7.0 Instrumentation and Controls

7.1 Introduction

Chapter 7 describes the instrumentation and controls (I&C) systems for the U.S. EPR. 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 U.S. EPR I&C systems and the design features associated with these systems.

Figure 7.1-1—Chapter 7 Symbol 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.

Anticipated Operational Occurrence (AOO) - anticipated operational occurrences mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to the recirculation pumps, tripping of the turbine generator (TG) set, isolation of the main condenser, and loss of offsite power.

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.

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

Control Unit (CU) - a functional unit in an I&C system that contains a function processor. A Control Unit is a generic functional term and is neither system nor technology specific. Generally, a CU consists of function processors, I/O modules, and communication modules necessary to implement its functions. However, specific details of each system design are unique to the technology chosen to implement its functions.

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.

Checkback – a signal that contains information about the completion of an actuation order. This signal can be used in an automatic function or displayed to the operator.

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.

Manual Component Control – a single operator action results in a single actuated component being operated.

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.

Discrete – a distinct, quantifiable value from one of two states (e.g., TRUE/FALSE or ON/OFF)

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.

Electrical I&C Technology – I&C technology that is based on electro-mechanical components. Examples include relays, buttons, switches, and contactors.

Electronic I&C Technology – I&C technology that is based on solid state components. Examples include transistors, diodes, discrete logic gate, A/D converters, and digital potentiometers.

Feedback – a signal that is used in a control function to manipulate a variable to a desired result.

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 programmable electronic system hardware, system software, and engineering tools that can be configurated for a wide variety of instrumentation and control functions.

Hardwired Signal – an analog or binary signal that does not use a data communications protocol.

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

Latched Signal – a signal which is generated (set) when a process condition appears and is maintained even after the process condition is cleared. A signal can be unlatched (reset) either automatically or manually. The memory logic block (U.S. EPR FSAR, Tier 2, Figure 7.1-1) is one means of latching/unlatching a signal.

Manual Grouped Control – a single operator action results in two or more actuated components being operated.

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.

Postulated Accident (PA) - unanticipated occurrences that are postulated to occur but are not expected to occur during the life of the nuclear plant unit.

Programmable Electronic I&C Technology - I&C technology that is based on solid state components whose function is programmed via software. Common forms of programmable electronic I&C technology are microprocessor based, PLD based, or FPGA based.

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-Related 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-Related 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 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 – the layers of software that are not configured uniquely for a specific I&C application. System software has a different functional purpose compared to "application software" (defined above) and is the same on all TXS processors. In contrast, application software is configured to reflect a nuclear power plant's specific safety system functional requirements, different application software functions reside on individual TXS processors within the overall TXS system. For TELEPERM XS, system software is defined as the operating system and platform software layers shown in Figure 3.5 of EMF-2110(NP)(A) (Reference 3).

Vote:

- 1 out of x, where x is the number of inputs to the logic block. If one or more inputs is TRUE, then the output will be TRUE. This logic may implemented with an OR gate.

- x out of x, where x is the number of inputs to the logic block. If x number of inputs are TRUE, then the output will be TRUE. This logic may be implemented using an AND gate.

- y out of x, where x is the number of inputs to the logic block and y is a value between 2 and x minus 1. If the number of inputs equal or greater than y is TRUE, then the output will be TRUE.

7.1.1 U.S. EPR I&C Systems

7.1.1.1 Overview

The U.S. EPR implements a modern I&C design. The U.S. EPR I&C systems implement these design features to optimize overall plant safety:

- Use of state of the art I&C technology:

  The I&C design maximizes the use of programmable electronic I&C technology. Many features of this technology 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 primary I&C systems used for control and monitoring in the plant are collectively referred to as the distributed control system (DCS). The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. Section 7.1.1.3 and Section 7.1.1.4 describe the DCS and its constituent subsystems. Section 7.1.1.6

describes the design principles of the DCS. Figure 7.1-2 and Figure 7.1-22—Distributed Control System Physical Architecture show the U.S. EPR DCS design.

The DCS implements functional requirements specified by the various plant mechanical and electrical systems, provided in the following list. The allocation of these functional requirements within the DCS is shown in Table 7.1-3—DCS Functional Requirements Allocation Matrix:

- The process control functions are described in Section 7.7.
- The process limitation functions are described in Section 7.7.
- The reactor trip functions are described in Section 7.2.
- The engineered safety feature (ESF) actuation functions are described in Section 7.3.
- The safety control functions are described in the following sections:
  - The control of safety systems in continuous operation is described in Chapter 8 and Chapter 9.
  - The control of safety systems following ESF actuation is described in Section 7.3.
  - The control of safety systems to reach and maintain safe shutdown is described in Section 7.4.
- The safety interlock functions are described in Section 7.6.
- The severe accident control functions are described in Chapter 19.
- The diverse reactor trip functions are described in Section 7.8.
- The diverse ESF actuation functions are described in Section 7.8.
- The process indications are described in Chapters 5, 6, 8, 9, 10, and 11.
- The post-accident monitoring (PAM) indications are described in Section 7.5.
- The severe accident indications are described in Chapter 19.
- The alarms are described in Section 7.5.

Black box I&C systems in the plant include dedicated systems for specific functions, such as acquisition and processing of neutron flux measurements. Section 7.1.1.5 describes these systems.

I&C equipment is also contained in mechanical and electrical systems. This equipment includes instrumentation and black boxes for packaged equipment, such as emergency diesel generators (EDGs). I&C equipment contained in mechanical and electrical systems are described in Chapters 5, 6, 8, 9, 10, and 11.

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

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

The U.S. EPR implements the TXS platform as described in TELEPERM XS: A Digital Reactor Protection System Topical Report (EMF-2110(NP)(A) (Reference 3) with the following exceptions:

- Defense-in-depth and diversity is implemented as described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 8).
- Surveillance testing of protective functions is performed in accordance with the U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report (ANP-10315P) (Reference 46).

The associated NRC Safety Evaluation Report (SER) for Reference 3 lists seventeen action items to be addressed for implementation of a TXS platform. Those seventeen action items are listed and addressed for the U.S. EPR as follows:

1. "The licensee must demonstrate that the generic qualification bounds the plant specific condition (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the TXS equipment is to be installed. The generic qualification data must comply with U.S. EPRI qualification requirements specified in EPRI TR-107330 and TR-102323-R1."
   The U.S. EPR design implements requirements contained in EPRI TR-107330 for the TXS I&C systems listed in Table 7.1-2 (SICS, PS, SAS, RPMS) by meeting the requirements of 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 are designed to meet the guidance of RG 1.209, which endorses IEEE Std 323-2003 (Reference 21) with modifications. The equipment qualification program is described in Section 3.11. The electromagnetic compatibility (EMC) requirements in EPRI TR-102323, Rev 3, are applicable to the TXS I&C systems as shown in Table 3.11-1.

2. "The licensee's plant-specific software development V&V activities and configuration management procedures must be equivalent to industry standards and practices endorsed by the NRC (as referenced in SRP BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"."
   The U.S. EPR design implements BTP 7-14 requirements for the TXS I&C systems listed in Table 7.1-2 (SICS, PS, SAS, RPMS) by using the software development

and V&V processes described in ANP-10272-A (Reference 5). The full extent of the concerns captured in ANP-10272-A will be addressed by the combined license (COL) applicant, as described in Section 7.1.1.2.2. Section 7.1.3.5.12 provides additional clarification.

3. "If the licensee develops a TXS auxiliary feedwater control system, the licensee must include automatic initiation and flow indication (TMI Action Plan Item II.E.1.2). The licensee needs to confirm that the plant-specific application conforms to the requirements of 10 CFR 50.34 (f)(2)(xii)."
   The U.S. EPR design implements the requirements of 10 CFR 50.34 (f)(2)(xii) for the PS, SCDS, PACS and SICS systems associated with the Emergency Feedwater Control as listed in Table 7.1-2 and detailed in Section 7.5.2.1.1.

4. "If the licensee replaces existing accident monitoring instrumentation (TMI Action Plan Item II.F.1) display capabilities with a TXS system, including the bypass and inoperable status information, the licensee needs to confirm that the new system provides equivalent sampling and analyzing features, and meets the requirement of 10 CFR 50.34 (f)(2)(xvii)."
   The U.S. EPR design implements the requirements of 10 CFR 50.34 (f)(2)(xvii) for the SCDS and SICS systems associated with the accident monitoring instrumentation as listed in Table 7.1-2 and detailed in Section 7.5.2.1.1.

5. "If the licensee installs a TXS inadequate core cooling detection system, the licensee needs to confirm that the new system conforms to the requirements of 10 CFR 50.34(f)(2)(xviii)."
   The U.S. EPR design implements the requirements of 10 CFR 50.34 (f)(2)(xviii) for the SCDS, Incore, SICS, and PS systems associated with the inadequate core cooling detection system as listed in Table 7.1-2 and detailed in Section 7.5.2.1.1.

6. "If the licensee installs a TXS containment isolation system (TMI Action Plan Item II.E.4.2), the licensee must verify that the plant-specific application conforms to the requirement of 10 CFR 50.34 (f)(2)(xiv)."
   The U.S. EPR design implements the requirements of 10 CFR 50.34 (f)(2)(xiv) for the PACS, PS, and SCDS systems associated with the containment isolation system as listed in Table 7.1-2 and detailed in Section 7.1.3.1.7.

7. "For monitoring plant conditions following core damage, the licensee must verify that the TXS system meets the processing and display portions of the requirements of 1 0 CFR 50.34(f)(2)(xix)."
   The U.S. EPR design implements the requirements of 10 CFR 50.34 (f)(2)(xix) for the SICS, SCDS, Excore, Incore, and BCMS systems associated with monitoring plant conditions following core damage as listed in Table 7.1-2 and detailed in Section 7.5.2.1.1.

8. "If the licensee installs a TXS system for monitoring reactor vessel water level during post -accident conditions, the licensee must provide plant-specific verification of the ranges, and confirm that human factors issues have been addressed, as required by 1 0 CFR 50.34(f)(2)(xxiv)."
   The U.S. EPR reactor pressure vessel level (RPVL) measurement system is classified as non-safety-related, supplemented grade (NS-AQ), and is not

implemented with the TXS platform, so this requirement is not applicable to the U.S. EPR.

9. "If the licensee installs a TXS reactor protection system, the licensee must provide confirmation that the TXS system is diverse from the system for reducing the risk from anticipated transients without scram (ATWS), as required by 10 CFR 50.62. If the licensee installs a TXS ESFAS, the licensee must provide confirmation that the diversity requirements for plant systems (e.g., feedwater, auxiliary feedwater, turbine controls) are maintained."
   The U.S. EPR design implements the requirements of 10 CFR 50.62 for the DAS, SCDS and PACS systems associated with anticipated transients without scram as listed in Table 7.1-2 and detailed in Section 7.8.2.1.3.

10. "Setpoints will be evaluated on a plant-specific basis. The licensee must ensure that, when the TXS system is installed, overly conservative setpoints that may occur due to the elimination of analog system drift are not retained, as this would increase the possibility that the TXS equipment may be performing outside the vendor specifications. The licensee must provide the staff with a revised setpoint analysis that is applicable to the installed TXS system(s)."
    The U.S. EPR design implements TXS system setpoints on a plant-specific basis by the applicable Chapter 16 COLA Setpoint Control Program.

11. "The licensee must evaluate plant-specific accident analyses to confirm that a TXS reactor trip system (RTS) includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with the accident analysis presented in Chapter 15 of the plant safety analysis report"
    The Chapter 15 U.S. EPR safety analysis confirms that the TXS RTS includes the provisions to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown consistent with the accident analysis. The accident analysis accuracy and response time values are described in Table 15.0-7. Table 7.2-3 describes the PS (a TXS system) response times used for reactor trip functions.

12. "The staff requires that each licensee ensure that the plant-specific TXS application complies with the criteria for defense against common-mode failures in digital instrumentation and control systems."
    The U.S. EPR design implements the requirements for defense against common-mode failures in digital instrumentation and control systems by incorporation of Reference 8, ANP-10304, Revision 4, "U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report."

13. "The licensee should propose plant-specific Technical Specifications including periodic test intervals."
    The U.S. EPR FSAR includes Technical Specifications with periodic test intervals for TXS I&C systems in Chapter 16.

14. "The licensee should demonstrate that the power supply to the TXS system complies with EPRI TR-1 07330 requirements."
    The U.S. EPR design implements requirements contained in EPRI TR-107330 for

the TXS I&C systems listed in Table 7.1-2 (SICS, PS, SAS, RPMS) by meeting the requirements of 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 are designed to meet the guidance of RG 1.209, which endorses IEEE Std 323-2003 (Reference 21) with modifications. The equipment qualification program is described in Section 3.11.

15. "The licensee should demonstrate that the qualification of the isolation devices were performed in accordance with EPRI TR-1 07330 requirements."
The U.S. EPR isolation devices meet the requirements of BTP 7-11 – Guidance on Application and Qualification of Isolation Devices. The TXS systems listed in Table 7.1-2 (SICS, PS, SAS, Excore, Incore, BCMS, RPMS, PACS, SCDS) are 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. Additionally, guidelines for environmental qualification per EPRI TR-107330 for the TXS I&C systems listed in Table 7.1-2 (SICS, PS, SAS, RPMS) by meeting the requirements of RG 1.209 – Guidelines for Environmental Qualification of Safety-Related Computer-based Instrumentation and Control Systems in Nuclear Power Plants.

16. "The licensee should demonstrate that Siemens TXP (control systems) or other manufacturer's control systems satisfy the acceptance guidance set forth in Section 4.1 of this safety evaluation."
The U.S. EPR design implements the requirements set forth in Section 4.1 of the safety evaluation for the TXS Topical Report by incorporation of Reference 8, ANP-10304, "U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report."

17. "The licensee should address the need for a requirement traceability matrix (RTM) for enumerating and tracking each system requirement throughout its life cycle, particularly as part of making future modifications".
The U.S. EPR design implements the Requirements Traceability Matrix through Reference 5, ANP-10272-A, Revision 3, "Software Program Manual TELEPERM XS™ Safety Systems Topical Report," which describes the standard engineering process used to develop TELEPERM XS Application Software for U.S. projects. The Software Program Manual is used to address plant-specific action items 2 and 17 from the NRC Safety Evaluation Report for the TELEPERM XS Topical Report. Action item 17 is addressed by the inclusion of the Application Software Requirements Traceability Matrix as a required development process document.

7.1.1.2.1 TXS Platform Design

The TXS platform is described in Reference 3. Because of advances in technology and rapid obsolescence of components, the various modules described in Reference 3 will be modified and upgraded over time, and new modules will be developed. The design and qualification of new or upgraded TXS hardware and system software used in U.S. EPR plants will be performed in accordance with the methods described in Reference 3.

7.1.1.2.2 Application of the TXS Platform

TELEPERM XS Software Topical Report (ANP-10272-A) (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 verification and validation (V&V) processes. These phases are listed below along with the primary activities included in each phase:

- Basic design:
  - System requirements.
  - System design.
  - Software requirements.
  - Initiate software requirements traceability.
  - Summary reports for V&V activities (i.e., acquisition support, planning, concept, and requirements).
- Detailed design:
  - Software design.
  - Automatic code generation.
  - Application software integration validation test planning (using an NRC-approved simulation test tool).
  - Application software integration validation test execution (using an NRC-approved simulation test tool).
  - Application software integration validation test reporting (using an NRC-approved simulation test tool).
  - Software safety analyses.
  - Continue software requirements traceability.
  - Hardware design.
  - Summary reports for V&V activities (i.e., design and implementation).
- Manufacturing:
  - Hardware manufacturing.
  - Approval of supplier manufactured, tested hardware, and required supplier hardware documentation.

- Cabinet design.
- Cabinet internal wiring design.

- System integration and testing:
  - Integration of hardware and software.
  - Software integration, system and acceptance validation test planning.
  - Software integration, system and acceptance validation test execution.
  - Software integration, system and acceptance validation test reporting.
  - Continue software requirements traceability.
  - Summary reports for V&V activities.
- Installation and commissioning:
  - Installation and commissioning test planning.
  - Installation and commissioning test execution.
  - Installation and commissioning test reporting.
  - Summary reports for V&V activities.
- Final Documentation:
  - Generation of final documentation before system is placed in service.

The primary documentation generated as outputs of each of these phases is described in ANP-10272-A (Reference 5), Section 4.5.

The U.S. EPR I&C systems supported by the TXS platform are described in Sections 7.1.1.4.1, 7.1.1.4.2, and 7.1.1.4.5 for review against NRC regulations and guidance. The U.S. EPR-specific system architectures supersede the example system architectures that were included in EMF-2110(NP)(A) (Reference 3) to provide context for the review of the generic TXS platform.

A COL applicant that references the U.S. EPR design certification will establish a plan to address the site-specific implementation of the limitation and conditions identified in Section 4 of the NRC Safety Evaluation for Topical Report ANP-10272A, “Software Program Manual for TELEPERM XS Safety Systems.”

7.1.1.2.3 Reliability of Communications with the TXS Platform in the U.S EPR

The safety-related I&C systems use proprietary, time-triggered operating systems that do not rely on hardware and interrupt only on cyclic processing of the software. Because there are no process-driven interrupts, every operation is cyclic and predictive, which verifies that the output of messages on networks links prevents collision.

