Table 1.6-1—Reports Referenced
Sheet 2 of 4

Report No. (See Notes 1, 2, and 3)	Title	Date Submitted to NRC	FSAR Section Number(s)
ANP-10285P ANP-10285NP	U.S. EPR Fuel Assembly Mechanical Design Topical Report	10/02/07	4
ANP-10286P ANP-10286NP	U.S. EPR Rod Ejection Accident Methodology Topical Report	11/20/07	4.3 and 15
ANP-10287P ANP-10287NP	Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report	11/27/07	4, 6, 7, and 15
ANP-10288P ANP-10288NP	U.S. EPR Post-LOCA Boron Precipitation and Boron Dilution Technical Report	12/6/07	15
ANP-10290, Revision 1	AREVA NP Environmental Report Standard Design Certification	12/6/07	19.2
ANP-10291P ANP-10291NP	Small Break LOCA and Non-LOCA Sensitivity Studies and Methodology Technical Report	5/09	15
ANP-10292, Revision 1	U.S. EPR Conformance with Standard Review Plan (NUREG-0800) Technical Report	5/09	1.9
ANP-10293	U.S. EPR Design Features to Address GSI-191 Technical Report	2/08	15.6.5.4.3
ANP-10294, Revision 1	U.S. EPR Reactor Coolant Pump Motor Flywheel Structural Analysis Technical Report	3/09	5.4.1.6.6
ANP-10295, Revision 1	U.S. EPR Security Design Features	10/09	13.6
ANP-10296	U.S. EPR Design Features that Enhance Security	12/08	13.6
ANP-10304	U.S. EPR Instrumentation and Control Diversity and Defense in Depth Methodology Technical Report	5/09	7.1, 7.2, 7.3, 7.7, 7.8
BAW-10132-A	Analytical Methods Description – Reactor Coolant System Hydrodynamic Loadings During a Loss-of-Coolant Accident	7/20/79	App. 3C
BAW-10133P-A BAW-10133-A Revision 1, Addendum 1 and 2	Mark-C Fuel Assembly LOCA-Seismic Analysis	10/30/00	4.2

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

7.1.1.2.2 Application of the TXS Platform

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

- Basic design phase:
  - Functional requirements specification.
  - Software requirement specification.
  - Hardware requirement specification.
  - Concept activity V&V summary report.
  - Requirements activity V&V summary report.
- Detailed design phase:
  - Software design description.
  - Cabinet design and layout.
  - Code generation and documentation.
  - Software test plan.
  - Software test report.
  - Design activity V&V summary report.
  - Implementation activity V&V summary report.
- Manufacturing Phase.
- Testing Phase:
  - Factory acceptance test plan.

7.1.1.3.2 Process Information and Control System

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

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

Classification

The PICS is classified as non-safety-related.

Functions

The PICS performs these functions:

- Monitoring and control of process systems during normal operation, including startup, power, and shutdown operation.
- Monitor the status of the automatic reactor trip and ESF systems during abnormal events, including anticipated operational occurrences (AOO)~~ and~~, postulated accidents, and special events.
- Manual reset of automatic reactor trip and ESF actuation functions.
- Non-credited means to monitor and control systems required to achieve and maintain safe shutdown.
- Manual component level control of safety-related process systems via the process automation system (PAS) and priority and actuator control system (PACS)~~ diverse from the TXS-based safety systems~~.
- Manual actuation of critical safety functions via the DAS or PAS.
- Primary SPDS functions.
- Display of Type A-E PAM variables.
- Monitoring and control of systems required to mitigate severe accidents.
- Display bypassed and inoperable status of safety systems.
- Alarm management.

- Service equipment.

Equipment

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

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

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

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

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

Qualification Requirements

There are no qualification requirements for the PICS equipment.

Quality Requirements

The PICS is designed, fabricated, erected, and tested under the quality assurance program described in Chapter 17.~~There are no quality requirements for the PICS equipment.~~

Diversity Requirements

The PICS is credited by the defense-in-depth and diversity analysis described in ~~Section 7.8.2~~Section 7.8. ~~These diversity requirements are established~~Diversity requirements for the PICS are identified in Reference 8:

- ~~The system hardware in the PICS is diverse from the TXS system hardware.~~
- ~~The system software in the PICS is diverse from the TXS system software.~~
- The PICS displays are diverse from the SICS displays (QDS).

Data Communications

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

Power Supply

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

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

7.1.1.4 Level 1 - System Automation

7.1.1.4.1 Protection System

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

Classification

The PS is classified as safety-related.

Functions

The PS performs these functions:

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

Architecture

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

The PS is organized into four redundant, independent divisions located in separate Safeguards Buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement functional diversity for reactor trip functions.

The PS consists of these functional units:

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

Details on these functional units, along with details of the PS architecture, are described in Digital Protection System ~~Topical~~Technical Report (ANP-~~10281~~10309P) (Reference 6).

Equipment

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

The RAUs, RCCAUs, APUs, ALUs, and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable 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 8.3.1.1.9.

Qualification Requirements

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

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

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

Diversity Requirements

There are no equipment diversity requirements for the PS.

Data Communications

The data communications for the PS are described in ANP-~~10281~~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 selected manual control functions to perform safety-related controls during normal operations, mitigate the effects of abnormal operational occurrences and postulated accidents, and to achieve and maintain safe shutdown.

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

Classification

The SAS is classified as safety-related.

- GW-Plant Data Network – non-safety-related, divisional, bi-directional, networked communications.

Power Supply

The SAS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of 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.

7.1.1.4.3 Priority and Actuator Control System

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

Classification

The PACS is classified as safety-related.

Functions

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

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

Architecture

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

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

~~The PACS is composed primarily of priority and actuator control (PAC) modules. A PAC module is provided for each actuator.~~The PACS is composed of safety-related priority modules, and non-safety-related communication modules. One priority module and one communication module are provided for each safety-related actuator.

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

Equipment

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

- ~~Each PAC module consists of two parts: a safety part and an operational part.~~
- The ~~safety part~~ priority module consists of logic implemented with firmware-only based devices (e.g., EEPROM), with no system software or application software.
- The inputs and outputs of the ~~safety part~~ priority module are via hardwired connections.
- The logic of the ~~safety part~~ priority module is ~~fully testable~~subject to 100 percent combinatory proof-of-design testing and not subject to software common cause failure.
- The ~~operational part~~communication module is qualified as an associated circuit.
- The data communications from the PAS is only via the ~~operational part~~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

~~Quality for the PAC modules is described in ANP-10273P (Reference 4)~~The PACS is designed under the TXS quality program described in Section 7.1.1.2.1.

Diversity Requirements

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

Data Communications

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

Power Supply

The PACS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of 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.

7.1.1.4.4 Severe Accident Instrumentation and Control

Classification

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

Functions

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

Architecture

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

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

The SA I&C consists of these functional units:

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

The CUs perform data acquisition and control functions. Hardwired inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems. Hardwired outputs are sent to the DCMs or PACS for component actuation. DCMs are

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

Architecture

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

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

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

Nuclear Island Subsystem

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

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

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

Turbine Island Subsystem

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

The TIS is located in the Switchgear Building.

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

Balance of Plant Subsystem

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

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

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

~~*Diverse Actuation Subsystem*~~

~~Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant Subsystem) provides a functional representation of the DAS.~~

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

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

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

Equipment

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

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

Qualification Requirements

~~There are no qualification requirements for the PAS equipment.~~There are no qualification requirements for the NIS, TIS, or BPS equipment.

Quality Requirements

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

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

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

Diversity Requirements

~~The PAS is credited by the defense-in-depth and diversity analysis described in Section 7.8.2. These diversity requirements apply to the PAS equipment:~~There are no diversity requirements for the PAS.

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

Data Communications

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

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

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

Other types of data connections may be implemented within the same division of the NIS and the DAS.~~Other data connections may be implemented as required.~~

The TIS and BPS are not divisionalized. Other types of data connections may be implemented within the TIS and BPS.

Power Supply

The various subsystems of the PAS have different power supplies.

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

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

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

7.1.1.4.7 Diverse Actuation System (DAS)

The DAS is the non-safety-related I&C system that provides diverse actuation of protective functions in the unlikely event of an ATWS or a software common cause failure of the PS.

Classification

The DAS is classified as non-safety related.

Functions

The DAS performs automatic risk-reduction functions, including:

- Mitigation of ATWS and PS software common cause failure.
- Manual, system-level actuation of critical safety functions.
- Mitigation of SBO.
- Mitigation of other risk significant events.

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 Safeguards Buildings. Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the PS, as described in Section 7.1.1.6.4, and compared to a setpoint. Fiber optic data connections are provided to share trip

requests, and two-out-of-four voting is done in each DAU. Outputs are sent to the PACS via hardwired connections.

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

Equipment

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

The DAS generally consists of subracks, I/O modules, function processors, communication modules, and link modules. Fiber optic and copper cable is used for the various data and hardwired connections. Specialized components may be used.

Qualification Requirements

In the unlikely event of a software common cause failure of the PS, the DAS equipment must function properly under conditions during and following design basis events. The DAS equipment is located in Safeguard Buildings that provide a mild environment during and following design basis events. Equipment selected for use in the DAS shall be rated by the manufacturer (or otherwise reasonably expected) 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 the effects of CCF of the safety systems, 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 augmented quality program as described in Chapter 17.

- 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.
- Verification and validation (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, providing traceability of every software requirement to one or more system requirements.
- The DAS design is validated through acceptance test in the system validation (or equivalent) phase.

Diversity Requirements

The DAS is credited by the defense-in-depth and diversity analysis described in Section 7.8. Diversity requirements for DAS are described in Reference 8:

Data Communications

The DAS interfaces with the PICS via the plant data network and implements point-to-point data connections between the DAUs for voting purposes.

Other types of data communications may be implemented within the same division in the DAS.

Power Supply

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

~~7.1.1.4.7~~ ~~**Turbine Generator I&C**~~

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

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

7.1.1.5 Level 0 - Process Interface

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

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

7.1.1.6 I&C Architecture Design Principles

7.1.1.6.1 Defense-in-Depth

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

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

These lines of defense are described in the Instrumentation and Controls ~~Topical~~Technical Report (ANP-~~10284~~10304) (Reference 8).

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

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

- Section 7.7 – Control functions.

- Operational I&C functions:
  - Section 7.7 – Control functions.

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

7.1.1.6.2 Diversity

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

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

- ~~Functional diversity.~~
- ~~Platform diversity.~~

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

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

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

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

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

~~Refer to ANP-10284 (Reference 8) for more information regarding diversity features of the U.S. EPR.~~ANP 10304 (Reference 8) describes the diversity present in the I&C architecture based on the diversity attributes identified in NUREG/CR-6303.

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

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

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

Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related ~~part of the~~ PACS communication module. Connections between the ~~non-safety-related~~communication module and safety-related ~~part of the PAC~~priority module are hardwired. The ~~non-safety-related part~~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 design basis event that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and accommodate failures.

7.1.1.6.5 Priority

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

The U.S. EPR is designed in accordance with IEEE Std 603-1998 (Reference 1). ANP-~~10281~~10309P (Reference 6) describes how IEEE Std 603-1998 (Reference 1) meets or exceeds the requirements established in IEEE Std 603-1991 (Reference 2).

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

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

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

7.1.2.1 Compliance to 10 CFR 50 and 52

7.1.2.1.1 10 CFR 50.55a(a)(1) – Quality Standards and Records for Systems Important to Safety

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

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

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

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

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

information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.19 GDC 35 – Emergency Core Cooling

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

7.1.2.2.20 GDC 38 – Containment Heat Removal

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

7.1.2.2.21 GDC 41 – Containment Atmosphere Cleanup

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

7.1.2.2.22 GDC 44 – Cooling Water

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

7.1.2.3 Conformance to Staff Requirements Memoranda

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

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of the SRM to SECY 93-087 II.Q (Reference 10).~~, with the exception of providing system~~

~~level actuation of critical safety functions.~~ The diversity and defense-in-depth (D3) ~~methodology~~assessment for the U.S. EPR is described in ANP-~~10284~~10304 (Reference 8). Section 7.1.1.4.6 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8~~.1.2 describes the functional requirements for the DAS. The D3 analysis is described in Section 7.8.2.2~~ identifies the functions performed by the DAS.

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

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

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

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

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

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

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

approval. AREVA NP provided additional information on alignment with BTP HICB-14 during the review of the topical report. Both BTP HICB-14 (Revision 4, June 1997) and BTP 7-14 (Reference 33) are based on the same regulations, RGs, and endorsed IEEE Standards. As such, acceptance of the topical report, based on these common regulatory requirements, is sufficient to address conformance with BTP 7-14. The software quality assurance plan, software safety plan, software verification and validation plan, and software configuration management plan required by ANP-10272 (Reference 5) 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.

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

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

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

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

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

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-19 (Reference 36), with the exception of providing system level actuation of critical safety functions. The diversity and defense-in-depth (D3) ~~methodology~~assessment for the U.S. EPR is described in ~~Section 7.1.1.6 and~~ ANP-~~10284~~10304 (Reference 8). ~~Section 7.1.1.4.6~~Section 7.1.1.4.7 describes the DAS, including architecture, quality and diversity requirements, and power supplies. ~~Section 7.8.1.2~~ Section 7.8 ~~describes the functional requirements for the DAS. The D3 analysis is described in Section 7.8.2.2~~identifies functions performed by the DAS.

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

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

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-21 (Reference 37). The design features that provide for real-time, deterministic

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

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

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

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

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

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

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

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

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

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

A software CCF of the ~~safety systems~~PS concurrent with a design basis event is considered in the design. The D3 principles described in Section 7.1.1.6 provide sufficient means to mitigate ~~a~~this software CCF. Section 7.8 describes the D3 ~~analysis~~assessment.

7.1.2.6.12 Single Failure Criterion (Clause 5.1)

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

The safety systems are arranged in four independent divisions, located in four physically separated Safeguards Buildings. The PS acquires redundant sensors and generally implements 2/4 voting logic to accommodate single failures. This approach

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

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

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

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

7.1.2.6.21 Repair (Clause 5.10)

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

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

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

7.1.2.6.22 Identification (Clause 5.11)

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

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

- Continuous online fault detection and accommodation abilities.
- High quality software design process.
- Strong operating experience of the TXS platform.

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

7.1.2.6.27 Common Cause Failure Criteria (Clause 5.16)

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

The U.S. EPR architecture is designed so that plant parameters are maintained within acceptable limits established for each DBE in the presence of a single, credible common cause failure. The defense-in-depth and diversity principles that minimize the probability of a CCF and mitigate the consequences of a CCF are described in ~~Section 7.1.1.6.1 and~~ ANP-~~10284~~10304 (Reference 8). ~~The D3 analysis is provided in Section 7.8.~~

7.1.2.6.28 Automatic Control (Clauses 6.1 and 7.1)

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

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

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

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

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

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

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

7.1.2.6.31 Derivation of System Inputs (Clause 6.4)

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

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

The U.S. EPR implements an evolutionary means of reactor protection by acquiring a three-dimensional measurement of reactor flux through the use of 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.

7.1.2.6.32 Capability for Testing and Calibration (Clause 6.5)

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

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

2. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"1991.

3. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

4. ANP-10273P, Revision 0, "AV42 Priority Actuation and Control Module Topical Report," AREVA NP Inc., November 2006.

5. ANP-10272, Revision 0, "Software Program Manual TELEPERM XS™ Safety Systems," AREVA NP Inc., December 2006.

6. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March 2007~~November 2009.

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

8. ~~ANP-10284, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007~~ANP-10304P, Revision 1, "U.S. EPR Diversity and Defense-In-Depth Assessment Topical Report," AREVA NP Inc., November 2009.

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 II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," United States Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, 1993.

11. IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," 2000.

12. IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1992.

13. IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," 2002.

14. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., March 2007.

15. ANSI/ISA-67.04.01-2006, "Setpoints for Nuclear Safety Related Instrumentation," 2006.

16. IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," 1987.

17. ISA-67.02-1980, "Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," 1980.

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

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

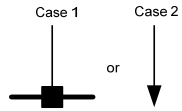
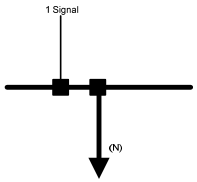
Notes:

1. SA I&C is implemented with four divisions of I&C. Plant severe accident mitigation features are implemented with varying levels of redundancy.

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

3. ~~This is the minimum level of redundancy for the TG I&C.~~

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 2 of 16

Symbols – Logic Figures	Definition
	Multiple Signals of the Same Type
	Single Signal (2 Cases)
	Signal Transfer Between Divisions
	Signal Sent Elsewhere in Figure
	Signal Received from Elsewhere in Figure
	The logic within the block is duplicated in other divisions of the system.

