AREVA

U.S. EPR Protection System

ANP-10309NP
Revision 4

Technical Report

May 2012

AREVA NP Inc.

Nature of Changes

Revision	Section(s) or Page(s	Description and Justification
1	All	Complete revision to incorporate changes based on new I&C architectural design.
	Appendix A	APPENDIX A has been replaced in its entirety. The previous Appendix A, 'COMPARISON OF IEEE STD 603-1991 TO IEEE STD 603-1998' has been removed and is being processed under a separate alternative request. The new Appendix A is 'The Protection System Failure Modes and Effects Analysis' which has been incorporated into the Protection System Technical Report Document as Appendix A, as described in the Response to RAI 442, Question 7.1-27.
	Appendix B	The Protection System Response Time Document was incorporated into the Protection System Technical Report Document as Appendix B, as described in the Response to RAI 442, Question 7.3-33.
2	All	Revised certain statements to replace 'design basis event (DBE)' with 'anticipated operational occurrence (AOO)' or 'postulated accident (PA).'
	Sections 1.0 and 16.0	Added a reference to the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report.
	Sections 4.2.2 and A.2.1	Revised certain statements to replace 'bus' or 'busses' with 'emergency uninterruptible power supply (EUPS).'
	Section 6.2	Added a statement clarifying the arrangement of the ring networks within the PS.
	Sections 7.0 and 8.0	Revised Section 7.0 and 8.0 to remove or replace the term 'typical.'
	Section 11.2	Added a statement concerning the voting logic within the PS.
	Section 12.0	Added statements, and a new section (Section 12.6) addressing the unidirectional communication between safety and non-safety components in the PS.
	Section A.1.1	Added statements, and a new table (Table A.1-1) addressing communication failures of the PS.
3	Title	Revised the title to remove the term "Digital."
	All	Revised the document to limit the usage of the term "digital."

	Figure 6-13	Revised lines to show unidirectional communication from MSI to GW, and bidirectional from SU to MSI.
	Section 8.5 and Figure 8-.3	Incorporated the term "system-level" to the discussion for Manual ESF Actuations.
	Section 11.2	Added a statement about interdivisional communication for voting only.
	Section A.1.1	Added a statement that Table A.1-1 applies to all TXS systems.
4	Section 1.0	Removed statement saying the PS takes credit for signal diversity.
	Section 14.0	Revised response time methodology to encompass the DCS response time, instead of only including the PS response time.
	Appendix B	Revised response time methodology to encompass the DCS, instead of only the including PS response time, per RAI 414.

Contents

List of Tables

List of Figures

Nomenclature

Acronym	Definition
ALU	Actuation Logic Unit
APU	Acquisition and Processing Unit
CFR	Code of Federal Regulations
CLEG	Cold Leg
CRDM	Control Rod Drive Mechanism
ΔP	Differential pressure
DPRAM	Dual Port Random Access Memory
(L)DNBR	(Low) Departure from Nuclear Boiling Ratio
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EFWS	Emergency Feedwater System
EMI	Electromagnetic Interference
EOC	Electrical to Optical Converter
EPRI	Electric Power Research Institute
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features Actuation System
GW	Gateway
HLEG	Hot Leg
HLPD	High Linear Power Density
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
IRD	Intermediate Range Detector
MAX	Maximum setpoint
MCR	Main Control Room
MCR A/C	Main Control Room Air Conditioning
MIN	Minimum setpoint
MSI	Monitoring and Service Interface
MSI-MU	Monitoring and Service Interface – Main Unit
MSI-AU	Monitoring and Service Interface – Auxiliary Unit
MSIV	Main Steam Isolation Valve
MSRT	Main Steam Relief Train
NR	Narrow Range
NRC	Nuclear Regulatory Commission
OLM	Optical Link Module
PAC(S)	Priority and Actuator Control (System)

PICS	Process Information and Control System
PRD	Power Range Detector
PROFIBUS	Process Field Bus
PS	Protection System
PSRV	Pressurizer Safety Relief Valve
PZR	Pressurizer
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RPS	Reactor Protection System
RSS	Remote Shutdown Station
RT	Reactor Trip
SCDS	Signal Conditioning and Distribution System
SG	Steam Generator
SI	Safety Injection
SIS	Safety Injection System
SICS	Safety Information and Control System
SPACE	Specification and Coding Environment
SPND	Self-Powered Neutron Detector
SU	Service Unit
TT	Turbine Trip
TXS	TELEPERM XS
V&V	Verification and Validation
WR	Wide Range

1.0 INTRODUCTION

This technical report describes the design of the U.S. EPR™ protection system (PS), which includes the PS architecture and the typical implementation of functionality within this architecture, and is provided to support the design certification application for the U.S. EPR. Generic terms for the PS equipment are used (e.g., function processor, communication module, input module). Table 1-1 lists the generic equipment references used in correlation with the equivalent specific equipment that was audited as part of the NRC review of the TXS topical report (References 23 and 24).

The PS is a reactor protection system (RPS) and an engineered safety features actuation system (ESFAS) that is implemented using TELEPERM XS (TXS) technology. The TXS platform, described in Siemens Topical Report EMF-2110 (Reference 24), has been approved by the U.S. Nuclear Regulatory Commission (NRC) for use in safety-related instrumentation and control (I&C) applications (Reference 23). The PS detects plant conditions that indicate the occurrence of an anticipated operational occurrence (AOO) and postulated accident (PA) and initiates the plant safety features required to mitigate the AOO and PA. These actions are accomplished through automatic actuation of reactor trips (RT) and engineered safety features (ESF) systems.

The PS uses state-of-the-art TXS hardware and software, adheres to the approved TXS system design principles (both hardware and software), and meets applicable regulatory requirements and industry standards.

The PS provides signal diversity for reactor trip functions, as described in Section 10.0, "Signal Diversity." The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). The diversity attributes of the PS are described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report, ANP-10304 (Reference 30).

Table 1-1—Generic Hardware Equivalence

Generic Equipment Designation Used in this Report	Equivalent Equipment from Reference 24
Function Processor	
PROFIBUS Communication Module	
Ethernet Communication Module	
Input Modules	
Output Modules	
Optical Link Module	

2.0 BACKGROUND

The safety and reliability of nuclear installations heavily depend on I&C systems. The TXS platform is designed for use in safety-related automation applications and to meet safety-related I&C requirements. Typical uses include RPS and ESFAS functions, but the TXS platform can also perform a wide variety of functions (e.g., core monitoring and control, rod position monitoring, emergency diesel generator controls).

2.1 *NRC Approval of the TXS Platform*

As previously noted, the TXS platform is described in Reference 24, which has been reviewed and approved by the NRC (Reference 23). Reference 24 describes the TXS hardware and operating system software design, platform qualification testing, and application software capabilities. As noted in Reference 24, TXS is a qualified I&C platform that meets the applicable regulatory requirements and can be used for a wide range of plant-specific applications in the United States. In Reference 23 the NRC concluded that the TXS design meets the requirements of General Design Criteria 1, 2, 4, 13, 19-25, and 29 (Reference 1) as well as the applicable requirements of 10 CFR 50.55a (Reference 2).

Reference 23 states that "the TXS system is acceptable for safety-related instrumentation and control (I&C) applications and meets the relevant regulatory requirements." Reference 23 also states "Because this topical report is for a generic platform, licensees referencing this topical report will need to document the details regarding the use of TXS design in plant-specific applications and address all plant-specific interface items . . . ."

The NRC's approval of the TXS platform as a qualified, I&C platform also constitutes approval of the TXS system design principles and methods for safety-related applications that were documented in Reference 24. These TXS system design principles and methods include:

- Use of the four system building blocks described in Reference 23:
  - System hardware.
  - System operating software.
  - Application software.
  - Specification and coding environment (SPACE) tool for application software development.
- Equipment qualification methods.
- Operating system software development process, including verification and validation (V&V) methods.
- Processing principles:
  - Operating system operation.
  - Runtime environment operation.
  - Cyclic, deterministic, asynchronous operation.
- Inter-channel communication principles.
- Service unit (SU) maintenance interface.

The qualification of specific TXS hardware products and the V&V of specific TXS software versions were evaluated by the NRC in Reference 23.

2.2 *Plant Specific Action Items*

Reference 23 identified seventeen plant-specific action items to be addressed by an applicant when requesting installation of a TXS system.

The scope of this report does not include installation of the TXS system; therefore, resolution of the action items in Reference 23 is not specifically addressed.

Resolution of the plant specific action items is addressed in one of two ways:

- In U.S. EPR FSAR Tier 2, by demonstrating compliance with specific regulatory requirements.
- In U.S. EPR FSAR Tier 1, by including ITAAC or design acceptance criteria (DAC) that verify specific system characteristics.

3.0 DESCRIPTION OF THE U.S. EPR PROTECTION SYSTEM

3.1 *System Role*

The PS is an RPS and ESFAS. The purposes of the PS are to detect plant conditions that indicate the occurrence of an AOO or PA and initiate the plant safety features required to mitigate the AOO or PA. These purposes are fulfilled through the automatic actuation of RT and ESF systems.

The PS also generates permissive and interlock signals used to enable or disable certain protective actions according to current plant conditions (e.g., to ensure high pressure to low pressure system interlocks).

In addition to automatic functions, the PS also processes manual commands and issues corresponding actuation orders.

3.2 *System Organization*

The PS is organized into four redundant divisions located in separate Safeguard Buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement signal diversity for RT functions. Each subsystem is divided into functional units based on the types of functionality required (e.g., signal acquisition, processing, voting, actuation). Descriptions of the PS functional units are provided in Section 5.0.

3.3 *System Implementation*

The PS is implemented using the TXS platform. The TXS platform encompasses system hardware components; operating system and application software; and engineering, diagnostic, maintenance, and service software tools.

The TXS platform is applied to the PS design to obtain a system distributed among four redundant divisions consisting of eight actuation paths (two subsystems per division).

All PS functions are performed in two layers. The first layer is used for acquisition and data processing. The second layer is the actuation signal voting layer. Sections 7.0 and 8.0 describe the layers of operations in the PS design.

4.0 SYSTEM ARCHITECTURE

4.1 *Overall System Architecture*

The architecture of the PS is shown in U.S. EPR FSAR Tier 2, Figure 7.1-6. The four sections in the figure represent the four physically separated, redundant PS divisions. The equipment assigned to each PS division is located in the corresponding Safeguard Building.

In the PS architecture, the monitoring and service interface (MSI) serves as the safety to non-safety isolation point for networked connections. Those on the safety-related side of the MSI main unit (MSI-MU) are required to be Class 1E networks. Network connections on the non-safety side of the MSI-MU are non-Class 1E. Hardwired connections are used for signal acquisition via the SCDS (signal conditioning and distribution system), actuation orders to the PACS and RT as well as connections to the SICS and other I&C systems.

The networks shown in U.S. EPR FSAR Tier 2, Figure 7.1-6 represent functional connections, and are not representative of the detailed network topologies as implemented. Examples of the detailed individual network topologies are provided in Section 6.0 of this report.

4.2 *System Architecture Features*

The system architecture features are described in Section 4.2.1 through Section 4.2.4.

4.2.1 *Physical Separation*

The four redundant divisions of the PS are physically separated in their respective Safeguard Buildings. In addition to the spatial separation features, Safeguard Buildings 2 and 3 are designed to protect against external hazards. The four divisionally separated rooms containing the PS equipment are in different fire zones. Therefore, the consequences of internal hazards (e.g., fire) would impact only one PS division.

4.2.2 *Power Supply*

Each PS division is supplied by the independent Class 1E emergency uninterruptible power supply (EUPS). The EUPS are backed by the emergency diesel generators to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by two redundant, uninterruptible 24 Vdc feeds. To cope with loss of onsite and offsite power, the uninterruptible feeds to the PS cabinets are supplied with two-hour batteries.

4.2.3 *Redundancy*

The PS architecture contains four redundant divisions. For RT functions, each PS division actuates one redundancy of the RT devices based on redundant processing performed in four divisions. For ESFAS functions, the redundancy of the safety function as a whole is defined by the redundancy of the ESF system mechanical trains. In general, this results in one PS division actuating one mechanical train of an ESF system based on redundant processing performed in four divisions. The PS not only supports the redundancy of the mechanical trains, but also enhances this redundancy through techniques, such as redundant actuation voting.

4.2.4 *Subsystems*

Each PS division is divided into two independent subsystems (i.e., A and B). Subsystem A in each division is redundant to Subsystem A of other divisions; the same is true of Subsystem B. The primary purpose of this arrangement is to provide signal diversity for RT functions. Section 10.0 presents the design rules for assigning PS functions to the subsystems.

5.0 PROTECTION SYSTEM UNITS

There are five types of functional units that compose the PS: acquisition and processing, actuation logic, monitoring and service interfaces, service unit, and gateways.

Each unit type description includes its high-level functionality and how it fits into the overall system architecture. Unless specified otherwise, the units described in this section perform safety-related functions and consist of Class 1E equipment.

5.1 *Acquisition and Processing Units*

The APU primary functions are to:

- Acquire the signals from the process sensors and monitoring systems via the SCDS.
- Perform processing (e.g., calculations, setpoint comparisons) using the input signals.
- Distribute the results to the actuation logic units (ALU) for voting.

Each APU consists of a function processor, input and output modules, and communication modules.

Each PS division contains five APUs; three assigned to Subsystem A and two assigned to Subsystem B. Each APU communicates its results to the ALU within its subsystem in each division. Each APU of a division is redundant to the corresponding APU of other divisions. For example, APU A1 in each division acquires one of four redundant input signals, and each APU A1 performs identical processing. The four redundant results are then voted on in all divisions by the ALU. This arrangement allows the system to perform in the event of a single failure coincident with a pre-existing failure, or with maintenance or testing being performed on another division.