The hardware components only read the incoming memory buffer or generate a packet to send only when the operating system generates the order. The cyclic operations of the processing units verify that the operator does not simultaneously perform a reading and writing operation.

The communication process sends information written in memory and writes in memory received information. Packet numbering verifies that information is only processed once and that the information is processed without relying on synchronizing both tasks.

For the U.S. EPR, only the TXS Profibus communication protocol is used for safety-related communications. See EMF-2110(NP)(A) (Reference 3) for more information on the TXS Profibus protocol.

7.1.1.3 DCS HMI Systems

7.1.1.3.1 Safety Information and Control System

The SICS is provided as a safety-related HMI and is specifically designed to provide the operator the necessary inventory of controls and indications for the following:

- Mitigation of anticipated operational occurrences (MCR).
- Mitigation of postulated accidents (MCR).
- Reach and maintain safe shutdown (MCR and RSS).
- Mitigation of anticipated operational occurrences concurrent with a CCF of the PS (MCR).
- Mitigation of postulated accidents concurrent with a CCF of the PS (MCR).
- Mitigation of severe accidents (MCR).
- Diverse and flexible mitigation strategies (FLEX) (MCR). See NEI 12-06 (Reference 47) and ANP-10329 (Reference 48) for more information about FLEX.

The SICS in the MCR is not normally used by the operator. The SICS is used under the following conditions:

- For controls not available on PICS (such as manual RT, ESFAS, and permissives).
- When PICS is not available.

SICS in the RSS is used to operate controls not available on PICS in the RSS to reach and maintain safe shutdown following an evacuation of the MCR.

Classification

The SICS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the SICS.

Interfaces

Table 7.1-4—DCS Interface Matrix shows the interfaces of the SICS.

Architecture

Figure 7.1-2 shows the basic architecture of the SICS.

Figure 7.1-3—Safety Information and Control System Architecture (QDS Portion) shows the QDS architecture.

The SICS provides control capabilities in the main control room (MCR) and limited control capabilities in the remote shutdown station (RSS). At each control location, the inventory of controls and indications is laid out in accordance with relevant electrical separation criteria and the HFE principles described in Chapter 18.

The controls and indications required to be on the SICS are implemented with dedicated, hardwired I&C. In addition, a subset of plant parameters are duplicated on the non-safety-related QDS for situational awareness. Chapter 18 describes the subset of parameters chosen are selected in accordance with the HFE principles. The non-safety-related QDS is capable of trending of information, including Type A, B, and C PAM variables, needed to provide situational awareness by the operator.

Each QDS receives input only from the four divisions of the protection system (PS). Isolation between the PS and the QDS is provided by the PS. The four QDS shown on Figure 7.1-2 are a nominal number. The final number and placement of the QDS is determined in accordance with the HFE principles described in Chapter 18.

The QDSs have dedicated non-safety-related SUs for service and maintenance of the QDS. The number and location of SUs is determined based on the number and layout of QDSs.

Equipment

The SICS is implemented with various types of I&C technology to support its functions. Manual controls are implemented with buttons and switches. Indications are provided via dedicated indicators. A limited number of indications are provided on the QDS for situational awareness. The QDS consists of a display, computer, and input devices such as a touch screen or trackball.

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

Qualification Requirements

The safety-related equipment used in 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

Safety-related hardwired I&C will meet the general quality requirements outlined in ANP-10266A. The non-safety-related portions of the SICS are designed, fabricated, erected, and tested under the quality assurance program described in ANP-10266A, Addendum A. This quality assurance program is consistent with the guidance of Generic Letter 85-06.

Diversity Requirements

There are no diversity requirements for SICS. See the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 8) for further information on defense-in-depth and diversity.

Data Communications

Data communications implemented in the SICS include:

- PS-SICS (QDS) – uni-directional (PS to SICS), point-to-point data connections implemented with the TXS Ethernet protocol.

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 EDGs 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 (SBODGs).

The non-safety-related portion of the SICS is powered from the 12-hour uninterruptible power supply (12UPS). The 12UPS provides backup power with 12-hour batteries and the SBODGs during a 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 human-system interface (HSI). The operator primarily uses the PICS during normal, abnormal, and accident operation. There are a limited number of controls for the PS, Safety Automation System (SAS), and Diverse Actuation System (DAS) that are only available on SICS. The PICS is provided in both the MCR and the RSS. Monitoring-only capabilities are provided in the technical support center (TSC) for support of emergency response operations.]**

Classification

*[The PICS is classified as non-safety-related, supplemented grade (NS-AQ).]**

Functions

Table 7.1-3 shows the functions of the PICS.

Interfaces

Table 7.1-4 shows the interfaces of the PICS.

Architecture

Figure 7.1-2 shows the basic architecture of the PICS.

The PICS consists of:

- Operator Workstations.
- Operator Terminals.
- Gateways (GW).
- Server Units (SU).
- Plant Overview Panels (POP).
- Firewalls.

[Operator workstations with control and monitoring capabilities are located in the MCR and RSS. The operator workstation provides visual representation of plant systems and components. The operator workstation also provides an interface for

operators to initiate control commands for plant systems and components as well as alarm management. Normally, the operator workstations in the RSS are in supervisory mode (view only) to prevent plant control until authorized in accordance with plant procedures. Operator workstations are provided in the TSC with monitoring only capabilities to assist in plant emergency response.

*The operator terminal is a local computer which is part of the operator workstation. The operator terminal performs functions such as HSI functions (information and operation), storage of process data in a short-term archive, and local storage of all displays to allow immediate access to the operator. The operator terminal is also the connecting device for the operator workstation monitor, keyboard, and mouse. The operator terminal is connected to the SU through the HSI Bus.]**

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

[Communications with the PS, SAS, RCSL, and TG I&C are performed via redundant gateways. The gateways are provided for unidirectional communication with the PS and SAS and bidirectional communication with the process automation system (PAS), reactor control, surveillance and limitation system (RCSL), and turbine generator I&C (TG I&C). The PICS receives unidirectional signals from the PS and SAS for status information on those systems. The PICS communicates bidirectionally with the RCSL and TG I&C for control of reactivity control systems and the TG respectively.

Server units are provided for data exchange between the automation bus and the HSI bus. The SUs perform functions such as data message validation, short-term data storage, and alarm management. Redundant SUs are provided so that the PICS remains operational in case of a failure of a single SU. The SU houses the software needed for data archiving as well as for data retrieval. The archiving function provides continuous archiving capabilities and fast retrieval of archived data for reporting and trending. The archiving system performs functions such as archiving of all process data, calculated values from other DCS systems, and operator commands including the command value (ON, OFF, analog value). The SU also performs data retrieval for logs and plots as well as an evaluation of all archived data. The SU is connected to the processing units (PU) of the PAS through the automation bus.

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.

Redundant firewalls are provided for unidirectional transfer of information from the PICS to plant business networks. Remote access to the PICS is not possible.

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.]**

PICS Design Principles

The design principles listed below will be used for the software design of PICS.

- A structured and modular architecture is applied.
- Operating system and application software are separated. The operating system (OS) software serves to provide basic features (i.e., recording, display, communication, etc.). OS software does not create signals or determine how the plant should respond to events (i.e., operator action, interlocks, automatic functions, etc.). OS software is already available for the platform, and is not programmed for project specific designs. Application software is programmed with project specific design information related to implementation of control functions.
- Detection of failures is facilitated by the self-diagnosis functions of the digital system.
- Application software is designed in a graphically symbolized manner using object oriented language so that functions can be easily understood.
- For PICS, the development processes and procedures are described in Software Development Lifecycle in this section.
- The PICS manages and isolates network communications independently from the application software. Communication activity does not affect execution sequence or timing of the application software.

The design for PICS complies with the design principles in DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)." Those principles include:

- Redundancy.
- Independence:
  - One-way Communication.
  - Electrical Isolation.
  - Physical Separation.

- EMI/RFI Requirements.

*[The server units are configured in a distributed redundancy. The redundancy of the two servers is established though a software package which combines the physical resources of two servers into a single operating environment with redundancy of the underlying hardware and data. The operating environment evaluates the status of the redundant server units. In the event of a detected malfunction, the function is switched to the corresponding reserve server unit. The server units operate in lockstep providing redundancy of hardware, data, and networks for automated fault management.]**

Redundancy

The PICS is designed such that a single failure will not prevent the system from performing any of its functions. Overall system redundancy is achieved through the following means:

- Redundancy in Plant Systems – The plant automation systems with which the PICS interfaces are designed to continue to operate automatically upon a loss of a PICS signal.

- Divisional Redundancy – PICS server units are divided between the Safeguards Building divisions 2 and 3 by placing them in computer rooms 1 and 2.

- Control Redundancy – The PICS provides multiple operator terminals in the control rooms. Loss of an operator terminal results in the loss of Visual Display Units (VDU) connected to the affected unit only. In the event of loss of a PICS operator terminal, control of the systems, functions, and components can be accomplished from another PICS operator terminal. Loss of a single VDU does not impact the use of the remaining VDUs.

- Power Supply Redundancy – The PICS and its components are powered by two redundant uninterruptible power supplies. Loss of one power supply will result in the loss of operator terminals and monitors associated with the unavailable power supply. Arrangement at the operator workstations will be such that a loss of one power supply will not result in a total loss of all operator terminals and monitors located at this workstation.

PICS is in a non-critical failure configuration if one component of the PICS has failed. In the event of a single component failure, sufficient redundancy still exists to permit a redistribution of tasks to continue utilization of the PICS to control and monitor the plant.

PICS is in a non-critical failure configuration in the event of:

- Failure of a component of the processing structures – The redistribution of the process resources or interface resources is performed automatically by the PICS (redundant mechanisms, for instance) in most cases. The HSI structures and components are not affected by such a failure. The operator can use the PICS as usual.

- Failure of a screen at an operator workstation – The screens at an operator workstation are standardized. The operator can use one of the remaining screens for monitoring or control.

- Failure of an operator terminal – Each operator workstation has access to all PICS features. The operator can use one of the remaining operator terminals for monitoring or control.

- Failure of a component of the POP – The POP is organized in the same way as a standard PICS operator workstation which uses several screens. Failure of a component in POP may cause the loss of this POP but does not influence the remaining units.

- Total failure of the POP – The POP is not necessary for control and monitoring of the plant as it is used for monitoring only. Operation and monitoring by the operator can be performed without the POP in the event of its complete failure. The PICS is considered to be operable in case of a POP failure.

In case of inoperability of PICS in a design basis accident or beyond design basis accident, the safety classified SICS will ensure that the operating and monitoring capabilities needed to control and monitor the plant are maintained.

Independence

The PICS is designed such that there is independence between the PICS and any safety-related systems or functions. All credible failures of the non-safety I&C systems are bounded by the Chapter 15 safety analysis, and all implausible failures of the non-safety I&C systems are bounded by best estimate analysis. Failures of the non-safety-related I&C system do not impair or inhibit operation of safety-related functions that are credited for the mitigation of AOO or PAs.

The non-safety-related I&C systems can prevent a safety-related component from performing its safety function, however the safety function of the system can still be performed by the redundant components.

The following principles are utilized to ensure independence:

- One-way communication between safety-related and non-safety-related systems – Signals from PICS cannot be transmitted directly to safety-related I&C systems. Communication from safety-related I&C systems is unidirectional. Commands for actuating plant equipment are generated in PICS and subsequently sent to PAS for further processing and distribution. Therefore, a failure of the PICS will not prevent safety-related systems from performing their functions. A failure of PICS does not automatically result in a loss of the PAS automatic function execution.

- Electrical isolation – PICS equipment is electrically separated from safety related power supplies. Power will be supplied by the redundant non-safety-related power supply. PICS does not directly interface with safety-related systems or plant automation systems, with the exception to PAS, and is therefore electrically isolated and separated.

- Physical separation – Physical separation of redundant components into different rooms and different fire areas ensures independence of redundant structures of PICS. PICS components utilize redundant support systems (e.g., HVAC, Power Supply System, etc.).

*[PICS server units are located in computer room 1 (Safeguard Building 2) and computer room 2 (Safeguard Building 3). Operator Terminals are located in the MCR and the RSS which are located in different fire zones. A fire in the MCR does not affect the operability of PICS in the RSS.]**

Equipment

[The PICS is implemented with an industrial I&C platform.

The server units consist of industrial computers. Operator workstations typically consist of operator terminals, VDUs, 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 PICS equipment is capable of trending of information to provide situational awareness by the operator. In addition, the PICS has recording capability so that historical data can be recalled by the operator.

*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 relevance to plant safety.]**

The PICS is used to control both safety-related (via the PAS and the priority and actuator control system (PACS)) 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. See Section 7.1.1.6.6 for more information about the manual control of components from the PICS.*

- *Touch screen displays are not used.]**

Qualification Requirements

*[The PICS is intended to be used during normal, accident, and severe accident conditions as long as it is available. The PICS equipment is located in Safeguard Buildings that provide a mild environment during and following design basis events (DBEs). Equipment selected for use in the PICS will be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used.]**

EMI/RFI Requirements

The equipment used in the PICS is evaluated for EMI/RFI performance using the principles described in RG 1.180, IEC 61000-3, IEC 61000-4, and IEC 61000-5 for limits for electromagnetic compatibility. Strict compliance with these requirements is not required; however, the following shall be demonstrated:

- The electromagnetic emissions from this equipment are sufficiently low so that safety-related equipment in proximity is not adversely affected.

- The electromagnetic susceptibility of this equipment is adequate so that emissions from other equipment do not cause adverse effects within the system. Examples of adverse effects include: spurious actuation of plant components that results in an undesirable plant transient, large electrical surges that can damage equipment and other adjacent equipment, or corruption of data that can result in confusing indications to the operator.

Quality Requirements

[In its role as the primary operator interface, the PICS is required to be of supplemented quality to perform its functions in a reliable manner. The PICS is designed using a robust engineering process with appropriate reviews, verifications, tests, and approvals. Supplemented quality is achieved in the design of the PICS through the following measures:

- *The PICS is designed, fabricated, erected, and tested under the quality assurance program described in ANP-10266A, Addendum A (Reference 42). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 43).]**

- The design of the PICS is accomplished through a phased approach as described in the software development lifecycle.

- A criticality analysis is performed for the PICS software in accordance with accepted industrial practice.

- V&V of the PICS software is performed according to a V&V plan that is consistent with accepted industrial practice.

- PICS requirements are documented in a traceable form that is under configuration management.
- The PICS design is validated through acceptance test in the system validation (or equivalent) phase.

Diversity Requirements

There are no diversity requirements for PICS. See ANP-10304 (Reference 8) for further information on defense-in-depth and diversity.

Data Communications

*[The server units communicate with the automation systems via automation bus and gateways for the PS, SAS, RCSL, and TG I&C. The server units, operator terminals, POPs, and firewalls exchange data via the HMI bus. These networks implement periodic communications and message validation for robust data communications. Remote access of the PICS is not possible.]**

The redundant servers and redundant segments of the automation busses are physically located in separate fire areas so that a fire in the MCR does not result in a loss of the PICS at the RSS. The HMI bus hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the overall functionality of the HMI bus. Portions of the HMI bus required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shut down the plant from the PICS workstations in the RSS.

Sound engineering and design practices will be applied to the development of the PICS automation bus, HMI bus, and the DCS systems connected to the bus. The PICS automation and HMI busses will be designed to withstand data traffic, and the interfacing DCS systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the busses. Specific design details regarding preclusion of data storm events on a non-safety-related network depends on the specific technology chosen for these non-safety-related networks, and they are not included in the U.S. EPR FSAR.

The PICS will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The PICS is powered from the two non-safety-related uninterruptible redundant electrical trains. A loss of one electrical train shall not result in a loss of the entire PICS.

The PICS cabinets are powered by the trains in which they reside. These redundant power supplies meet the following requirements:

- The power supplies are uninterruptible to provide continued operation in case of a LOOP.
- The power supplies include a battery backup to provide continuous operation following a station blackout.

The PICS is powered from the 12UPS. The 12UPS provides backup power from the 12-hour batteries for up to two (2) hours and from the SBODGs during a LOOP.

PICS is powered by two independent power trains. The loss of one electrical train results in a partial loss of PICS only. Component assignment to the bus systems will ensure that the PICS is still operable after the failure of one power bus.

Each PICS cabinet is powered by redundant uninterruptible power supplies (UPS). These power supplies continue to power the PICS system for up to two hours powered by 12UPS that is backed by SBODGs following a LOOP. At least one of the redundant power supplies for each cabinet is backed up by a diesel generator. During normal operation, the 12-hour UPS is powered from offsite power via the non-Class 1E power supply system (NPSS).

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

Self-Diagnostic Features

The PICS provides self-diagnostic features for a real-time representation of its system status. Various self-testing features are built into the software. Software execution and hardware are monitored and a switch-over to a redundant server unit is initiated upon detection of a software or hardware failure. Self-monitoring features include but are not limited to:

- System memory.
- Bus communication between operator terminals, server units, and PAS.
- Software execution.
- Power supply failure.

A CRC self-test is implemented to ensure that no code corruption has occurred.

