 1).

Allowance for uncertainties between the process analytical limit and the setpoint used in the protective functions of the PS is determined using a documented methodology. The U.S. EPR setpoint methodology is described in ANP-10275P (Reference 14). The methodology developed establishes that setpoints used within the PS are determined so that plant safety limits are not exceeded.

Where multiple setpoints are used for adequate protection under different plant conditions, the more restrictive setpoint is used when required. The logic that detects the need to change setpoints is part of the PS. Refer to Section 7.2 and Section 7.3 for functions that use multiple setpoints.

7.1.2.6.36 Electrical Power Sources (Clause 8.1)

The safety systems meet the requirements of Clause 8.1 of IEEE Std 603-1998 (Reference 1).

The safety systems are powered by the EUPS and EPSS. These systems provide reliable, Class 1E power that is backed by the EDGs. The EUPS provides uninterruptible power in case of an LOOP. Refer to Section 8.3 for information regarding the EUPS and EPSS.

7.1.2.6.37 Non-electrical Power Sources (Clause 8.2)

The safety systems do not rely on non-electrical power sources for operation. The requirements for actuated equipment that utilize non-electrical power sources (e.g., compressed gas or media actuated valves) are described within the process system descriptions.

7.1.2.6.38 Maintenance Bypass (Clause 8.3)

The safety systems can perform their safety functions while power source are in maintenance bypass. Details on the electrical power systems that fulfill this requirement are described in Chapter 8.

7.1.3 References

1. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1998.
2. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," 1991.
3. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

4. ANP-10273P, Revision 0, "AV42 Priority Actuation and Control Module Topical Report," AREVA NP Inc., November 2006.
5. ANP-10272, Revision 0, "Software Program Manual TELEPERM XS™ Safety Systems," AREVA NP Inc., December 2006.
6. ANP-10281P, Revision 0, "U.S. EPR Digital Protection System Topical Report," AREVA NP Inc., March 2007.
7. ANP-10287P, Revision 0, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," AREVA NP Inc., November 2007.
8. ANP-10284, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007.
9. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
10. SRM to SECY 93-087 II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," United States Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, 1993.
11. IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," 2000.
12. IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1992.
13. IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," 2002.
14. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., March 2007.
15. ANSI/ISA-67.04.01-2006, "Setpoints for Nuclear Safety Related Instrumentation," 2006.
16. IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," 1987.
17. ISA-67.02-1980, "Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," 1980.
18. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," 2003.
19. IEEE 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," 1996.
20. IEEE Std C62.23-1995, "IEEE Application Guide for Surge Protection of Electric Generating Plants," 1995.

21. IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," 2003.
22. BTP 7-1, "Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
23. BTP 7-2, "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
24. BTP 7-3, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
25. BTP 7-4, "Guidance on Design Criteria for Auxiliary Feedwater Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
26. BTP 7-5, "Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
27. BTP 7-8, "Guidance for Application of Regulatory Guide 1.22," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
28. BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
29. BTP 7-10, "Guidance on Application of Regulatory Guide 1.97," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
30. BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
31. BTP 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
32. BTP 7-13, "Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
33. BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

-
34. BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
 35. BTP 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
 36. BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
 37. BTP 7-21, "Guidance on Digital Computer Real-Time Performance," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.
 38. BTP 5-2, "Overpressurization Protection of Pressurized-Water Reactors While Operating at Low Temperatures," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

Table 7.1-1—Levels of Redundancy in I&C Architecture

I&C System	Level of Redundancy
SICS	4
PICS	2
PS	4
SAS	4
PACS	4
SA I&C	4 (Note 1)
RCSL	2 (Note 2)
PAS (NIS, TIS, BPS)	2
PAS (DAS)	4
TG I&C	2 (Note 3)

Notes:

1. SA I&C is implemented with four divisions of I&C. Plant severe accident mitigation features are implemented with varying levels of redundancy.
2. RCSL is a redundant control system, but acquires sensor inputs in all four divisions.
3. This is the minimum level of redundancy for the TG I&C.