REV 002
EPR3000-2 T2

Figure 7.1-2—U.S. EPR I&C Architecture

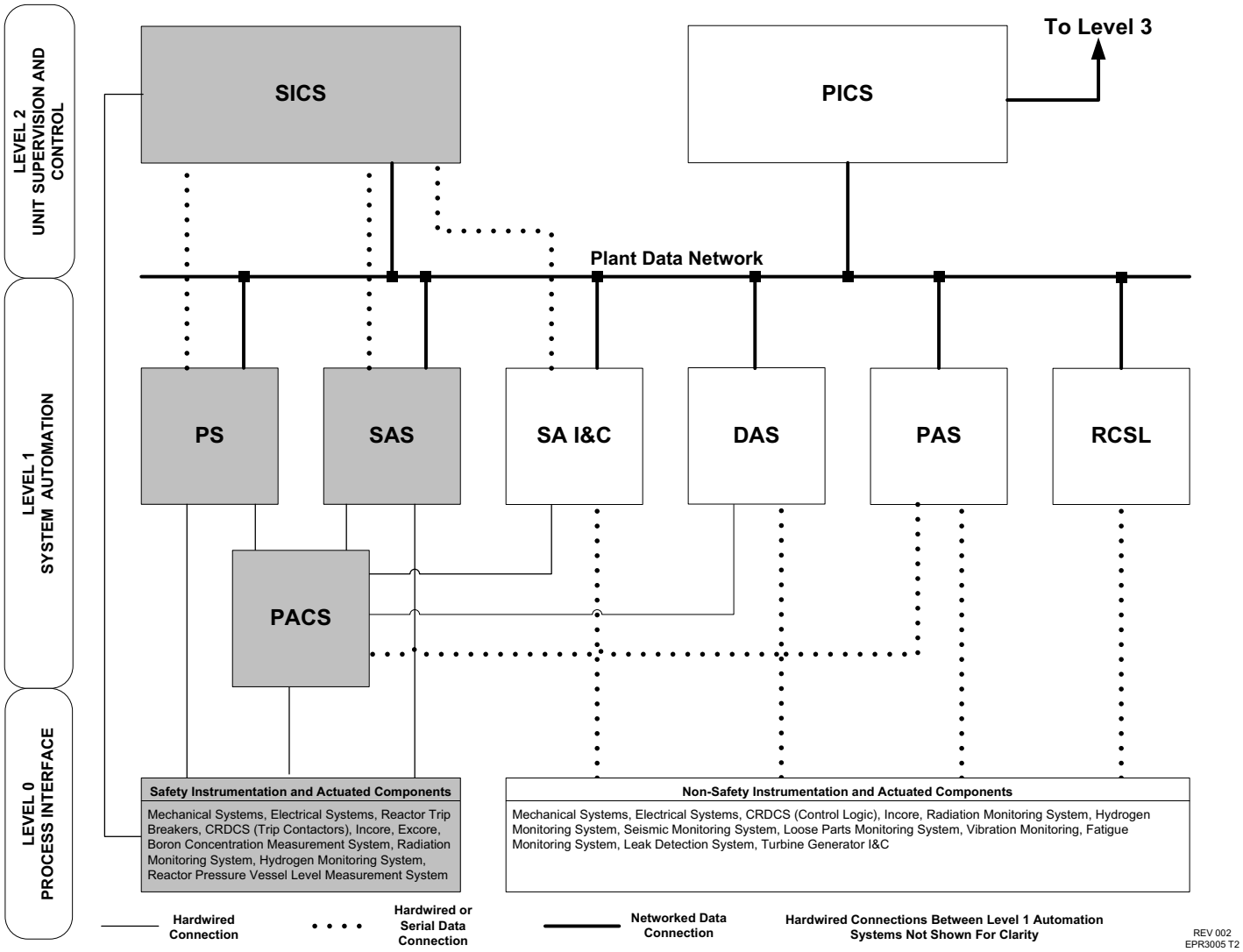


Figure 7.1-3—Safety Information and Control System Architecture (Safety-Related Portion)

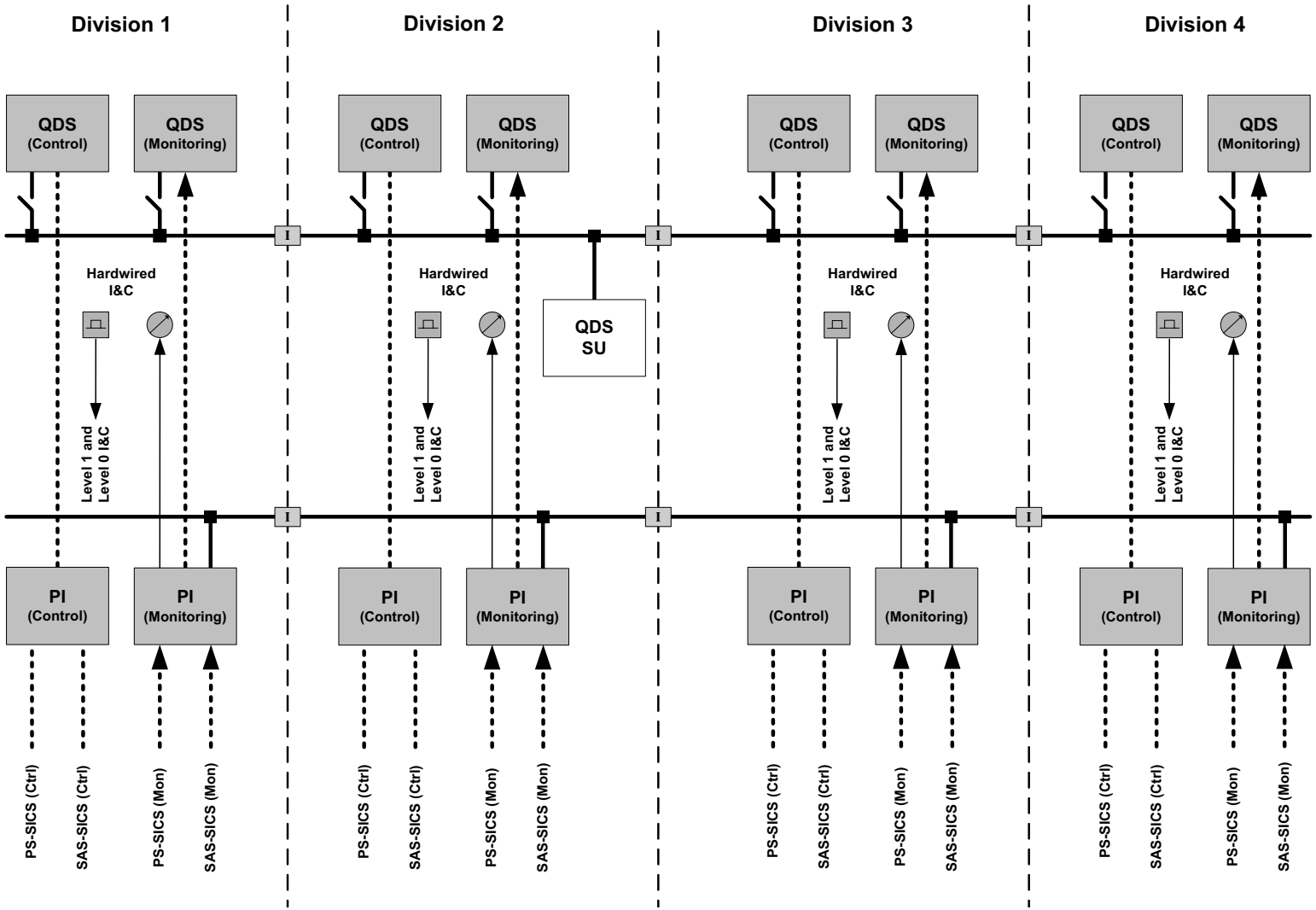
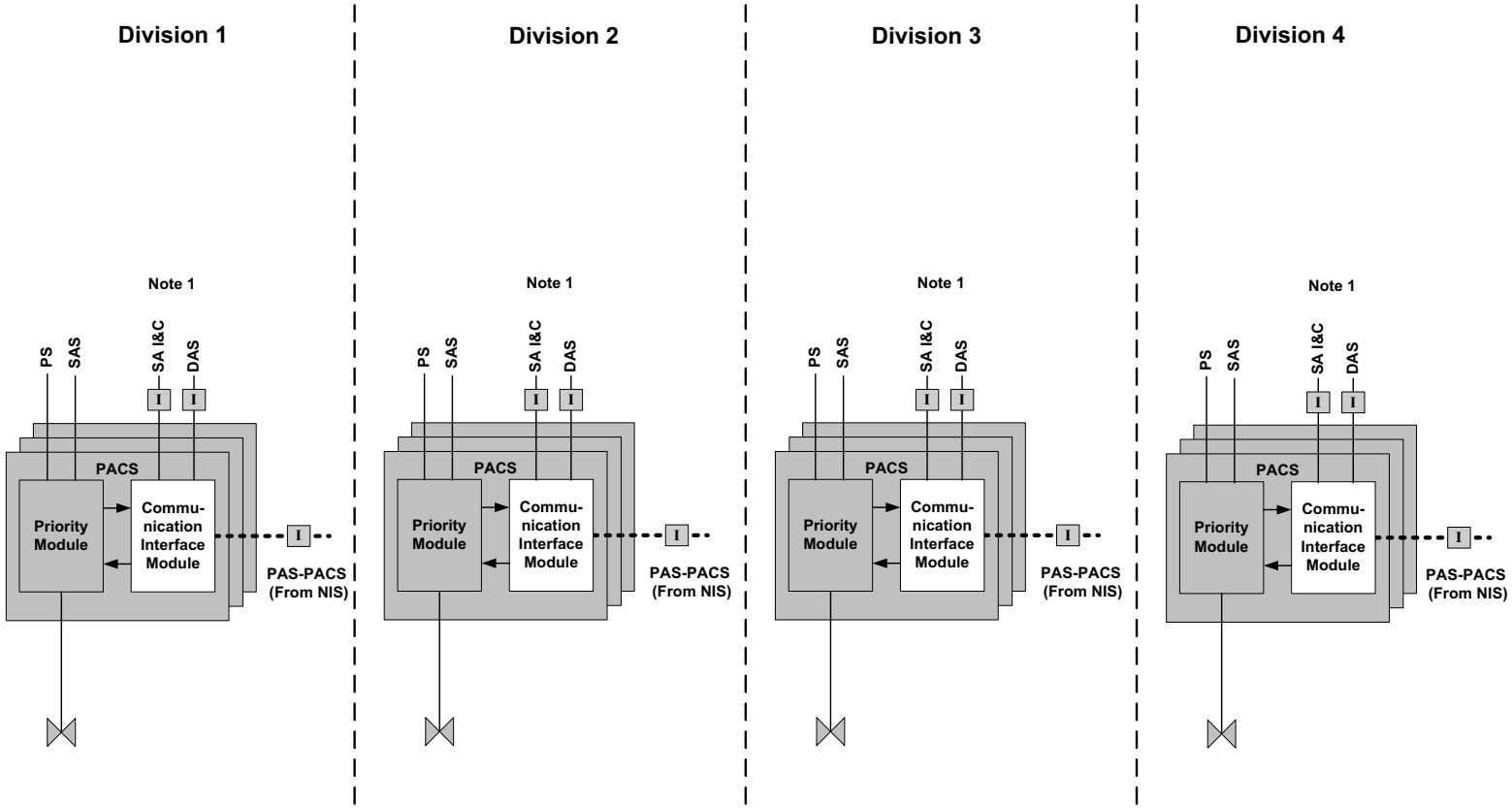


Figure 7.1-8—Priority and Actuator Control System Architecture



Note 1 – The assignment of the hardwired inputs is in accordance with the functional requirements for the actuator and the priority principles

REV 002
EPR3035 T2

Figure 7.1-13—~~Process Automation~~ Diverse Actuation System Architecture ~~(Diverse Actuation Subsystem)~~

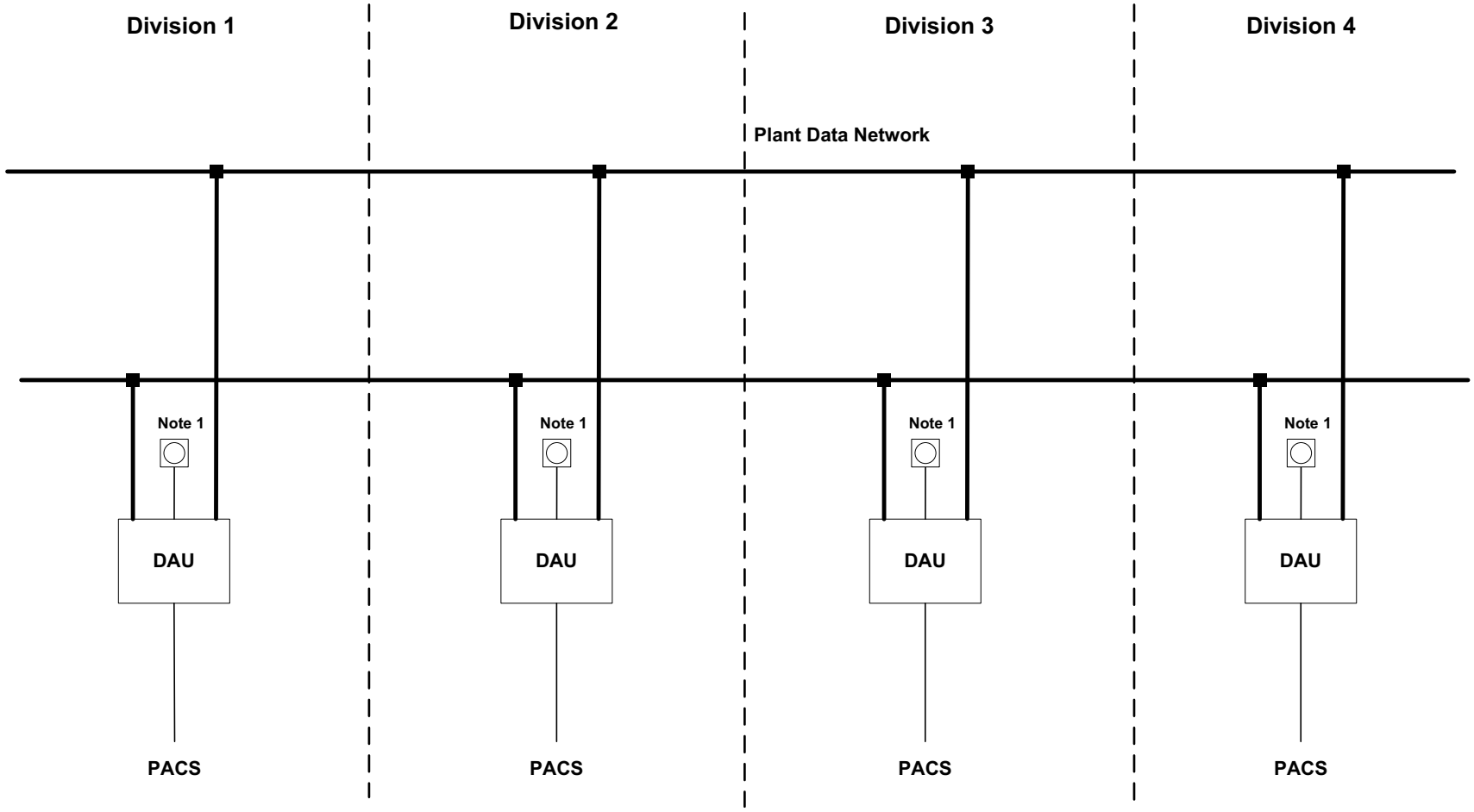
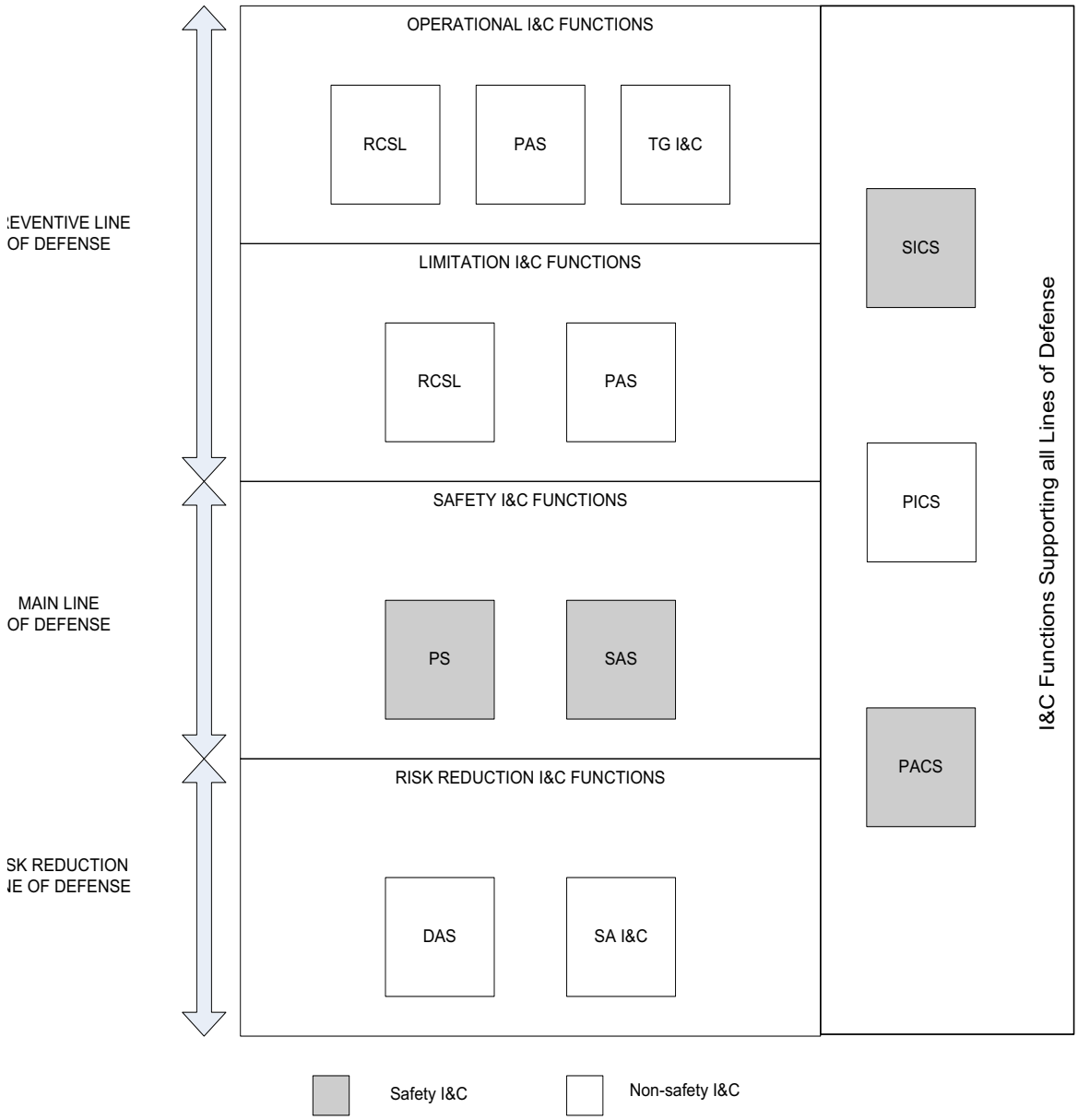