The Server Units are configured in a distributed redundancy. The redundancy of the two servers is established through a software package which combines the physical resources of two servers into a single operating environment with redundancy of the underlying hardware and data. The operating environment evaluates the status of the redundant server units. In the event of a detected malfunction, the function is switched to the corresponding reserve server unit. The server units operate in lockstep providing redundancy of hardware, data, and networks for automated fault management.

Self-diagnostics provide indication of status of the PICS, and a life-signal ("heart beat") provides indication to the operator that the self-diagnostics are operating as designed.

Software Development Lifecycle

The life cycle approach used to develop PICS is one for programming and configuring individual applications for specific nuclear power plant systems. Each system application of the PICS is subjected to activities for specifying, designing, developing, verifying, validation, testing, and requirements testing.

The software application life cycle activities for PICS are as follows:

1. Software Basic Design Phase:

   A. System Requirements.

   B. System Design.

   C. Software Requirements.

   D. Initiate Software Requirements Traceability.

   E. Summary Reports for Verification and Validation Activities (i.e., Acquisition Support, Planning, Concept, and Requirements).

2. Software Detailed Design Phase:

   A. Software Design.

   B. Automatic Code Generation.

   C. Software Requirements Traceability.

   D. Summary Reports for Verification and Validation Activities.

3. Software Integration and Validation Phase (including Factory Acceptance):

   A. Integration of Hardware and Software.

   B. Application Software Integration, System and Acceptance Test Planning.

   C. Application Software Integration, System and Acceptance Test Execution.

   D. Application Software Integration, System and Acceptance Test Reporting.

E. Software Requirements Traceability.

F. Summary Reports for Verification and Validation Activities (i.e., Test).

4. Site Acceptance Test and Installation and Commissioning:

A. Installation and Commissioning Test Planning.

B. Installation and Commissioning Test Execution.

C. Installation and Commissioning Test Reporting.

D. Summary Reports for Verification and Validation Activities (i.e., Installation and Checkout).

7.1.1.4 DCS Automation Systems

7.1.1.4.1 Protection System

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

Classification

The PS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the PS.

Interfaces

Table 7.1-4 shows the interfaces of the PS.

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 Safeguard 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:

- Acquisition and Processing Units (APU).

- Actuation Logic Units (ALU).
- Monitoring Service Interfaces (MSIs).
- Gateways (GWs).
- Service Unit (SU.)

Details on these functional units, along with details of the PS architecture, are described in the U.S. EPR Protection System Technical Report (ANP-10309P) (Reference 6).

Equipment

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

The 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 are used for the various data and hardwired connections.

The data communication modules (e.g., communication modules, optical link modules) that are part of the PS are located within the PS cabinets. These cabinets are located in mild environment areas within the four Safeguard Buildings. The cables used to interconnect functional units within the PS are considered part of the PS. Cabling independence and separation are described in Section 8.3.1.1.10.

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 diversity requirements for the PS. See ANP-10304 (Reference 8) for further information on defense-in-depth and diversity.

Data Communications

The data communications for the PS are described in ANP-10309P (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 a 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 a Class 1E control system. The SAS performs automatic and manual grouped control functions to perform safety-related controls during normal operations, mitigate the effects of AOOs and PAs, and to achieve and maintain safe shutdown.

Classification

The SAS is classified as safety-related.

Functions

Table 7.1-5 shows the functions of the SAS.

Interfaces

Table 7.1-4 shows the interfaces of the SAS.

Architecture

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

A system-level failure modes and effects analysis (FMEA) is performed on the SAS to identify potential single point failures and their consequences. The architecture of the SAS provides redundant divisions with redundant CUs within each division. The system is designed so that a single failure during corrective or periodic maintenance, or a single failure and the effects of an internal hazard does not prevent performance of the safety functions.

Hardware is subject to self-tests and is monitored at startup, as well as cyclically. A hardware watchdog monitors cyclic operation of every microprocessor and signals a failure independently from the monitored processor and its software during startup and as part of cyclic testing.

The functions of the SAS are implemented with two types of software on the CUs:

System Software

The system software is independent of the specific automation tasks and is identical in the CUs. It carries out the following functions:

- Calls up and controls the processing sequence of the user program.
- Monitors and activates the subordinate modules. Subordinate modules are modules connected to the function processor such as the communication, input, and output modules. Subordinate modules are connected to the function processor to provide specific capabilities (e.g., Profibus communication, Ethernet communication, analog outputs).
- Controls communication.
- Performs system startup.
- Performs monitoring and diagnostics.

Application Software

The application software carries out the specific automation tasks:

- Step sequence controls.
- Closed loop controls.
- Open loop controls.
- Set point elaboration.
- Alarm logics.
- Component and system interlocking.
- Manages and executes the master/standby redundancy switchover.

Figure 7.1-7—Safety Automation System Architecture provides the SAS architecture. Each division of the SAS implements redundant CU pairs that operate in the master / standby configuration. To avoid delay in switching from master CU to standby CU, the pair of CUs receive identical input data.

Figure 7.1-29 shows the logic for the master/standby configuration. The master CU controls the process. The outputs to the PACS module of each pair of CUs are ORgated by hardwiring, but only the master CU is able to send signals to the PACS modules, while the output signals of the standby CU to the PACS modules are blocked. Each CU blocks its own outputs through the software of the CU.

A CU operates properly and is capable of becoming the master CU if all of the following are true:

- The CU is in the cyclic processing state. If the CU is out of the cyclic processing state this is an indication that the CU is not operable (i.e. the CU is placed in functional test state, an error that causes a reset of the CU, an error that causes the shutdown of the CU). A CU may be in cyclic processing state with error flags in the message buffer (e.g. minor communication error) and is capable of becoming the master CU.

- No input module faults found during the CU self-test.

- No output module faults found during the CU self-test.

- The insertion monitoring for the CU finds no faults. A fault occurs if the modules of the CU are not inserted correctly into the cabinet racks. The insertion monitoring function is part of the cabinet monitoring unit.

- The cyclic self-test of the CU completes in less than an hour. If the cyclic self-test of the master CU does not complete in less than an hour, this may be an indication that there is an error in the CU processing.

If a CU operates properly (as described above), no manual master/standby switchover is initiated, and the other paired CU is not the master, then that CU will designate itself to be the master CU. Once a CU is designated the master CU, if the other paired CU operates properly (as described above) and no manual master to standby switchover is initiated, then the other paired CU designates itself to be the standby CU.

Each CU sends two discrete hardwired signals to their paired CU for the master/ standby switchover process. A signal is sent when a CU determines it is capable of being the master CU (CU operates properly, as described above, and no manual master to standby switchover is initiated). The master CU sends out both signals to the other paired CU showing that it has designated itself the master and is capable of being the master. The standby CU sends out a signal to the other paired CU showing that it is capable of being the master, but does not send out a signal saying that it has designated itself the master.

If the master CU does not operate properly (as described above) then it blocks its outputs to the PACS modules and does not designate itself to be the master CU. If the other paired CU has designated itself the standby CU (operates properly and no manual master to standby switchover initiated), then it will change its designation to master CU and will allow its outputs to send signals to the PACS modules.

If the standby CU does not operate properly (as described above), then it continues to block its outputs to the PACS modules and will not be capable of being designated the master CU until it operates properly (as described above). The master CU will continue to control the process and is able to send its output signals to the PACS modules.

If both CUs do no operate properly (as described above), then both CUs block their outputs to the PACS modules and there will be no master CU designated, until one of the CUs operates properly (as describe above). This results in a loss of a division of SAS and Table 7.1-7—SAS FMEA Results describes the effects on the plant for a loss of a division of SAS.

Manual master to standby switchover capability is provided through the Service Unit (SU). A manual master to standby switchover is executed by manually placing the master CU into standby (blocks its outputs to the PACS modules). The other paired CU in standby will detect that the former master CU is no longer designated the master and designates itself the master CU (allows itself to send output signals to the PACS modules). A manual master to standby switchover is not possible unless the paired CU is in standby.

If a master CU is switched to standby, then the CU cannot be switched back to master within 500 ms. This is implemented in both CUs. This prevents the paired CUs from switching between master to standby and from standby to master within a short time period.

During startup of the CUs, the CU that starts up first is designated the master CU. The second CU that starts up afterwards operates as the standby CU. If both paired CUs startup at the same time, a CU is predetermined in the software as the default master CU and the other operates as the standby CU.

The logic within the CUs require that a message be a specific signal name and from a specific processor for the message information to enter the logic and be acted upon. This prevents a CU from being incorrectly influenced to take actions by a CU that is communicating with it in error.

The SAS is organized into four independent divisions located in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

The SAS consists of these functional units:

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

The CUs execute the logic for the assigned automatic and manual grouped control functions. There are redundant pairs of CUs within a division. The number of redundant pairs of CUs is dependent on sizing requirements for the SAS. Redundant pairs of CUs that perform functions requiring interdivisional communication identified in Table 7.1-5 have data communications between CUs in different divisions. For those redundant pairs of CUs that do not have any functions allocated that require interdivisional communication, there are no data connections between redundant pairs CUs in different divisions. The CUs acquire hardwired inputs from the signal conditioning and distribution system (SCDS), the PS, or the SICS via hardwired connections. Hardwired outputs from the CUs are sent to the PACS for signal prioritization and drive actuation. Hardwired outputs may also be sent to the PAS to coordinate logic for related actuators within PAS. The connection from SAS to PAS is a one-way hardwired and isolated connection (shown on U.S. EPR FSAR, Tier 2, Figure 7.1-7) to send SAS information to PAS. Some functions of PAS may require inputs from SAS to execute its functionality (e.g., CCWS Emergency Leak Detection function sends a signal to disable CCWS Normal Operation Switchover if there is a leak). Data are sent from the CUs to the MSIs for display on SICS, or via the MSIs and redundant GWs for display on the PICS.

The MSIs also provide a path to the service unit (SU) for testing and maintenance of the CUs.

Equipment

The SAS is implemented with the TXS 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. SU and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable are 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 diversity requirements for the SAS. See ANP-10304 (Reference 8) for further information on defense-in-depth and diversity.

Data Communications

Data communications implemented in the SAS are:

- CU-CU – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. Separate connections are used for redundant CUs. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4. These data connections are provided to implement only those automatic functions requiring interdivisional communication, which are listed in Table 7.1-5—SAS Automatic Safety Function.
- CU-Monitoring Service Interface (MSI) – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- MSI-GW – uni-directional, point-to-point data connections implemented with the TXS Ethernet protocol. This network is provided so the SAS can provide status information to 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 –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-PICS - bi-directional, point-to-point data communications. Signals are only engineered to be sent from the SAS to the PICS. Signals coming from the PICS to the SAS GW are to request messages to be sent.

Fault Detection

Signal faults in the SAS are detected via diverse means dependent on the signal type.

Hardwired signals, which fail within range, are detected during the periodic testing of the CU. Hardwired signals which fail out of range are automatically disregarded.

Data signals within the SAS carry a value and a status. The signal status can be propagated through the software function block; therefore, if an input signal to a function block has a faulty status, the output of the function block also has a faulty status. When a signal with a faulty status reaches the voting function block, the signal is disregarded through modification of the vote. This results in the output of the voting function block having a non-faulty status. A signal typically obtains a faulty status through the following mechanisms:

- During sensor maintenance, or when a sensor is suspected to be faulty, the sensor can be placed in maintenance bypass. This lockout attaches a faulty status to the sensor's signal. The lockout is a software function performed in the CU layer before any processing is performed using the signal.
- If the SAS detects a faulty sensor through range monitoring, or by monitoring the status of the signal conditioning hardware, the corresponding signal is marked with a faulty status. Range monitoring is the detection of sensor that has provided a value outside of the calibrated range (e.g., 4-20 mA). This monitoring is also performed in the CU layer.
- In case of a communication failure between SAS functional units, the receiving functional unit detects errors such as incorrect message length, format, or age. This detection occurs when the functional unit retrieves the message from the associated communication module before the individual signals are extracted from the message. If a communication failure is detected, a faulty status is attached to the signals in the message before they are used in function block processing.

Single failures upstream of the CU layer that could result in an invalid signal being used in the SAS actuation are accommodated by modifying the vote in the CU layer. Each SAS actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an SAS function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The steam generator MSRCV regulation during pressure control and CCWS emergency temperature control functions are modified toward actuation. The In-containment Refueling Water Storage Tank (IRWST) system boundary isolation for preserving IRWST water inventory interlock function is modified toward no actuation. The concepts of voting towards actuation and no actuation are described in ANP-10309P (Reference 6).

When an invalid signal is received by "functional AND" logic, the signal is ignored. For example, a "functional AND" logical operation with four inputs requires that all four inputs be TRUE to obtain a TRUE output. When an invalid signal is input to this operation, only the remaining three valid inputs must be TRUE to obtain a TRUE output.

Likewise, when an invalid signal is received by "functional OR" logic, the signal is ignored. For example, if a "functional OR" logical operation with four inputs requires that any one of the four inputs must be TRUE to obtain a TRUE output. When an invalid signal is input to this operation, only one of the remaining three valid inputs must be TRUE to obtain a TRUE output.

Failure Modes and Effects Analysis

In order to bound the possible failures, both detected and undetected failures of sensors and digital equipment are analyzed and the worse case effect of each failure is identified. Detected failures are defined as those automatically detected by the inherent and engineered monitoring mechanisms of the system. Two types of undetected failures are analyzed. A failure denoted "undetected-spurious" is defined as failure not automatically detected which results in an actuation. A failure denoted "undetected-blocking" is defined as a failure not automatically detected which results in failure to issue an actuation when needed.

Failures in the hardwired output logic are generally not detected automatically by the SAS. Therefore, only undetected single failures of these devices are considered. A failure of the output logic can result in spurious actuation ("undetected-spurious"), or failure to actuate when needed ("undetected-blocking").

Network failures within the SAS allow the receiver of data to be affected in one of three ways. First, the network failure can result in an invalid message being received. By definition, invalid messages are always detected failures, and are analyzed as single failures. Second, a network failure can result in a message received as valid that contains spurious information. This type of failure is bounded by the "undetected-spurious" failure of the sending equipment. Third, a network failure can result in a message received as valid that fails to request an action when one is needed. This type of failure is bounded by the "undetected-blocking" failure of the sending equipment.

The architecture of the SAS allows CUs to be analyzed for single failure without regard to which specific CU in the division is the failure point. For these single failures, the functions of the system are considered affected, because each function is processed by at least one CU in a division. Considering the effect on each function of the system bounds the cases of specific CU single failures.

When referring to the nature of a single failure, the terms "detected" and "undetected" as used in the context of the SAS FMEA do not correspond to the definition of a detectable failure in IEEE 603-1998. All of the failures denoted "undetected" in the FMEA are detectable through periodic testing. The terms "detected" and "undetected", as used in the FMEA, refer to the ability of SAS to automatically detect a failure through self-monitoring features. As defined by IEEE 603-1998, the SAS has only detectable failures and no identifiable, but non-detectable failures.

The assumptions listed below are taken into account in the SAS system-level FMEA.

- The loss of a checkback signal is considered the same as a sensor failure and is bounded by that analysis.
- Network failures defined as undetected-spurious, and undetected-blocking are bounded by the similar failure of the sending functional unit. Therefore, only detected network failures need to be analyzed.
- No single failure in the electrical supply systems upstream of the SAS cabinets can result in loss of power to an entire cabinet.
- The distribution of power within a single SAS cabinet is such that no single failure in the electrical distribution can cause loss of function of more than one CU functional unit.
- Plant actuators which, if spuriously actuated, can challenge plant safety require actuation signals from more than one division of SAS to actuate (e.g., more than one pilot operator actuated from different divisions are required to change the state of the main valve).
- A spurious blocking of the CU through the master/standby logic is treated as a undetected-blocking failure of the CU. A failure of the CU to block its outputs through the master/standby logic is treated as a undetected-spurious failure of the CU.
- If a hardware failure occurs in a CU of Division 1 of SAS, the fault could be propagated to other CUs. Most of these faults would be detected by the TXS continuous self-test features, and ignored by the other divisions. A hardware failure could go undetected if it is sent to a connected division, such as SAS automatic functions that have CUs in redundant train pairs (Divisions 1 & 2 or 3 & 4) communicating with each other. While this would cause a failure of Divisions 1 and 2 for this function, the failure is not propagated to Divisions 3 and 4. For a function in redundant train pairs as previously described, the Division 1 CU and the Division 3 CU do not communicate with each other. If the hardware fault in Division 1 sends a signal to Division 3 (connection is provided for a different function on the same CUs), the CU in Division 3 will detect that this is a faulty signal and ignore it.
- A failure in the application layer of the TXS software responds similarly to a hardware failure. A faulted sensor or an error within the software logic of a function in redundant train pairs in Division 1 could adversely impact Division 2. However, because this function does not communicate with Divisions 3 and 4, any signals received by Divisions 3 and 4 from 1 and 2 will be detected as an error and ignored, and the error is not propagated beyond Division 2.
- An error that occurs on the system software layer and is propagated to all four divisions, is considered a software common cause failure. This can be described as a triggering event that exposes a latent defect in the system software. This type of failure is beyond the scope of the SAS FMEA. In the event of a software common

cause failure of SAS, a plant shutdown is executed. See the D3 Technical Report (ANP-10304) for more information about the plant response to a software common cause failure.