5.2 *Actuation Logic Units*

The ALU primary functions are to perform voting of processing results from the redundant APU in the various divisions and to issue actuation orders based on voting results. The ALU also contains the logic used to latch and either manually or automatically unlatch actuation outputs. Each ALU consists of a function processor, input and output modules, and communication modules. Each ALU has a hardwired connection from the SICS for manual system level actuations. ALUs are also hardwired to provide outputs to other I&C systems. Class 1E isolation is used for hardwired connections between the ALUs and non-safety-related I&C systems.

Each PS division contains four ALUs; two assigned to each subsystem. The two ALUs of the same subsystem within a division are redundant. The outputs of two redundant ALUs are combined in a hardwired "functional AND" logic for RT outputs (Section 7.4) and in a hardwired "functional OR" logic for ESFAS outputs. This avoids both unavailability of ESFAS actuations and spurious RT actuations. The actuation orders from the ALU are sent to the PAC system (PACS) for ESFAS actuations, or to the trip devices for RT actuations.

5.3 *Monitoring and Service Interfaces*

Each PS division contains two MSIs; the main unit (i.e., MSI-MU), and the auxiliary unit (i.e., MSI-AU). The MSI performs functions related to both subsystems; therefore, they are not assigned to a particular subsystem. Each MSI consists of function processors, input and output modules, and communication modules.

The MSI-AU primary function is to acquire the checkback signals for periodic testing of the PAC modules.

The MSI-MU primary functions are to provide status monitoring and data transfer. The MSI-MU facilitates monitoring for conditions, such as communication failures between other PS units for protection channel status information. The MSI-MU also provides information for display to the operators. The MSI-MU provides the required Class 1E

isolation to prevent non-safety-related systems from affecting the performance of the PS.

5.4 *Service Unit*

The primary function of the service unit (SU) is to facilitate maintenance activities related to the PS. These activities include:

- System diagnosis.
- Monitoring the system functional status.
- Performing periodic tests of the system.
- Modifying the changeable software parameters.
- Loading new software versions.

The PS contains one SU; the SU communicates with the units in the four PS divisions by accessing one division at a time. The SU serves both subsystems in every division; therefore, it is not assigned to a particular subsystem. The SU communicates with the PS units through each division's MSI-MU and can be accessed through a service terminal in the I&C service center. The path between the PS units and the SU is isolated by a hardwired disconnect when the service unit is not in use. The hardwired disconnect also verifies that only one division can be connected at a time. The hardwired disconnection will be accomplished with key operated switches located in the control room. This allows the control room operators to monitor the position of the hardwired disconnects providing them with control over the use of the service unit.

The SU is non-safety-related and does not directly influence the execution of safety-related PS functions.

5.5 *Gateways*

The gateway (GW) primary function is to send information from the PS to the process information and control system (PICS). The GW transfers information from the PS to

the PICS for display and archival storage. The GW converts TXS communication mechanisms into those used by the PICS.

Each GW communicates with the MSI-MU in the four PS divisions.

The GW is non-safety-related. A failure of the GW does not directly influence the execution of the automatic, safety-related PS functions.

6.0 DETAILED SYSTEM ARCHITECTURE

6.1 *General Network Concepts*

The detailed system architecture is represented through a series of figures (Figure 6-3–Figure 6-13) showing network connections between the different units of the PS. In general, two types of Class 1E network topologies are used within the PS. These are redundant point-to-point and redundant ring topologies. A given network topology includes optical link modules (OLM) and the connections between them. Multiple PS units can access a network through the same OLM; therefore, the OLMs are considered part of the network and are not part of any PS unit.

6.1.1 *Redundant Point-to-Point Network Topology*

A redundant point-to-point network topology consists of two OLMs and two double fiber optical links between them. Each double fiber optical link consists of a separate transmit and receive channel. In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of the OLM, does not affect network availability. If an OLM is lost, the affected network becomes unavailable, but the redundant architecture of the PS allows the safety function to be performed through other unaffected networks. The redundant point-to-point topology is shown in Figure 6-1.

6.1.2 *Redundant Ring Network Topology*

A redundant ring network topology consists of at least three OLMs and their corresponding double fiber optical links. A given redundant ring network topology can contain only a finite number of OLMs. Each network in the PS contains fewer OLMs than the maximum allowed. Each double fiber optical link consists of a separate transmit and receive channel. In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of one OLM, does not affect network availability. If an OLM is lost, only the unit(s) directly connected to the failed OLM is

affected. The remaining units accessing the ring network can still communicate with one another. The redundant ring topology is shown in Figure 6-2.

6.1.3 *Network Topologies – Independence of PS Divisions*

Independence between the redundant divisions of the PS is achieved by maintaining both electrical isolation and communication independence between divisions. In both network topologies, electrical isolation is achieved through the use of optical communication paths between OLMs in redundant divisions.

Communication independence is not a function of the network topology or the operation of the OLMs. Communication independence is achieved, regardless of the physical topology of the network, through the features designed in the TXS platform for interference-free communication. Communication independence is addressed further in Section 11.0.

6.1.4 *Network Operation Concepts*

The OLM propagates messages to other OLMs on a given network. Additionally, the OLM is capable of monitoring the optical bus segments for conductor breaks or interruptions, and signaling the interruption locally and remotely. This functionality is achieved through the use of echo and segmentation functions. The echo and segmentation functions are performed by the OLM independently of the operation and communication monitoring functions of any PS units. Additional information on the echo and segmentation functions is provided in Section 6.1.4.1 through Section 6.1.4.4.

6.1.4.1 *Send Echo*

When an OLM receives a message via any channel, the message is forwarded to the other channels for transmission. If the receiving channel is an optical channel, the module also returns the message to the sending OLM as an echo. Accordingly, a message is propagated to the other OLMs on a network, and the echo is sent to the sending OLM to verify the integrity of the optical segment. The echo is terminated when

received by the OLM and is not allowed to propagate to the connected PS function processors.

6.1.4.2 *Monitor Echo*

When an OLM sends a message that is not an echo to an optical channel, the module expects an echo. If the echo does not arrive within a specified time, an echo monitoring error is signaled locally, and the receive side of the channel is segmented (Section 6.1.4.4). The echo monitoring error can also be indicated via remote alarm through the TXS cabinet monitoring features.

6.1.4.3 *Suppress Echo*

When the sending of a message begins, the applicable receiver is separated from the remaining channels until the complete echo has been received.

6.1.4.4 *Segmentation*

If an echo monitoring error occurs on an optical channel, the OLM assumes that a line interruption has occurred and blocks the receive side of this channel for user data. The OLM that detected the error sends optical pulses to the send side of the segmented channel. These optical pulses signal the partner OLM that one optical path is in proper service condition (for break of a single fiber of a double fiber optical cable) and prevents segmentation by the partner module. Segmentation is automatically cancelled when the optical receiver recognizes an optical impulse from the segmented receive side of the channel.

6.2 *APU – ALU Architecture (Subsystem A)*

[

]

6.3 *APU – ALU Architecture (Subsystem B)*

[

]

6.4 *MSI-MU – APU Architecture*

6.5 *MSI-MU – ALU – MSI-AU Architecture*

[

]

6.6 *MSI-MU – GW – SU Architecture*

[

]