Figure 7.1-17—Implementation of Defense-In-Depth



REV 002
EPR3080 T2

Figure 7.1-18—~~Implementation of Diversity~~Deleted

Figure 7.1-20—Implementation of Independence Between Safety and Non-Safety I&C

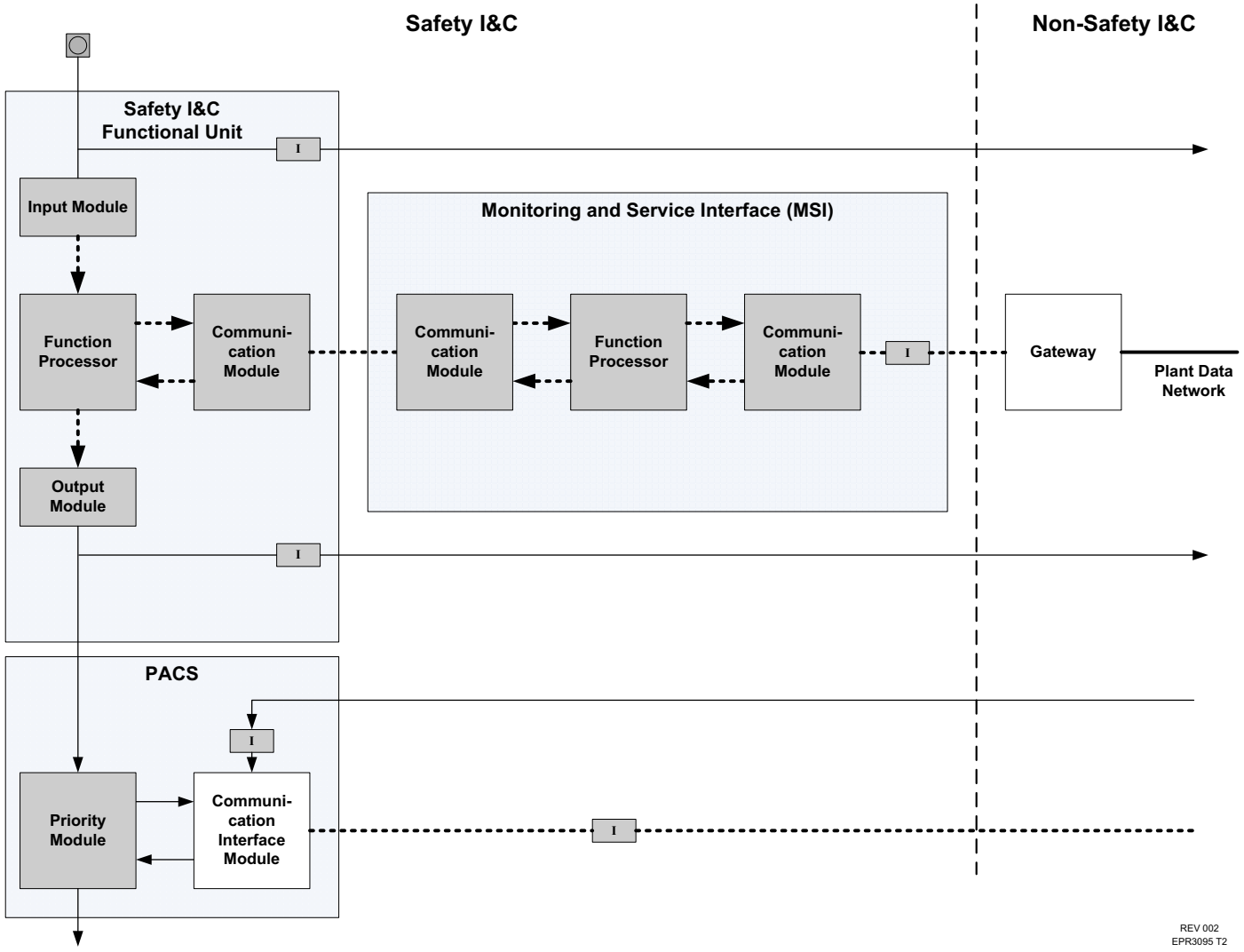
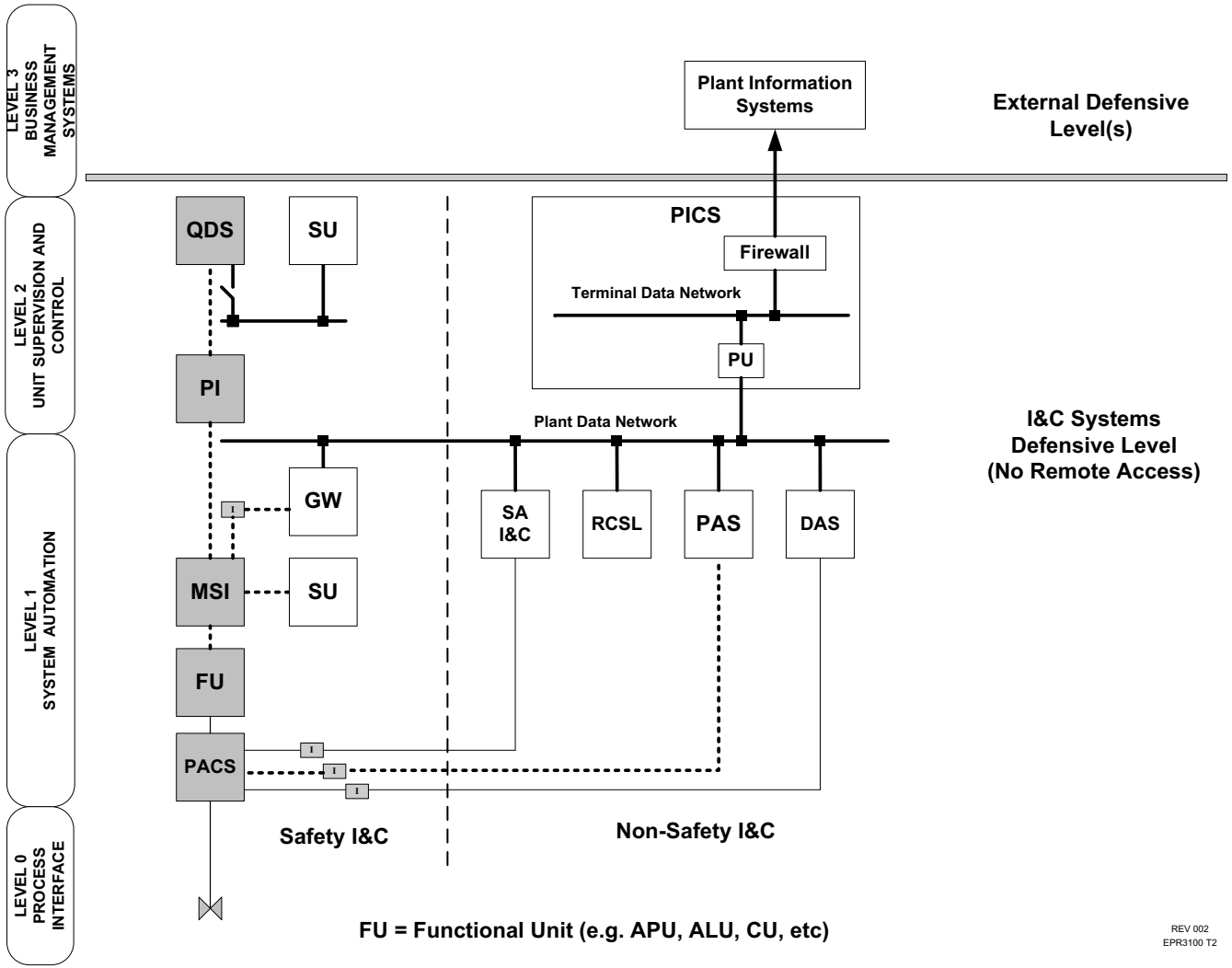


Figure 7.1-21—Levels of Defense for Cybersecurity



Next File

Automatic RT functions that use SPND measurements as inputs utilize an additional level of computer function. This additional level consists of redundant remote acquisition units (RAU) in each division dedicated to the acquisition and distribution of the SPND measurements. The RAU in each division acquire one-fourth of the total SPND measurements and distribute those measurements to APU in all four divisions allowing for an accurate calculation over the whole reactor core in each division. Once the SPND measurements have been received by the APU, the RT function is carried out as described previously in this section for the typical RT function. Figure 7.2-2—Typical SPND-based RT Actuation illustrates the typical RT initiation sequence for SPND-based RT functions.

The capability for manual RT is available to the operator through the safety information and control system (SICS) in both the MCR and RSS. At each location, four manual RT buttons are provided to correspond to the four PS divisions. Manual RT initiation is illustrated in Figure 7.2-3—Manual RT and is also described in ANP-~~10281~~10309P, "U.S. EPR Digital Protection System ~~Topical~~Technical Report" (Reference 1). The SICS is described in Section 7.1.1.2.

7.2.1.2 Reactor Trip Functional Description

The variables monitored by the PS are used either directly or as an input to a calculation, to detect the plant conditions which initiate reactor shutdown:

- Low departure from nucleate boiling ratio.
- High linear power density.
- High neutron flux rate of change.
- High core power level.
- Low saturation margin.
- Low reactor coolant system loop flow (two loops).
- Low-low reactor coolant system loop flow (one loop).
- Low reactor coolant pump speed.
- High neutron flux.
- Low doubling time.
- Low pressurizer pressure.
- High pressurizer pressure.
- High pressurizer level.

7.2.3 References

1. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March 2007~~November 2009.

2. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

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

4. ANP-~~10284~~10304, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology ~~Topical~~Technical Report," AREVA NP Inc., ~~June 2007~~May 2009.

5. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., March 2007.

6. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

7. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

7.3 Engineered Safety Features Systems

7.3.1 Description

The U.S. EPR provides safety-related instrumentation and controls to sense accident conditions and automatically initiate the engineered safety features (ESF) systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions that require protective action. Additionally, the ability to manually initiate ESF systems is provided in the main control room (MCR). Manual actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions.

7.3.1.1 System Description

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the protection system (PS) when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the priority and actuator control system (PACS) for prioritization and interface to the actuators. The typical ESF actuation sequence performed by the protection system is illustrated in Figure 7.3-1—Typical ESF Actuation, and is described as follows:

- An acquisition and processing unit (APU) in each division acquires one-fourth of the redundant sensor measurements that are inputs to a given ESF actuation function.
- The APU in each division performs any required processing using the measurements acquired by that division (e.g., filtering, range conversion, calculations). The resulting variable is compared to a relevant actuation setpoint in each division. If a setpoint is breached, the APU in that division generates a partial trigger signal for the appropriate ESF function.
- The partial trigger signals from each division are sent to redundant actuation logic units (ALU) in the PS division responsible for the associated actuation. Two out of four voting is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated.
- The actuation signals of the redundant ALU in each subsystem are combined in a hardwired "OR" configuration so that either redundant unit can actuate the function.

Actuation orders are sent from the PS to the PACS priority module associated with each actuator required for the function. Exceptions to this are the emergency diesel generator (EDG) start function and the turbine trip function. These actuation orders are received by the associated control system (EDG or turbine controls) and do not involve ~~a~~the PACS~~ module~~. The PS and the PACS are discussed in Section 7.1.

The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in Section 7.3.1.2 with their associated actuation functions. The SAS is described in Section 7.1.

The capability for manual ESF actuations is available to the operator through the safety information and control system (SICS) in the MCR. These manual actuations ~~either~~ are acquired by the ALUs in the protection system and combined with the automatic actuation logic.~~, or are implemented to bypass the computerized portions of the protection system.~~ The manual actuations are described with the corresponding automatic function in Section 7.3.1.2.

The capability for manual reset of sense and command ESF actuation outputs is provided on both the process information and control system (PICS) and the SICS. Not all ESF actuations require a manual reset. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is described in Section 7.3.1.2. Further description of the operation of the PICS and SICS is presented in Section 7.1.

7.3.1.2 Engineered Safety Features Actuation Functional Descriptions

7.3.1.2.1 Safety Injection System Actuation

To mitigate a loss of coolant accident (LOCA) or overcooling event, a safety injection signal is required to actuate the appropriate ESF and support systems and to isolate non-qualified reactor coolant system (RCS) piping.

In case of a decrease in RCS water inventory due to a LOCA, the RCS is supplied by medium head safety injection (MHSI) in the high pressure phase of the event and low head safety injection (LHSI) in the low pressure phase.

In case of an overcooling event, boron addition via MHSI can offset positive reactivity insertion if the RCS pressure decreases below the shut-off head of the MHSI pumps.

The operation of the MHSI and LHSI systems is described in Section 6.3.

The U.S. EPR design provides for automatic generation of the safety injection signal during all modes of plant operation by utilizing three different initiation parameters depending on the current plant state:

- Pressurizer pressure <Min3p.
- Hot leg ΔP_{sat} <Min1p.
- RCS loop level <Min1p.

This isolation is performed in two stages with staggered setpoints. The following initiating conditions are used to perform the two stages of CVCS isolation:

- Pressurizer Level > Max1p.
- Pressurizer Level > Max2p.

If two-out-of-four level measurements exceed the Max1p setpoint, orders are generated to isolate the normal and auxiliary pressurizer spray lines. If two-out-of-four level measurements exceed the Max2p setpoint, orders are generated to isolate the CVCS charging flow as well.

These CVCS isolation functions are bypassed when cold leg temperature is below the P17 permissive setpoint. The bypass is automatically removed above the P17 setpoint. Generation of the P17 permissive signal is discussed in Section 7.2.1.3.