Table 7.1-7—SAS FMEA Results demonstrates the SAS failure modes.

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 a 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.

Safety Analysis

The following three SAS functions are included within the scope of the Safety Analysis in Chapter 15:

- EFW level control
- EFWS pump overflow protection
- Steam generator main steam relief control valve (MSRCV) regulation during pressure control.

The measuring range of the process variables associated with each aforementioned function is shown in Table 7.1-8. Due to the intrinsic properties of a closed loop control function, the system response time is directly proportional to the settling time of the control loop. This settling time is adjusted during the fine-tuning of the control loop.

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

Table 7.1-3 shows the functions of the PACS.

Interfaces

Table 7.1-4 shows the interfaces of the PACS.

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 the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

In each division, there are safety-related and non-safety-related PACS equipment to interface with safety-related and non-safety-related actuators, respectively. The safety-related PACS and non-safety-related PACS equipment is located in separate cabinets.

The PACS is composed of priority modules and communication modules. One priority module and one communication module are provided for each actuator/black box.

The PACS receives actuation orders sent by the various DCS 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. Checkback signals are used in PACS to remove the PACS actuation output signal once the actuator has reached its final position. SICS and PICS use the checkback signals for indication and display in the MCR and RSS. The PS, SAS, and PAS use checkback signals when device status or position is involved with the execution of a function. Priority between actuation requests from the various DCS systems is established by wiring the inputs using the priority principles described in Section 7.1.1.6.5. The PACS priority logic diagram is shown in Figure 7.1-21—PACS Priority Module Logic Diagram.

Equipment

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

The PACS equipment may be modified and upgraded as needed, but shall exhibit these characteristics.

- The priority module consists of logic that can not be modified while the module is installed. To modify the priority module logic, the module must be removed prior to any modifications being performed.
- The inputs and outputs of the priority module are via hardwired connections.
- The logic of the priority module is subject to 100 percent combinatory proof-of-design testing to eliminate consideration from software common cause failure (SWCCF).
- The communication module is qualified as an associated circuit.
- The data communications from the PAS is only via the communication module.

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

The PACS is designed under the TXS quality program described in Section 7.1.1.2.1.

Diversity Requirements

The priority modules are diverse from the microprocessor-based TXS function processors. In addition, the priority modules must be 100 percent tested to eliminate consideration of SWCCF as described above. The testing methodology is described in ANP-10310P (Reference 44).

Data Communications

Non-safety-related, bi-directional, data connections are implemented between the communication modules and the PAS.

Power Supply

The safety-related PACS equipment 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 a LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

The non-safety-related PACS equipment in the Safeguard Buildings is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The non-safety-related PACS equipment in the Emergency Power Generating Buildings and the Essential Service Water Pump Buildings is powered from a UPS and a diesel backed source.

7.1.1.4.4 Deleted.

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, supplemented grade (NS-AQ).

Functions

Table 7.1-3 shows the functions of the RCSL.

Interfaces

Table 7.1-4 shows the interfaces of the RCSL.

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 Safeguard 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 the SCDS.

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 of control rods, or to PAS for commands of other actuators.

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).

The MSIs provide a communication path between the RCSL and the PICS via redundant GWs for both display of information and transfer of manual commands. The MSIs also provide a path to the SU for testing and maintenance of the various functional units of the RCSL.

Equipment

The RCSL is implemented with the TXS 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

The RCSL equipment is located in Safeguard Buildings that provide a mild environment during and following DBEs. Equipment used in the RCSL will be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used.

Quality Requirements

For the RCSL equipment, the quality requirements will be consistent with the Quality Assurance Plan for non-safety-related equipment as described in ANP-10266A, Addendum A.

Diversity Requirements

There are no diversity requirements for the RCSL equipment.

Data Communications

Non-safety-related data communications implemented in the RCSL are:

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

- CU-DU – bi-directional, networked data connections implemented with the TXS Profibus protocol.

- AU-MSI - bi-directional, networked 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-PICS – bi-directional, point-to-point data communications.

The RCSL will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The RCSL is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs during a 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. For safety-related equipment, PAS only provides automatic control of non-safety-related functions. Safety-related control functions for safety equipment are provided by the protection system or safety automation system. All functions of the PAS can be monitored by PICS. The PAS manual functions are initiated by the plant operators using PICS.

Classification

The PAS is classified as non-safety-related.

Functions

Table 7.1-3 shows the functions of the PAS.

Interfaces

Table 7.1-4 shows the interfaces of the PAS.

Architecture

Figure 7.1-11—Process Automation System Architecture (Nuclear Island) provides a functional representation of the PAS in the Nuclear Island (NI).

Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant) provides a functional representation of the PAS in the Turbine Island (TI) and Balance of Plant (BOP).

The PAS is composed of three subsystems: NI subsystem, TI subsystem, and the BOP subsystem. The PAS is comprised of four divisions located in the NI in the following buildings:

- Safeguard Buildings 1 to 4.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.
- Nuclear Auxiliary Building (Division 4 only).
- Radioactive Waste Building (Division 4 only).

In addition, the PAS TI and BOP subsystems include two trains that are located in the Turbine Island and Balance of Plant in the following buildings:

- Switchgear Buildings.
- Circulating Water Cooling Tower Structure.

The PAS divisions align with the division of the controlled process function and actuators.

The PAS consists of:

- Processing Units (PU).
- Control Units (CU).
- Process System Interface Modules (PSIM).
- Optical Converter Modules (OCM).

The PAS is a redundant computer system which operates in a master/hot-standby configuration. The PAS uses PUs in each division and train to process the PAS functions. Each PU is set up in a master/hot-standby redundancy configuration and is composed of two subunits, CU(A) and CU(B), each with its own CPU. Both CPUs work together in a master/hot-standby configuration. If the master fails, the standby takes over the master's tasks.

The PU is connected through the OCMs to the PACS for safety-related actuators. The PU is also connected though the OCMS to the PACS for control of non-safety-related actuators which are also controlled by SICS and DAS. The PU is connected to PSIMs for control of non-safety-related actuators and interface with sensors. The PSIMs are also connected to other I&C systems and to the non-safety-related field process components via hardwired connections from terminal points in the cabinet to the field device. The CUs communicate with each other via the automation bus.

Each CU performs the following functions:

- Controls and monitors specific process automation functions.
- Carries out open-loop control, protection automation tasks, and alarm logic.
- Carries out closed-loop control.
- Acquires measured values and status information from the process equipment.
- Transfers commands from the PICS to the process equipment and sends back process information to the PICS.
- Communicates to other CUs.
- Executes the application program.
- Controls and monitors application specific automation functions.
- Calls up and controls the processing sequence of the user program.
- Monitors and activates the subordinate modules.
- Reads in information from the process peripheral devices and transfers data to the PICS.
- Controls communication between the CU and the PSIM.
- Manages and executes the master/slave redundancy switchover.
- Provides monitoring and diagnostics.

The PSIM performs the following functions. Each of these modules is connected to both of the redundant processors such that loss of one processor does not prevent loss of the communication to the I/O modules.

- Supplies power to the sensors.
- Acquisition of analog and binary signals.
- Drive control.
- Automation functions for individual open-loop and closed-loop controls.
- Time tagging for all input signals.

- Monitoring functions of the input signals (i.e., sensor line break).
- Self-monitoring of the card internals (i.e., power distribution, reference voltages for monitoring A/D converters, etc.).

The OCM links the PU to the PACS.

PAS Design Principles

The design for PAS complies with the design principles from the regulatory requirements. These principles include:

- Redundancy.
- Independence:
  - One-way Communication.
  - Electrical Isolation.
  - Physical Separation.
- EMI/RFI Requirements.
- Segmentation.

Operating system and application software are separated. The operating system (OS) software serves to provide basic features (i.e., recording, display, communication, etc.). OS software does not create signals or determine how the plant should respond to events (i.e., operator action, interlocks, automatic functions, etc.). OS software is already available for the platform and is not programmed for project specific designs. Application software is programmed with project specific design information related to implementation of control functions.

Redundancy

The redundancy within the PAS is shown on Figure 7.1-11—Process Automation System Architecture (Nuclear Island) and Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant). For the PAS (NI) there are four redundant divisions. For the PAS (Turbine Island and Balance of Plant) there are two redundant trains. Redundancy between divisions or trains refers to the hardware architecture only. Software functionality differs between divisions or trains (see Segmentation).

Within each division or train, two redundant CUs are provided for processing. Note that the PAS architecture figures only display one CU pair per division or train; however, the segmentation of control functions will demonstrate that each division or train contains multiple CU pairs.

The PAS contains sufficient redundancy to prevent a single failure in the following conditions:

- Loss of power to the system, subsystem, or component including main processors, network modules, I/O modules, and I/O.
- Loss of a single PAS CU.
- Loss or failure of the communications path to the PICS.

All CUs are provided as dual redundant hot stand-by configuration. Two CUs run in parallel and process the same inputs. If the master CU fails, the redundant CU immediately takes over operation in a bumpless manner.

Hot-standby is the ability to switch over to a standby device in the event of a fault automatically and without detrimental effect. For operation in this mode it is absolutely essential that both subunits are able to exchange data quickly and reliably. In the PAS, the two CUs are linked by the central controller interface via which they are both supplied with:

- The same user program.
- The same data blocks.
- The same process I/O image contents.
- The same receive buffer contents (e.g., when using communications processors).

The standby CU is therefore always up to date and ready to take over control immediately if a fault occurs in the master CU. Both the master and hot-standby CU operate on identical versions of the operating system.

Location of different PAS divisions or trains in physically separate buildings provides physical separation of redundant functions.

Independence

The PAS is designed such that there is independence between the PAS and any safety-related systems or functions. A failure of PAS shall not prevent any of the safety-related systems from performing their functions.

The following principles are utilized to ensure independence:

- Communication independence – The PAS system communicates with the safety related I&C systems (PS, SAS, SCDS) and DAS via isolated uni-directional hardwired signals. There is no data communication from PAS to any of these systems.

- Electrical isolation and separation – Electrical isolation is achieved by galvanic isolation (optical isolation). Electrical separation is achieved by separated cable trays (different rooms).
- Physical separation – The PAS systems are located in the four Safeguard Buildings, four EDG Buildings, four Essential Service Water Pump Buildings, Nuclear Auxiliary Building (Division 4 only), and the Radioactive Waste Building (Division 4 only). Two trains of the PAS systems are located in the Electrical Switchgear Building and the Circulating Water Cooling Tower Structure. The rooms of the buildings are in different fire areas. Therefore, the consequences of internal hazards such as a fire would impact only one PAS division. Redundant communication system cable is routed via separate paths. The PAS cabinets will be sufficiently separated from the safety-related components so that a failure of PAS will not prevent safety-related systems from performing their safety-related functions.

Equipment

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

The PAS generally consists of subracks, I/O modules, function processors, and optical converter modules (OCM). Fiber optic and copper cable is used for the various data and hardwired connections.

Segmentation

Segmentation is the systematic allocation of critical control functions such that only one critical control function is processed on each CU pair as well as the systematic allocation of non-critical functions such that processors with critical functions do not have the same non-critical functions.

The initiation of critical control functions using different sensed parameters for each segment creates signal diversity.

Critical functions are functions associated with plant systems which have an ability to de-stabilize the plant by causing a transient or release of radiation due to a software common cause failure of the non-safety I&C control system, if the worst case plant system failure causes at least one of the following:

- Increased heat removal.
- Decreased heat removal.
- Increased primary reactivity.
- Increased primary inventory.
- Decreased primary inventory.

- Secondary pressure increase or decrease.
- Immediate release to the environment.
- Loss of spent fuel cooling.

Non-critical functions are functions associated with plant systems which have no ability to destabilize upon a software common cause failure of the non-safety I&C control system.

Critical functions are segmented into various CUs using the following numbering scheme. There are four divisions and two trains of PAS. CU pairs located in a division of PAS are numbered x-y, where "x" identifies in which division/train the pair is located and "y" is the sequential number assigned to the CU pair within "x".

All segmented CU pairs may communicate with other CU pairs in the same division or between divisions. All PAS control functions must be segmented.

As the application software and operating software in the PAS CUs are separated; all corrupted messages from the PICS or corrupted check-back from the PSIM or PACS which could potentially be triggers for spurious actuation only affect the application software. Segmentation introduces diversity in the application software of CUs.

Integrated control functions are automatic control functions that require control of multiple process systems. The limitation functions and integrated control functions will also be segmented in various CU pairs. These functions will be classified as critical or non-critical and segmented according to a predefined methodology.

EMI/RFI Requirements

The PAS cabinets contain all electronic equipment associated with the system. Proper grounding and limitation of the effects of EMI and RFI are essential for the functionality of PAS electronics components and are maintained by the cabinets. The design of the PAS takes into account the requirements of IEC 61000-3, IEC 61000-4, and IEC 61000-6 for limits for electromagnetic compatibility, electromagnetic compatibility testing, and electromagnetic standards. However, strict compliance with this requirement is not required.

Quality Requirements

The PAS is designed, fabricated, erected, and tested under an augmented quality program that is consistent with the guidance of Generic Letter 85-06 (Reference 43).

The design of the PAS is accomplished through a phased approach as described in the software development lifecycle.

A criticality analysis is performed for the PAS software in accordance with accepted industrial practice.

V&V of the PAS software is performed according to a V&V plan that is consistent with accepted industrial practice.

PAS requirements are documented in a traceable form that is under configuration management.

The PAS design is validated through acceptance test in the system validation (or equivalent) phase.

Diversity Requirements

The PAS will be implemented with a commercial grade I&C platform that is not the TXS platform.

Data Communications

The functional units in the PAS interface to the PICS via networked connections. The PAS may implement networked data connections between the CUs in each division to share signals as needed (e.g., to implement signal selection algorithms).

The PAS will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The PAS is powered by the following power supplies:

- Safeguard Buildings – 12UPS.
- Switchgear Building – non-Class 1E uninterruptible power supply (NUPS).
- Other buildings – UPS and diesel backed source.

The 12UPS provides backup power with 12-hour batteries and the SBODGs in the event of a LOOP. The PAS is battery powered for 2 hours after which it may be de-energized per the load shedding scheme. In this situation the PAS will be re-energized once the diesel generator-backed power supply is restored or when offsite power is restored.

The NUPS provides backup power with 2-hour batteries and the SBODGs in the event of a LOOP.

The PAS power supply contains redundant power supplies for both the cabinet chassis and the field devices. If one supply fails, the redundant supply automatically supplies the load without interruption to the PAS system and components. The intent is to minimize the possibility of a single failure in the non-safety-related system that will cause a transient or challenge a safety-related system.

Each supply is provided its own power supply feed from a separate source of power bus. The source of power to the PAS is provided by a critical non-class 1E battery-backed source. In case of a total loss of power to the plant, the battery source permits continued operation of the plant controls for a period that allows safe shutdown of the process. The intent is to minimize the possibility of a single failure in the non-safety related system that causes a transient or challenges a safety-related system.

Replacement of supplies are permitted on-line without affecting operation.

Control voltage and field device voltage is 24 Vdc unless specified otherwise.

Battery-backed systems that provide power to the PAS are being monitored by the PAS for internal cabinet temperature/humidity and input/output voltages, with appropriate alarms for off normal conditions. The intent is an automatic surveillance function to identify degradation and, therefore, early repair of non-safety-related systems that may challenge safety-related systems.

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

Self-Diagnostic Features

The PAS provides self-diagnostic features for a real-time representation of its system status. Various self-testing features are built into the software. Software execution and hardware are monitored and a switch-over to the hot-standby CU is initiated upon detection of a software or hardware failure. Self-monitoring features include but are not limited to:

- System memory.
- Bus communication between CUs and PICS.
- Software execution.
- Power supply failure.

A CRC self-test is implemented to ensure that no code corruption has occurred.

The redundant control units within the processing unit communicate with each other to provide mutual monitoring and synchronization of both units. A switchover between master and hot-standby occurs when a fault is detected in a CU.

For example, in a scenario involving the failure of CU A which is the master CU, the data flow will switch to CU B. After the switchover, all active automation processing will be handled by CU B, the new master. When CU A is restored, it will be the new standby. The operator will be informed by an alarm indicated on the HSI screens.

Software Development Lifecycle

A life cycle process is a set of interrelated activities that result in the development or assessment of software applications. An application or system life cycle refers to the life cycle activities for specifying, designing, developing, verifying, validating, testing, and requirements tracing.

The life cycle approach used to develop PAS is one for programming and configuring individual applications for specific nuclear power plant systems. Each system application of the PAS (e.g., main turbine controls, feedwater controls, etc.) is subjected to activities for specifying, designing, developing, verifying, validation, testing, and requirements testing.

The software application life cycle activities for PAS are as follows:

1. Software Basic Design Phase:

    A. System Requirements.

    B. System Design.

    C. Software Requirements.

    D. Initiate Software Requirements Traceability.

    E. Summary Reports for Verification and Validation Activities (i.e., Acquisition Support, Planning, Concept, and Requirements).