Figure 6-1—Example of Redundant Point-to-Point Connection

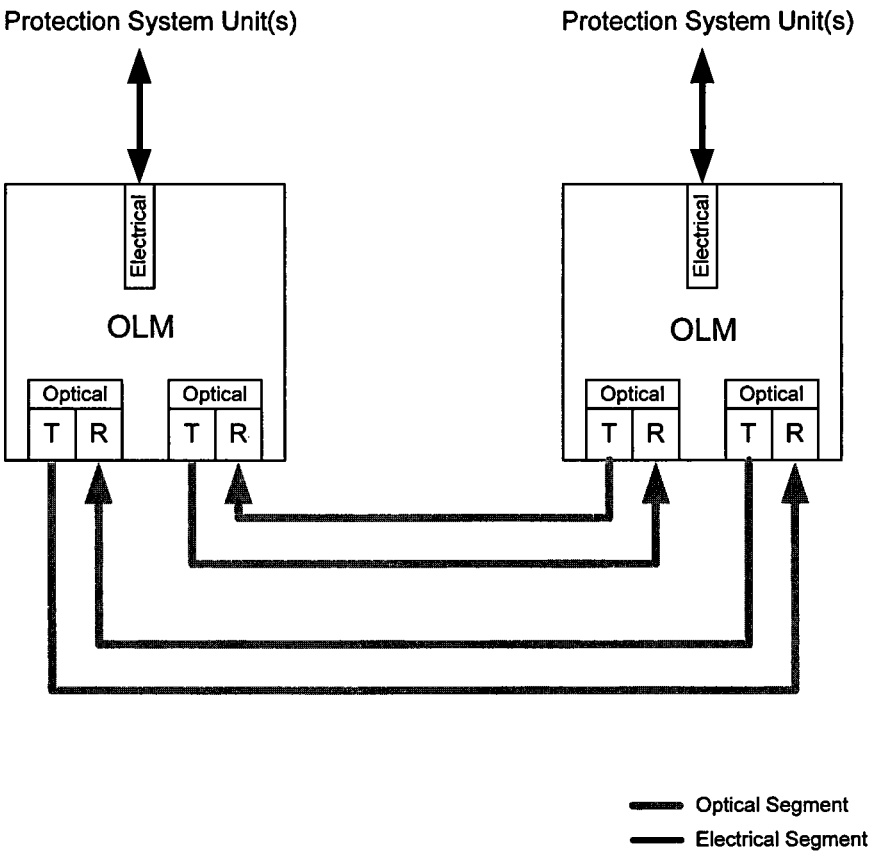


Figure 6-2—Example of Redundant Ring Connection

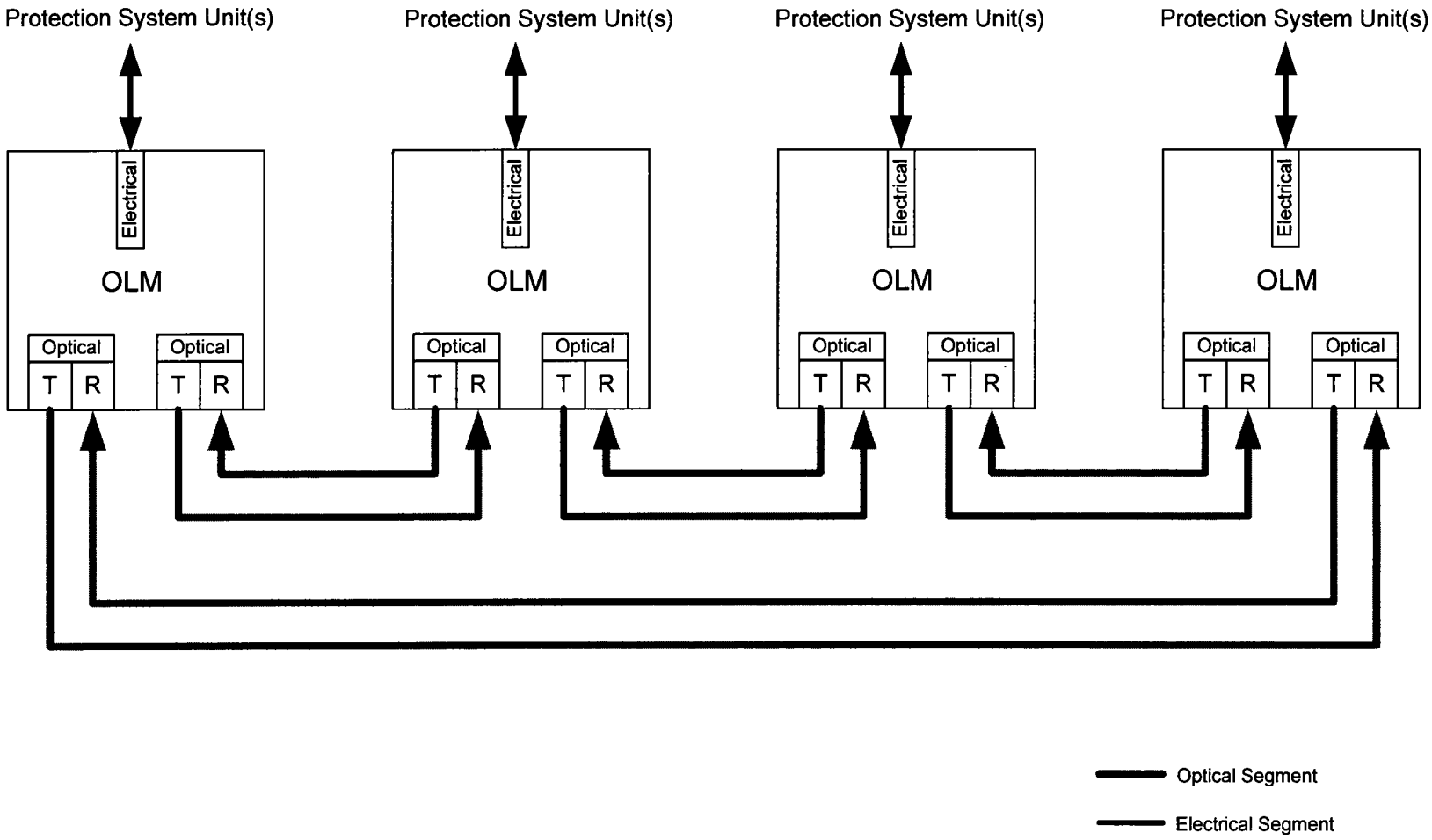


Figure 6-3—Subsystem A Division 1 APU – ALU Architecture

Figure 6-4—Subsystem A Division 2 APU – ALU Architecture

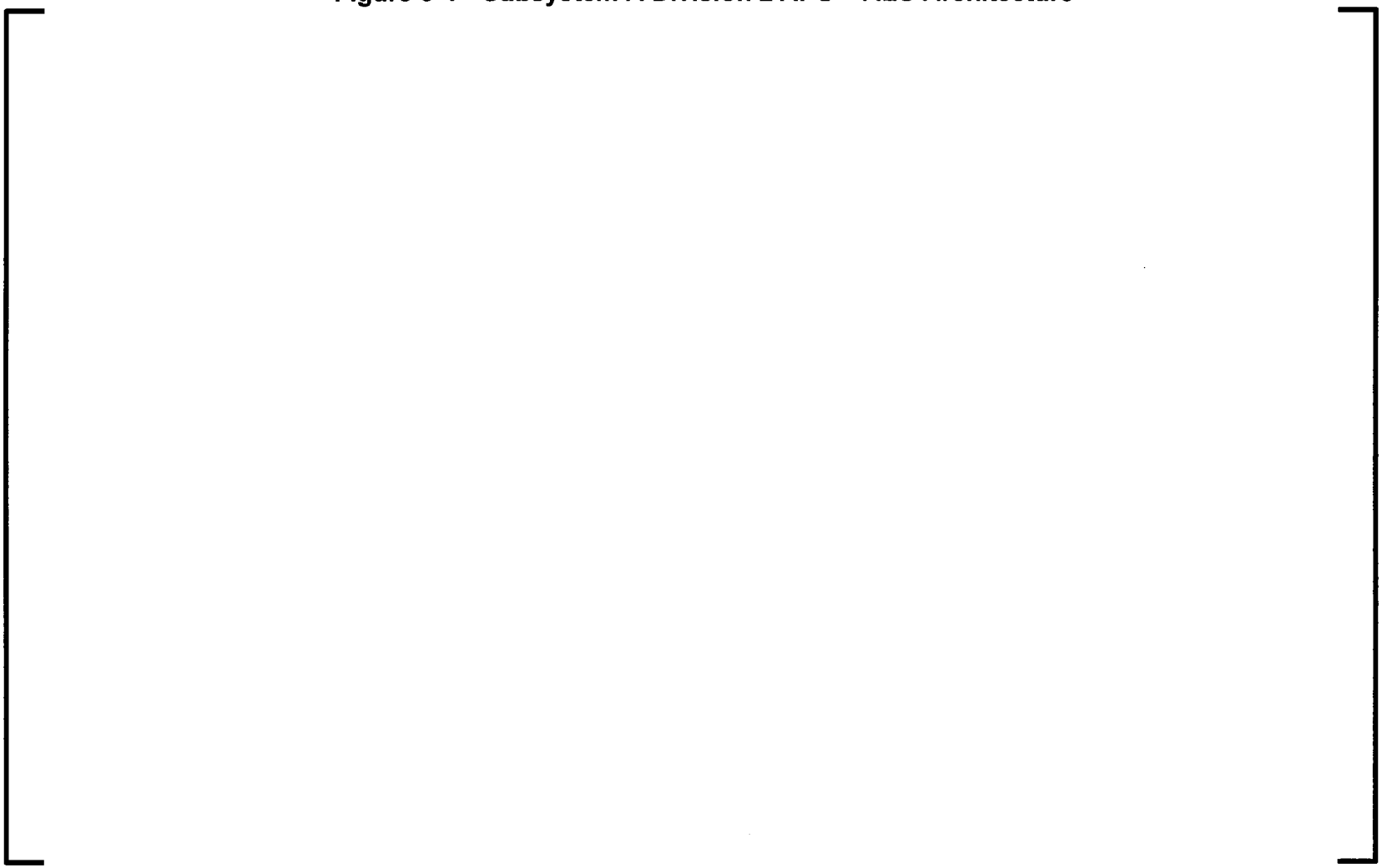


Figure 6-5—Subsystem A Division 3 APU – ALU Architecture

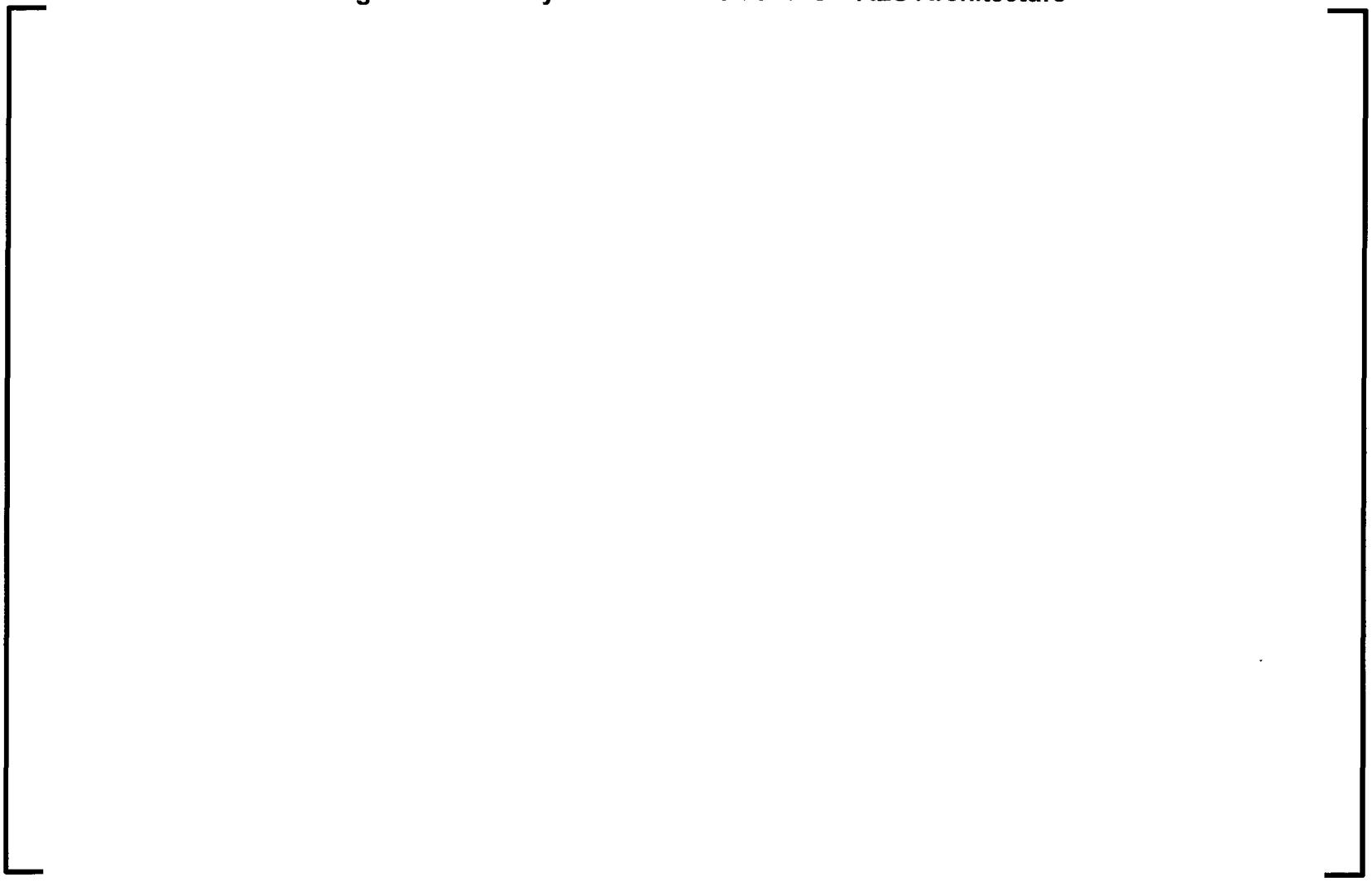


Figure 6-6—Subsystem A Division 4 APU – ALU Architecture

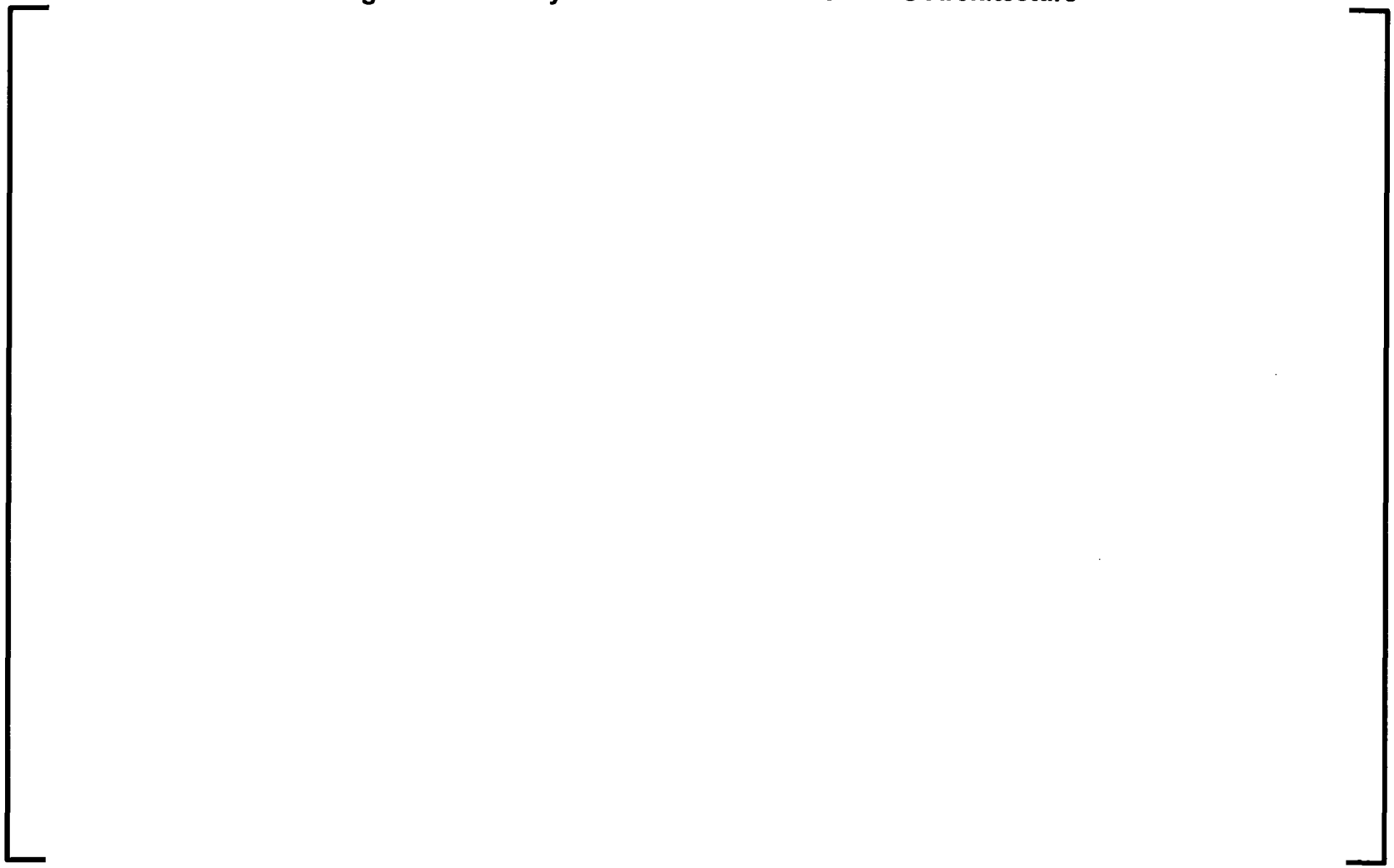


Figure 6-7—Subsystem B Division 1 APU – ALU Architecture

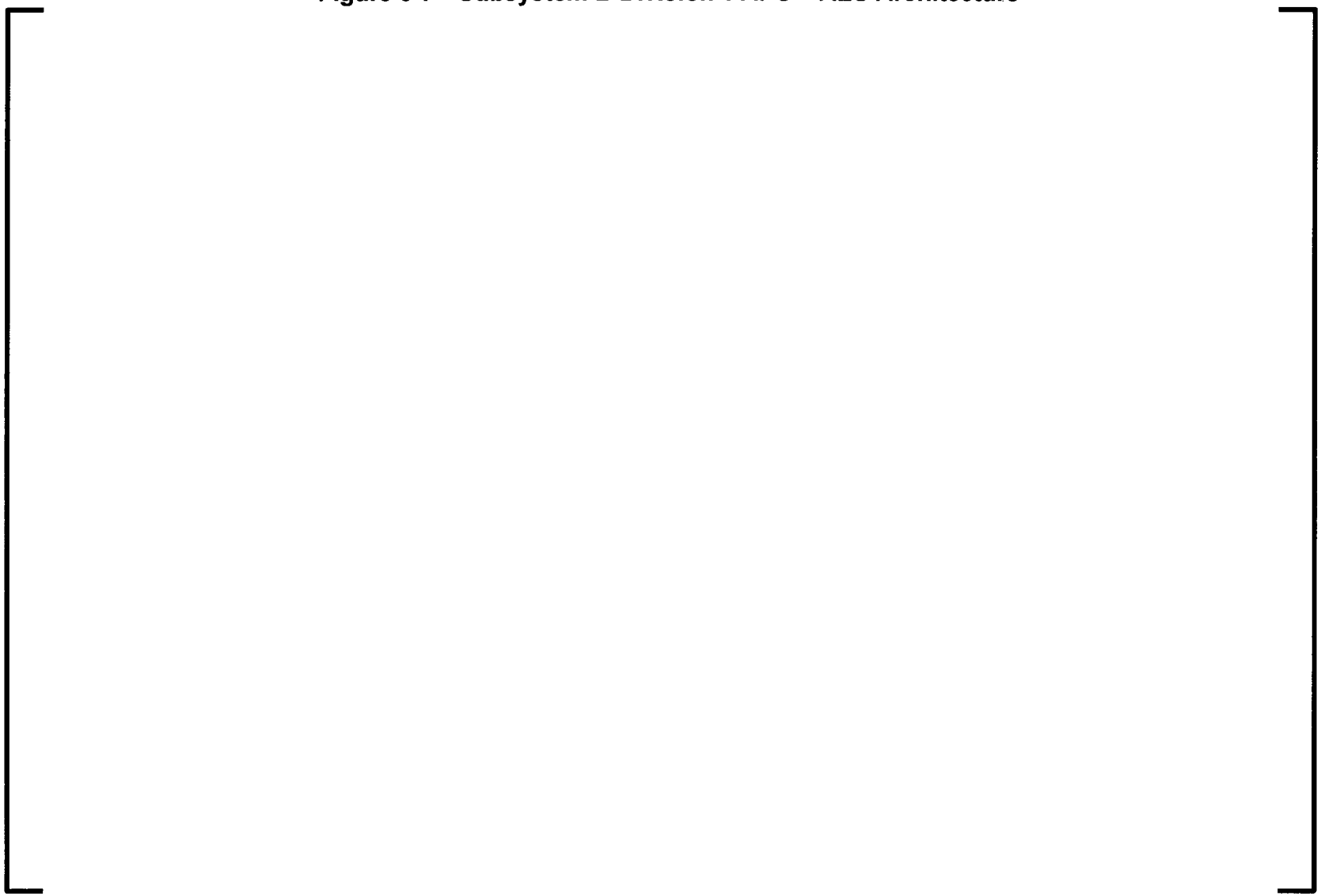


Figure 6-8—Subsystem B Division 2 APU – ALU Architecture

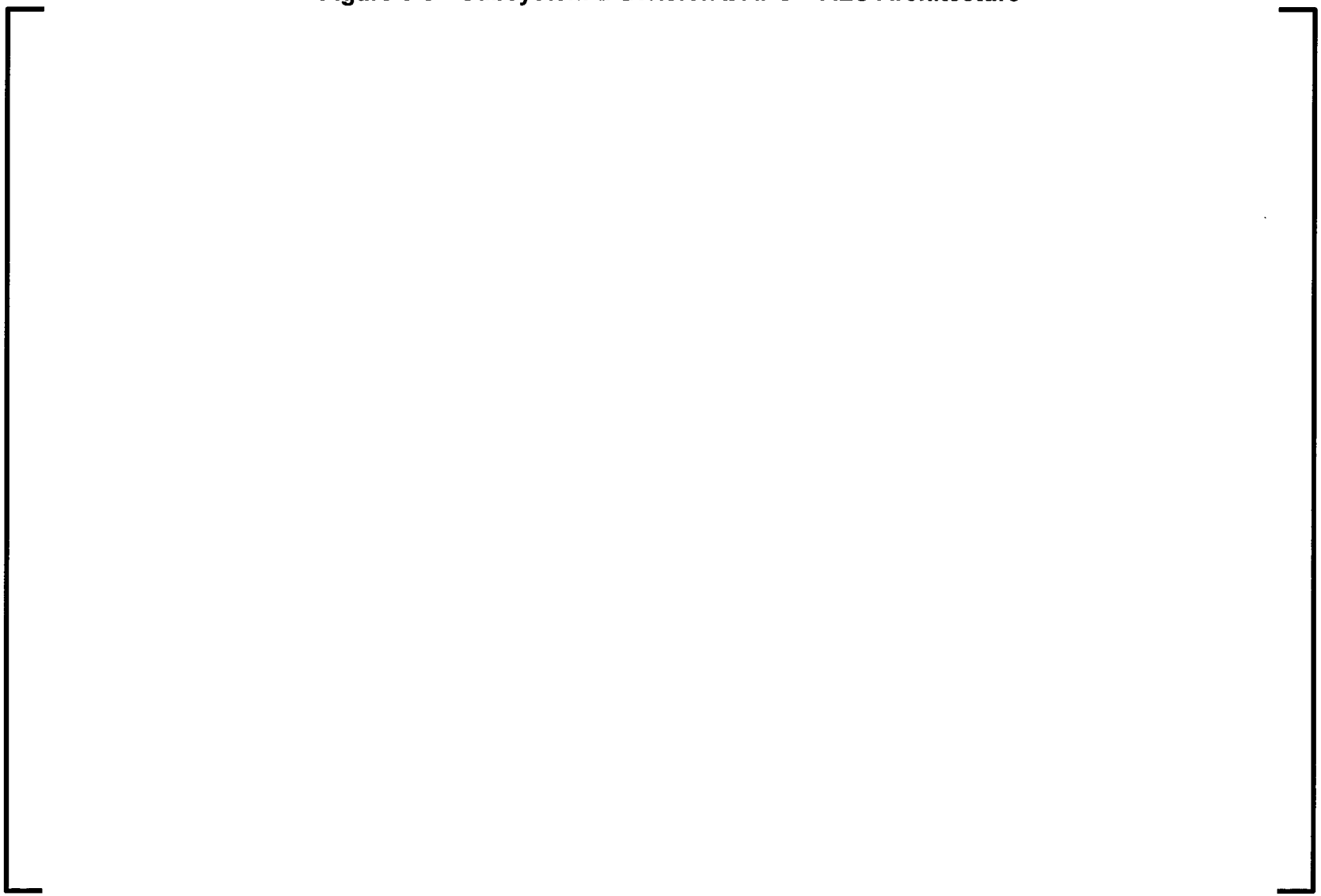


Figure 6-9—Subsystem B Division 3 APU – ALU Architecture

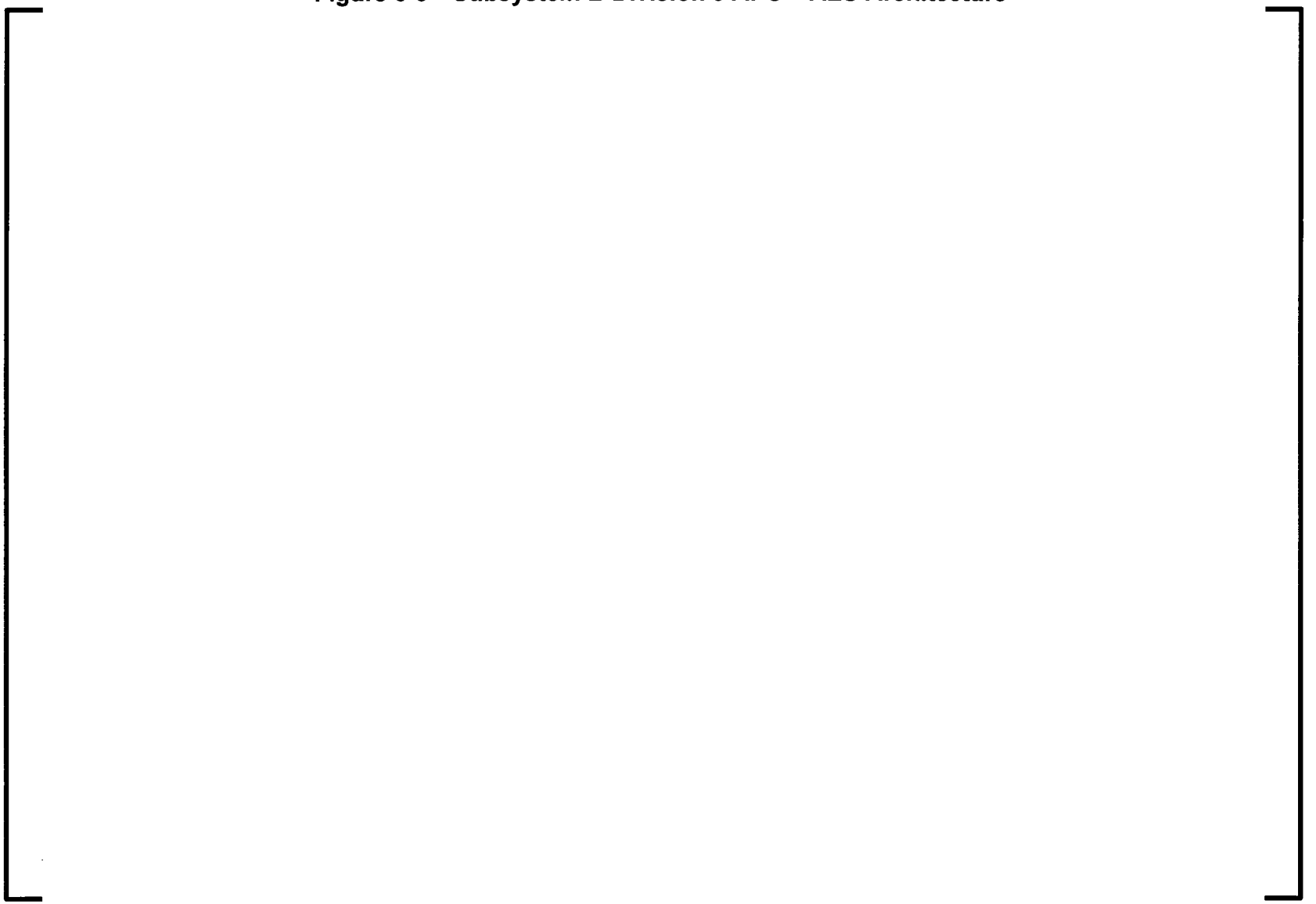


Figure 6-10—Subsystem B Division 4 APU – ALU Architecture

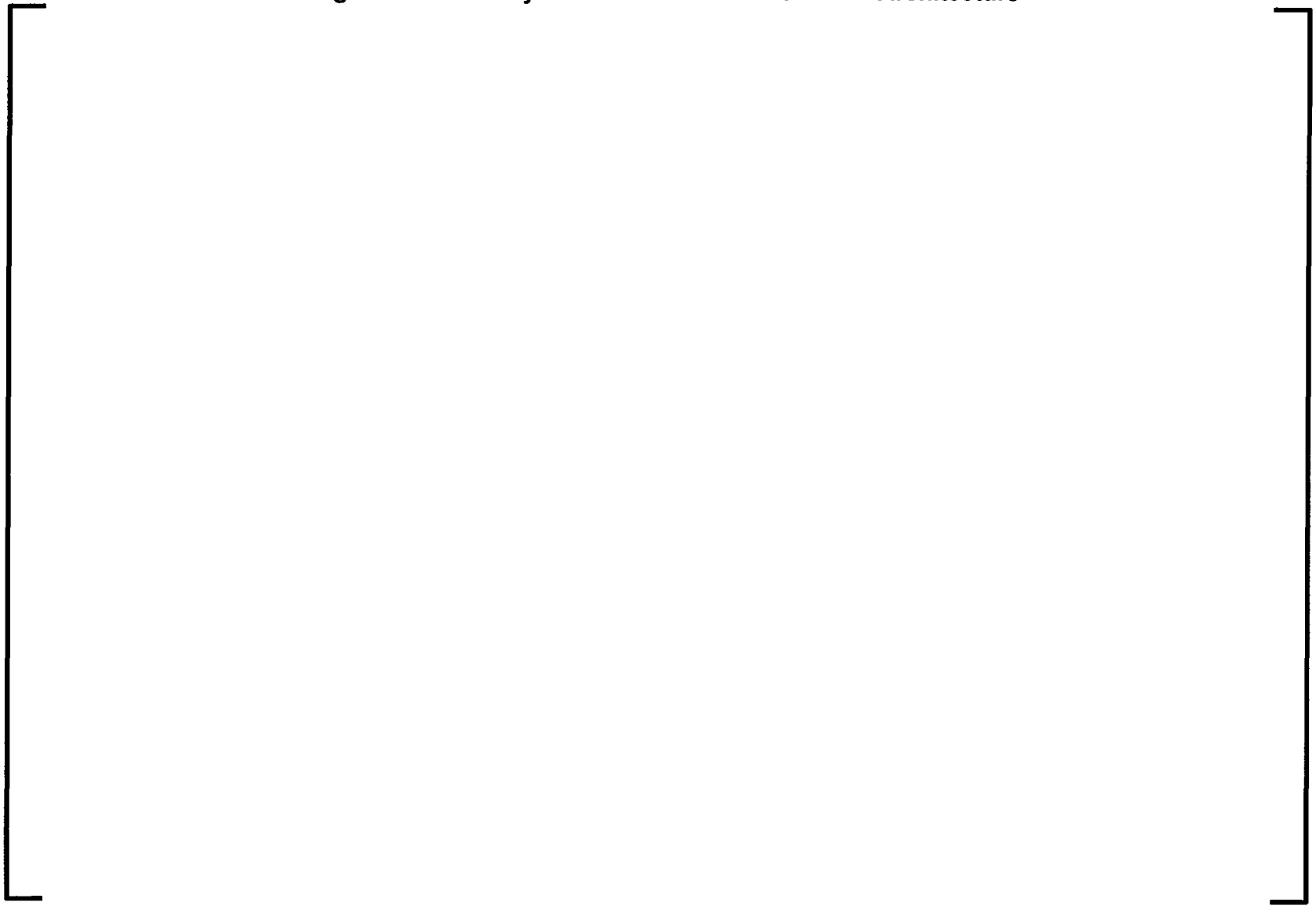


Figure 6-11—MSI-MU – APU Architecture

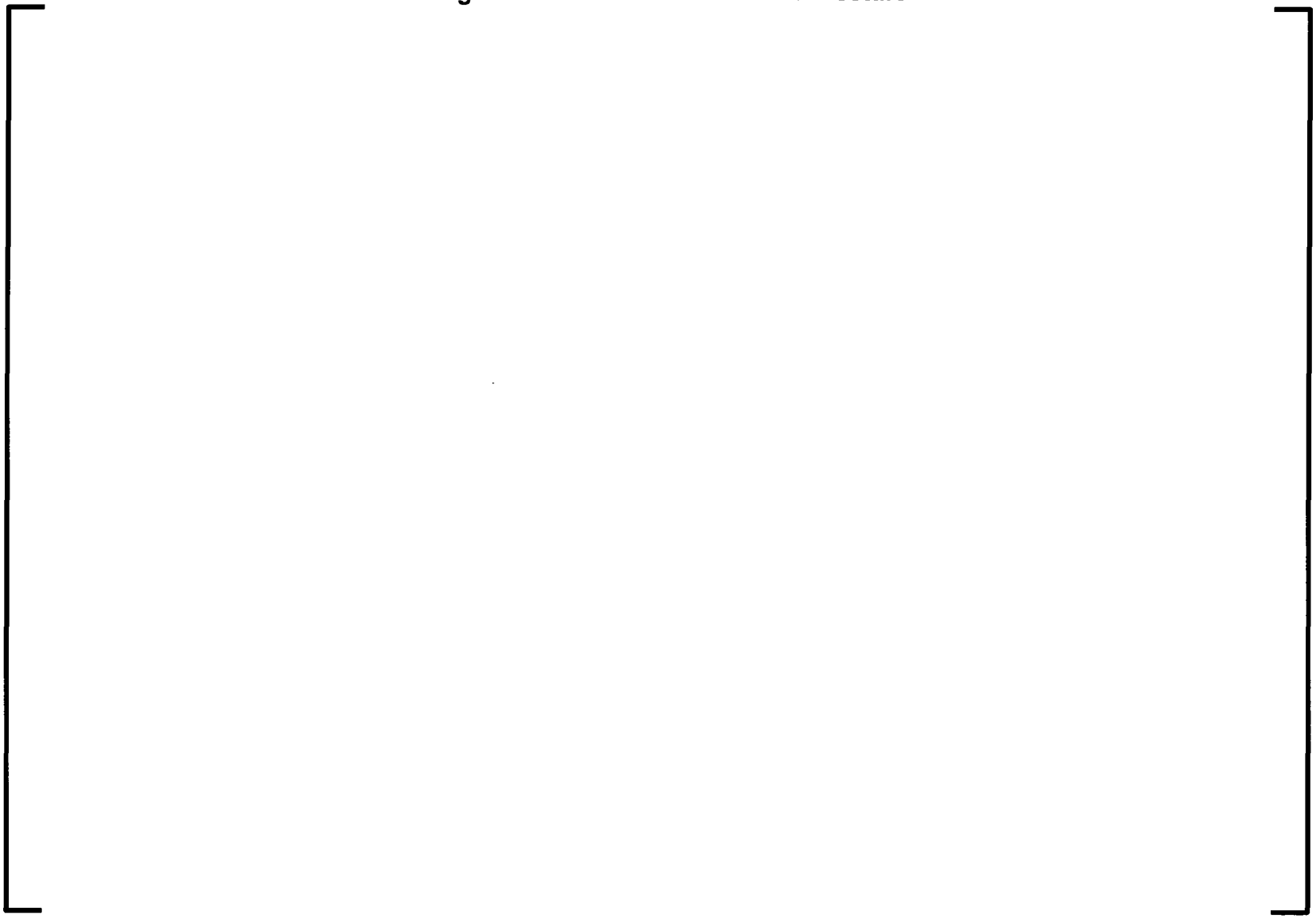


Figure 6-12—MSI-MU – ALU – MSI-AU Architecture

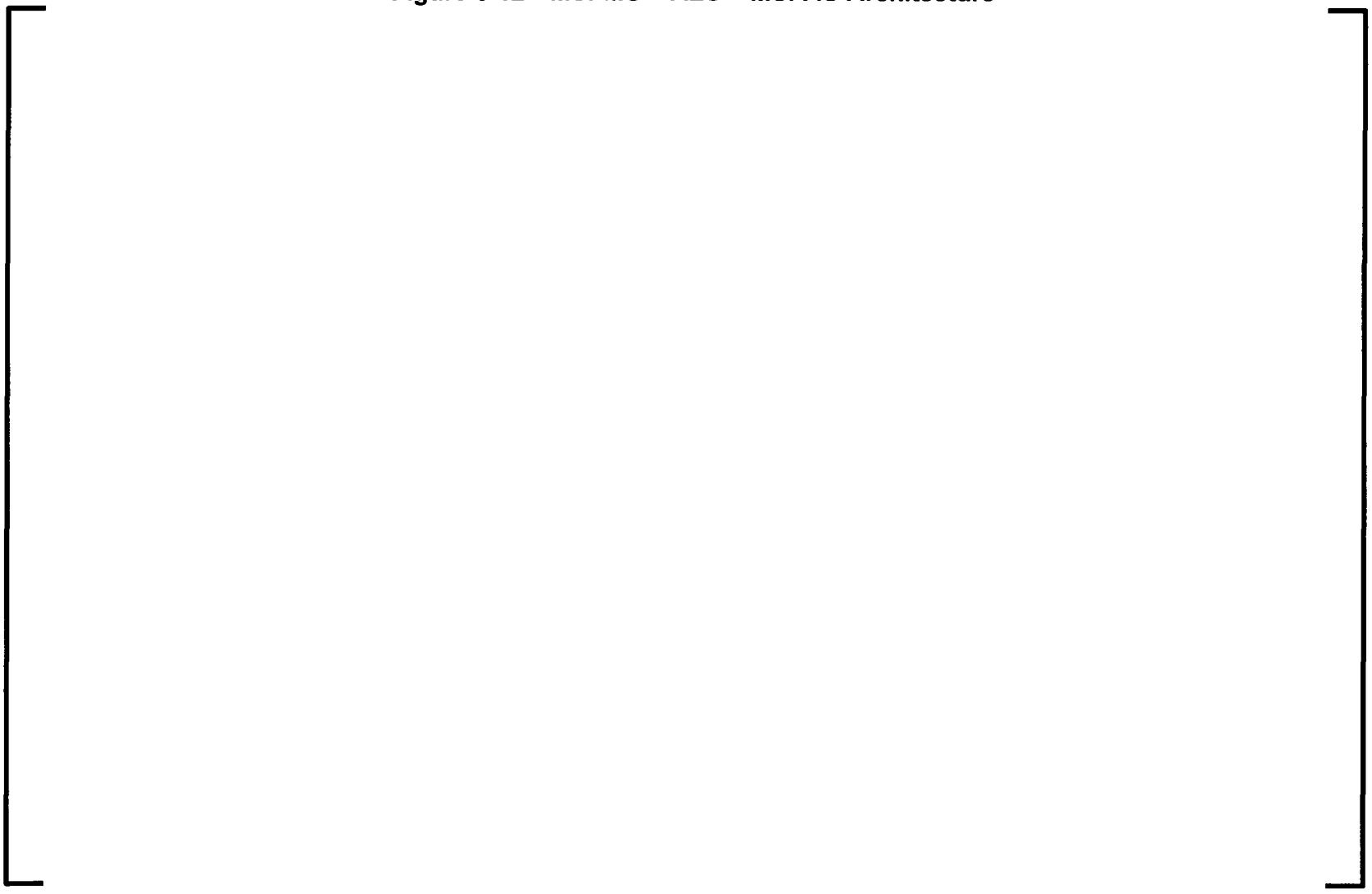
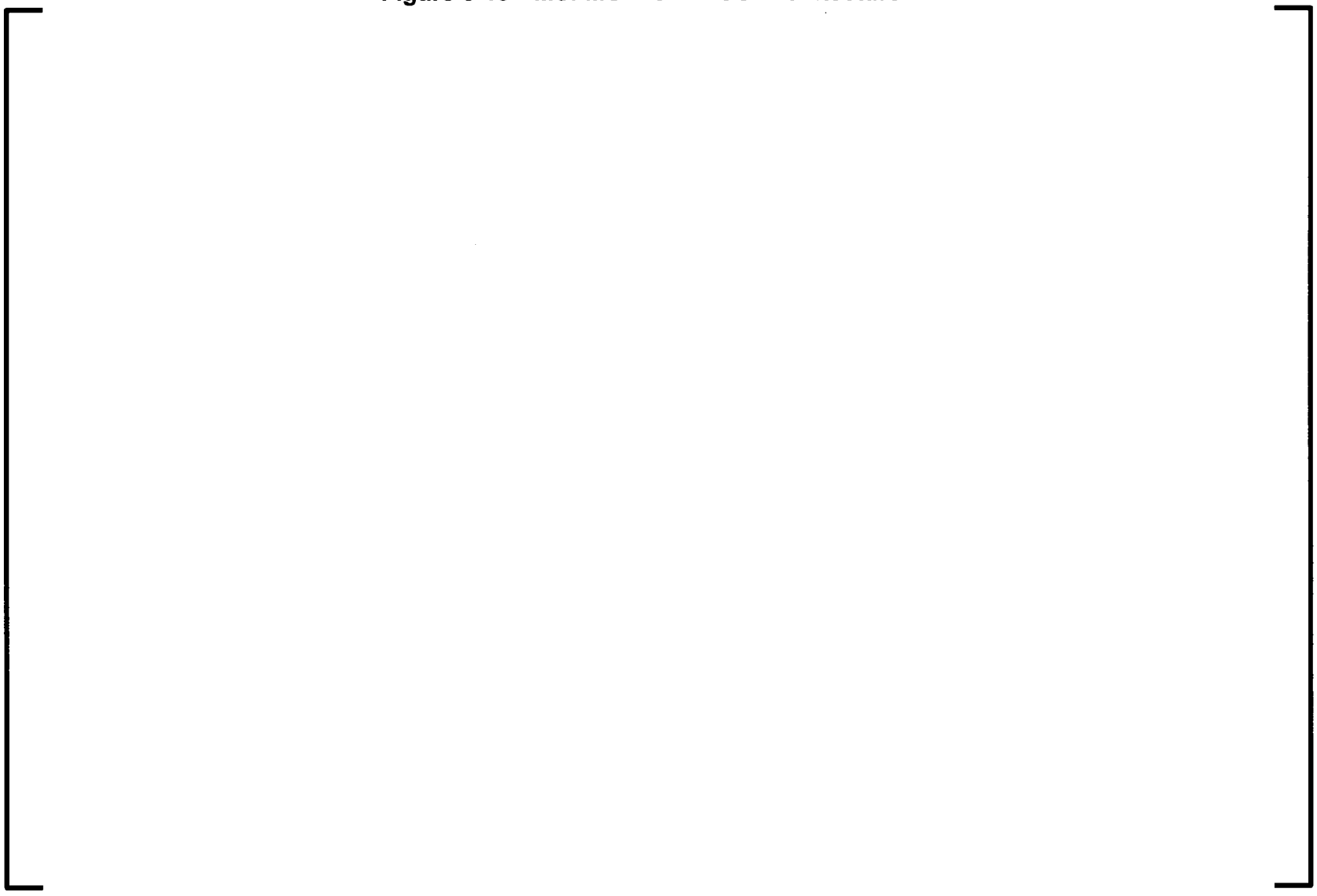


Figure 6-13—MSI-MU – GW – SU Architecture



7.0 REACTOR TRIP

7.1 *Automatic Reactor Trip Sequence*

Figure 7-1 represents a RT sequence. The sequence uses only safety-related sensor inputs from the SCDS and is performed in two layers: the APU layer and the ALU layer. Within a given division, the APU layer involves sensor acquisition, conversion to physical range, any required calculations, and setpoint comparisons. The ALU layer involves voting, actuation logic (e.g., checking permissive conditions), and output of actuation orders.