The capability for manual initiation of CVCS isolation ~~on a per-valve basis~~ is provided on a per-division basis on the SICS in the MCR. One manual isolation control is provided for ~~each valve. These controls bypass the functional units of the PS and are acquired by the PAC modules associated with each actuator~~PS Division 1, and one control is provided for PS Division 4.

A manual reset of the sense and command outputs is not required for the CVCS isolation function. The outputs are automatically reset when the level measurements return below the appropriate setpoint. A pulse order is used to provide assurance that the actions of the execute features go to completion. The automatic reset of the sense and command outputs does not result in change of state of the isolation actuators; it allows the operator to take further manual actions to change the state of individual actuators.

The functional logic for CVCS charging isolation is shown in Figure 7.3-21—CVCS Charging Isolation.

7.3.1.2.11 CVCS Isolation for Anti-Dilution

To mitigate the risk of dilution of the RCS boron concentration, a CVCS isolation is required to secure potential dilution flow paths. This function provides protection during all plant conditions by using different combinations of input signals depending on the current plant state. The function is divided as follows:

- Power operation (above permissive P8).
- Shutdown conditions with RCPs in operation (below permissive P8 and above permissive P7).
- Shutdown conditions without RCPs in operation (below permissive P7).

In shutdown conditions without RCPs in operation, the measured boron concentration is simply compared to a fixed setpoint. This setpoint represents the boron concentration required under outage conditions, minus built-in margin to prevent spurious actuations.

Regardless of the current operating conditions, if any two of the four PS divisions determine that dilution is occurring, redundant valves downstream of the volume control tank are closed. This isolates the main CVCS source of dilution. Additionally, the RHR letdown isolation valve is closed.

The capability for manual initiation of CVCS isolation for anti-dilution on a ~~per-valve~~per-division basis ~~is provided~~ on the SICS in the MCR. One manual isolation control is provided for ~~each valve. These controls bypass the functional units of the PS and are acquired by the PAC modules associated with each actuator~~PS Division 1, and one control is provided for PS Division 4.

The sense and command outputs for CVCS isolation for anti-dilution can be reset manually from both the PICS and SICS. Reset of the sense and command outputs does not result in change of state of the isolation valves; it allows the operator to take further manual actions to change the state of individual actuators.

The functional logic for CVCS isolation for anti-dilution is shown in Figure 7.3-22—CVCS Isolation for Anti-Dilution.

7.3.1.2.12 Emergency Diesel Generator (EDG) Actuation

During normal plant operation, the electrical power for the safety-related loads is provided by dedicated offsite emergency auxiliary transformers (EAT) for distribution to the emergency power supply system (EPSS). To mitigate the effects of a loss of offsite power (LOOP) event, each division of the EPSS is provided an EDG as a standby source to supply electrical power to the necessary loads.

The EPSS consists of different voltage levels: medium voltage (MV) for large safety-related loads and low voltage for other loads. The four main MV distribution buses that provide power to the four divisions of the EPSS have a normal connection to one of the two dedicated EATs but can be alternately supplied from the other dedicated EATs or the EDG for that division.

The three phases of voltage on each main MV bus are monitored by the PS to detect either a degraded voltage condition or a loss of voltage condition. If the voltage measurements for two of the three phases on a bus fall below a fixed setpoint for a fixed amount of time, a degraded voltage condition exists. If the voltage measurements for two of the three phases on a bus fall below a lower fixed setpoint for a fixed amount of time, a loss of voltage condition exists. In either case, a LOOP signal is generated within the PS which starts the corresponding EDG and begins the loading sequence.

All four EDGs are also started automatically when a safety injection signal is generated, but they are not connected to the EPSS unless a LOOP signal is also generated.

The automatic EDG start and load sequence consists of the following:

- Each main MV bus is monitored for proper voltage and if the voltage is below a setpoint for greater than a predetermined period of time, a LOOP signal is generated.
- The EDG is started.
- The EPSS is isolated from the division's preferred sources of power.
- The large loads are removed from the EPSS.
- The EDG is connected to the EPSS.
- The loads are sequenced onto the EPSS.

In general, smaller loads that were energized before the loss of power automatically re-start when power from the EDG becomes available. This functionality is provided by the ~~PAC~~priority modules associated with each actuator. Large electrical loads are sequenced onto the EPSS according to diesel load steps (DLS) to maintain EDG output voltage and frequency reductions within acceptable limits. The PS performs the DLS functionality by maintaining an "off" signal to the actuators, and then removing the signal to a sub-set of actuators at each load step which allows them to be re-started. CVCS charging pumps are not re-started automatically regardless of whether or not they were previously running. Essential service water (ESW) and component cooling water (CCW) pumps are automatically started as part of the load sequence regardless of whether or not they were previously running.

When a LOOP signal is generated, different DLS sequences are used depending on whether or not a safety injection signal is also present. The different sequences are detailed in Table 8.3-4 through Table 8.3-7.

In absence of a safety injection signal, the CCW and ESW pumps are started as part of the first two load steps. The "off" signal is removed from the safety injection components at their predefined steps, but the safety injection pumps are not started. If a safety injection signal is generated after the LOOP-only loading sequence has begun, the sequence is stopped, the LOCA mitigation loads are started, then the LOOP-only sequence is re-entered and completed.

If a safety injection signal is present when the LOOP signal is generated, the LOCA mitigation loads are started in the first several steps of the load sequence. The other loads are then sequenced onto the EPSS according to pre-defined load steps.

The capability for manual PSRV opening on a per-PSRV basis is provided to the operator on the SICS in the MCR. Two manual initiation controls are provided per PSRV, both of which must be activated to open a PSRV. ~~These manual controls bypass the functional units of the PS and are acquired by the PAC modules associated with each actuator.~~

No manual reset of the PSRV opening sense and command output is required. The output is automatically reset when the hot leg pressure measurements return within an acceptable range. Reset of the sense and command output results in valve closure.

The functional logic for automatic PSRV opening is shown in Figure 7.3-24—PSRV Opening (Brittle Fracture Protection).

7.3.1.2.14 Steam Generator Isolation

In case of an SGTR, partial cooldown is initiated to depressurize the RCS to the point where MHSI becomes effective. The SG containing the tube rupture is isolated after the partial cooldown is initiated if a high SG level or high main steam activity level is detected. This is done to prevent the release of contaminated fluid from the affected SG, and to prevent other water sources from adding to the uncontrolled SG level increase. SG isolation consists of the following main actions:

- MSRT opening setpoint increase.
- MSIV, MSIV bypass, and SG blowdown closure.
- MFW and SSS isolation.
- EFWS isolation (confirmatory action; EFWS should already be isolated as described in Section 7.3.1.2.3).

Operation of the main steam system is described in Section 10.3. Operation of the SG blowdown system is described in Section 10.4.8. Operation of the MFW and SSS systems is described in Section 10.4. Operation of the EFW system is described in Section 10.4.9.

The U.S. EPR design uses the following initiating conditions to actuate SG isolation:

- Partial cooldown actuated and SG level NR > Max2p.
- Partial cooldown actuated and main steam activity > Max1p.

SG isolation orders are generated when two-out-of-four SG level NR measurements on any one SG exceed the Max2p setpoint and partial cooldown has been actuated. The same isolation orders are generated when two-out-of-four main steam activity measurements on any one SG exceed the Max1p setpoint and partial cooldown has

been actuated. In both cases, only the affected SG is isolated and the partial cooldown function is performed via the remaining SGs.

~~There is no operating bypass explicitly associated with the SG isolation function.~~ The SG Isolation function is bypassed when hot leg temperature is below the P13 permissive setpoint. Generation of the P13 signal is discussed in Section 7.2.1.3. However, when the partial cooldown actuation function is bypassed (Section 7.3.1.2.4), the SG isolation function is bypassed by association to the partial cooldown actuation signal.

The capability for manual initiation of SG isolation on a per SG basis is provided on the SICS in the MCR. Four manual initiation controls are provided per SG, any two of which will isolate the desired SG.

Reset of the SG isolation sense and command output is available from both the PICS and SICS. A reset of the sense and command output does not result in a change of state of the isolation actuators; it allows the operator to take further actions to manipulate individual components as may be necessary to follow plant operating procedures.

The functional logic for automatic SG isolation is shown in Figure 7.3-25—SG Isolation (Div. 1&2) and in Figure 7.3-26—SG Isolation (Div. 3&4).

7.3.1.2.15 Reactor Coolant Pump Trip

In case of a SBLOCA, RCPs are tripped when conditions indicate that two-phase flow is present. This is done because the RCPs may subsequently be lost due to cavitation or operation in a degraded environment. Forced convection of the two-phase flow increases the mass lost via the break. If the RCPs are permitted to operate for an extended period of time in this condition and then are shut down, an inadequate core cooling condition may occur due to insufficient liquid inventory as the two phases separate. For this reason, an automatic RCP pump trip is provided early after two-phase flow is indicated, while the void fraction is still relatively low, to enhance long term accident mitigation and minimize the potential for RCS mass depletion.

Additionally, the RCPs are tripped on a containment isolation stage two signal.

The operation of the RCPs is described in Section 5.4.1.

The U.S. EPR design uses the following initiating conditions to actuate RCP trip:

- ΔP across RCP < Min1p and SIS actuation signal generated.
- Stage two containment isolation signal generated.

The RCP trip based on differential pressure across the RCP results from one of two ΔP measurements below the Min1p setpoint on any two-of-the-four RCPs. A safety

7.3.2.1.5 Design Basis: Spatially Dependent Variables (Clause 4.f of IEEE Std 603-1998)

The U.S. EPR design uses no spatially dependent variables as inputs to ESF actuation functions.

7.3.2.1.6 Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j of IEEE Std 603-1998)

The PS initiates operation of ESF systems when selected variables exceed the associated setpoints. The plant conditions that define the proper completion of the safety function performed by an ESF system are defined on an event-by-event basis in the Chapter 15 analyses. The actions of the execute features for an ESF actuation function are complete when, for example, a valve has reached its full open or full closed position, or required flow has been established by a pump.

The ESF actuation logic generally allows ESF actuation outputs generated by the PS to be reset after completion of the actions of the execute features. The reset of the ESF actuation signal does not result in change of state (return to normal) of the ESF actuator. Plant specific operating procedures govern the point in time when the ESF actuators can be returned to normal following their actuation.

7.3.2.2 Failure Modes and Effects Analysis

A system-level failure modes and effect analysis (FMEA) is performed on the PS to identify potential single point failures and their consequences. The architecture of the PS as defined in the U.S. EPR Digital Protection System ~~Topical~~Technical Report (Reference 1) is used as the basis for the analysis. The FMEA considers each major part of the system, how it may fail, and the effect of the failure on the system.

Because the PS is an integrated RT and engineered safety features actuation system (ESFAS), a single failure in the system has the potential to affect both types of functions. Therefore, a single FMEA is performed on the PS and the effects on both RT and ESFAS functions are considered. The result of the FMEA with regard to ESF actuation functions is summarized in this section. A summary of the effects of single failures on the RT functions is provided in Section 7.2.

To define the major parts of the system for which failures are assumed, a single division of the PS is divided into functional units as described in Reference 1. The PS consists of four identical divisions, so the definition of functional units is the same for each division. The following are defined as functional units that participate in the generation of automatic ESF actuation functions and are included in the analysis:

- Acquisition and processing units (APU).
- Actuation logic units (ALU).

In addition to the equipment defined as functional units of the system, the following equipment contribute to automatic ESF actuation functions and are analyzed as part of the system-level FMEA:

- Sensors that provide input measurements to ESF actuation functions.
- Hardwired output logic used in ESF actuation function.
- PACS priority modules.

In order to bound the possible failures, both detected and undetected failures of sensors and digital equipment are analyzed and the worst 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 a failure not automatically detected which results in a spurious partial trigger or actuation. A failure denoted "undetected – blocking" is defined as a failure not automatically detected which results in failure to issue a partial trigger or actuation when needed.

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

Network failures within the PS 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, and is therefore not considered. 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, and is therefore not considered. Further information regarding the communication methods used and communication failure detection capabilities is found in Reference 1 and in the Reactor Protection System Topical Report (Reference 2).

The architecture of the PS allows APUs and ALUs to be analyzed for single failure without regard to which specific APU or ALU in the division is the failure point. For these single failures, all functions of the system are considered affected, as every function is processed by at least one APU and two ALU in a division. Considering the effect on every function of the system bounds all cases of specific APU and ALU single failures.

When referring to the nature of a single failure, the terms “detected” and “undetected” used in the context of the PS FMEA do not correspond to the definition of a detectable failure in Reference 5. 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 the PS to automatically detect a failure through self-surveillance.

Failures of instrument air systems are not considered in support of the PS FMEA. The ESF actuation and control functions in the U.S. EPR design do not rely on common instrument air systems.

The results of the FMEA with regard to the effects of single failures on ESF actuation functionality are summarized in Table 7.3-2—FMEA Summary for ESF Actuations.

The unique nature of the EDG actuation function described in Section 7.3.1.2.12 requires unique treatment in the FMEA. In this case, redundancy is obtained completely within a single division of the PS, so the results of the system level FMEA do not hold true for this function. The FMEA results for the EDG actuation function are summarized in Table 7.3-3—FMEA Summary for EDG Actuation.

The number and allocation of sensors as inputs to the RCP trip function described in Section 7.3.1.2.15 require unique treatment in the FMEA as well. The FMEA Results for the RCP trip function are summarized in Table 7.3-4—FMEA Summary for RCP Trip.

7.3.2.3 Conformance to Applicable Criteria

7.3.2.3.1 Compliance of ESF Actuation Functions to the Single Failure Criterion (Clause 5.1 of IEEE Std 603-1998)

The PS maintains the ability to perform all ESF actuation functions in the presence of any credible single failure of an input sensor, functional unit of the PS, or PACS priority module. This is an extension of the redundancy designed into the ESF systems themselves. In general, different divisions of the PS are assigned to actuate those parts of an ESF system considered redundant to one another. Additional redundancy is designed into the PS in the form of redundant ALUs within each division, each capable of actuating one redundant portion of an ESF system.

In most cases, single failures upstream of the ALU voting logic (sensor or APU failure) are accommodated by the voting logic. The voting logic is modified to disregard the input affected by the failure and the ability to actuate based on the remaining inputs is retained. In the case of the EDG actuation function, sensor failures are accommodated by a second min. signal selection. Failure of an APU is accommodated in the EDG actuation function by a redundant APU in the other subsystem of the same division performing the same function.

Single failures at the level of the voting logic are accommodated by both redundancy within each division and redundancy between more than one division. In all cases, either of two redundant ALU within a division can actuate one redundant portion of an ESF function and, except for EDG actuation and EFWS isolation, at least one other division can actuate a second redundant portion of the same ESF function. In the cases of the EDG actuation and the EFWS isolation functions, either of two redundant ALU within a division can perform the voting logic and actuation portions of the functions.

Single failures of PACS priority modules are bounded by the single failure tolerance of the ESF systems themselves. An individual PACS priority module is assigned to each individual actuator so that the failure of a single PACS priority module is no different than the failure of the actuator itself.

A system level FMEA is performed to verify conformance with the single failure criterion. The FMEA is described in Section 7.3.2.2, and the results are summarized in Table 7.3-2, Table 7.3-3, and Table 7.3-4.

7.3.2.3.2 Compliance to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE 7-4.3.2-2003)

Protection system components and modules that are required to perform ESF actuation functions are classified as safety-related, are designed to Class 1E standards, and are applied in accordance with a stringent quality assurance program. Software used to perform ESF actuation functions is developed and applied in accordance with a safety-related software program. Further discussion of conformance to requirements for quality is found in Section 7.1.

7.3.2.3.3 Compliance to Requirements for Independence of ESF Actuation Functions (Clauses 5.6 and 6.3 of IEEE Std 603-1998 and GDC 24)

Redundant portions of the PS are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing an ESF actuation function. Both electrical and communication independence are maintained as described in Section 7.1 and in Reference 1.

Equipment required to perform ESF actuation functions is independent from the effects of the events which the ESF function mitigates. The functional units of the PS are located in areas that are not subject to degraded environmental conditions as the result of an event. Equipment located in areas subject to a degraded environment following an event (e.g., sensors) is qualified to operate as required in the expected post-event environment. Environmental qualification of instrumentation and control equipment is discussed in Section 3.11 and Section 7.1.