2. Software Detailed Design Phase:

    A. Software Design.

    B. Automatic Code Generation.

    C. Software Requirements Traceability.

    D. Summary Reports for Verification and Validation Activities.

3. Software Integration and Validation Phase (including Factory Acceptance):

    A. Integration of Hardware and Software.

    B. Application Software Integration, System and Acceptance Test Planning.

C. Application Software Integration, System and Acceptance Test Execution.

D. Application Software Integration, System and Acceptance Test Reporting.

E. Software Requirements Traceability.

F. Summary Reports for Verification and Validation Activities (i.e., Test).

4. Site Acceptance Test and Installation and Commissioning:

A. Installation and Commissioning Test Planning.

B. Installation and Commissioning Test Execution.

C. Installation and Commissioning Test Reporting.

D. Summary Reports for Verification and Validation Activities (i.e., Installation and Checkout).

7.1.1.4.7 Diverse Actuation System (DAS)

The DAS is the non-safety-related I&C system that is provided to mitigate an AOO or PA concurrent with a CCF of the PS.

Classification

The DAS is classified as non-safety related, supplemented grade (NS-AQ).

Functions

Table 7.1-3 shows the functions of the DAS.

Interfaces

Table 7.1-4 shows the interfaces of the DAS.

Architecture

Figure 7.1-13—Diverse Actuation System Architecture provides a functional representation of the DAS.

The DAS is organized into four redundant divisions located in separate Safeguard Buildings. Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the SCDS and compared to a setpoint. Hardwired connections are provided to share trip requests, and two-out-of-four voting is done in each DAU. Outputs are sent to the reactor trip breakers, CRDCS, TG I&C, and PACS via hardwired connections. Signals are also sent to the PAS to display information on PICS and to coordinate logic, as necessary. This logic is not relied upon to mitigate an AOO or PA concurrent with a CCF of the PS.

The DAUs interface with the SICS via hardwired connections to receive manual system level commands and to display information.

Equipment

The DAS generally consists of various modules, such as threshold comparators, voting, and alarm modules. Copper cable is used for the hardwired connections. Specialized components may be used.

Qualification Requirements

The DAS equipment must function properly under conditions during and following AOOs or PAs concurrent with a SWCCF of the PS. The DAS equipment is located in Safeguard Buildings that provide a mild environment during and following AOOs or PAs. Equipment selected for use in the DAS shall be rated by the manufacturer to operate under the mild environmental conditions expected to exist at its location during the events for which the equipment is expected to respond.

Quality Requirements

As a system relied on to mitigate AOOs and PAs concurrent with a SWCCF of the PS, the DAS is required to be of sufficient quality to perform its functions in a reliable manner. The DAS is therefore designed using a robust engineering process with appropriate reviews, verification, tests, and approvals. Sufficient quality is achieved in the design of the DAS through the following measures:

- The DAS is designed, fabricated, erected, and tested under the quality assurance program described in ANP-10266A, Addendum A (Reference 42). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 43).
- The design of the DAS is accomplished through a phased approach including the following (or equivalent) phases:
    - System requirements phase.
    - System design phase.
    - Software/hardware requirements phase.
    - Software/hardware design phase.
    - Software/hardware implementation phase.
    - Software/hardware validation phase.
    - System integration phase.

  - System validation phase.

- A criticality analysis is performed for the DAS software in accordance with accepted industrial practice.
- V&V of the DAS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- DAS requirements are documented in a traceable form that is under configuration management.
- The DAS design is validated through acceptance test in the system validation (or equivalent) phase.

Diversity Requirements

The DAS is required to be non-microprocessor based technology. See ANP-10304 (Reference 8) for further information on defense-in-depth and diversity.

Data Communications

There are no data communications associated with the DAS.

Power Supply

The DAS is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs in the event of a LOOP.

7.1.1.4.8 Signal Conditioning and Distribution System (SCDS)

The SCDS is a safety-related system that performs signal conditioning and distribution of signals from sensors or black boxes.

Classification

The SCDS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the SCDS.

Interfaces

Table 7.1-4 shows the interfaces of the SCDS.

Architecture

Figure 7.1-23—Signal Conditioning and Distribution System Architecture provides a functional representation of the SCDS.

The SCDS is organized into four independent divisions located in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

In each division, there are safety-related and non-safety-related SCDS equipment to interface with safety-related and non-safety-related sensors, respectively. The safety-related SCDS and non-safety-related SCDS equipment is located in separate cabinets.

The SCDS is composed of non-computerized signal conditioning modules and signal distribution modules that are part of the TXS platform. Multiple signal conditioning modules or signal distribution modules may be used for a particular signal, depending on the required conditioning and the number of DCS systems to which the output signal is required to go.

The SCDS receives hardwired signal inputs from sensors or black boxes. The SCDS sends hardwired signal outputs to the SICS, DAS, PS, SAS, RCSL, and PAS, as needed. Outputs from safety-related SCDS equipment to non-safety-related DCS systems are electrically isolated by the signal distribution modules.

Equipment

The SCDS is implemented with TXS signal conditioning and distribution equipment.

The SCDS is implemented primarily with subracks, signal conditioning modules, and signal distribution modules.

Qualification Requirements

The equipment used in the SCDS 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

The SCDS is designed under the TXS quality program described in Section 7.1.1.2.1. The non-safety-related portions of the SCDS are designed, fabricated, erected, and tested under the quality assurance program described in ANP-10266A, Addendum A. This quality assurance program is consistent with the guidance of Generic Letter 85-06.

Diversity Requirements

The signal conditioning and distribution modules are diverse from the digital TXS function processors. See Reference 8 for more information on diversity and defense-in-depth.

Data Communications

There are no data communications in the SCDS.

Power Supply

The safety-related SCDS equipment 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 a LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

The non-safety-related SCDS equipment in the Safeguard Buildings is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The non-safety-related SCDS equipment in the Emergency Power Generating Buildings and the Essential Service Water Pump Buildings is powered from an UPS and diesel backed source.

7.1.1.5 Black Box I&C Systems

7.1.1.5.1 Control Rod Drive Control System

Classification

The CRDCS is classified as non-safety-related, supplemented grade (NS-AQ). The trip contactors are safety-related.

Description

Figure 7.1-26—Control Rod Drive Control System Arrangement illustrates the arrangement of the CRDCS.

The CRDCS controls the actuation of the 89 rod cluster control assemblies (RCCA) in the reactor vessel. The RCSL logic transmits the direction of movement (i.e., withdrawal or insertion), speed of movement, and drop and hold information to the rod control units of the CRDCS. Each rod control unit generates the cycling sequence input to the corresponding CRDCS coil modules in order to control the rod speed and movement for one RCCA. The coil modules control the amount of current applied to the operating coils (i.e., lift coil, movable gripper coil and stationery gripper coil) of the control rod drive mechanism (CRDM) in order to move the corresponding RCCA.

A feedback signal is sent from the rod control unit to the RCSL. This feedback signal is used by the RCSL to generate a digital position indication of the RCCA and is based on the number of rod movement steps sent from the CRDCS to the operating coils of the CRDM. A description of the CRDM and its associated operating coils is provided in Section 3.9.4.

The rod position measurement system (RPMS), described in Section 7.1.1.5.14, uses analog rod position measurement coils located within the CRDM to provide an indication of RCCA position that is separate from the position signal developed by the rod control unit of the CRDCS.

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, EMI, and RFI effects.

The DAS provides a reactor trip signal to the CRDCS in case of an AOO or PA concurrent with a CCF of the PS. The reactor trip signal is sent to the rod control unit to drop the rods in a diverse manner from the trip contactors.

Drop orders are issued 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.

The non-safety-related portion of the CRDCS will be designed, procured, installed, and tested in accordance with the Quality Assurance Plan for non-safety-related equipment as described in ANP-10266A, Addendum A.

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 (Top View) shows the arrangement of the various components within the core.

Figure 7.1-24 shows the signal path of the SPNDs through the incore equipment into the SCDS for distribution in the other DCS systems.

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 the Incore Trip Setpoint Transient Methodology for the U.S. EPR Topical Report (ANP-10287P) (Reference 7).

The COTs continuously measure coolant temperature at the outlet of the fuel assembly. 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 the 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 Instrument 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 (SRD) are provided at three radial locations around the core (0°, 90°, 270°). The source range detectors monitor 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 conditioned and compensated for temperature effects. The resulting signal is sent to the SCDS for distribution to various systems within the DCS. The signal is 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 U.S. EPR radiation monitoring system (RMS) instrumentation and control includes self-testing features and diagnostics that allow early detection of failures. The tests and inspections of the RMS include checks, calibrations, and functional tests of the individual instrumentation channels which can be performed during power operation or refueling. Calibrations are performed in accordance with industry standards and manufacturer recommendations.

In addition, the RMS subsystems and components incorporate features for periodic and unscheduled maintenance, repair, and inspection. The purpose of these system inspection and maintenance capabilities is to minimize the occurrence of system faults and to increase RMS availability. Inspection intervals depend on the local situation and the working condition of the RMS. If a subsystem or component of the RMS is unavailable or removed for maintenance, inspection or repair, the ability of the redundant divisions to perform their safety-related functions is not impaired.

Access to the internally set parameters (e.g., calibration factors, alarm thresholds, and analog output ranges) is prohibited while the instrument is in operation. However, a dedicated portable test computer allows access to the internal parameters when the RMS is removed from service, and the test procedures described above are done with the help of this test computer. While the instrument is removed from service for testing, maintenance, or repair, it is put in a test mode that makes any output signal or alarm invalid.

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 non-safety related, supplemented grade (NS-AQ).

Description

The HMS is described in Section 6.2.5.

The HMS components incorporate features for periodic and unscheduled maintenance, repair, and inspection. The purpose of these system inspection and maintenance capabilities is to minimize the occurrence of system faults and to increase HMS availability. Inspection intervals depend on the local situation and the working condition of the HMS. If a subsystem or component of the HMS is unavailable or removed for maintenance, inspection or repair, the ability of the redundant divisions to perform their functions is not impaired.

Access to the internally set parameters (e.g., calibration factors, alarm thresholds, and analog output ranges) is prohibited while the instrument is in operation. However, a dedicated portable test computer allows access to the internal parameters when the HMS is removed from service, and the test procedures described above are done with the help of this test computer. While the instrument is removed from service for testing, maintenance, or repair, it is put in a test mode that makes any output signal or alarm invalid.

7.1.1.5.7 Reactor Pressure Vessel Level Measurement System

Classification

The reactor pressure vessel level (RPVL) measurement system is classified as non-safety-related, supplemented grade (NS-AQ).

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. 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, supplemented grade (NS-AQ).

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, supplemented grade (NS-AQ).

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, supplemented grade (NS-AQ).

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 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 main steam lines (MSL) inside of the containment to detect and localize leakages from the lines. The local humidity detection system is capable of detecting MSL leakage as low as 0.1 gallons per minute.

The condensate flow measurement devices inside containment measure condensate flow from the Reactor Containment Building fan cooler collectors. Changes in the Reactor Containment Building relative humidity levels result in changes in the condensate flow rate. The condensate flow measurement devices inside containment are capable of measuring fan cooler condensate collector flow rates as low as 0.5 gallons per minute. Alarms and indications associated with the LDS are available to the operators in the MCR.

Humidity/temperature sensors are located inside containment inaccessible areas (equipment compartments). These areas surround the reactor coolant piping and sections of larger RCS components. The sample area is a low air flow and limited volume area, this design feature enhances the ability of the local humidity and temperature sensors to identify and quantify any leakage.

7.1.1.5.13 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. The TG I&C also performs a turbine trip when requested by either the PS or DAS. See Figure 7.1-27 for details. Refer to Section 10.2 for further information on the TG I&C.

7.1.1.5.14 Rod Position Measurement System (RPMS)

Classification

The RPMS is classified as safety-related.

Description

Figure 7.1-25 shows the signal path of the rod position measurements through the RPMS equipment into the DCS for distribution.

The rod position measurement system (RPMS) measures the position of a RCCA located in the reactor vessel and provides the measurement to the DCS for control and indication to the operator.

CRDM Position Measurement Coils

The rod position measurement coils are part of the CRDM.

The rod position sensor is comprised of one primary and three secondary coils. Two of the secondary coils, called auxiliary secondary coils, indicate the rod at its lowest or highest end position. The third secondary coil, or main secondary coil, indicates the entire range of RCCA travel. The analog position measurement of the RCCA is derived from the magnetic coupling through the control rod between the primary coil and the secondary coils. The auxiliary secondary coil signal determines the extreme positions of the drive rod.

The primary coil also provides an input to the RPMS equipment to compensate any variations in indicated RCCA position resulting from temperature effects.

Signal Conditioning and Processing Equipment

The signal conditioning and processing equipment is part of the RPMS.

The RPMS receives four inputs from the CRDM, which are the rod top signal, analog rod position signal, rod bottom signal, and temperature measurement signal for compensation.

The RPMS conditions these signals, and also performs temperature compensation of the analog rod position measurement. The signal processing is performed by analog conditioning modules and a TXS processing unit, the rod position measurement unit (RPMU).

The RPMS provides three signal outputs to the DCS for each RCCA, which include top, bottom, and temperature compensated analog position.

The RPMS is arranged in four divisions located in each of the four Safeguard Buildings. Divisions 1, 2, and 3 process measurement for 22 RCCAs, and Division 4 processes measurements for 23 RCCAs, for a total of 89 RCCA position measurements.

Each division of the RPMS has a MSI for testing and maintenance of the RPMS. Each MSI connects to a dedicated SU for the RPMS, which resides in the I&C service center. The RPMS MSI does not have any other connections than to its dedicated SU. The SU connections to the MSI and the associated key control program are implemented in the same manner as the PS and SAS, which are described in Section 7.1.1.6.4.

7.1.1.6 DCS Design Principles

7.1.1.6.1 Defense-in-Depth

The overall defense-in-depth and diversity concept is described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 8).

7.1.1.6.2 Diversity

ANP-10304 describes the diversity present in the DCS design based on the diversity attributes identified in NUREG/CR-6303.

7.1.1.6.3 Redundancy

Redundancy is implemented throughout the DCS design 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 7.1-1—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-related 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-related 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—Implementation of Independence Between Redundant Divisions illustrates the implementation of inter-divisional independence.

The PS, SAS, SCDS 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 Safeguard Buildings.

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

The 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.

Section 11.2 of ANP-10309P (Reference 6) provides more information about communication independence for TXS systems.

Refer to Section 2.9 of EMF-2110(NP)(A) (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-Related I&C Systems and Non-Safety-Related I&C Systems

Figure 7.1-20—Implementation of 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.

Class 1E communication independence is provided between the PS, SAS, and RPMS and the following non-safety-related components:

- QDS (PS only).
- GW.
- SU.

Connection between the MSI and QDS

The connection between the MSI and the QDS is limited to one-way data communication from the MSI to the QDS. This is accomplished via a segment that is physically restricted to unidirectional communication (transmit only port connected to receive only port). This interface is described in more detail in ANP-10309P (Reference 6).

Communications independence is achieved by physically limiting communication to one way from the MSI to the QDS.

Connection between the MSI and GWs

The connection between the MSI and the GW is limited to one-way data communication from the MSI to the GW. This is accomplished via a segment that is physically restricted to unidirectional communication (transmit only port connected to receive only port). This interface is described in more detail in ANP-10309P.

Communications independence is achieved by physically limiting communication to one way from the MSI to the GW.

Connection between the MSI and the SUs

The SU is a non-safety-related, standard computer that is temporarily connected to a TXS system when needed to perform surveillances or troubleshoot.

The SU connection is located in the I&C service center. *[The communication path between the SU and the divisional MSIs for PS, SAS, and RPMS are isolated by hardwired disconnects while not in use.]** [*This is achieved with key-operated* *isolation switches located in the main control room.*]* This allows the control room operators to monitor the position of the isolation switches, providing them with control over the connection of the SU. [*A local connection point for SU connection is located in the lockable MSI cabinet in each PS, SAS, and RPMS division. Control room annunciation will communicate the access to the local connection using the door open alarm. This local connection is isolated by a key-operated isolation switch. The isolation switches in a system are keyed so that a single key operates the eight switches (four MCR and four local), and they are physically retained in the switch when positioned to allow the SU connection to the system. Only one SU isolation switch key is provided per system.*]* *[This switch is hardwired and physically prevents the connection of a SU to more than one single division of the PS, SAS, or RPMS at a time.]**

The SU isolation switches are connected to prevent the SU from being connected to more than a single division of a system at a time. In the unlikely event of a fault caused by the non-safety-related SU, the fault will be confined to a single division, which is bounded by the current plant design basis. [*The application software of the safety-related systems will prevent the operation of plant equipment via the SU.*]*

*[Connections of the SU for the PS, SAS, and RPMS are controlled and limited by the operability requirements of the components being connected to the SU. The SUs for the various systems will only connect to one division in Modes 1 through 4 (e.g. PS, RPMS, and SAS SUs are connected only to Division 1). This design requirement will be enforced by the use of an administrative procedure during plant operations.]** When operability requirements allow for more than one division of the PS, SAS, and RPMS to be inoperable (i.e. modes 5 and 6), it is permissible for a system's SU to be connected to one division, and a separate system's SU to be connected to a separate division (e.g. the PS SU connected to Division 1 and the RPMS SU connected to Division 2). This is assuming the impacted divisions are not required to be operational. This design requirement will also be enforced by the use of an administrative procedure.