For the four divisions functioning together, the RT sequence is as follows:

- One APU in each division of the PS acquires signals from one-fourth of the redundant sensors that are inputs to a given RT function. The only exceptions are the SPND signals, where each PS division acquires each of the 72 measurements.
- The APU converts the signals to physical range and performs any required filtering functions (e.g., lead, lag).
- The APU performs any required calculations using the converted and filtered sensor measurement and compares the resulting variable to a relevant setpoint. If a setpoint is breached, the APU generates a partial trigger signal.
- The partial trigger signal from the APU in each division is transferred to redundant ALU in each PS division.
- Two out of four voting is performed on the partial trigger signals in each ALU. If additional logic is needed (e.g., comparison to permissive conditions), the ALU performs this logic.
- If the vote result is TRUE and the actuation logic (if any) is satisfied, the ALU generates an RT signal.

- The RT signals of the redundant ALU in each subsystem are combined in a hardwired "functional AND" logic (Section 7.4), resulting in an RT output.
- The RT outputs from each subsystem within a division are then combined into a hardwired "functional OR" logic (Section 7.4), resulting in a divisional RT order. The divisional RT order is propagated to the corresponding divisional trip devices.

7.2 *Reactor Trip Voting Logic*

Single failures upstream of the ALU layer that could result in an invalid signal being used in the RT actuation are accommodated by modifying the vote in the ALU layer. For RT functions, the vote is always modified toward actuation. The concept of modification toward actuation is described as follows, based on the number of input signals to the voting function block that carry a faulty status:

- 0 faulty input signals: Vote is 2/4.
- 1 faulty input signal: Vote is 2/3.
- 2 faulty input signals: Vote is 1/2.
- 3 faulty input signals: Actuation.
- 4 faulty input signals: Actuation.

The methods used to confirm that an invalid signal is marked with a faulty status before reaching the voting function are described in Section 7.3.

7.3 *Identification of Invalid Signals*

[
]

Further information concerning the identification of invalid signals in a TXS-based system is provided in Reference 24.

7.4 *Reactor Trip Outputs*

The RT outputs of the two redundant ALUs in a subsystem are combined in a hardwired "functional AND" configuration. This requires both ALUs to output the RT order for the associated RT device to be actuated. The outputs of the "functional AND" from both

subsystems within a division are combined in a "functional OR" logic. These configurations are shown in Figure 7-2.

The RT devices used by the PS are de-energize to actuate (i.e., the PS outputs must be in a zero-voltage state to actuate the RT). The normal state of the RT outputs is a high-voltage state, maintaining the trip devices in a closed position.

The term "functional AND" describes the logical operation where both inputs must be in a zero-voltage state to obtain a TRUE output. The TRUE output corresponds to a zero-voltage state.