The PS does not rely on input from any non-safety-related control system to perform an ESF actuation function. The plant accident analysis does not credit actions taken by

non-safety-related control systems to improve the response of ESF actuation functions. If a control system action can make the effects of an event more severe, then the action is assumed to occur. In this way, the ESF actuation function is demonstrated to mitigate the event independently of any non-safety-related control system. Certain sensor measurements are shared as inputs to both an ESF actuation function and a plant control function. In these cases, the measurement is acquired by the signal conditioning of the PS. The signal is multiplied and passed to the control system through an electrically isolated connection, to maintain the independence of the ESF actuation function. Single failures of shared sensors do not impair the functioning of the control system or the ESF actuation function.

Conformance to requirements concerning independence of safety-related instrumentation and control (I&C) systems is addressed further in Section 7.1.

7.3.2.3.4 Compliance to Requirements for Completion of Protective Action (Clauses 5.2 and 7.3 of IEEE Std 603-1998)

Once an ESF actuation function is initiated by the PS, the intended actions of the execute features proceed to completion. The return-to-normal state of ESF actuators requires deliberate operator intervention. In most cases, operator action is required to reset the actuation signal, and separate operator action is required to change the state of the actuated device. When operator action is not required to reset the actuation signal, measures are taken to prevent change in state of the actuated device until the intended actions of the execute features are completed. In many cases, the removal of the PS actuation order from the associated PACS priority module does not result in a change of state of the actuator (e.g., motor operated valves). In cases where removal of the PS actuation order from the associated PACS priority module would result in the actuator changing state (e.g., certain solenoid operators), seal-in features are incorporated in the execute features. These seal-in features allow the reset of the actuation signal while requiring additional operator action to affect the state of the actuated device.

7.3.2.3.5 Compliance to Requirements Concerning Diversity and Defense in Depth (Clause 5.16 of IEEE Std 603-1998)

A non-safety-related diverse actuation system (DAS) is provided to perform selected automatic ESF actuation functions in the unlikely event of a common cause software failure that renders the entire PS inoperable. The hardware and software utilized in the DAS are diverse from that used in the PS so that the DAS cannot be subject to the same common cause failure as the PS. The functionality of the DAS is described in Section 7.1 and Section 7.8.

Additionally, manipulation of every ESF system component at the individual component level is available through a processing path completely diverse from the software-based portions of the PS.

The overall EPR I&C approach to diversity and defense in depth is described in the Instrumentation and Control Diversity and Defense in Depth ~~Topical~~Technical Report (Reference 3).

7.3.2.3.6 Compliance to System Testing and Inoperable Surveillance Requirements (Clause 5.7 of IEEE Std 603-1998)

The design of the PS allows for testing of automatic ESF actuation functions while retaining the capability to perform the functions in response to an event requiring protective action. The majority of the PS and PACS components required for ESF actuation can be tested with the reactor at power. Surveillance of the PS consists of overlapping tests to verify performance of the ESF actuation function from sensor to PACS priority module. Surveillance of the ESF system components consists of actuating the component through the PACS priority module in a manner that overlaps the PS surveillance of the PACS priority module.

The computerized portions of the PS are continuously monitored through self-testing during power operation. During outages, extended computer self-testing is performed to verify functionality that cannot be tested with the reactor at power.

Sensors and acquisition circuits are periodically tested. The input channel to be tested is placed in a lockout condition, and the downstream voting logic is automatically modified to disregard the input being tested. The ESF actuation functions are still performed using the redundant input channels.

The connections between the PS output circuits and the PACS priority modules can be tested during power operation. One division of the PS is tested at a time and the outputs of the PACS priority modules are disabled so that the actuators are not affected by the test. If an ESF actuation order is generated during the time that a PACS priority module is in test mode, the outputs of the PACS priority module are enabled and the ESF actuation is carried out.

7.3.2.3.7 Compliance to Requirements Regarding the Use of Digital Systems (IEEE-7-4.3.2-2003)

The automatic ESF actuation functions are implemented using the TELEPERM XS digital platform (Reference 2) which is approved for use in safety-related systems of nuclear power generating stations in the United States. The ESF actuation functions are implemented in an architecture designed to satisfy requirements applicable to all safety-related I&C systems, digital or otherwise.

Implementation of safety-related I&C systems is governed by the requirements of Reference 5. Guidance on the use of digital computers in safety-related systems is provided by Reference 6. Conformance to these standards is described in Section 7.1.

7.3.2.3.8 Conformance to Requirements for ESF Actuation Setpoint Determination

Each setpoint used to actuate an ESF system is selected based on the safety limits assumed in the plant accident analysis. The ESF actuation setpoints provide margin to the safety limit and take into account measurement uncertainties. The methodology to determine setpoints for ESF actuation functions is documented in the Instrument Setpoint Topical Report (Reference 4).

7.3.3 References

1. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March 2007~~November 2009.

2. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

3. ~~ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 20, 2007~~ANP-10304P, Revision 1, "U.S. Diversity and Defense-In-Depth Assessment Technical Report," AREVA NP Inc., November 2009.

4. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., March 26, 2007.

5. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

6. IEEE 7.4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

Table 7.3-1—ESF Actuation Variables

Protective Function	Variables To Be Monitored	Range of Variables
Safety Injection System Actuation	Pressurizer Pressure (NR)	1615-2515 psia
	Hot Leg Pressure (WR)	15-3015 psia
	Hot Leg Temperature (WR)	32-662°F
	RCS Loop Level	0-30.71 in.
Reactor Coolant Pump Trip	RCP differential pressure	0-120% nominal
	RCP current measurement	0-120% nominal
Emergency Feedwater Actuation	SG Level (WR)	0-100% MR
Emergency Feedwater Isolation	SG Level (WR)	0-100% MR
SG Isolation	Main Steam Line Activity	$1x10^{-1}$ – $1x10^{4}$ counts/ sec.
	SG Level (NR)	0-100% MR
Main Steam Relief Train Actuation	SG Pressure	15-1615 psia
Main Steam Relief Train Isolation	SG Pressure	15-1615 psia
Main Steam Isolation	SG Pressure	15-1615 psia
Main Feedwater Isolation	SG Level (NR)	0-100% MR
	SG Pressure	15-1615 psia
	RT Breaker Position	Open/Closed
Containment Isolation	Cont. Service Compartment Pressure (NR)	-3 to +7 psig
	Cont. Service Compartment Pressure (WR)	~~0-75~~-5-220 psig
	Cont. Equipment Compartment Pressure	-3 to +7 psig
	Containment High Range Activity	$1x10^{-1}$ – $1x10^{7}$ Rad/hr
Emergency Diesel Generator Actuation	6.9 kV Bus Voltage	0-8.625 kV
PSRV Opening	Hot Leg Pressure (WR)	15-3015 psia
CVCS Charging Isolation	Pressurizer Level (NR)	0-100% MR
CVCS Isolation for Anti-Dilution	Boron Concentration	0-5000 ppm
	Boron Temperature	32-212°F
	CVCS Charging Flow	0-320,000 lb/hr
	Cold Leg Temperature (WR)	32-662°F
MCR A/C Isolation and Filtering	MCR Air Intake Duct Activity	$1x10^{-5}$ – $1x10^{1}$ Rad/hr
Turbine Trip	RT Breaker Position	Open/Closed

Table 7.3-2—FMEA Summary for ESF Actuations
Sheet 2 of 2

Single Failure	Nature of Failure	System Response (Effect on ESF Actuation Portion)	Effect on Plant
Priority ~~and Actuator Control~~ Module	Undetected - Spurious	Spurious actuation signal given to attached actuator	Spurious actuation of a single actuator (Note 1)
	Undetected - Blocking	Failure to actuate attached actuator; Redundant divisions remain operational (Note 2)	None

Notes:

1. Plant actuators which, if spuriously actuated, can challenge plant safety require actuation signals from more than one division to actuate (e.g., more than one pilot operator actuated from different divisions are required to change the state of the main valve).

2. For EFWS isolation function, redundancy is within the same division with two sets of hardwired logic and two separate ~~PACS~~priority modules.

Table 7.3-3—FMEA Summary for EDG Actuation
Sheet 2 of 2

Single Failure	Nature of Failure	System Response (Effect on ESF Actuation Portion)	Effect on Plant
Priority ~~and Actuator Control~~ Module	Undetected - Spurious	Not Applicable; The EDG start signal does not use a PAC module, it is sent to the EDG controls	None
	Undetected - Blocking	Not Applicable; The EDG start signal does not use a PAC module, it is sent to the EDG controls	None

Notes:

1. The outputs to start EDG from the two ALU in each sub-system are combined in "AND" logic. The result of the "AND" logic of each sub-system is combined with the same from the other sub-system within the division. In this configuration, redundancy is obtained between sub-systems rather than between the two ALU within a sub-system.

Table 7.3-4—FMEA Summary for RCP Trip
Sheet 2 of 2

Single Failure	Nature of Failure	System Response (Effect on ESF Actuation Portion)	Effect on Plant
Priority ~~and Actuator Control~~ Module	Undetected - Spurious	Spurious actuation signal given to attached actuator	Spurious trip of 1 RCP
	Undetected - Blocking	Failure to actuate attached actuator; After time delay, another division opens redundant breaker	None

Note:

1. The failure of a processing unit such that all outputs are "1" is not a postulated single failure mode. The failure in question would result from an output card failing with all outputs "1". Therefore the two RCP trip outputs from the same ALU (to two different pumps) must be through different output cards. This precludes the single failure from resulting in multiple spurious pump trips.

Figure 7.3-21—CVCS Charging Isolation

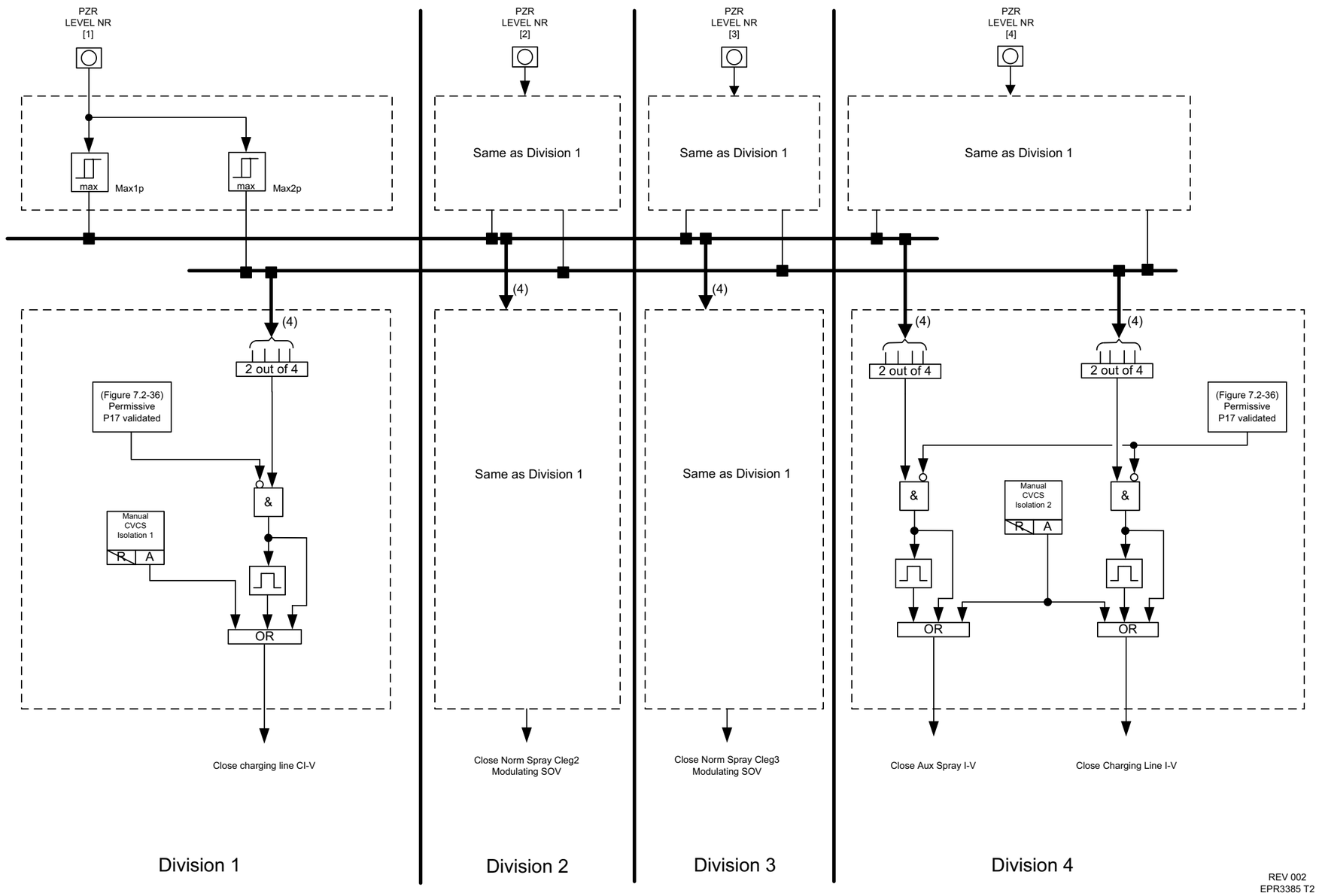


Figure 7.3-22—CVCS Isolation for Anti-Dilution

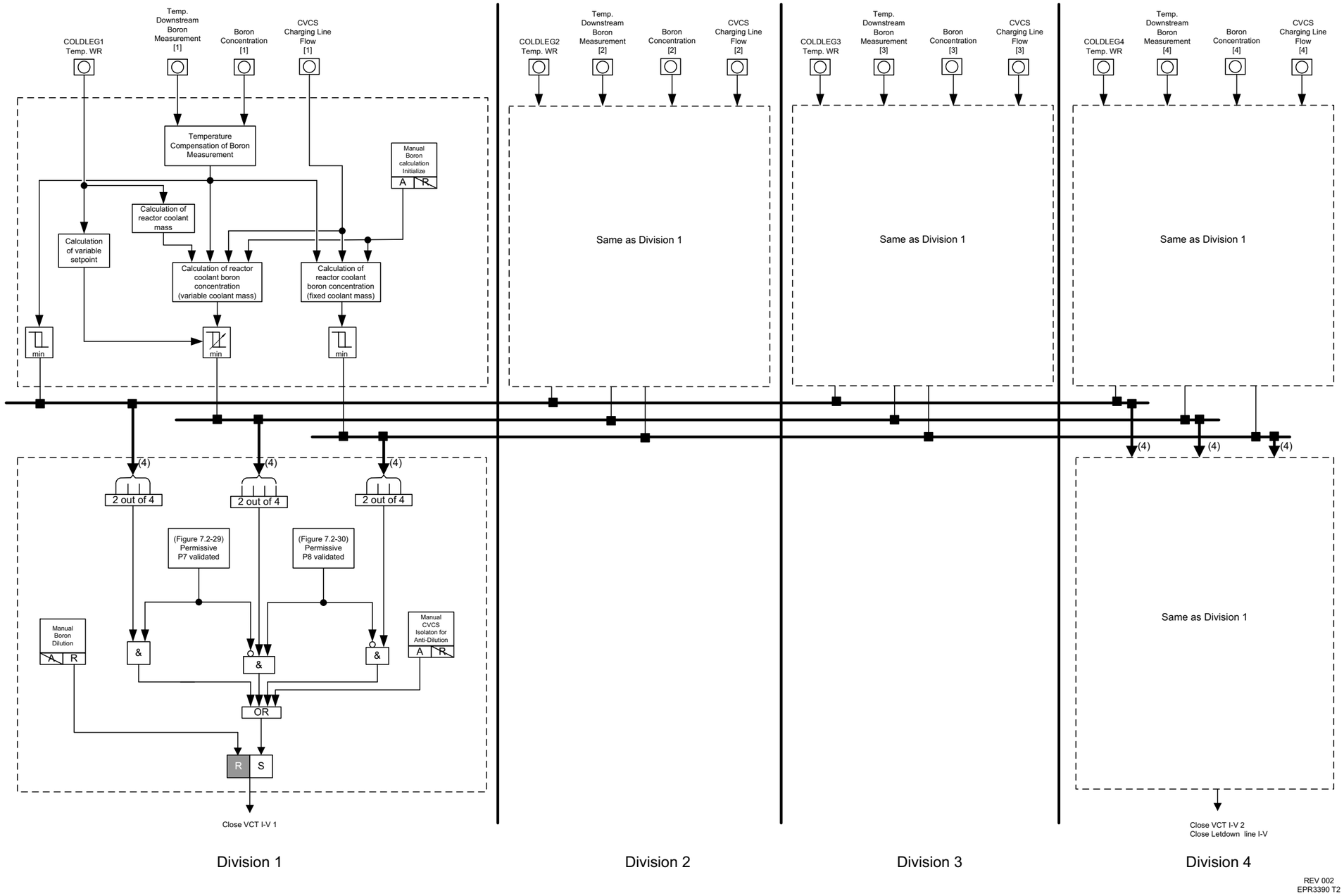


Figure 7.3-24—PSRV Opening (Brittle Fracture Protection)