Each PS, SAS, and RPMS function processor has a CPU state switch that controls each processor's operation state. These key-operated switches are located in the associated processor's TXS cabinet. The key-operated switches prevent alteration of modifiable parameters and changes to software from the SU, except when the processor is placed in the proper operational state for the change. TXS processors can be in one of four operating states using the CPU state switch. These four states are described in Table 7.1-6—Function Processor Operational States.

To change the operating state of a safety-related CPU:

1. The CPU state switch is positioned to the desired mode.

2. The SU sends a request to change states.

3. The CPU receives the request and verifies the CPU state switch position.

4. The CPU enters the desired operating state.

During the performance of some surveillances, it is necessary for the function processor to be in multiple operation states. The operability is based on the current operating state of the function processor according to Table 7.1-6. For example, during an Actuating Device Operational Test, the processor is operable with exception of the no-go test. During that portion of the test, the SU will be used to change a parameter to block actuation at the PACS. This requires the function processor to be taken to Parameterization State.

The keys associated with the CPU state switches and the SU isolation switches are part of the key control program. This provides a layer of protection via administrative controls and allows the operators to have specific control of what items are able to be made inoperable and what software/setpoints are available for alteration.

During normal operation (SU isolation switches open), fault alarms are collected in the application software of the PS, SAS, or RPMS processors and are sent to the PICS for alarm annunciation and logging. The detailed information about these faults will be downloaded to the SU from the message buffer on the next SU connection. In the event where multiple fault alarms occur in the system, some messages may be lost because the message buffer has limited space. The messages are stored in the order received, with any messages received after filling the buffer being lost, which allows the initiating fault messages to be retained.

The SU will only be connected to a division to:

1. Perform Technical Specification Surveillance Requirements and Actions.

2. Diagnose system faults following indication of a fault.

3. Load new software versions needed to implement approved plant design changes.

*[The SU shall not be continuously connected or used. It is only used as part of approved procedures that implement the functions listed above. When the SU is not in use as described, it is disconnected from the safety-related components by the hardwired SU isolation switch.]**

Before closing the SU isolation switch and establishing communication between the SU and the safety system, it is necessary to perform and pass cyber security checks to verify the condition of the SU in accordance with the Cyber Security Program.

Communications independence between the MSI and the SU is verified by the following measures:

- The SU is normally disconnected.
- The processing principles of the TXS platform while the SU is connected. These principles are addressed in Section 2.9 of Reference 3.

Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related PACS communication module. Connections between the communication module and safety-related priority module are hardwired. The communication module 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 DBE 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 for the PACS are provided. The following systems inputs to the PACS are listed in order of priority:

- PS/DAS.
- SAS.
- SICS.
- PAS.

The PACS priority logic diagram is shown in Figure 7.1-21—PACS Priority Module Logic Diagram and the input/output signals for the diagram are described in Table 7.1-10—PACS Priority Module Signal Descriptions.

The DAS is given a higher priority than the SAS because it is a functional substitute to the PS and is needed at this level of priority to verify proper operation of SAS functions on a SWCCF of the PS. In the event of a malfunction in DAS the safety functions in PS would not be blocked, despite the shared priority of the two systems.

Based on the inventory of functions in the DAS and PS, the following situations present an opportunity for DAS to challenge a PS function:

- EFW Actuation/isolation – The PS has the ability to both actuate and isolate EFW, while the DAS only has the ability to actuate EFW. During an event where PS is performing EFW Isolation (OFF), a DAS malfunction could create a conflicting EFW Actuation (ON) signal.
- EDG Loading Sequence – The PS starts the EDGs and begins the loading sequence. Large loads are removed from the EPSS and loaded back in a sequential order once the EDG has been connected. The PS sends an OFF signal to the PACS modules for these large loads until it is time to load the equipment onto the EPSS. The EFW pumps and Safety Injection pumps are included in the list of large loads. A DAS malfunction could send a conflicting ON signal to these pumps.

Within the PACS module, OFF/CLOSE orders have priority over ON/OPEN orders. In both cases described above, the OFF command is given priority. Therefore, a malfunction of the DAS will not block a safety function of the PS.

The SICS manual component level commands are momentary signals that are removed once the actuator has reached its final limit position. Once the SICS component level command signal is removed, the PAS has the ability to manipulate the actuator. This may be undesirable to the operator controlling the device. Therefore, four safety-related Operational I&C Disable switches are implemented to prevent PAS from manipulating the actuator.

The Operational I&C Disable switch will be necessary for an AOO or PA for which the operator uses credited SICS component-level commands to mitigate the event. Once the component-level command from SICS has been completed, the opportunity exists for PAS to send a conflicting signal to the actuator. In this case, the Operational I&C Disable switch prevents the PAS command from interfering with the credited component-level commands on SICS.

There are situations when SICS commands do not necessitate the use of the Operational I&C Disable switch. One example is the use of system-level manual commands on SICS. Credited system-level manual commands on SICS are latched in by either the PS or DAS to the PACS. Because these signals are unlatched by manual resets, PAS commands are not able to interfere and the Operational I&C Disable switch is not needed. Another example is the execution of surveillance testing of component-level SICS commands.

During testing, PAS control of a safety-related device is overridden by the component-level SICS commands, actuating the component to the test state (e.g., OPEN/CLOSE or ON/OFF). Once the test state is reached, the surveillance test ends and the SICS commands are removed. Control of the component is returned to PAS. The use of the Operational I&C Disable switch during a surveillance test prevents PAS from controlling safety-related components, even those outside of the scope of the surveillance test.

During normal operation, the Operational I&C Disable switches on the SICS are set so that the PAS can send commands to the PACS. If at least two of the four switches (2 out of 4 voting) are set to DISABLE by the operator, the PAS input is blocked by the PAC modules. This configuration is shown in Figure 7.1-30—Operational I&C Disable Switch Configuration. The hardwired logic is implemented within the SICS and the blocking function is implemented within the PACS. The other PACS inputs remain operational. This includes the control of non-safety related equipment, receiving checkback signals from the PACS, and sending information to PICS for display. Table 7.1-9—Prioritization Scheme Analysis provides an analysis of the priority scheme when applied to various interfacing signal conditions.

Signals with overlapping durations (e.g., a safety related pulse signal conflicting with a non-safety related control signal of longer duration) and signals received during a coordinated sequence of actions, can be treated as a combination of the concurrent and conflicting signals (for the time period both signals are present) and non-concurrent signals (for the time period that only one of the conflicting signals is present). In both of these cases, the outcome is still the safety related actions with higher priority will maintain the plant in a safe state.

7.1.1.6.6 Non-Safety System Design Requirements

Network data communication messages contain status, address, and message information. If a CU doesn't recognize the address or status portions of a message, the message is ignored and not processed. Any message failure which causes an invalid message as described above will not be recognized and will be ignored by PICS and PAS. This prevents these types of message failures from causing inadvertent plant actuations.

When communication is lost between the server units and controller units (e.g., hardware defect, degraded wiring, faulty component), the CUs will continue to control processes (without taking into account operator action from PICS, or sending information for display on PICS).

The critical functions in PAS are designed so that each function either receives different sensor inputs, or multiple functions use the same sensor where the software is structured differently between the two functions.

Sensors and the SCDS do not contain running software, are electrically isolated between divisions, and are physically separated between divisions; therefore only single failure applies to these components and not common cause failure.

Each actuator that receives signals from multiple systems has its own PACS module; therefore failure of a PACS module is considered a failure of the actuator and is addressed by the process system redundancy.

In order to manually control a component, which has both MANUAL and AUTOMATIC functionality, from PICS, the following sequence must be executed:

- The operator selects a specific plant display via the operator terminal (PICS display).
- The server unit receives a command from the operator terminal to provide specific data related to the requested plant display.
- Server unit provides operator terminal with process data related to requested plant display.
- To initiate a manual control function, the operator must select a control icon on the operator terminal to switch from AUTOMATIC mode to MANUAL mode.
- The operator terminal then sends a command to the server unit to change the manual control function from AUTOMATIC mode to MANUAL mode.
- The server unit sends a command to the CU to change the manual control function from AUTOMATIC mode to MANUAL mode. This is done using network communication between the server unit and the CU.
- The CU switches the device from AUTOMATIC mode to MANUAL mode and returns an acknowledgement signal to the server unit.
- The operator must select an additional icon from the operator terminal monitor in order to send an actuation command.
- The operator terminal sends the actuation command to the server unit.
- The server unit sends the actuation command to the CU. This is done using network communication between the server unit and the CU.
- The CU sends the actuation command to the device via the PACS or PSIM.
- A feedback signal is sent from the PACS or PSIM to the CU.
- The feedback signal is sent from the CU to the server unit.
- The feedback signal is sent from the server unit to the Operator terminal to update the operator on the status of the actuator.
- Following manual operation, the function will typically be placed back in AUTOMATIC mode.

Based on the above sequence of events, in order for PICS to cause the actuation of a function, at least two valid signals need to be sent from PICS to PAS using network communication; the first to shift the mode of the function from AUTOMATIC to MANUAL, and the second to actuate the function. This means that no single signal on the automation highway can cause an actuation.

In order to manually control a component, which has only MANUAL functionality, from PICS, the following sequence must be executed:

- The operator selects a specific plant display via the operator terminal (PICS display).
- The server unit receives a command from the operator terminal to provide specific data related to the requested plant display.
- Server unit provides operator terminal with process data related to requested plant display.
- To initiate a manual control function, the operator must select a control icon on the operator terminal to switch from BLOCKED mode to MANUAL mode.
- The operator terminal sends a command to the Server Unit to change the manual control function from BLOCKED mode to MANUAL mode.
- The server unit sends a command to the CU to change the manual control function from BLOCKED mode to MANUAL mode. This is done using network communication between the sever unit and the CU.
- The CU switches the device from BLOCKED mode to MANUAL mode and returns an acknowledgement signal to the sever unit.
- The operator must select an additional icon from the operator terminal monitor in order to send an actuation command.
- The operator terminal then sends the actuation command to the server unit.
- The server unit sends the actuation command to the CU. This is done using network communication between the server unit and the CU.
- The CU sends the actuation command to the device via the PACS or PSIM.
- A feedback signal is sent from the PACS or PSIM to the CU.
- The feedback signal is sent from the CU to the server unit.
- The feedback signal is sent from the server unit to the Operator terminal to update the operator on the status of the actuator.
- Following manual operation, the function will typically be placed back in BLOCKED mode.

Based on the above sequence of events, in order for PICS to cause the actuation of a function, at least two valid signals need to be sent from PICS to PAS using network communication; the first to shift the mode of the function from BLOCKED to MANUAL, and the second to actuate the function. This means that no single signal on the automation highway can cause an actuation.

Note: The term BLOCKED is used to describe that manual operation is BLOCKED. The terminology which will be used in the final design is not yet determined, and the terminology used will be determined in a later phase of design.

If a device is in AUTOMATIC or BLOCKED mode, and it receives a signal to manually actuate, an indication or alarm will be sent to the operator. This indication will inform the operator that a failure exists which is attempting to manually operate the function while it is in AUTOMATIC or BLOCKED mode. This prevents the function from being inadvertently actuated when the operator shifts to MANUAL mode due to a constant spurious manual actuation signal.

The only functions which can be inadvertently actuated due to a spurious valid signal being sent from either the operator terminal or server unit are functions which are already in manual mode when the spurious signal is sent. Because of this, a procedural requirement will be made requiring that following the MANUAL operation of a function, the function will be shifted back to either AUTOMATIC or BLOCKED mode. At any given time, the only functions which are in MANUAL mode are those which are required to be in MANUAL mode due to a procedural requirement.

Once the faceplate on the operator terminal is available to the operator, a minimum of two steps are required to cause an actuation (i.e., shifting between auto/manual followed by the actuation request). These two steps require that a communication signal be sent from the operator terminal to the server unit, and another communication signal be sent from the server unit to the control unit. This ensures that in order for an actuation to occur, at least two signals must be sent both from the operator terminal to the server unit, and from the server unit to the control unit.

The operator terminal does not have application software. The graphics software resides in the server unit. The only software that is installed on the operator terminal is the operating system and basic software used to facilitate sending operator actuations (e.g., mouse clicks, and video). Failures caused by software in the operator terminal are caused by operating system software, not application software.

A CRC self-test is implemented to ensure that no code corruption has occurred.

For critical functions on PAS and PICS, application software will be qualified to SIL 3 standards.

Application software execution is asynchronous. The cycle time is set in each CU. Application software is executed based on internal timing of the CU. The synchronous clock for the DCS is only used for time stamping of data which is broadcast onto the data networks.

Critical functions shall not require signals from other CUs to execute the function. While all CUs will be connected via a common data network, the design and programming of critical functions will not use communications from other CUs. For example, Division 1 of the MFW flow control function gathers information from sensors and does not require information from CUs in other divisions to execute its function.

Application software executes with cyclical single task processing with no process interrupts.

Following a seismic event, the operator will make an assessment of the plant status. If a plant transient is in progress due to the seismic event, the operator will use SICS to place the plant in safe condition.

PICS is programmed such that inadvertent actuations and/or inconsistent status information will produce warnings or alarms to alert the operator that an abnormal condition exists which requires attention.

Operating system (OS) software serves to provide basic features (e.g., recording, display, communication, etc.). OS software does not create signals or determine how the plant should respond to events (e.g., operator action, interlocks, automatic functions, etc.). OS software is already available for the platform.

A failure in the OS software will either prevent all communication from the device or it will cause garbled communication from the device (bits sent out which are completely random).

The platform for PAS and PICS is not yet specified. Therefore, no specific features can be discussed. OS software is standard software for a given platform which is already available. It is not programmed specifically for a project. In general, operating system (OS) software serves to provide basic features (e.g., recording, display, communication, etc.). OS software does not create signals or determine how the plant should respond to events (e.g., operator action, interlocks, automatic functions, etc.). For an OS software failure to produce a spurious valid message, the designer must program in an incorrect or corrupt logic block and link the outputs of this logic block to the application software of the other devices. For this series of incorrect programming to occur, it is considered a malicious action, which is covered by the cyber security requirements and outside of the scope of this section. Therefore, should the OS software fail, the application software would stop operating (i.e., no outputs sent). Due to the fact that failure of the operating system software will not result in a spurious valid actuation signal, a single failure or SWCCF in the operating system will not cause spurious actuations and is not programmed for project specific designs.

Once a platform is selected for PAS and PICS, an analysis will be performed for PAS and PICS to verify that none of the failures listed as incredible or implausible in this document have ever occurred in an existing implementation of the platform.

7.1.1.6.7 Non-safety-related I&C Failures Affecting Safety-Related Equipment

The following is a description of the postulated non-safety-related I&C failures that result in spurious actuations of multiple trains of safety-related equipment where the Chapter 15 safety analysis limits are exceeded. These failures are considered incredible. Credible non-safety-related I&C system failures do not cause plant conditions more severe than those analyzed in Chapter 15 accident analyses, and implausible non-safety-related I&C system failures are enveloped by the Chapter 15 accident analyses or other best estimate analyses. Failures of the non-safety-related I&C system do not impair or inhibit operation of safety-related equipment that is credited for the mitigation of Chapter 15 AOOs or PAs.

Main Steam Isolation Valve Closing

A MSIV has four pilot valves (one in each division) that drive a main valve. Any two of the four pilot valves can close the main valve. These pilot valves have no automatic functions in PAS and manual controls in PICS. The MSIV pilot valves are manually grouped so that one manually grouped command drives only one MSIV, not multiple MSIVs.

It is considered implausible that a spurious closure of one MSIV occurs due to a PICS failure. This requires both of the following to occur:

- A failure of a PICS manually grouped command which provides a spurious valid actuation signal to four CUs in the PAS to actuate the four pilot valves of the MSIV.
- At least two of the pilot valves must be placed in MANUAL mode.

It is considered incredible that a failure of the PICS provides a spurious closure to all four MSIVs. This requires both of the following:

- A failure of multiple PICS manually grouped command which provides a spurious valid actuation signal to the sixteen CUs in the PA to actuate the four pilot valves of the four MSIVs.
- At least two of the pilot valves must be placed in MANUAL mode for all four MSIVs.

Main Steam Relief Train Opening

A MSRT has a MSRIV and a MSRCV in series. The MSRCV is controlled by SAS and follows the plant power levels. At full power the MSRCV is fully opened. The worst case failure scenario is at full power with the MSRCVs fully opened and having all MSRIVs open. A MSRIV has four pilot valves (one in each division) that drive a main valve. Any two of the four pilot valves can open the main valve. These pilot valves have no automatic functions in PAS and manual controls in PICS. The MSRIV pilot valves are manually grouped so that one manually grouped command drives only one MSRIV, not multiple MSRIVs. A PS function for MSRT isolation on low SG pressure helps to mitigate the event of an SG depressurization.

It is considered implausible that a spurious opening of one MSRIV occurs due to a PICS failure. This requires both of the following to occur:

- Failure of a PICS manually grouped command to provide a spurious valid actuation signal to four CUs in the PA to actuate the four pilot valves of the MSRIV.
- At least two of the pilot valves must be placed in MANUAL mode.

It is considered incredible that a failure of the PICS provides a spurious opening to all four MSRIVs. This requires both of the following:

- Failure of a PICS manually grouped command to provide a spurious valid actuation signal to four CUs in the PA to actuate the four pilot valves of the four MSRIVs.
- At least two of the pilot valves must be placed in MANUAL mode for all four MSRIVs.