The "functional AND" provides protection against spurious RT while maintaining the ability to actuate a trip if an ALU has failed. If both ALUs in a sub-system fail, the corresponding RT device is actuated. This results from the failure state of the outputs of the ALU in a zero-voltage state.

The term "functional OR" describes the logical operation where at least one of the inputs must be in a zero-voltage state to obtain a TRUE output. The TRUE output corresponds to a zero-voltage state.

The "functional OR" allows the RT to be actuated by either subsystem regardless of the state of the other subsystem. This arrangement supports the concept of functionally independent subsystems for functional diversity.

7.5 *Manual Reactor Trip*

In addition to the automatic RT processed by the PS, the capability for manual RT is provided to the operator. There are four dedicated RT buttons in the MCR and RSS, one for each division. Any two of these buttons together will actuate an RT. Each button is wired directly into the hardwired logic for trip actuation (functional OR) that bypasses the electronics of the PS. For added reliability and operational purposes, each button is also hardwired to a digital input card on each ALU in the corresponding division. The manual input to the ALU is combined with the automatic RT logic so that

either an automatic function or the manual command sets the RT outputs of the ALU. In both of these configurations, the manual RT from the MCR acts on the same RT devices as the PS automatic RT functions. Figure 7-3 illustrates the manual RT.

7.6 *Reactor Trip Devices*

The automatic RT orders issued by the PS act on the following two levels of the control rod drive power supply system, each capable of actualizing the full RT:

- Trip breakers (safety-related).
- Trip contactors (safety-related).

The automatic orders to the trip devices from the PS are de-energize to actuate. This removes the power to the control rod grippers and allows the rods to drop. Figure 7-4 shows the arrangement of the various RT actuators.

7.6.1 *Trip Breakers*

Each PS division is assigned to one of four trip breakers; each divisional RT order acts on the under-voltage coil of the assigned breaker (de-energize to open). PS Divisions 1 and 2 open trip breakers located in Division 2. PS Divisions 3 and 4 open trip breakers located in Division 3. The trip breakers are arranged in a "1 out of 2 taken twice" configuration that withstands single failure and requires the following logical combination of PS divisional RT orders to actuate an RT: (1 or 2) and (3 or 4).

7.6.2 *Trip Contactors*

There are 23 sets of four trip contactors. Each set can remove power to four CRDM power supplies. Eleven sets of contactors are in Division 1, and 12 sets are in Division 4. Each PS division is assigned to one contactor in each of the 23 sets. Each set of four contactors is arranged in a 2 out of 4 configuration. Together the trip breakers and trip contactors withstand single and double failures. Additionally, the trip contactors are diverse from the trip breakers to add reliability to the reactor trip function as a whole.

Figure 7-1—Reactor Trip Sequence (One Division)

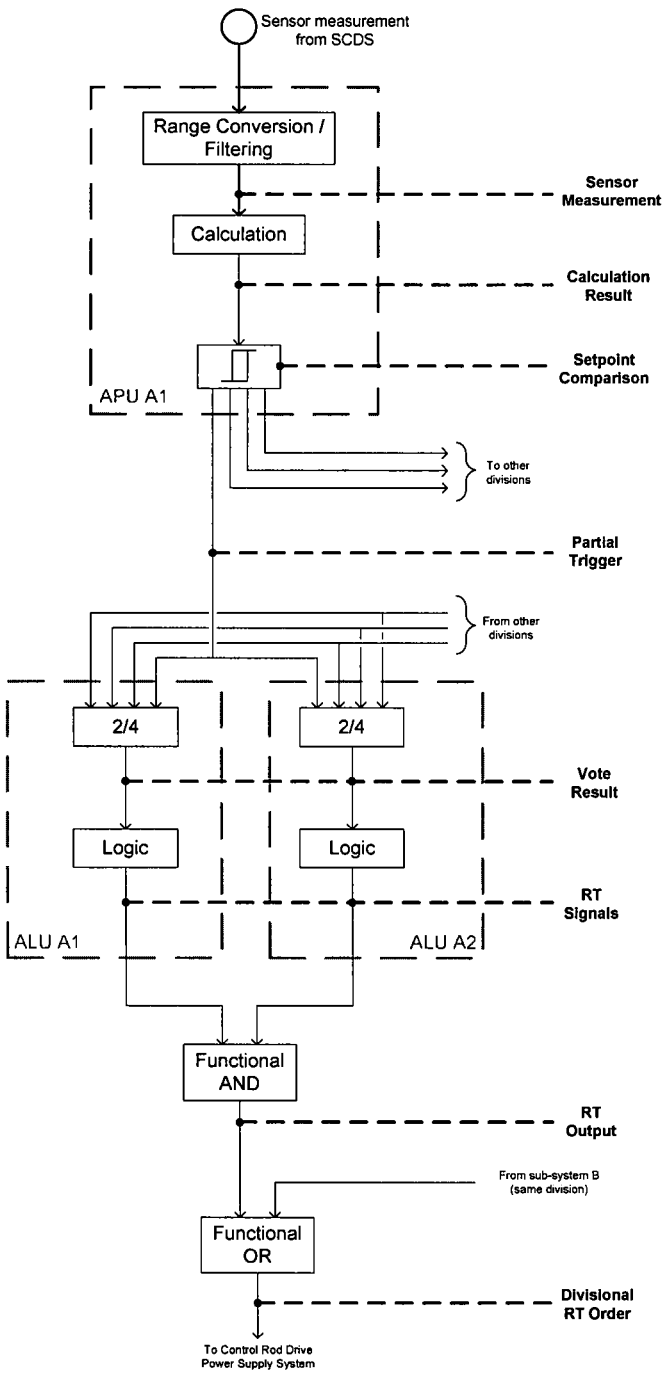


Figure 7-2—Reactor Trip Outputs in One Division

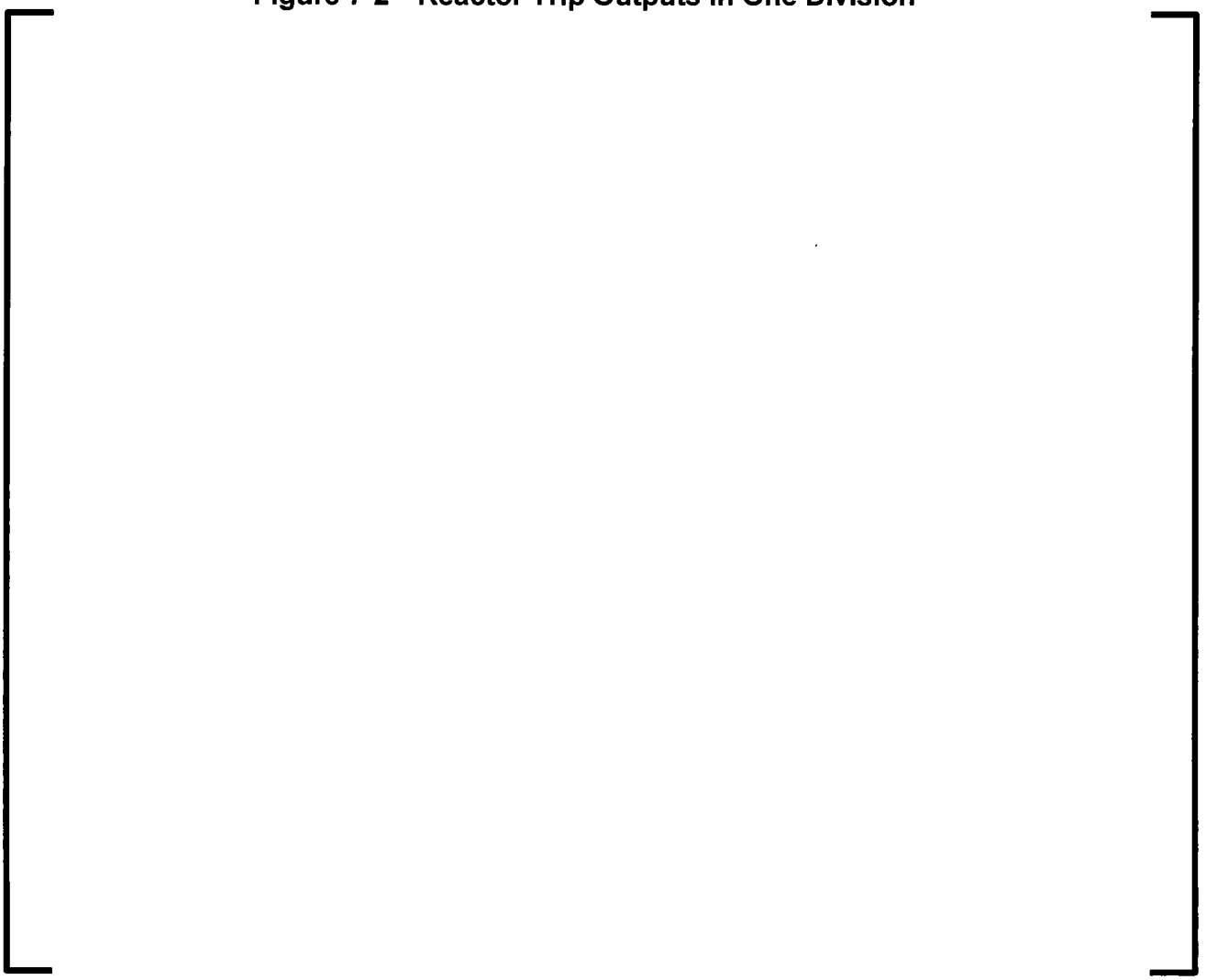


Figure 7-3—Manual Reactor Trip (One Division)

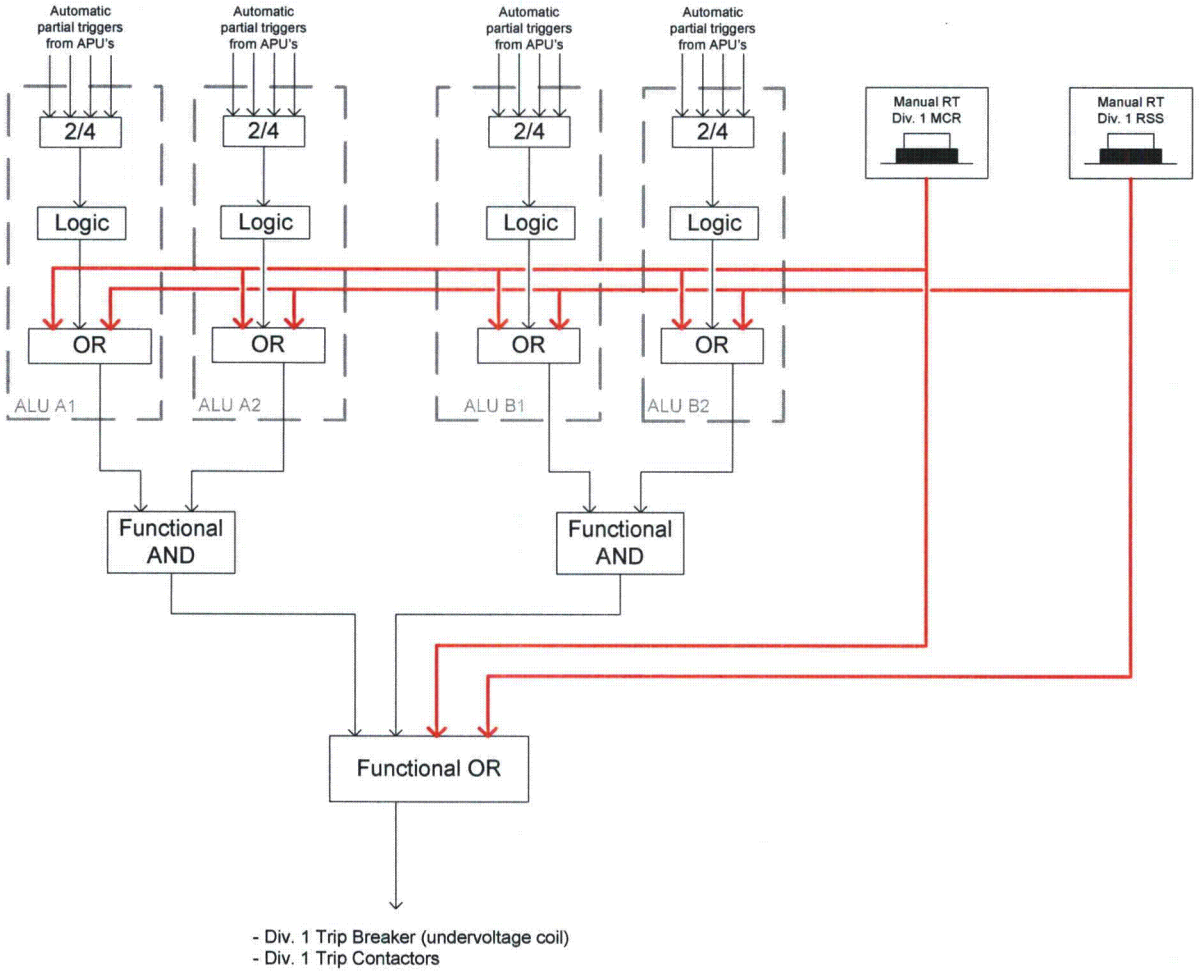
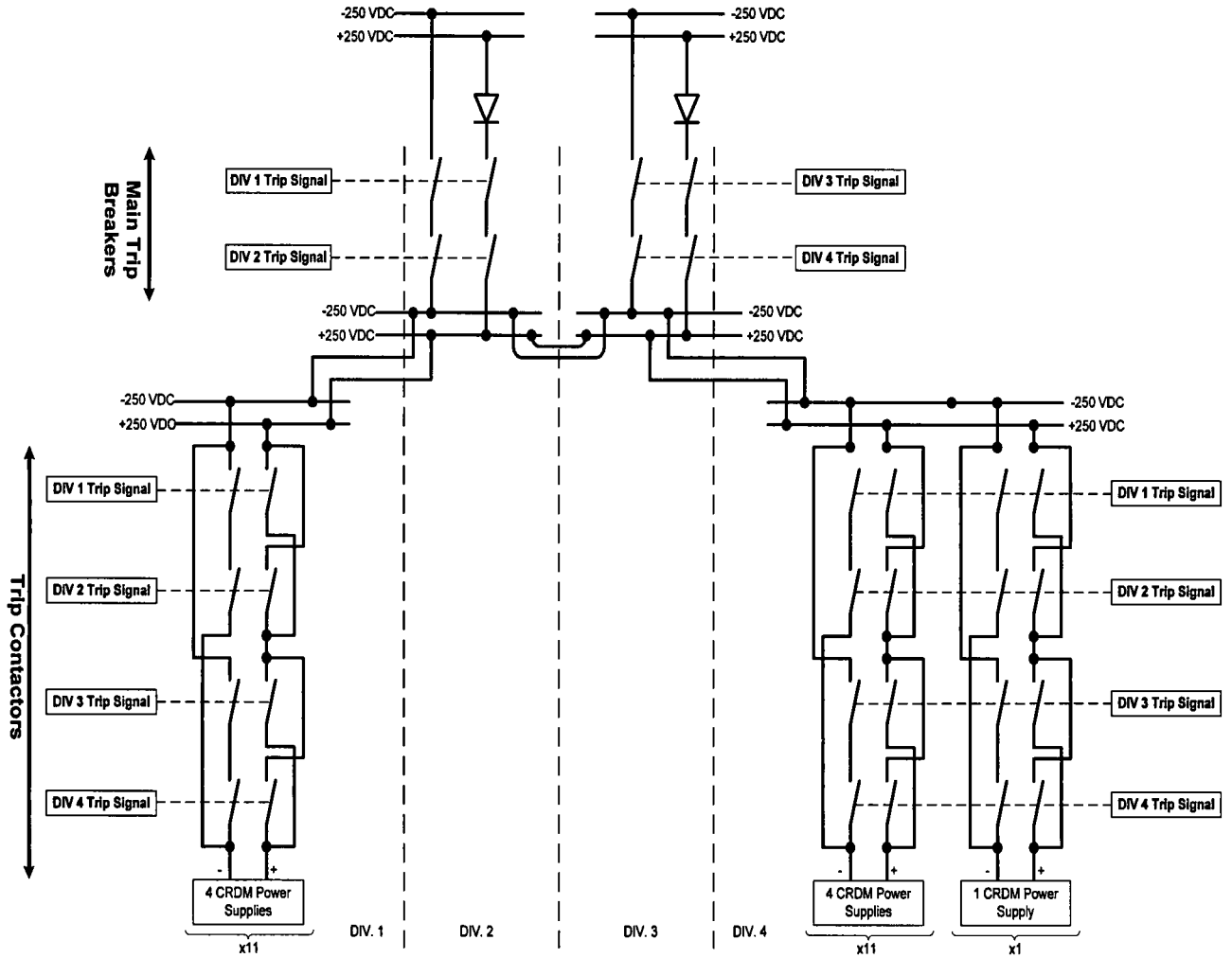