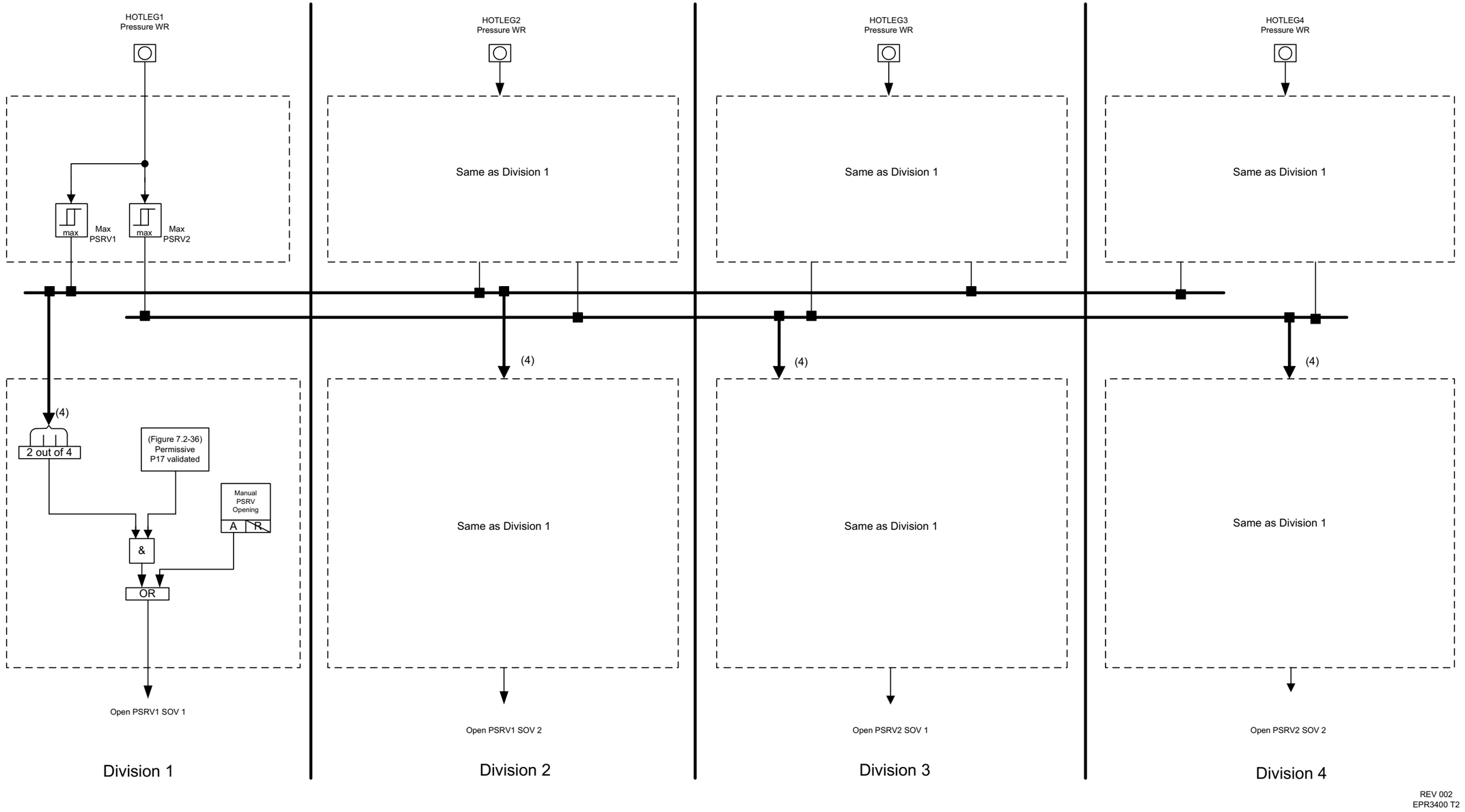
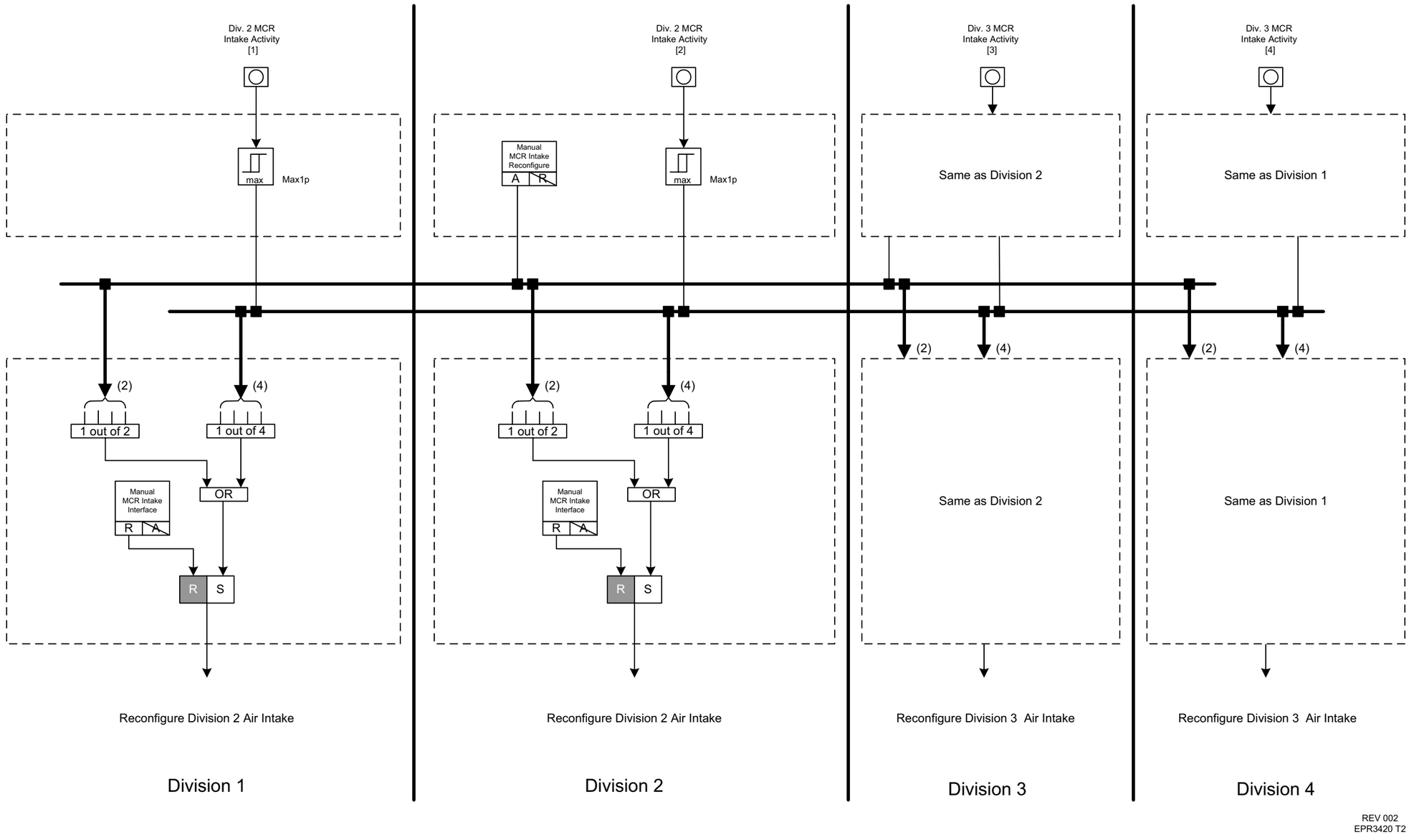


Figure 7.3-28—MCR Isolation and Filtering



In certain scenarios, non-safety-related systems perform shutdown functions. These functions are initiated in the process automation system (PAS). The priority and actuator control system (PACS) ~~module is assigned to~~ controls safety-related components associated with safe shutdown. The functions performed by the priority and actuator control system (PACS) ~~modules~~ are described in Section 7.1.1.4.3.

The human machine interface (HMI) is the PICS. In case of unavailability of the PICS, functions needed to achieve and maintain a safe shutdown condition can be controlled through the SICS. Monitoring and control of the safety-related systems are both available in the main control room (MCR) and the remote shutdown station (RSS).

7.4.1.2 Safe Shutdown Using Safety-Related Systems and Equipment

The plant is designed so that it can be taken from normal operating conditions to cold shutdown using only safety-related systems. The safety-related systems and equipment, that with proper alignment are capable of achieving a safe shutdown of the plant, are described in Section 7.4.1.2.1 through Section 7.4.1.2.13. These systems satisfy GDC 1, GDC 2, GDC 3, and GDC 4.

The systems and equipment described in Section 7.4.1.2.1 through Section 7.4.1.2.13 are capable of bringing the plant to a cold shutdown condition, with only offsite or onsite power available along with the most limiting single failure. The entire shutdown procedure is completed from the MCR.

7.4.1.2.1 Emergency Feedwater System

The emergency feedwater system (EFWS) provides a safety-related means of supplying feedwater to the steam generators (SG) for decay heat removal. This system is capable of maintaining hot standby and facilitating a plant cooldown. The I&C associated with the EFWS, are described in Section 10.4.9.

7.4.1.2.2 Main Steam Supply System

The main steam supply system (MSSS) contains the main steam relief train (MSRT). The MSRT provides secondary side pressure control capability. The MSRT valves are located outside of containment upstream of the main steam isolation valves (MSIV). These valves are used to remove decay heat via the SGs in the event the condenser is unavailable (including loss of power), and to dissipate the heat to atmosphere. The MSRT may be used to cool and depressurize the reactor coolant system (RCS) to conditions necessary to initiate residual heat removal. The MSSS contains the MSIVs and associated bypass valves that are necessary to isolate the secondary plant and to allow decay heat removal by the MSRT. The I&C associated with the MSSS are described in Section 10.3.

Also, the non-safety-classified PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS software. Type A, B, and C accident monitoring variables are acquired by the PAS from the PS or SAS via isolation devices, processed by PAS, and then transmitted to the non-safety classified PICS for display. Therefore, the PAS and the PICS provide a redundant and diverse path for display of the variables.

7.5.2.2.7 Independence and Compliance with IEEE Std 603-1998

Section 7.1 describes the overall I&C system architecture and how independence is achieved between safety and non-safety I&C systems. Compliance to Clause 5.6.3, "Independence Between Safety Systems and Other Systems," and Clause 6.3, "Interaction Between the Sense and Command Features and Other Systems," are addressed in Section 7.1. Requirements of Reference 3 for safety systems meet or exceed the requirements of the endorsed version, IEEE Std 603-1991. A comparison of IEEE Std 603-1991 and IEEE 603-1998 is described in Digital Protection System ~~Topical~~Technical Report ANP-~~10281~~10309P (Reference 9).

7.5.2.2.8 Self Test Provisions

Branch Technical Position BTP 7-17 (Reference 8), provides guidance on the use of self-testing features of digital I&C system. The SICS is designed to maximize the use of automated self-testing features to minimize the burden on plant personnel. The safety-related qualified display system (QDS) within the SICS has the capability to perform automatic self-testing to verify its ability to perform the intended functions. This self-testing feature includes, but is not limited to, the availability of components such as processors, communication and link modules, power supplies, and input-output modules. The positive aspect of these self-testing features is to provide a mechanism for detecting all detectable failures. Furthermore, the positive aspects of the self-test features are not compromised by the additional complexity added to the system design. The self-test features of the SICS do not affect the ability of the system to perform its safety functions.

7.5.3 References

1. IEEE Std 497-2002, "Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2002.

2. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

3. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

4. NUREG-0696, "Functional Criteria for Emergency Response Facility," Nuclear Regulatory Commission, 1981.

5. NUREG-0654, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," Nuclear Regulatory Commission, 1980.

6. NUREG-0737, "Clarification of TMI Action Plan Requirements," Nuclear Regulatory Commission, 1980.

7. NUREG-0800, BTP 7-10, "Guidance on Application of Regulatory Guide 1.97," Nuclear Regulatory Commission, March 2007.

8. NUREG-0800, BTP 7-17, "Guidance on Self Test and Surveillance Provisions," Nuclear Regulatory Commission, March 2007.

9. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March~~November ~~2007~~2009.

10. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Nuclear Regulatory Commission, March 2007.

is prompted to manually acknowledge P12, which allows the isolation valves to be closed before RCS pressure is reduced below the accumulator pressure.

A pressure region exists below the P12 pressure threshold where the accumulators are required to be available but Plant Technical Specifications allow an accumulator isolation valve to be closed for a short period of time. To accommodate operation in this pressure region, an automatic 'open' signal is sent to the accumulator isolation valves when an SIS actuation occurs. The SIS actuation function is described in Section 7.3.1.2.

Two redundant ALU within a division send the automatic opening signal to the isolation valve of the corresponding accumulator (i.e., PS division one opens the isolation valve related to the train 1 accumulator). This arrangement precludes a single actuator logic unit (ALU) failure from preventing the opening of a valve. Any other single failure which could prevent opening of a valve, such as failure of a PACS priority ~~actuation and control (PAC)~~ module or of the valve itself, is detected immediately by failure of the valve to open. Corrective actions can then be taken before continued increase in pressure.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P12 permissive signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Pressure and level of each accumulator.
- Open or closed position of each accumulator isolation valve.

7.6.1.2.3 Interlocks Isolating Redundant CCWS Trains

The CCWS is comprised of four closed-loop, safety-related supply trains that function to cool and transfer heat load from safety users to the heat sink. The common loads cooled by the CCWS consist of two separate sets, referred to as Common-1 and Common-2. The Common-1 header is supplied by either CCW train one or train two while the Common-2 header is supplied by either CCW train three or train four. Each common header is further divided into two sub-headers designated as Common 1a and 1b or Common 2a and 2b.

The operation of the CCWS is described in Section 9.2.2.

Interlocks are provided so that no two redundant CCWS trains are connected to the same common header at the same time. Each CCWS train is provided with four switchover valves to perform the required train separation.

CCWS train one has a single valve on the supply side and a single valve on the return side of Common 1a. Train two also has a single valve on both the supply and return

sides of Common 1a. These valves are interlocked so that both valves (supply and return) on train one must be closed before either valve on train two can be opened. Likewise, both valves on train two must be closed before either valve on train one can be opened. The same valve arrangement and interlocks are provided relative to Common 1b to provide separation between trains one and two, and on Common 2a and 2b to provide separation between trains three and four. The functional logic for the switchover valve interlock is shown in Figure 7.6-1.

Another interlocking function is required concerning the cooling paths of the Common 1b and Common 2b headers toward the reactor coolant pump (RCP) thermal barriers. Either the Common 1b or 2b headers can provide cooling to the RCP thermal barriers. To maintain strict CCWS train separation, the containment isolation valves (CIV) on the RCP thermal barriers cooling path on the supply and return side of Common 1b cannot be opened unless the CIVs on both the supply and return side of Common 2b are closed, and vice versa. The functional logic for the CIV interlock is shown in Figure 7.6-2.

The interlock functions maintaining separation between redundant CCWS trains are performed by the SAS. Each switchover valve is assigned to a SAS division based on the CCWS train it belongs to (i.e., switchover valves on train one are assigned to SAS division one). Each division of SAS acquires position information from the valves to which it is assigned, and controls those same valves. In any SAS division, the information about the position of valves in other trains that is needed to control a switchover valve is provided via network connection by the SAS division which acquires the information. For example, the positions of the train two valves on the supply and return of Common 1a are acquired by SAS division two. This information is transmitted to SAS division one to perform the interlock function for the train one valves on the supply and return of Common-1a.

The interlock function concerning the CIVs is also performed by the SAS, but is only performed in divisions one and four. The CIVs are assigned to SAS divisions for control based on which electrical division provides power to the valves (i.e., valves powered by electrical division one are controlled by SAS division one). The closed position indications of the CIVs on Common-1b are used to allow opening of the CIVs on Common 1a, and vice versa.

Redundant SAS controllers are provided in each division, and redundant networks are used between the divisions so that no single failure within the SAS can result in inadvertent connection of redundant CCWS trains. Each valve is equipped with redundant open/closed position sensors so that a single sensor failure does not result in inadvertent connection of redundant CCWS trains. While each switchover valve is controlled by one I&C division, multiple PACS priority modules in that division, acting on multiple solenoid devices, are required in order to change the position of a switchover valve. Therefore, a single PACS priority module failure does not result in

Accommodation of single failures at the system level for the mechanical safety systems described in this chapter is addressed in the relevant sections identified in Section 7.6.1.2.