Withdrawal of all Control Rods

The only transient producing failure from the RCSL is the inadvertent withdrawal of RCCAs (from the RCCA shutdown banks and RCCA control banks) out of sequence and overlap. The RCSL has an interlock function that is independent of the withdrawal function that prevents the withdrawal of RCCAs out of sequence and overlap. Therefore, a single failure of the interfacing systems (PICS failure) that causes a RCCA withdrawal will be prevented by the RCSL interlock function. A latent defect within the RCCA withdrawal function will not affect the RCSL interlock function that prevents the out of sequence and overlap withdrawal. Therefore, an SWCCF of the RCCA withdrawal function will not cause an inadvertent withdrawal through a failure of the RCCA withdrawal function and also a failure of separate RCSL interlock function that prevents the out of sequence and overlap withdrawal.

As part of the software program lifecycle for the RCSL system, the functions programmed within RCSL are verified, tested, and simulated throughout the normal plant startup and plant power levels. Therefore SWCCFs that are triggered through plant parameters that are experienced during normal plant startup and power levels will be identified and resolved during the software verification, testing, and simulation phases. Failures experienced during a normal plant startup with an AOO or PA occurrence, are considered failures during an AOO or PA.

During the shutdown modes (Modes 3, 4, 5, and 6), the RT breakers are opened, therefore it is not possible to have an inadvertent RCCA withdrawal due to an I&C failure. There is a period of time during shutdown when the RT breakers are closed for rod drop testing. During this time period the reactor is borated to the shutdown margin (Technical Specifications Sections 3.1.1, 3.1.4, and 3.1.9). If there is a withdrawal of the RCCA shutdown banks or RCCA control banks, the reactor will stay in shutdown. The RT breakers are opened again at the conclusion of this test. If an inadvertent withdrawal occurred during this test, the operator will trip the reactor and open the RT breakers.

During Modes 2 and 3, the shutdown and control banks of RCCAs are manually withdrawn to get to critical power. During the manual withdrawal, substantial operator attention is given to rod position, and RCSL provides three automatic rod stop points. At these points the operator must verify that the system is operating properly by observing the correct rod movement before continuing rod withdrawal. The boron levels at startup are maintained such that the reactor only reaches criticality when all of the RCCAs except for RCCA control banks C and D are fully withdrawn. This process for plant startup is procedurally driven for manual operator actions.

During Mode 1, all of the RCCA shutdown banks (SA, SB, and SC) are fully withdrawn, and the majority of the RCCA control banks (control banks A, B, and C) are fully withdrawn. Only two RCCA control banks (control banks C and D), are not fully withdrawn to control power to ramp up to 100% power. During this time, manually initiated automatic functions use dilution and RCCA control banks C and D to control power ramp up. There will be periodic stops at different power levels (e.g., 25%, 75%, 98%) to do verification, calibration, and testing. During these power modes before the plant reaches full power, an inadvertent RCCA withdrawal will only be able to affect RCCA control banks C and D and none of the other banks. Once the plant has reached full power, all of the RCCA banks are fully withdrawn except for Control Bank D. Therefore, it is not possible to have a withdrawal out of sequence and overlap with just one control bank inserted. A latent defect within the RCCA withdrawal function will not affect the RCSL interlock function that prevents the out of sequence and overlap withdrawal. Therefore, a SWCCF of the RCCA withdrawal function will not cause an inadvertent withdrawal through a failure of the RCCA withdrawal function and also a failure of separate RCSL interlock function that prevents the out of sequence and overlap withdrawal. During ramp up of power, the process is procedurally driven and the operator is monitoring and verifying that the reactor is operating properly and will mitigate an inadvertent RCCA withdrawal (Technical Specifications Section 3.1.6).

Therefore, it is incredible to consider that a RCCA withdrawal out of sequence and overlap will occur due to:

- In shutdown modes, the RCS is borated to shutdown limits or the RT breakers are open.
- In Modes 2 and 3, the RCCAs are withdrawn manually and RCSL provides an interlock to prevent the withdrawal of RCCAs out of sequence and overlap. Therefore, to have a RCCA withdrawal out of sequence and overlap, there must be two separate failures in two systems:
  - A failure within the RCSL software to prevent the functioning of the interlock function.
  - A failure in the PICS to cause an inadvertent RCCA withdrawal.
- During Mode 1 an inadvertent RCCA withdrawal will only be able to affect RCCA control banks C and D and none of the other banks. If an inadvertent RCCA withdrawal occurs, the operator will mitigate the event. For a failure to cause an RCCA withdrawal out of sequence and overlap, the following must occur within the time frame of plant startup:
  - The latent defects triggered through plant parameters that are experienced during normal plant startup and power levels are not identified and resolved during the software verification, testing, and simulation phases of the software program lifecycle.
  - The plant power level is between critical and full power where both RCCA control banks C and D are inserted.
  - A SWCCF of the manually initiated automatic function to withdraw RCCAs.
  - A failure within the RCSL software to prevent the functioning of the interlock function.

This addresses the concerns in NRC Information Notice 2010-10: Implementation of a Digital Control System Under 10CFR50.59 on the single failure and SWCCF of the rod control system, and how these failures could impact the plant.

Emergency Power Supply System Breaker Opening

The event caused by opening multiple Emergency Power Supply System (EPSS) breakers is not bounded by the Chapter 15 safety analysis.

The manual control for these manual group commands for the EPSS breakers are hardwired from SICS to SAS. Only manual component level commands are provided on the PICS for EPSS control.

Therefore, it is considered incredible for a non-safety I&C failure to open multiple EPSS breakers. The opening of a single EPSS breaker is bounded by the Chapter 15 safety analysis. For opening multiple EPSS breakers due to a non-safety I&C failure, all of the following must occur:

- Multiple failures in the PICS that cause multiple PICS manual component level command functions which provide spurious valid actuation signals.

The EPSS breakers receiving the spurious valid actuation signals must be placed in MANUAL mode.

7.1.2 Response Time

Figure 7.1-28—Definition and Allocation of Response Times shows the equipment and response times for the U.S. EPR design. The equipment shown in Figure 7.1-28 is defined as follows:

- Sensor - The device that responds to changes in a plant variable or condition and converts the measured process variable into an electric, optic, or pneumatic signal. This includes the primary element and the transmitter.
- Black box signal conditioning - Equipment that transforms a sensor output into a signal level that is appropriate for acquisition by the DCS. Examples include incore and excore signal conditioning cabinets. (Note - this does not include the signal conditioning and distribution system, which is internal to the Distributed control system (DCS)).
- Distributed control system - The system that performs the logic solving function. The DCS receives input signals from the sensors, compares the signals to setpoints, performs voting, prioritizes the safety signal with other commands, and sends an actuation output to the actuation device. The DCS includes the following systems: SICS, PICS, DAS, PS, SAS, RCSL, PAS, SCDS and PACS.
- Actuation device - A component or assembly of components that directly controls the motive power, such as electricity, compressed air, or hydraulic fluid, for actuated equipment. Examples include breakers, motor controllers and solenoids.
- Actuated equipment - The assembly of prime movers, such as actuators such as motors or hydraulic operators, and driven equipment, such as actuated components (pumps and valves, for example). This also applies to non-moving actuated equipment such as heaters.

The response times are allocated based on the type of equipment as defined. The allocation of the response times are defined as follows:

- T - Overall loop response time from the change of the process variable at the process-sensor interface to the actuated equipment completing the safety function such as to isolate flow, and provide rated flow.

- T1 - Allocated portion of the overall response time from the change of the process variable at the process-sensor interface to the input to the DCS.

- T2 - Allocated portion of the overall loop response time from the input to the DCS to the input of the actuation device.

- T3 - Allocated portion of the overall loop response time from the input of the actuation device to the input to the input of the actuated equipment.

- T4 - Allocated portion of the overall loop response time from the input to the actuated equipment to the completion of the safety function.

7.1.3 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). Refer to Section 7.1.3.6 for an explanation for using IEEE Std 603-1998 in lieu of IEEE Std 603-1991 per the alternative request in Reference 45.

The following 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).

- Signal conditioning and distribution system.

- Rod position measurement system.

- Priority and actuator control system.

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.

7.1.3.1 Compliance with 10 CFR 50

7.1.3.1.1 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 are 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).

7.1.3.1.2 Deleted

7.1.3.1.3 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 of 10 CFR 50.55a(h)(3). 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).

7.1.3.1.4 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 of 10 CFR 50.34(f)(2)(v). This is provided by compliance with 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.

7.1.3.1.5 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 of 10 CFR 50.34(f)(2)(xi). Refer to Section 7.5.2.1.1 for more information.

7.1.3.1.6 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 of 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.

7.1.3.1.7 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 of 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.

7.1.3.1.8 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 of 10 CFR 50.34(f)(2)(xvii). Refer to Section 7.5.2.1.1 for more information.

7.1.3.1.9 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 of 10 CFR 50.34(f)(2)(xviii). Refer to Section 7.5.2.1.1 for more information.

7.1.3.1.10 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 of 10 CFR 50.34(f)(2)(xix). Refer to Section 7.5.2.1.1 for more information.

7.1.3.1.11 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 of 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.

7.1.3.1.12 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.

7.1.3.2 Compliance with 10 CFR 50, Appendix A GDC

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

7.1.3.2.1 GDC 1 – Quality Standards and Records

The applicable I&C systems listed in Table 7.1-2 are 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).

7.1.3.2.2 GDC 2 – Design Bases for Protection against Natural Phenomena

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of GDC 2. The applicable I&C systems are located within the four Safeguard 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.

7.1.3.2.3 GDC 4 – Environmental and Dynamic Effects of Design Bases

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

7.1.3.2.4 GDC 10 – Reactor Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 are determined using the methodology described in U.S. EPR Instrument Setpoint Methodology Topical Report (ANP-10275P-A) (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.2.5 GDC 13 – Instrumentation and Control

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

7.1.3.2.6 GDC 15 – Reactor Coolant System Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 are determined using the methodology described in ANP-10275P-A (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.2.7 GDC 16 – Containment Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of GDC 16. Section 7.3.1.2.9 describes the containment isolation function. Section 6.2.4 describes the containment isolation system. Section 7.3.1.2.1 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.

7.1.3.2.8 GDC 19 – Control Room

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 system 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 safe shutdown conditions from the RSS.

7.1.3.2.9 GDC 20 – Protection System Functions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 are determined using the methodology described in ANP-10275P-A (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.2.10 GDC 21 – Protection System Reliability and Testability

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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.

7.1.3.2.11 GDC 22 – Protection System Independence

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of GDC 22. This is provided by compliance with Clause 5.6.2 (independence) of IEEE Std 603-1998 (Reference 1).

7.1.3.2.12 GDC 23 – Protection System Failure Modes

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

7.1.3.2.13 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 of GDC 24. This is provided by compliance with IEEE Std 603-1998 (Reference 1). Specifically, compliance with Clause 5.1 (single-failure criterion), Clause 5.6.3 (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.

An analysis was performed to determine the effects of worst case credible and implausible failures of the non-safety I&C systems on the plant. The results of the analysis were that credible non-safety-related I&C system failures do not cause plant conditions more severe than those analyzed in Chapter 15 accident analyses, and implausible non-safety-related I&C system failures are enveloped by the Chapter 15 accident analyses or other best estimate analyses. Failures of the non-safety-related I&C system do not impair or inhibit operation of safety-related equipment that is credited for the mitigation of Chapter 15 AOOs or PAs. The priority and actuator control system (PACS) prioritizes commands between the safety-related and non-safety-related I&C systems. The PACS prevents a non-safety-related I&C system from interfering with the safety-related I&C system once the safety-related I&C system is controlling the actuator.

7.1.3.2.14 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 of GDC 25. 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.

7.1.3.2.15 GDC 28 – Reactivity Limits

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 PAs. Section 5.2.2 describes the overpressure analyses of the RCS, and Chapter 15 describes the safety analyses for given malfunctions of control systems.

7.1.3.2.16 GDC 29 – Protection against Anticipated Operational Occurrences

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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 are determined using the methodology described in ANP-10275P-A (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.2.17 GDC 33 – Reactor Coolant Makeup

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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.

7.1.3.2.18 GDC 34 – Residual Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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.

7.1.3.2.19 GDC 35 – Emergency Core Cooling

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 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.

7.1.3.2.20 GDC 38 – Containment Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of GDC 38. The SIS performs the 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.

7.1.3.2.21 GDC 41 – Containment Atmosphere Cleanup

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

7.1.3.2.22 GDC 44 – Cooling Water

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of GDC 44. The essential service water system (ESWS) and component cooling water system (CCWS) are provided to transfer heat from plant systems 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.

7.1.3.3 Conformance to Staff Requirements Memoranda

7.1.3.3.1 SRM to SECY 90-016 II.A – Anticipated Transient Without Scram (ATWS).

The DAS provides full diverse scram capabilities as described in SECY 90-016 II.A.

7.1.3.3.2 Interim Staff Guidance DI&C-ISG-02 – Task Working Group #2: Diversity and Defense-in-Depth Issues, Interim Staff Guidance, Revision 2.

The DAS system design shall be assessed with respect to diversity and defense-in-depth as a guard against common mode failure. The DAS provides adequate diversity and manual operator actions to be consistent with D3 guidelines.

7.1.3.3.3 SRM to SECY 93-087 Issue 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 Issue II.Q (Reference 10). The diversity and D3 assessment for the U.S. EPR is described in ANP-10304 (Reference 8). Section 7.1.1.4.7 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8 identifies the functions performed by the DAS.

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

7.1.3.3.4 SRM to SECY 93-087 Issue 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 Issue II.T (Reference 10). Conformance is provided by these design features:

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

7.1.3.4 Conformance to Regulatory Guides

7.1.3.4.1 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 of 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, Section 7.3.2.3.6 and in U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report (ANP-10315P) (Reference 46).

7.1.3.4.2 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 of 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.

7.1.3.4.3 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 ANP-10309P (Reference 6).

7.1.3.4.4 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.

7.1.3.4.5 RG 1.75 – Criteria for Independence of Electrical Safety Systems

The applicable I&C systems listed in Table 7.1-2 are 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.

7.1.3.4.6 RG 1.89 – Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants.

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.89, which endorses IEEE 323-1974. IEEE 323-2003 is used as it meets or exceeds the requirements of IEEE 323-1974.

7.1.3.4.7 RG 1.100 – Seismic Qualification of Electrical and Mechanical Equipment for Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.100, which endorses IEEE 344-1987. IEEE 344-2004 is used as it meets or exceeds the requirements of IEEE 344-1987.

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

The applicable I&C systems listed in Table 7.1-2 are 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.

7.1.3.4.9 RG 1.105 – Setpoints for Safety-Related Instrumentation

The setpoints for the applicable I&C systems listed in Table 7.1-2 are developed using the guidance of RG 1.105, with the exception of those differences described in ANP-10275P-A (Reference 14). The setpoint methodology described in ANP-10275P-A (Reference 14) implements the guidance of ANSI/ISA-67.04.01-2006 (Reference 15) which accounts for recent industry advances in setpoint methodologies. ANP-10275P-A provides justification for its use as an acceptable method for calculating setpoints. The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.4.10 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.

7.1.3.4.11 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 are designed to meet the guidance of RG 1.152, which endorses IEEE Std 7-4.3.2-2003 (Reference 18). Conformance to IEEE Std 7-4.3.2-2003 is described in Section 7.1.3.6 with the compliance of IEEE Std 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 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-A (Reference 5). The cyber security controls for TXS application software development fully meet the intent of Regulatory Positions C.2.1 through C.2.5.

7.1.3.4.12 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 are designed to meet the guidance of RG 1.168, except for the differences described in ANP-10272A (Reference 5) with regard to the use of alternate V&V methods. The methods used for software V&V are described and justified in ANP-10272-A.

7.1.3.4.13 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 are designed to meet the guidance of RG 1.169. The methods used for software configuration management plans are described and justified in ANP-10272-A (Reference 5).

7.1.3.4.14 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 are designed to meet the guidance of RG 1.170. Refer to ANP-10272-A (Reference 5) for a description of the software test documentation.

7.1.3.4.15 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 are designed to meet the guidance of RG 1.171. Refer to ANP-10272-A (Reference 5) for a description of software unit testing.

7.1.3.4.16 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 are designed to meet the guidance of RG 1.172. Refer to ANP-10272-A (Reference 5) for a description of software requirement specifications.

7.1.3.4.17 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 are designed to meet the guidance of RG 1.173. Refer to ANP-10272-A (Reference 5) for a description of software requirement specifications.

7.1.3.4.18 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 are designed to meet the guidance of RG 1.180. The equipment qualification program, which includes EMI/RFI qualification, is described in Section 3.11.

7.1.3.4.19 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 safe shutdown from the RSS in case of a fire. Fiber optic cable is extensively used for communications within the DCS systems to reduce the risk of fires and hot shorts. The fire analysis for the U.S. EPR is described in Chapter 9.

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

The applicable I&C systems listed in Table 7.1-2 are 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.

7.1.3.4.21 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 are designed to meet the guidance of RG 1.209, which endorses IEEE Std 323-2003 (Reference 21) with modifications. The equipment qualification program is described in Section 3.11.