Figure 7-4—Reactor Trip Breakers and Reactor Trip Contactors



8.0 ENGINEERED SAFETY FEATURES ACTUATION

8.1 *Automatic ESF Actuation Sequence*

The example of an ESF actuation sequence is shown in Figure 8-1, and is similar to the RT sequence. The ESF actuation is performed in two layers: APU and ALU. Within a given division, the APU layer involves sensor acquisition, conversion to physical range, any required calculations, and setpoint comparisons. The ALU layer involves voting, actuation logic (e.g., checking permissive conditions, sequencing), signal latching, and output of actuation orders.

For the four divisions functioning together, the example of an ESF actuation sequence is as follows:

- One APU in each division of the PS acquires one-fourth of the redundant inputs from the SCDS for a given ESF actuation function.
- The APU converts the signals to physical range and performs any required filtering functions (e.g., lead, lag).
- The APU performs any required calculations using the converted and filtered sensor measurement, and compares the resulting variable to a relevant setpoint. If a setpoint is breached, the APU generates a partial trigger.
- The partial trigger signal from the APU in each division is transferred to redundant ALUs in the PS division responsible for the ESF system actuation.
- Two out of four voting is performed on the partial trigger signals in each ALU. If any additional logic is needed (e.g., comparison to permissive conditions), the ALU performs this logic.
- If the vote result is TRUE and the actuation logic, if any, is satisfied, the ALU generates an ESF actuation signal.
- The actuation signal is latched via a set-reset function block in the ALU to confirm completion of the function.

- The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired "functional OR"; therefore, either of the redundant ALUs can actuate an ESF function. The result of the "functional OR" is an ESF actuation order.

8.2 *ESF Actuation Voting Logic*

Single failures upstream of the ALU layer that could result in an invalid signal being used in the ESF actuation are accommodated by modifying the vote in the ALU layer. Each ESF actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an ESF function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The concept of modification toward actuation is described in Section 7.2. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows:

- 0 faulty input signals: Vote is 2/4.
- 1 faulty input signal: Vote is 2/3.
- 2 faulty input signals: Vote is 2/2.
- 3 faulty input signals: No actuation.
- 4 faulty input signals No actuation.

Section 7.3 describes the methods used to mark an invalid signal with a faulty status before reaching the voting function.

8.3 *ESF Actuation Outputs*

Each ESF actuator can receive actuation orders from multiple I&C systems. Therefore, the priority and actuation control system (PACS) is used to prioritize the actuation orders. The PACS collects the actuation signals from multiple I&C systems and

transfers the proper actuation order to the actuator according to pre-defined priority assignments.

8.4 *Divisional Assignments – ESF Actuation Outputs*

Determining which division of the PS will act on a given ESF actuator is made on a case-by-case basis. The underlying requirement is that the assignment of PS divisions must not degrade the intended redundancy designed into the mechanical portions of the ESF system. When the divisional assignment is performed correctly (i.e., the redundancy of the mechanical system is maintained), an extra measure of redundancy is obtained because either of the two redundant ALU within the PS division can actuate the same ESF function.

Overall plant safety may dictate that special attention is required to prevent the spurious actuation of certain ESF systems. In these cases, the PS divisional assignment must maintain the redundancy of the entire ESF system and implement measures to avoid spurious actuation. One example of such an implementation is provided below.

Figure 8-2 is a simplified representation of a main steam isolation valve (MSIV) and its associated solenoid pilot valves. The ESF actuation function initiates MSIV closure. There are two redundant mechanical paths (one on each side of the valve as shown in Figure 8-2); either can accomplish the closure function. The three solenoid pilot valves in one redundancy must actuate to close the MSIV. The PS divisional assignment must maintain the level of redundancy inherent in the mechanical design. MSIV closure is a function that also requires special attention to avoid spurious actuation. To accomplish both objectives, PS Divisions 1 and 3 are assigned to one mechanical redundancy, and PS Divisions 2 and 4 are assigned to the other mechanical redundancy. The following logical combination of PS divisional actuation is required to close the MSIV: (1 and 3) or (2 and 4).

Therefore, no single divisional failure of the PS results in either a failure to close when needed, or a spurious actuation.

8.5 *System Level Manual ESF Actuations*

In addition to the automatic ESF actuation functions performed by the PS, the capability to manually initiate these functions at the system level is provided in the MCR. The U.S. EPR design includes the ability to manually manipulate these actuators at the individual component level from the safety-related SICS and non-safety-related PICS (the component level manipulations are not processed through the PS). The system level actuations addressed in this section are implemented through Class 1E actuation paths and are single failure tolerant.

The manual system-level ESF actuation functions are available to the operator on the safety information and control system (SICS). The signals from the SICS are acquired by the ALUs of the PS and are combined with the automatic actuation logic for the corresponding automatic ESF function. Figure 8-3 shows the implementation of a manual system-level ESF actuation. This way, the same PS outputs are energized whether the actuation occurred automatically or manually. The implementation of each system level manual ESF function is described in U.S. EPR FSAR Tier 2, Section 7.3.

Figure 8-1—ESFAS Actuation Sequence (One Division)