7.6.2.1.2 Compliance to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE 7-4.3.2-2003)

Components and modules that are required to perform the interlocking functions described in this section are classified as safety-related. They are designed to Class 1E standards and are applied in accordance with a stringent quality assurance program. Software used in these functions is developed and applied in accordance with a safety-related software program. Further discussion of safety-related I&C system conformance to requirements for quality is found in Section 7.1.

7.6.2.1.3 Compliance to Requirements for Independence (Clauses 5.6 and 6.3 of IEEE Std 603-1998)

Redundant divisions of the safety-related I&C systems are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing their function. Both electrical and communication independence are maintained as described in Section 7.1.

I&C equipment required to perform the interlock functions described in this section is independent from the effects of design basis events. The computerized portions of the safety systems are located in areas that are not subject to degraded environmental conditions as the result of an event. Equipment that may be located in areas subject to a degraded environment (e.g., sensors) is required to be qualified to operate in the expected post-event conditions. Environmental qualification of instrumentation and control equipment is discussed in Section 3.11 and Section 7.1.

The PS and SAS do not rely on input from non-safety-related systems to perform the interlock functions described in this section. Certain sensor measurements are used as inputs to both a safety-related interlock function, and a non-safety-related control function performed by a non-safety-related I&C system. In these cases, the measurement is acquired by the signal conditioning of the safety-related system, is multiplied, and then passed to the non-safety-related system through an electrically isolated connection.

7.6.2.1.4 Compliance to Requirements for System Testing and Inoperable Surveillance

Surveillance of the safety-related I&C systems consists of overlapping tests to verify performance of the interlock function from sensor to PACS priority module.

Sensors and acquisition circuits are periodically tested. The input channel to be tested is placed in a lockout condition, and the downstream logic is automatically modified to disregard the input under test and maintain the interlock function in its current state.

The computerized portions of the safety systems are continuously monitored through self-testing during power operation. During outages, extended computer self-testing is performed to verify functionality that cannot be tested with the reactor at power.

With respect to the connections between the output circuits of the PS and the ~~PAC~~ priority modules, and to the actuators themselves, surveillance of interlocking functions during power operations can be satisfied by observing the correct interlocked position of the actuators.

The safety-related I&C systems are designed to provide bypassed and inoperable status information to the operator. Sufficient indications are provided to the operator to evaluate the status of each interlock as described in the relevant functional descriptions in Section 7.6.1.2.

7.6.2.1.5 Conformance to Guidance Regarding the Use of Digital Systems (IEEE 7-4.3.2-2003)

The interlock functions described in this section are implemented in I&C systems using the TELEPERM XS platform, which is approved for use in safety systems of nuclear power generating stations in the United States. These systems are implemented in architectures designed to satisfy requirements applicable to all safety-related I&C systems, digital or otherwise.

Implementation of safety-related I&C systems is governed by the requirements of IEEE Std 603-1998 (Reference 1). Guidance on the use of digital computers in safety systems is provided by IEEE 7-4.3.2-2003 (Reference 2). Conformance to these standards is described in Section 7.1.

7.6.3 References

1. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

2. IEEE 7.4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

Next File

7.8 Diverse I&C Systems

The safety instrumentation and controls (I&C) systems that execute automatic reactor trip (RT) and engineered safety feature (ESF) actuation and control functions for accident mitigation are described in Sections 7.2 and 7.3. These systems are designed to perform the required safety functions in the event of a single random failure.

The overall I&C architecture can also withstand software common cause failure (SWCCF) that prevents the PS from performing its function~~multiple failures of the safety I&C systems~~. The design has sufficient diversity and defense-in-depth to tolerate the following beyond design basis events:

- An anticipated transient without scram (ATWS), which is defined as an anticipated operational occurrence (AOO) followed by a failure of the RT portion of the protection system (PS).
- An AOO or a postulated accident concurrent with a software common-cause failure (CCF) that prevents the ~~safety I&C systems~~PS from performing ~~their required~~ RT or ESF actuation functions.

This section describes the I&C systems and functional requirements provided to mitigate these events.

AREVA NP ~~Topical~~Technical Report ANP-~~10284~~10304 (Reference 1) describes the following:

- The defense-in-depth concept for the U.S. EPR.
- The design features that prevent and mitigate a software CCF of the safety I&C systems.
- ~~A methodology to evaluate the diversity and defense-in-depth of the U.S. EPR I&C architecture to determine if the I&C system will adequately protect the health and safety of the public in the unlikely event of a CCF~~An assessment of the I&C architecture relative to each of the 14 guidelines in NUREG/CR-6303.
- The results of a plant response analysis demonstrating that the U.S. EPR satisfies applicable acceptance criteria for a postulated SWCCF of the PS concurrent with an AOO or PA..

~~The methodology described in Reference 1 is summarized in six steps:~~

- ~~Step 1—Susceptibility analysis of safety I&C systems to CCF.~~
- ~~Step 2—Qualitative evaluation of AOOs and postulated accidents.~~
- ~~Step 3—Determine inventory of diverse controls and indications.~~
- ~~Step 4—Quantitative analyses of AOOs and postulated accidents.~~

- ~~Step 5 – Human factors engineering verification and validation.~~
- ~~Step 6 – Platform diversity analysis.~~

~~The results of steps 1 through 3 are summarized in Section as part of the evaluation of NUREG/CR-6303 (Reference 2) guidelines. Steps 4 and 5 are performed as part of the plant procedure and human factors engineering verification and validation programs. For more information on these programs see Section 13.5 and Chapter 18, respectively. Step 6 is performed as inspection as part of equipment procurement. Platform diversity requirements for the process information and control system (PICS) and the process automation system (PAS) are specified in Section 7.1.~~

7.8.1 Description

7.8.1.1 Systems Description

7.8.1.1.1 Safety Information and Control System

The safety information and control system (SICS) provides the ability to manually trip the reactor using a hardwired actuation path that is not affected by a software CCF of the ~~safety I&C systems~~PS.

The SICS is described in Section 7.1.

7.8.1.1.2 Process Information and Control System

The PICS provides monitoring and control of plant safety systems via the PAS, DAS, and the priority and actuator control system (PACS). The PICS is diverse from the SICS.

The PICS is not subject to the postulated CCF of the PS, and is the HMI normally used by the operator during all plant conditions, as long as it is available. Therefore, the postulated CCF of the PS will not affect the PICS in a manner that induces the operator to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation.

The PICS is described in Section 7.1.

7.8.1.1.3 ~~Process Automation System~~Diverse Actuation System

The ~~PAS~~DAS executes manual functions initiated from PICS and automatic functions to mitigate an ATWS or software CCF of the ~~safety I&C systems~~PS. ~~Two subsystems of the PAS are used for these functions: the nuclear island subsystem (NIS) and the diverse actuation subsystem (DAS).~~ The ~~PAS~~DAS is diverse from the PS ~~and safety automation system (SAS)~~.

~~The NIS enables manual component level control of safety-related plant systems. Manual commands are initiated from the PICS, processed in the NIS, and transmitted to the PACS for signal prioritization and actuation of plant components. This path allows the actuation and control of safety systems by the operator in the event of a software CCF of the safety I&C systems. Actuator related information is displayed on the PICS.~~

The DAS executes the automatic RT, ESF actuation, and alarm and display functions ~~described~~listed in Section 7.8.1.2. Sensor information is acquired by the DAS from the PS and SAS using a hardwired signal that is electrically isolated within the safety I&C systems and is not affected by a software CCF. This path is described in Section 7.1.1.6.~~ Setpoints for these functions are set so that the PS will actuate prior to the DAS.~~ The DAS also processes the manual, system level actuation of critical safety functions as described in Section .

For RT functions, outputs from the DAS are sent to the shunt trip coils of the RT breakers, which are a diverse means of opening the breakers from the undervoltage coils which are actuated by the PS.

For ESF ~~functions~~actuations, outputs from the DAS ~~bypass the PS and SAS and~~ are sent directly to the PACS. This path is not affected by a software CCF of the ~~computerized portions of the safety I&C systems~~PS. Outputs for turbine trip are sent directly to the turbine generator I&C.

The following features are implemented so that the automatic DAS functions do not interfere with PS actuations under normal circumstances and so that the PS is given the opportunity to actuate before the DAS:

- DAS setpoints are selected to provide reasonable assurance that they will be reached after a corresponding PS setpoint is reached.
- Voting logic within the DAS is such that single failures do not result in spurious actuations of the automatic DAS functions.
- Priority logic within the PACS dictates that in case of conflicting orders between the PS and the DAS, the PS orders have a higher priority (the priority rules are described in Section 7.1).

The DAS functions are designed so that once initiated, they proceed to completion. The DAS functions use the same techniques as the similar PS functions to satisfy this requirement. These techniques are described in Section 7.2.2.1.6 and Section 7.3.2.3.4.

The DAS has online self-testing features, which minimizes the need for bypassing the system for periodic testing. Portions of the DAS that are not tested by the self-test features shall be periodically tested to ensure the system will execute its functions. Sensors that are shared by the protection system and the DAS are periodically tested as

part of the PS and are not required to be tested separately as part of the DAS periodic testing.

Alarms and indications are processed by the DAS and are sent to the PICS for display. The DAS provides accurate status information to the operator in the main control room. This includes system operation status (i.e., bypass, initiate, standby, normal), power availability, and any system faults or messages pertinent to plant operation. Confirmation of actuation of components by DAS is obtained through check back signals from the PACS to verify the status of the actuator.

The ~~PAS (including the NIS and DAS)~~ DAS is further described in Section 7.1.

7.8.1.1.4 Priority and Actuator Control System

The PACS supports the execution of automatic and manual functions required to mitigate an ATWS and a software CCF of the ~~safety I&C systems~~PS. The PACS is diverse in operation from the ~~TELEPERM XS (TXS) platform used in the~~ PS ~~and SAS~~. The PACS is not used in the actuation path for the RT function.

~~The PACS receives commands from the PAS (either from the NIS or the DAS). The system prioritizes each actuation order and sends the proper command to the safety system components. Prioritization rules for the U.S. EPR are described in Section 7.1.~~

~~The PACS is described in detail in Section 7.1~~The PACS receives actuation orders from the various I&C systems and sends the order of highest priority to the plant actuators. The priority modules in the PACS are not subject to SWCCF by virtue of 100 percent combinatorial, proof-of-design testing. The PACS (including the methodology for performing 100 percent combinatorial testing) is described in Section 7.1.

7.8.1.2 Functional Descriptions

~~The functions described in this section provide the following in the event of an ATWS or software CCF of the safety I&C systems:~~

- ~~Automatic actuation of RT and selected ESF systems by the DAS.~~
- ~~Alarms generated by the DAS that alert the operator to an abnormal condition.~~
- ~~Indications and controls for manual actions.~~

~~Unless stated in the following sections, the design basis for the functions is described in Sections 7.2 and 7.3.~~

~~These functional requirements are categorized as risk reduction I&C functions.~~

7.8.1.2.1 Automatic DAS Functions

The following functions are performed automatically by the DAS to mitigate an ATWS or SWCCF of the PS concurrent with an AOO or PA:

- RT on low SG pressure.
- RT on low SG level.
- RT on high SG level.
- RT on low RCS flow (two loops).
- RT on low-low RCS flow (one loop).
- RT on high neutron flux (power range).
- RT on low hot leg pressure.
- RT on high pressurizer pressure.
- Turbine trip on RT.
- EFWS actuation on low SG level.
- SIS actuation on low pressurizer pressure with signal to PAS to generate partial cooldown through TBS.
- Main steam isolation on low SG pressure.
- Containment isolation on high activity (also includes functions that cascade from containment isolation: Annulus ventilation and Safeguards Building HVAC reconfiguration)
- MFW isolation on low SG pressure.
- MFW isolation on high SG level.
- Opening of containment H_2 mixing dampers on high containment pressure.
- Reference 1 describes how these functions act to mitigate AOOs or PAs in the presence of an SWCCF that renders the PS ineffective.

~~7.8.1.2.1 Reactor Trip on High Neutron Flux (Power Range)~~

~~This function is provided to protect the integrity of the fuel against excessive reactivity additions.~~

~~Each division of the DAS acquires two excore power range detector (PRD) measurements from the PS. The two excore PRD measurements are taken from the~~

~~top half and the bottom half of the core. The DAS calculates nuclear power using excore PRDs as described in Section 7.2.~~

~~The calculated nuclear power is compared to two different setpoints. When P2 is inhibited the lower setpoint is used, which provides protection during startup and shutdown operations. When P2 is validated the higher setpoint is used, which provides protection during power operations. If two-out-of-four calculations of the nuclear power indicate greater than the active setpoint, RT signals are generated.~~

~~There are no operating bypasses associated with this function.~~

~~The logic for this function is shown in Figure 7.8-1.~~

~~7.8.1.2.2 Reactor Trip on Low RCS Flow (Two Loops)~~

~~Each division of the DAS acquires four loop flow measurements (one per loop) from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.3 Reactor Trip on Low Low RCS Flow (One Loop)~~

~~Each division of the DAS acquires four loop flow measurements (one per loop) from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.4 Reactor Trip on High Pressurizer Pressure~~

~~Each division of the DAS acquires one pressurizer pressure narrow range (NR) measurement from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.5 Reactor Trip on Low Hot Leg Pressure~~

~~Each division of the DAS acquires one hot leg pressure wide range (WR) measurement from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.6 Reactor Trip on Low Steam Generator Pressure~~

~~Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.7 Reactor Trip on High Steam Generator Pressure~~

~~Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.8 Reactor Trip on Low Steam Generator Level~~

~~Each division of the DAS acquires four steam generator level NR measurements (one per steam generator) from the PS and executes the functional logic described in Section 7.2.1.~~

~~7.8.1.2.9 Reactor Trip on Safety Injection System Actuation~~

~~This function is provided to trip the reactor when the safety injection system (SIS) is automatically actuated by the DAS.~~

~~The logic for this function is shown in Figure 7.8-2.~~

~~7.8.1.2.10 Reactor Trip on Emergency Feedwater System Actuation~~

~~This function is provided to trip the reactor when the emergency feedwater system (EFWS) is automatically actuated by the DAS.~~

~~The logic for this function is shown in Figure 7.8-3.~~

~~7.8.1.2.11 Safety Injection System Actuation~~

~~The conditions used by the DAS to actuate the SIS are:~~

- ~~Low pressurizer pressure NR.~~

~~Each division of the DAS acquires one pressurizer pressure NR measurement from the PS. Each pressurizer pressure NR measurement is compared to a setpoint. If two-out-of-four measurements indicate less than the setpoint, safety injection is initiated.~~

~~When P12 is satisfied, this function is bypassed. Refer to Section 7.4.2 for a description of P12.~~

~~The logic for this function is shown in Figure 7.8-2.~~

~~7.8.1.2.12 Emergency Feedwater System Actuation~~

~~The conditions used by the DAS to actuate the EFW system are:~~

- ~~Low steam generator level WR.~~

~~Each division of the DAS acquires four steam generator level WR measurements (one per steam generator) from the PS. The steam generator level NR measurements are compared to a setpoint. If two out of four level measurements in any steam generator indicates less than the setpoint, emergency feedwater is initiated for that steam generator.~~

~~When P13 is satisfied, this function is bypassed. Refer to Section 7.2 for a description of P13.~~

~~The logic for this function is shown in Figure 7.8-3.~~

~~7.8.1.2.13 Main Steam Isolation~~

~~The conditions used by the DAS to isolate the main steam system are:~~

- ~~Low steam generator pressure.~~

~~Each division of the DAS acquires four steam generator pressure measurements (one per steam generator) from the PS. If two-out-of-four pressure measurements in any steam generator indicates less than the setpoint, main steam is isolated.~~

~~The logic for this function is shown in Figure 7.2-19.~~

~~7.8.1.2.14 Containment Isolation~~

~~The conditions used by the DAS to perform Stage 1 containment isolation are:~~

- ~~SIS actuation.~~

~~The logic for this function is shown in Figure 7.8-4.~~

~~7.8.1.2.15 Turbine Trip~~

~~Each division of the DAS acquires RT breaker position indications from the PS and executes the logic described in Section 7.3.1.~~

~~7.8.1.2.16 Manual Actuation of Critical Safety Functions~~

~~Manual actuation of the critical safety functions described in SECY-93-087 (Reference 3) is provided. Controls of safety-related process systems from the PICS via the PAS and PACS are implemented at the component level.~~