7.1.3.5 Conformance to Branch Technical Positions

7.1.3.5.1 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.

7.1.3.5.2 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 7.6.1.2.2.

7.1.3.5.3 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 the meet 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.

7.1.3.5.4 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 to withstand a postulated line break, an active single failure, and a LOOP.

7.1.3.5.5 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.

7.1.3.5.6 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 described in Chapter 16.

7.1.3.5.7 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 Std 603-1998 (Reference 1). The RCSL performs non-safety-related, non-credited partial trips and an anticipatory full reactor trip on a complete loss of feedwater. Refer to Section 7.7 for further information.

7.1.3.5.8 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.

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

The applicable I&C systems listed in Table 7.1-2 are 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.

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

The setpoints for the applicable I&C systems listed in Table 7.1-2 are developed using the guidance of BTP 7-12 (Reference 31). The setpoint methodology is described in ANP-10275P-A (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.3.5.11 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 ANP-10315P (Reference 46).

7.1.3.5.12 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 are designed using the software development and V&V processes described in ANP-10272-A (Reference 5).

Conformance with BTP 7-14 (Revision 4 of NUREG 0800, "Standard Review Plan," June 1997) is described in ANP-10272-A. The topical report identifies specific differences and provides appropriate justification. BTP 7-14 (Revision 4, June 1997) 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 7-14 during the review of the topical report. Both BTP 7-14 (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, and software configuration management plan required by ANP-10272-A are designed to make sure there is proper implementation of the TXS application software development activities and the proper production of the required design output documents.

7.1.3.5.13 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.

7.1.3.5.14 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-A (Reference 5).

7.1.3.5.15 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 D3 assessment for the U.S. EPR is described in ANP-10304 (Reference 8). Section 7.1.1.4.7 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8 identifies functions performed by the DAS.

7.1.3.5.16 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.

7.1.3.6 Compliance with IEEE Std 603-1998

This section describes compliance with 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 with IEEE Std 603-1998, compliance with 10 CFR 50.55a(h) is satisfied.

Pursuant to 10 CFR 50.55a(a)(3)(i), two alternatives to IEEE Std 603-1991 were proposed for the U.S. EPR design (Reference 45). First, regarding safety-related I&C and electrical systems, IEEE Std 603-1998 is used by the U. S. EPR design in lieu of IEEE Std 603-1991. Second, regarding the self-powered neutron detector (SPND)-based reactor trip functions, the use of a conservative setpoint selection method to satisfy single failure requirements is used by the U. S. EPR design as an alternative to independence between redundant divisions required by IEEE Std 603-1991, Clause 5.6.1.

Where applicable, compliance with Clauses of IEEE Std 603-1998 (Reference 1) is supplemented by conformance to guidance in IEEE Std 7-4.3.2-2003 (Reference 18) to address the digital safety systems (SICS, PS, and 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).
- Signal conditioning and distribution system.
- Rod position measurement system.

The execute features consist of:

- The reactor trip breakers (part of the NUPS).
- The reactor 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).

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

The safety-related systems meet the requirements of Clauses 4.a and 4.b of IEEE Std 603-1998 (Reference 1).

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

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

The safety-related systems meet the requirements of Clause 4.c of IEEE Std 603-1998 (Reference 1).

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

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

The safety-related systems meet the requirements of Clause 4.d of IEEE Std 603-1998 (Reference 1).

The variables used to initiate protective actions monitored by the protection system are described in Section 7.2.2 and Section 7.3.2.

The sensor response times and protection system cycle times required to accommodate the rates of change of monitored variables listed in Table 15.0-7 and Table 15.0-8. For the AOOs and PAs requiring protective action, the accident analysis models the rates of change of variables monitored by the protection system from the occurrence of the accident to where the plant has reached a controlled state following protection system actions. Relative to the design basis for the protection system, the rates of change of these variables are included to determine that the sensor response time and input sampling rate of the protection system are adequate to detect and mitigate the event. The response times assumed in the accident analysis include sensor response times and worst case input sampling rate (i.e., input to the protection system changes just after the beginning of a clock cycle and is not seen until the beginning of the next clock cycle).

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

The safety-related systems meet the requirements of Clause 4.e of IEEE Std 603-1998 (Reference 1).

Manual actions credited in the accident analysis are described in Section 15.0. 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 system 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.

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

The safety-related systems meet the requirements of Clause 4.f of IEEE Std 603-1998 (Reference 1).

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

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

The safety-related systems meet the requirements of Clause 4.g of IEEE Std 603-1998 (Reference 1).

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

- Environmental effects (e.g., temperature and humidity).

- Seismic effects.
- EMI/RFI effects.

The safety-related 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.

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

The safety-related systems meet the requirements of Clause 4.h of IEEE Std 603-1998 (Reference 1).

The safety-related systems are designed to perform their required functions in the presence of natural phenomena and unusual events, which include seismic events, hurricanes, 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.

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

The safety-related systems meet the requirements of Clause 4.i of IEEE Std 603-1998 (Reference 1).

Two methods are used to evaluate the reliability of the safety-related 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.

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

The safety-related systems meet the requirements of Clause 4.j of IEEE Std 603-1998 (Reference 1).

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

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

The safety-related systems meet the requirements of Clause 4.k of IEEE Std 603-1998 (Reference 1).

The I&C systems provide the capability to implement equipment protection of the safety-related process systems. Equipment protection can be implemented as an operational I&C function or a safety-related I&C function. The categorization is derived from process system requirements. Safety-related 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 for descriptions of the process systems.

The U.S. EPR contains equipment protective functions that may prevent a piece of safety-related equipment from performing its function. If a piece of safety-related equipment is prevented from performing its function by an equipment protective function, then a single failure has occurred. This scenario is functionally equivalent to that piece of equipment failing to perform its safety-related function due to any number of failure mechanisms. Failure modes and effects analysis (FMEA) have been performed for the safety-related process systems to demonstrate that no single failure can prevent performance of a safety-related function. Therefore, no single equipment protective function can prevent performance of a safety-related function.

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

The safety-related systems meet the requirements of Clause 4.l of IEEE Std 603-1998 (Reference 1).

A SWCCF of the PS concurrent with an AOO or PA is considered in the design. The D3 principles described in Section 7.1.1.6 provide sufficient means to mitigate this SWCCF. Section 7.8 describes the D3 assessment.

7.1.3.6.12 Single Failure Criterion (Clause 5.1)

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

As defined by IEEE 603-1998 (Reference 1), the PS, SAS, SICS, and PACS have only detectable failures, and no identifiable but non-detectable failures.

An FMEA for the protective functions executed by the PS is described in ANP-10309P (Reference 6). An FMEA for the functions executed by SAS is provided in Table 7.1-7. 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.

7.1.3.6.13 Completion of Protective Action (Clauses 5.2 and 7.3)

The safety-related systems meet the requirements of Clause 5.2 of IEEE Std 603-1998 (Reference 1). When initiated by a safety-related 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 can only be only cleared when the initiating plant variable returns to within an acceptable range.

A latched signal from I&C systems (e.g., PS, SAS, DAS, PAS) maintains a signal to the PACS to prevent any lower priority signal from interfering with a higher priority signal. For the SICS inputs to the PACS, the PACS has the ability to latch its outputs to the actuator so that it goes to its requested state. Once the actuator is to the desired state, indication is provided to the main control room, the PACS removes its outputs, and the higher priority signal is maintained to the PACS to prevent other systems from actuating the device to an undesirable end state. This adequately confirms the completion of the function.

Refer to Section 7.3.2.3 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, in accordance with IEEE Std 603-1998, Clause 7.3.

7.1.3.6.14 Quality (Clause 5.3)

The safety-related systems meet the requirements of Clause 5.3 of IEEE Std 603-1998 (Reference 1). The safety-related 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 (Reference 18). 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 the following exception:

- Alternate V&V methods are used. These methods are described and justified in ANP-10272-A (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-A. These processes provide an acceptable method of software development to meet the quality requirements of IEEE Std 603-1998 (Reference 1).

7.1.3.6.15 Equipment Qualification (Clause 5.4)

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

The digital safety-related systems meet the additional guidance of IEEE Std 7-4.3.2-2003 (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.

7.1.3.6.16 System Integrity (Clause 5.5)

The safety-related 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-related systems perform their function under the range of conditions required for operation. The PS, SAS, SCDS, and PACS are implemented in four divisions located in physically separated Safeguard 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.

The SAS implements a fail-safe design. ESF control is energized to actuate, so a loss of power results in a fail as-is condition.

Upon restoration of power to a SAS division, the CUs go through a extended self-test, during which the outputs remain in a “0” (no actuation) state. Upon successful completion of the extended self-test, each CU enters its normal cyclic operation mode of master/standby configuration. Upon successful completion of the startup self-test, when each CU enters its normal master/standby operational mode, outputs remain in a “0” (no actuation) state until the end of the first cycle of data input. After the first cycle of data input, the outputs change to match the plant conditions. If plant conditions change during restoration of power, the output states change accordingly to reflect plant conditions.

The PACS implements a fail-safe design. Actuators controlled by the PACS are energized to actuate, so a loss of power results in a fail as-is condition.

The SICS implements a fail-safe design. Indications and controls on the hardwired portion of the SICS are powered from the respective I&C systems (PS, SAS, DAS, SCDS, and PACS) from which the indications and controls originate.

Loss-of-power to a division of the PS, SAS, DAS, SCDS, and PACS will result in the loss of the corresponding indications on the SICS. Indications on the 3 other divisions will be available. Indications will be available upon restoration of power.

Loss-of-power to a division of the PS, SAS, DAS, SCDS, and PACS causes the corresponding controls on SICS to become inoperable. ESF controls are energized to actuate. Therefore, SICS implements a fail-safe design, for which a loss-of-power results in a fail as-is condition for the end component. A loss-of-power will prevent manual actions and spurious signals from being sent from the SICS.

Upon a loss-of-power, the ICIS, EIS, BCMS, RPMS, RMS, and SCDS outputs will fall to zero. The PS and SAS will recognize the failure and flag these signals as faulty. This failure is the same as if the sensors provide no output. The system level FMEA for the PS and SAS (ANP-10309 and Section 7.1.1.4.2 respectively) describe the PS and SAS behavior due to detected failed sensors.

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.

7.1.3.6.17 Independence (Clause 5.6)

The safety-related systems meet the requirements of Clause 5.6 of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18) subject to the alternative request in Reference 45.

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

7.1.3.6.18 Capability for Testing and Calibration (Clause 5.7)

The safety-related 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.

7.1.3.6.19 Information Displays (Clause 5.8)

The safety-related 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. The displays meet the requirements of IEEE Std 497-2002 (Reference 13). Refer to Section 7.5 for further information.

The safety-related 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 is determined using the HFE principles described in Chapter 18.

7.1.3.6.20 Control of Access (Clause 5.9)

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

Access to the cabinets of the SICS, PS, SAS, SCDS, 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 Safeguard Buildings and can only be accessed by authorized personnel.

Access to software of the digital safety-related systems is limited to the SU. The SU and the safety-related 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-related 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 EMF-2110(NP)(A) (Reference 3).

The SICS equipment is located in the MCR and RSS. Both rooms are controlled security areas.

7.1.3.6.21 Repair (Clause 5.10)

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

Safety-related 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).

7.1.3.6.22 Identification (Clause 5.11)

The safety-related systems meet the requirements of Clause 5.11 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-related system are distinctively marked. Equipment within a cabinet that belongs to the same division as the cabinet marking does not contain additional identification. However, equipment within a cabinet that is not the same division as the cabinet marking is marked to show its different division assignment. Equipment within the safety-related 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-related system. Versions of hardware are marked accordingly. Configuration management is used for maintaining identification of safety-related software.

7.1.3.6.23 Auxiliary Features (Clause 5.12)

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

The safety-related 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-related systems to perform their functions (e.g., SU) are designed to meet criteria that does not degrade the safety-related functionality of the safety-related systems below an acceptable level.

7.1.3.6.24 Multi-Unit Stations (Clause 5.13)

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

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

7.1.3.6.25 Human Factors Considerations (Clause 5.14)

The safety-related 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-related systems in accordance with the HFE principles described in Chapter 18.

7.1.3.6.26 Reliability (Clause 5.15)

The safety-related systems meet the requirements of Clause 5.15 of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18).

The safety-related systems are designed to accomplish their safety-related 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-related systems (including software) are analyzed as part of the probabilistic risk assessment, which is described in Chapter 19.

7.1.3.6.27 Common Cause Failure Criteria (Clause 5.16)

The safety-related 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 for an AOO or PA concurrent with a CCF of the PS. The defense-in-depth and diversity principles that minimize the probability of a CCF and mitigate the consequences of a CCF are described in ANP-10304 (Reference 8).

7.1.3.6.28 Automatic Control (Clauses 6.1 and 7.1)

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

The SCDS acquires sensor inputs, conditions, and distributes those signals to other systems within the DCS.

The PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of AOOs or PAs. The PS automatically initiates appropriate safety-related 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-related 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.

7.1.3.6.29 Manual Control (Clauses 6.2 and 7.2)

The safety-related 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. 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 an AOO or PA. This capability is provided through appropriate controls and indications. Refer to Section 7.4 and Section 7.5 for further information for achieving 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.

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

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

Sensors are shared between the safety-related and non-safety-related 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.

The following 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 DAS implements 2/3 or 2/4 voting. A single failed sensor does not result in a spurious action of the safety-related equipment.
- Independence between the safety-related and non-safety-related systems. The independence measures provided are described in Section 7.1.1.6.4.

7.1.3.6.31 Derivation of System Inputs (Clause 6.4)

The safety-related 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 safety-related 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.

7.1.3.6.32 Capability for Testing and Calibration (Clause 6.5)

The safety-related 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 include:

- Perturbing the monitored variable.
- Providing 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.

7.1.3.6.33 Operating Bypass (Clauses 6.6 and 7.4)

The safety-related systems meet the requirements of Clauses 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. Controls for manually validating and inhibiting PS permissives are provided on SICS in the MCR and RSS. The RSS only has those permissives needed to reach and maintain safe shutdown. See Section 7.4.1.1 for a list of permissives in the MCR and RSS.

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 the P17 permissive when at power. During shutdown operations, LTOP protection is enabled when the P17 permissive is manually validated by the operator once the conditions for the P17 permissive 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.

7.1.3.6.34 Maintenance Bypass (Clauses 6.7 and 7.5)

The safety-related 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 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. During maintenance bypass, the single failure criterion is still met, or acceptable reliability is demonstrated.

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, in accordance with IEEE Std 603-1998, Clause 7.5.

7.1.3.6.35 Sense and Command Features: Setpoints (Clause 6.8)

The safety-related 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-A (Reference 14). The methodology establishes that setpoints used within the PS are determined so that plant safety limits are not exceeded. The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

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.

7.1.3.6.36 Electrical Power Sources (Clause 8.1)

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

The safety-related 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 a LOOP. Refer to Section 8.3 for information regarding the EUPS and EPSS.

7.1.3.6.37 Non-Electrical Power Sources (Clause 8.2)

The safety-related 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.

7.1.3.6.38 Maintenance Bypass (Clause 8.3)

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

7.1.4 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. Deleted.

5. [*ANP-10272-A, Revision 3, "Software Program Manual TELEPERM XSTM Safety Systems Topical Report," AREVA NP Inc., July 2011.*

6. *ANP-10309P, Revision 5, "U.S. EPR Protection System Technical Report," AREVA NP Inc., May 2013.*

7. *ANP-10287P, Revision 0, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," AREVA NP Inc., November 2007.*

8. *ANP-10304, Revision 6, "U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report," AREVA NP Inc., May 2013.*]*

9. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," U.S. Nuclear Regulatory Commission, December 1994.

10. SRM to SECY 93-087 Issue 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-A, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc.,January 2008.*]*

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 Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," 2003.

19. IEEE Std 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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. 5, 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.

39. Deleted.

40. EPRI TR-106439, “Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” Electric Power Research Institute, October 1996.

41. Deleted.

42. [*ANP-10266A, Revision 1, “AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR Topical Report,” AREVA NP Inc., April 2007.*]*

43. Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related,” U.S. Nuclear Regulatory Commission, April 16, 1985.

44. [*ANP-10310P, Revision 2, “Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report,” AREVA NP Inc., May 2013.*]*

45. Letter, Sandra Sloan (AREVA NP Inc.) to Document Control Desk (NRC), “Request for Alternatives to IEEE Std 603-1991 to Satisfy 10 CFR 50.55a(h)(3) Requirements - U.S. EPR Design Certification,” May 24, 2011.

46. [*ANP-10315P, Revision 2, “U.S. EPR Protection System Surveillance Testing and Teleperm XS Self-Monitoring Technical Report,” May 2013.*]*

47. NEI 12-06, Revision 0. “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide,” Nuclear Energy Institute, August 2012.

48. ANP-10329 Revision 0, "U.S. EPR Mitigation Strategies for an Extended Loss of AC Power Event Technical Report," May 2013.

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
RCSL	2 (Note 1)
PAS	2 (Note 2)
DAS	4
SCDS	4

Notes:

1. RCSL is a redundant control system, but acquires sensor inputs in all four divisions.

2. PAS uses redundant controllers in each division and train. Some functions in the NI utilize multiple divisions (e.g., pressurizer level control).

Next File