- ~~Reactivity control—the reactor can be shut down by a manual actuation of RT from the SICS. Additionally, the operator can actuate the extra boration system (EBS) or the SIS from the PICS to provide the capability of injecting borated water into the core.~~

- ~~Core heat removal—once the reactor is shutdown, decay heat can be removed in a variety of ways. The preferred method of removing decay heat is provided by the turbine bypass, condensate and main feedwater systems. The EFW system and the main steam relief trains (MSRT) provide a safety-grade means of removing decay heat. In addition, decay heat may also be removed using feed and bleed of the reactor coolant system (RCS). Makeup water is provided by the SIS, EBS, or chemical volume and control system (CVCS). The bleed path is provided by the~~

~~pressurizer safety valves or primary depressurization valves of the RCS. Controls for these systems are available from the PICS.~~

- ~~Reactor coolant inventory – RCS inventory is maintained using the CVCS, if available. Safety-grade means of reactor coolant inventory control can be performed using the SIS or the EBS. Controls for these systems are available from the PICS.~~

- ~~Containment isolation – the containment is isolated by closure of containment isolation valves from the PICS.~~

- ~~Containment integrity – heat is removed from the containment by actuation of the SIS from the PICS.~~

~~Refer to Chapters 5, 6 and 10 for further information regarding these process systems.~~

~~7.8.1.2.17 Alarm on Main Control Room High Radiation~~

~~This function is provided to alert the operator of high radiation condition at the main control room (MCR) intake.~~

~~Each division of the DAS acquires one MCR intake duct radiation measurement from the PS. If any of the four radiation measurements are above the setpoint, an alarm is generated in the MCR.~~

~~7.8.1.2.18 Alarm on Rod Bottom Indication~~

~~This function is provided to alert the operator of a dropped rod.~~

~~Each division of the DAS acquires one quarter of the rod bottom signals from the PS. If any of the rod bottom signals are below the setpoint, an alarm is generated in the MCR.~~

~~7.8.1.2.19 Display of Post-Accident Monitoring Variables~~

~~This function provides the operator indications to monitor the plant following an actuation by the DAS.~~

~~Each division of the DAS acquires type A, B, and C post-accident monitoring variables from the PS and SAS. The DAS processes the information and sends it to the PICS for display. The NIS processes type D and E variables for display on PICS.~~

~~The post-accident monitoring variables are described in Section 7.5.~~

~~7.8.1.2.20 Indication and Alarm of DAS Status~~

~~For the automatic RT and ESF functions described in this section, alarms are generated and sent to the PICS to alert the operator. The PICS also displays the bypassed and inoperable status of the DAS.~~

7.8.1.2.2 Manual Actuation of Critical Safety Functions

Manual actuation of critical safety functions is provided in accordance with SECY 93-087 (Reference 3). These manual functions are processed by I&C systems that are not subject to the postulated SWCCF of the PS. The functions provided for each critical safety function, and the I&C systems that process each function are identified:

- Reactivity control – Manual RT (SICS).
- Core heat removal – Manual EFW actuation (PICS – DAS).

  Manual MSRT actuation (PICS – PAS).
- Reactor coolant inventory – Manual SIS actuation (PICS – DAS).
- Containment isolation – Manual stage 1 containment isolation (PICS – DAS).
- Containment integrity – Manual SIS actuation (PICS – DAS).

7.8.1.2.3 Indications and Alarms

The following indications and alarms are processed by the DAS and provided to the operator on the PICS:

- Post-Accident Monitoring Variables – The operator is provided with indications to monitor the plant following an actuation by the DAS. Each division of the DAS acquires Type A, B, and C post-accident monitoring variables. The DAS processes the information and sends it to the PICS for display to the operator. Post-accident monitoring variables are described in Section 7.5.
- Indication and Alarm of DAS Status – When an automatic RT or ESF function is actuated by DAS, alarms are generated and sent to the PICS to alert the operator. The PICS also displays the bypassed and inoperable status of the DAS when appropriate.

7.8.2 Analysis

7.8.2.1 Regulatory Requirements

7.8.2.1.1 10 CFR 50.55a(a)(1) - Quality Standards

The safety-related portions of the SICS and the PACS meet the requirements of 10 CFR 50.55a(a)(1). See Section 7.1 for a complete description on compliance with 10 CFR 50.55a(a)(1).

7.8.2.1.2 10 CFR 50.55a(h)(3) - Safety Systems

The safety-related portion of the SICS and the PACS meet the requirements of 10 CFR 50.55a(h)(3). The PICS and ~~PAS~~DAS are non-safety-related systems and are independent from the safety I&C systems. See Section 7.1 for a complete description on compliance with 10 CFR 50.55a(h)(3).

7.8.2.1.3 10 CFR 50.62 - Requirements for Reduction of Risk from ATWS Events for Light-Water-Cooled Nuclear Power Plants

The DAS is provided for ATWS mitigation, and meets the requirements of 10 CFR 50.62. The DAS automatically initiates RT, turbine trip, and EFW on conditions indicative of an ATWS to mitigate the event. The DAS performs its function reliably based on the system design and quality assurance measures taken. The DAS is independent from the PS. See Section 7.1 and Section 7.8.1.1.3 for more information on the DAS.

7.8.2.1.4 GDC 1 - Quality Standards and Records

See Section 7.1 for a description ~~on~~of compliance with GDC 1.

7.8.2.1.5 GDC 13 - Instrumentation and Control

See Section 7.1 for a description ~~on~~of compliance with GDC 13.

7.8.2.1.6 GDC 19 - Control Room

See Section 7.1 for a description ~~on~~of compliance with GDC 19.

7.8.2.1.7 GDC 24 - Separation of Protection and Control Systems

The SICS and PACS meet the requirements of GDC 24. See Section 7.1 for a description ~~on~~of compliance with GDC 24.

7.8.2.1.8 Generic Letter 85-06 - Quality Assurance Guidance for ATWS Equipment that is not Safety Related

AREVA NP Inc. implements quality requirements to ATWS equipment in accordance with Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety Related."

~~7.8.2.2 Evaluation of NUREG/CR-6303 Guidelines~~

~~7.8.2.2.1 Identifying System Blocks (Guidelines 1 and 5)~~

~~The blocks are identified at the system level within the I&C architecture described in Section 7.1. Within the PS, subsystems A and B provide for functional diversity.~~

~~7.8.2.2.2 Determining Degree of Diversity (Guideline 2)~~

~~The PICS and PAS are implemented with digital I&C equipment that is diverse from the TXS platform. The PACS is implemented using non-computerized technology that is diverse from the TXS digital platform. The hardwired portions of the SICS are diverse from TXS. The equipment for the PICS, PAS, PACS and SICS is described in Section 7.1.~~

~~7.8.2.2.3 System Failure Types (Guideline 3)~~

~~**Type 1 Failures**~~

~~Type 1 failures are caused by a failure of the I&C that induces a plant transient requiring a protective action.~~

~~These failures are mitigated in the U.S. EPR I&C design through the use of signal selection algorithms in control systems, and redundancy, fault detection and voting in the PS.~~

~~Chapter 15 identifies control system malfunctions that result in initiating events. The DAS is provided as a diverse means of actuating RT and ESF to mitigate these events concurrent with a CCF of the PS.~~

~~**Type 2 Failures**~~

~~Type 2 failures are undetected failures that prevent the safety I&C systems from executing safety functions, when required.~~

~~These failures are mitigated in the U.S. EPR design through two primary methods. Functional diversity within the PS is provided to mitigate an error due to a requirement specification. Equipment diversity is provided so that the PICS, PAS, PACS and hardwired portions of the SICS are not affected by a CCF of the TXS platform.~~

~~**Type 3 Failures**~~

~~Type 3 failures are caused by sensors that inaccurately measure the process parameter due to effects resulting from the initiating event.~~

~~These failures are mitigated in the U.S. EPR design by implementing functional diversity for RT within the PS.~~

~~7.8.2.2.4 Echelons of Defense (Guideline 4)~~

~~Four echelons of defense are defined in Reference 2:~~

- ~~Control echelon.~~
- ~~Reactor trip echelon.~~
- ~~Engineered safety feature actuation system (ESFAS) echelon.~~
- ~~Monitoring and indication echelon.~~

~~The control echelon consists of the RCSL, PAS, and turbine-generator (TG) I&C. The RT echelon consists of the PS. The ESFAS echelon consists of the PS. The SAS performs ESF control functions. The PICS and SICS comprise the monitoring echelon.~~

~~The relationship between the echelons of defense and the U.S. EPR lines of defense are described in Reference 1.~~

~~7.8.2.2.5 Postulated Common Mode Failures in System Blocks, Use of Identical Hardware and Software Modules, Effects of Other Blocks, and Output Signals (Guidelines 6, 7, 8, 9)~~

~~Systems that are implemented with the TXS platform are assumed to fail as is during a DBE. The PICS, PAS, PACS, and hardwired portions of the SICS are not affected because of diversity. Sensors shared between the safety I&C systems and the PAS are not affected by this postulated conservative failure because of the method of isolation and acquisition described in Section 7.8.1.1.3.~~

~~7.8.2.2.6 Diversity for Anticipated Operational Occurrences and Accidents (Guidelines 10 and 11)~~

~~In accordance with the methodology described in Reference 1, a qualitative evaluation of anticipated operational occurrences and postulated accidents was performed. This evaluation reviewed the design basis events analyzed in the accident analysis assuming a software common mode failure in the PS and SAS. The evaluation is strictly qualitative and credits functions designed into the DAS, primarily for ATWS, and credits limitation functions where they are diverse from the PS. Limitation functions in the RCSL share the same platform as the PS and were also assumed to fail.~~

Next File

~~Limitation and control functions in the PAS are considered. The PS includes both the reactor trip functions and the engineered safety features actuation functions. The results of the evaluation were reviewed by a multi-disciplinary team.~~

~~7.8.2.2.7 Diversity and Dependency between Echelons of Defense (Guideline 12)~~

~~**Control and Reactor Trip**~~

~~The DAS performs the RT functions described in Section 7.8.1.2 using equipment diverse and independent from the PS. Sensors acquired by the DAS from the PS are electrically isolated in the PS to enable independence. The reactor can be manually tripped from the SICS using a hardwired path not affected by a software CCF of the PS. Diversity in RT devices is described in Reference 1.~~

~~**Control and ESFAS**~~

~~The DAS performs the ESF actuation functions described in Section 7.8.1.2 using equipment diverse and independent from the PS and SAS. Sensors acquired by the DAS from the PS are electrically isolated in the PS to enable independence. Plant safety systems can be actuated at the system or component level from the SICS. Plant safety systems can be actuated at the component level from the PICS.~~

~~**Reactor Trip and ESFAS**~~

~~The PS performs RT and ESF actuation functions on the same processors. This reduces the number of components and improves reliability. The DAS is provided as a diverse backup in the event of a software CCF that disables both the RT and ESF actuation functions of the PS.~~

~~7.8.2.2.8 Plant Monitoring and Manual Operator Actions (Guidelines 13 and 14)~~

~~The PICS provides monitoring and control of plant systems during normal operation. In the event of a loss of the PICS, the SICS is provided as diverse backup. The safety-related portions of the SICS are independent from the PICS. The SICS and PICS are described in Section 7.1.~~

~~In the event of a CCF of the safety I&C systems, the indications and controls described in Section 7.8.1.2 are provided to the operator. These indications and controls are not subject to a CCF of the safety I&C systems. Chapter 18 describes the process of human factors engineering verification and validation for manual actions.~~

7.8.3 References

1. ~~ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007.~~ANP-10304, Revision 1, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP Inc., November 2009.

2. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems,” U.S. Nuclear Regulatory Commission, December 1994.

3. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, April 1993.

4. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," U.S. Nuclear Regulatory Commission, April 16, 1986.

Figure 7.8-1—~~Reactor Trip on Excore High Neutron Flux~~Deleted

Figure 7.8-2—~~Safety Injection Actuation~~Deleted

Figure 7.8-3—~~EFW Actuation~~Deleted

Figure 7.8-4—~~Containment Isolation on SIS Actuation~~Deleted

Next File

- Implement interlocks and preventive actions that cope with deviations from normal operation to prevent an event resulting in the actuation of a safety system.
- Mitigate events and bring the plant to a controlled state by the protection system that controls the RT actuation system and the engineered safety features.
- Cope with the complete failure of engineered safety features and protective systems by means of risk reduction functions.
- Preserve containment integrity in case of accidents resulting in mass and energy releases into the containment.

The following sections address U.S. EPR design features that function to mitigate or reduce the risk of ATWS events.

15.8.1.2 Protection System

The PS provides the primary means for protecting fission product barriers by tripping the reactor. A description of the PS is provided in Section 7.2.

An ATWS event occurs when the control rods fail to insert following the generation of an RT signal. The specific failure mechanism is not specified, but could be the result of mechanical blockage of the control rods or the result of electrical or mechanical failures within the PS. If the ATWS is the result of a mechanical blockage of the control rods, failures within the PS are not postulated. Details of mechanical blockage are provided in Section 15.8.1.6.

If the ATWS is the result of a failure within the PS, an independent and diverse RT signal within the ~~process automation~~diverse actuation system (~~PAS~~DAS) bypasses the PS and initiates an RT. The RT is initiated by opening the breakers mounted at the output of the motor- generator sets that energize the control rod drive mechanisms. The diverse system also processes other critical signals and initiates essential actions to trip the turbine and start other safeguards systems as needed to address the ATWS event. Details of these signals are addressed in Section 15.8.1.3.

15.8.1.3 ~~Process Automation System~~Diverse Actuation System

~~The main tasks performed by the PAS are monitoring and automation of plant mechanical and electrical systems for normal operating conditions and postaccident conditions.~~ The ~~PAS also~~DAS includes logic that fulfills the ATWS requirements of 10 CFR 50.62. The ~~PAS~~DAS logic is independent from sensor output to the final actuation device from the PS design features, and provides a diverse means to trip the reactor, trip the turbine, and initiate emergency feedwater (EFW) on conditions indicative of an ATWS. These diverse functions provided by the ~~PAS~~DAS provide reasonable assurance that a pressure increase does not exceed the ASME Service Level C limit of 3200 psig (Reference 1) or does not exceed containment safety parameters.

The diverse trip functions and capabilities are incorporated within ~~PAS~~DAS and used for ATWS mitigation are described in Section 7.8.1.2.

15.8.1.4 Emergency Feedwater System

The U.S. EPR provides automatic actuation of the EFW system on conditions indicative of an ATWS (see Section 15.8.1.3). The U.S. EPR is designed so that flow from the EFW system is not required for the first 30 minutes following an ATWS.

15.8.1.5 Extra Borating System

The extra borating system (EBS) is not required for ATWS mitigation. However, the system is available via manual actuation should additional negative reactivity be desired to bring the reactor into a subcritical state. A description of the EBS is provided in Section 6.8.

15.8.1.6 Mechanical Blockage of Rod Cluster Control Assemblies

ATWS events resulting from mechanical blockage of control rods are not postulated for the U.S. EPR design. The probability of an ATWS resulting from mechanical blockage of the control rods is an insignificant contributor to the overall probability of an ATWS.

As noted in the "Conclusions" section of NUREG-1780 (Reference 2), during ATWS rulemaking the NRC staff set a goal that the probability of an ATWS should be no more than 1.0E-05 per reactor year. The probability of an ATWS is defined by NUREG-1780 as "the annual frequency of an ATWS leading to plant conditions that exceed certain design parameters that can result in core melt, containment failure, and the release of radioactivity and can be viewed as the expected CDF of an unmitigated ATWS." NUREG-1780 updated the original generic ATWS regulatory analysis using operating data since the ATWS rule was implemented, and the updated results indicated that the four reactor types achieved the ATWS rule risk goal: General Electric, Westinghouse, Babcock and Wilcox (B&W), and Combustion Engineering (CE). Specifically, Table 3, Summary of ATWS Rule Risk Expectations and Outcomes, of NUREG-1780 shows that the pressurized water reactor vendors (Westinghouse, B&W, and CE) each achieved a probability of an ATWS that is at least a factor of 20 better than the goal (i.e., ≤5.0E-07 per reactor year).

Inherent to the development of ATWS probability is the assumption of successful mitigation upon insertion of 20 percent or more of the control rods per SECY-83-293 (Reference 3). The ATWS rule 10 CFR 50.62(c)(2) requires that reactors designed by CE and B&W have a diverse scram system. The diverse scram system increases the reliability for control rod insertion, which is reflected in the probability of having a common-cause failure that causes 50 percent or more of the control rods to fail insertion. These probability values include 3.6E-08 for CE per Table 3-2 of NUREG/