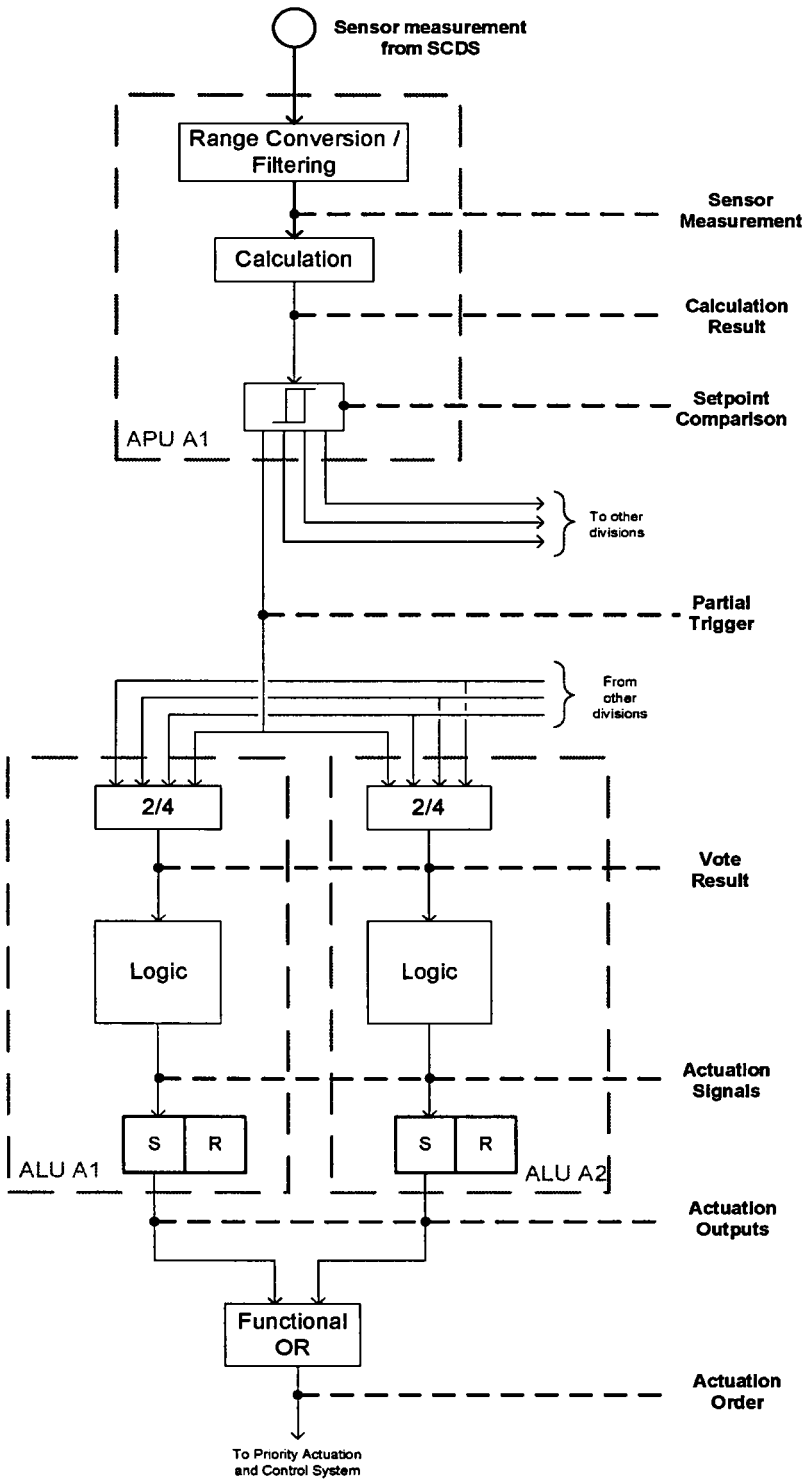


Figure 8-2—Example of PS Divisional Assignment to an ESF Actuation

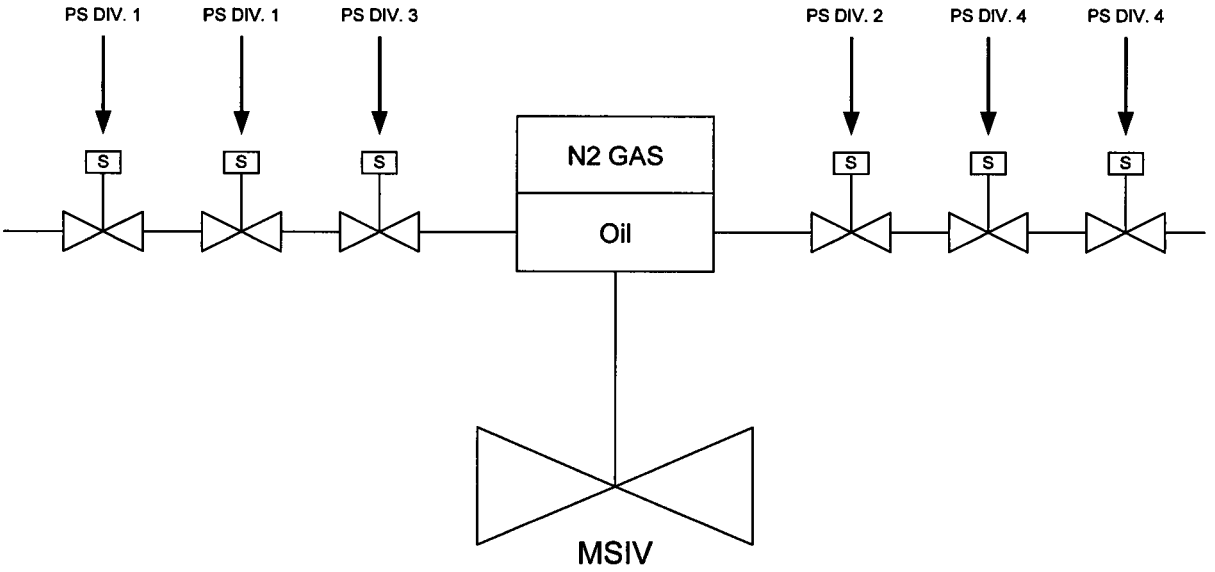
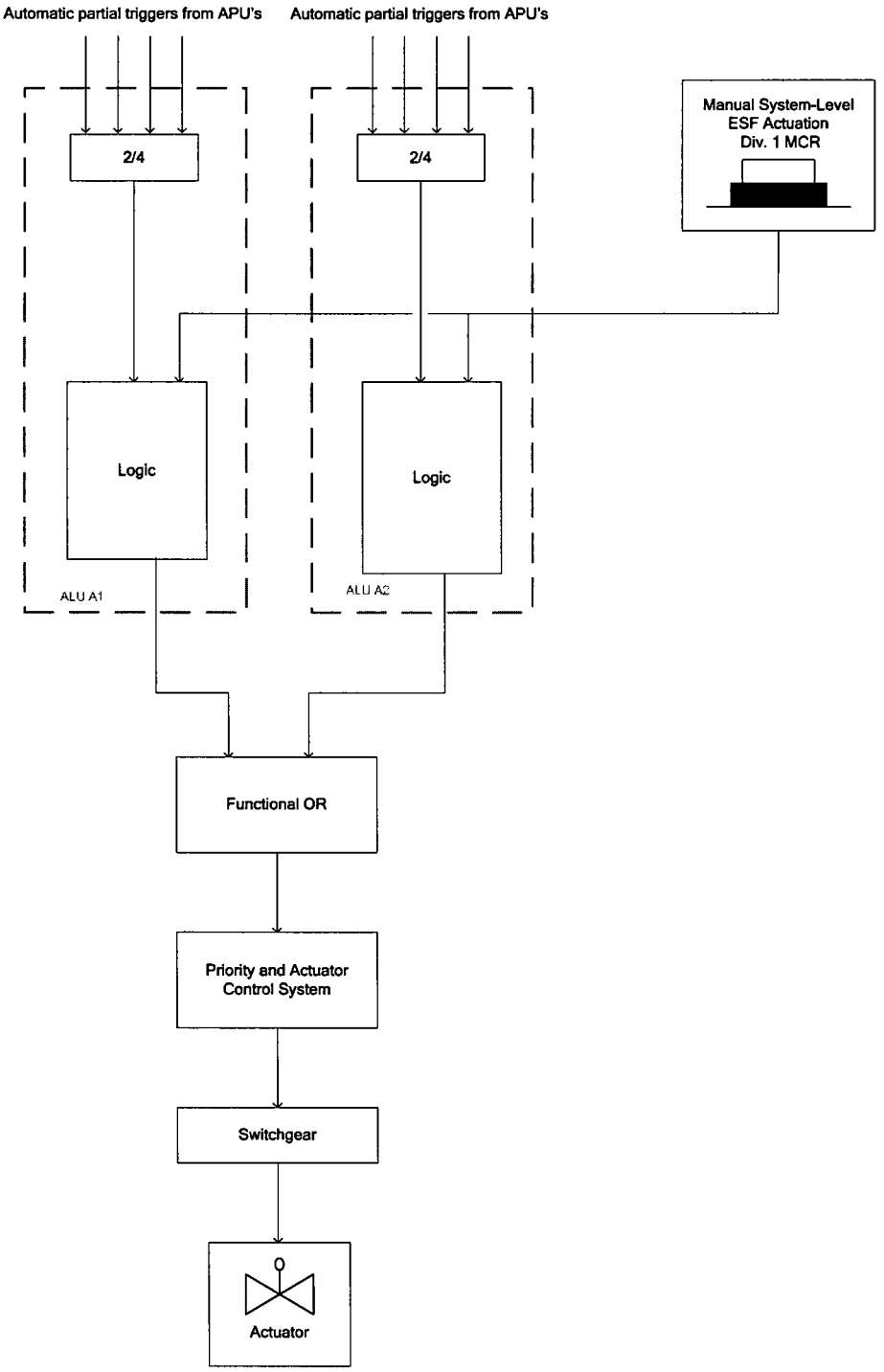


Figure 8-3—Manual System-Level ESFAS Actuation Sequence (One Division)



9.0 PERMISSIVE SIGNALS

9.1 *Definition*

The PS uses permissive signals to enable or disable protective functions according to the operating status of the plant. A permissive is a condition to be satisfied based on the information given by a set of sensors. The conditions associated with a permissive indicate the validity of certain protective functions with respect to the operating status of the plant.

The state of a permissive signal is defined as follows:

- A permissive is validated if the associated condition is satisfied. A validated permissive signal carries a logical value of "1."
- A permissive is inhibited if the associated condition is not satisfied. An inhibited permissive signal carries a logical value of "0."
- In some cases, in addition to the plant conditions being satisfied or not satisfied, a manual input is required to validate or inhibit the permissive.

A validated permissive can enable or disable protective functions. Likewise, an inhibited permissive can enable or disable protective functions. Additionally, a validated or inhibited permissive can directly launch selected actions and enable or disable complete functions.

The plant condition related to a permissive is automatically detected based on a given set of sensors. One-fourth of the redundant sensors are acquired by the SCDS, then routed to the APU in each division of the PS. The sensor measurements are compared to the related permissive setpoint in the division where they were acquired. The results of the setpoint comparisons are distributed to the ALU layer of the four divisions for voting. The voting logic used to validate the plant condition related to a permissive can be either "2 out of 4" or "3 out of 4" depending on how the related protective functions

are affected by the permissive. The design rules governing implementation of the voting logic are addressed in Section 9.2.

The validation or inhibition of permissive signals is defined as one of two types, depending on whether the state of the permissive is set automatically or manually. Those that are automatically validated or inhibited based on the corresponding plant condition are defined as P-AUTO. If an operator action is required to either validate or inhibit the permissive after the corresponding plant condition is satisfied, the permissive is defined as P-MANU.

A set of design rules (Section 9.2) governs the determination of permissive type and can result in any of the following for a given permissive signal:

- P-AUTO for both validation and inhibition.
- P-MANU for both validation and inhibition.
- P-AUTO for validation and P-MANU for inhibition.
- P-MANU for validation and P-AUTO for inhibition.

9.2 *Design Rules for Implementation of Permissive Signals*

For each permissive signal, the following set of design rules is applied to maximize the reliability of the affected protective actions:

- If validation (or inhibition) of a permissive signal disables a protective function, this validation (or inhibition) will be processed with a 3 out of 4 voting logic.
- If validation (or inhibition) of a permissive signal enables a protective function, this validation (or inhibition) will be processed with a 2 out of 4 voting logic.
- If validation (or inhibition) of a permissive disables some protective functions and enables other protective functions, the voting logic is chosen to maximize the reliability of those protective functions needed at power operation.
- If a permissive can be validated (or inhibited) automatically without disturbing normal or post-accident operation, the permissive is P-AUTO.

- If an automatic validation (or inhibition) of a permissive could disable protective functions needed in case of an event, the permissive is P-MANU.

If a special case is identified where deviation from a permissive design rule improves overall plant safety, then the deviation can be considered for implementation. For example, overall plant safety may dictate that a certain protective function receives special attention to avoid spurious actuation. In this case, the permissive used to enable the function would be considered for 3 out of 4 voting logic instead of 2 out of 4 as would be dictated by the design rules.

The logic that implements these design rules for each permissive used in the PS is described and illustrated in U.S. EPR FSAR Tier 2, Section 7.2.

10.0 SIGNAL DIVERSITY

10.1 *Definition*

Signal diversity, as applied to the PS, is the use of two diverse parameters to initiate RT to mitigate the effects of the same AOO or PA. This signal diversity is not credited in the diversity and defense-in-depth plant response analysis to mitigate any AOO or PA. However, this signal diversity provides an added layer of protection in the overall U.S. EPR defense-in-depth strategy. The two independent PS subsystems are used to initiate RTs using diverse signals as inputs. A set of design rules facilitates:

- A process for allocating PS functions to the subsystems.
- Minimizing the instances of acquiring a given sensor measurement from SCDS.
- Minimizing the number of actuation outputs.
- Independence between the two subsystems.

Signal diversity is not applied to ESFAS functions. However, these functions are distributed between the subsystems based on the design rules presented in Section 10.2.

10.2 *Design Rules*

The PS subsystem architecture is implemented according to the following rules:

- Units assigned to different subsystems have no network communications between them.
- Units assigned to different subsystems are not located within the same cabinet.
- Units not assigned to a subsystem that communicate with units of both subsystems must use a different network to communicate to each subsystem.

This architecture is designed to provide two functionally independent subsystems. This independence is maintained from the point where inputs enter the cabinet associated

with a subsystem through the actuation outputs of the ALU assigned to a subsystem. The cabinets of both subsystems within a division are supplied by the same divisional power sources, and the actuation outputs of the two subsystems can be combined in hardwired logic.

The reactor trip PS functions are assigned to a subsystem, in an iterative process according to the following rules (in order of decreasing priority):

1. A subsystem is assigned for the primary RT function for each AOO or PA based on the RT function credited for each AOO or PA in the Chapter 15 safety analysis.

2. The AOO or PA in the Chapter 15 safety analysis are modeled assuming failure of the primary RT function to identify a secondary RT function for each AOO or PA, which uses different sensor inputs than the primary function. The secondary RT function is assigned to the opposite sub-system of the primary RT function that protects against the same AOO or PA.

3. If a RT function is required in both subsystems for reasons other than signal diversity, the logic is duplicated and performed in both subsystems.

4. When the subsystem has been determined, the RT functions are assigned to the different APUs within the subsystem. Functions using the same sensors are assigned to the same APU.

ESFAS and permissive PS functions are then assigned to a subsystem, in an iterative process, according to the following rules (in order of decreasing priority):

5. ESFAS and permissive functions that use sensors already assigned to a subsystem (due to RT assignments) are assigned to the same subsystem as the sensors.

6. ESFAS and permissive functions that act on the same actuators are assigned to the same subsystem.

7. If an ESFAS or permissive function is required in both subsystems, the logic is duplicated and performed in both subsystems.

8. When the subsystem has been determined, the functions are assigned to the different APUs within the subsystem. Functions using the same sensors are assigned to the same APU.

11.0 INTERCHANNEL COMMUNICATION

11.1 *Communication Interfaces*

The use of interchannel communication in the PS is demonstrated by communication between two function processors located in two different divisions of the PS (Figure 11-1). The typical hardware configuration includes a function processor with a process field bus (PROFIBUS) communication module attached. Each communication module is connected to an OLM that converts the electrical communication signals to optical signals, which are transmitted over fiber-optic cables to other OLMs on the network.

Communication activities are performed sequentially and controlled by the central control unit of the runtime environment. The sending function processor initiates sending activities and the messages are addressed to the receiving function processor. The intermediate communication modules and OLMs transfer the messages without influencing the message data. The dual port random access memory (DPRAM) contained in the communication module serves as a buffering circuit and separates data flow between send and receive channels. The separation of data flow is continued within the function processor by the message input and message output buffers. The function processor accesses the DPRAM independently of access by the communication module's PROFIBUS controller, which sends and receives data to and from the network.

11.2 *Communications Independence*

The TXS platform is designed using principles to provide communication independence. These principles are referred to as principles for interference-free communication in Reference 23. These principles, which provide communication independence between the redundant divisions of the PS, are summarized as follows:

- Initiate message sending activities by the sending function processor addressed to the receiving function processor. The intermediate communication modules serve for data transfer only, and do not influence the message data.
- Control processing and communication actions in a discrete, cyclic manner.
- Use a communication module that serves as a buffering circuit in accordance with guidance from IEEE Std 7-4.3.2-2003, Annex E (Reference 14).

[ ]

- Provide individual memory locations for each message to allow separation between the send and receive data paths.

[ ]

- Check the status of individual signals that provide valid input data to function processing.
- Interdivisional communication between the redundant divisions of the PS, are for voting purposes only. Two-out-of-four and three-out-of-four voting protects against the effects of a single-failure in a division.

Communication independence is the ability of functional units in redundant divisions to exchange data without adverse interaction. Independence guidance from IEEE Std 603-1998 is supplemented by guidance in IEEE Std 7-4.3.2.

Guidance in IEEE Std 7-4.3.2 is supplemented by an annex on communication independence (Reference 14), which defines acceptable means for functional unit communications between redundant divisions and between safety and non-safety systems.

The TXS communication techniques provide communication independence between redundant divisions and are consistent with the guidance in Reference 14. The related figure from Reference 14 is duplicated in Figure 11-2. An equivalent figure describing the TXS communication is shown in Figure 11-3. Figure 11-3 depicts the use of buffering circuits and separation of data flow (communication isolation), which provide an acceptable method of communication independence and prevents adverse interactions.

For communication between redundant divisions in the PS, the buffering circuit consists of the PROFIBUS controller and the DPRAM; both are contained in the communication module. The communication module provides buffering so the function processors can read and write to the DPRAM independently of the PROFIBUS controller, which transfers data between the network and the DPRAM. Therefore, the function processor in one division operates independently of the operation of a function processor in a redundant division.

The DPRAM also begins the separation of data flow, which continues inside the function processor. Within the function processor, messages from the receive portion of the DPRAM are transferred to the message input buffers where data validation is performed before the data is used in function diagram processing. The results of function diagram processing are placed in the message output buffers (separate from the input buffers), for transfer to the send portion of the DPRAM. This separation of data flow constitutes communication isolation.

The DPRAM contributes to communication independence in two ways:

- It acts as a buffering feature that allows the function processor to operate independently from the PROFIBUS controller.

- It establishes separation of data flow by containing separate memory locations for sent messages and received messages.

The use of the buffering circuit together with communication isolation constitutes communication independence.

Figure 11-1—TXS Communication Principle

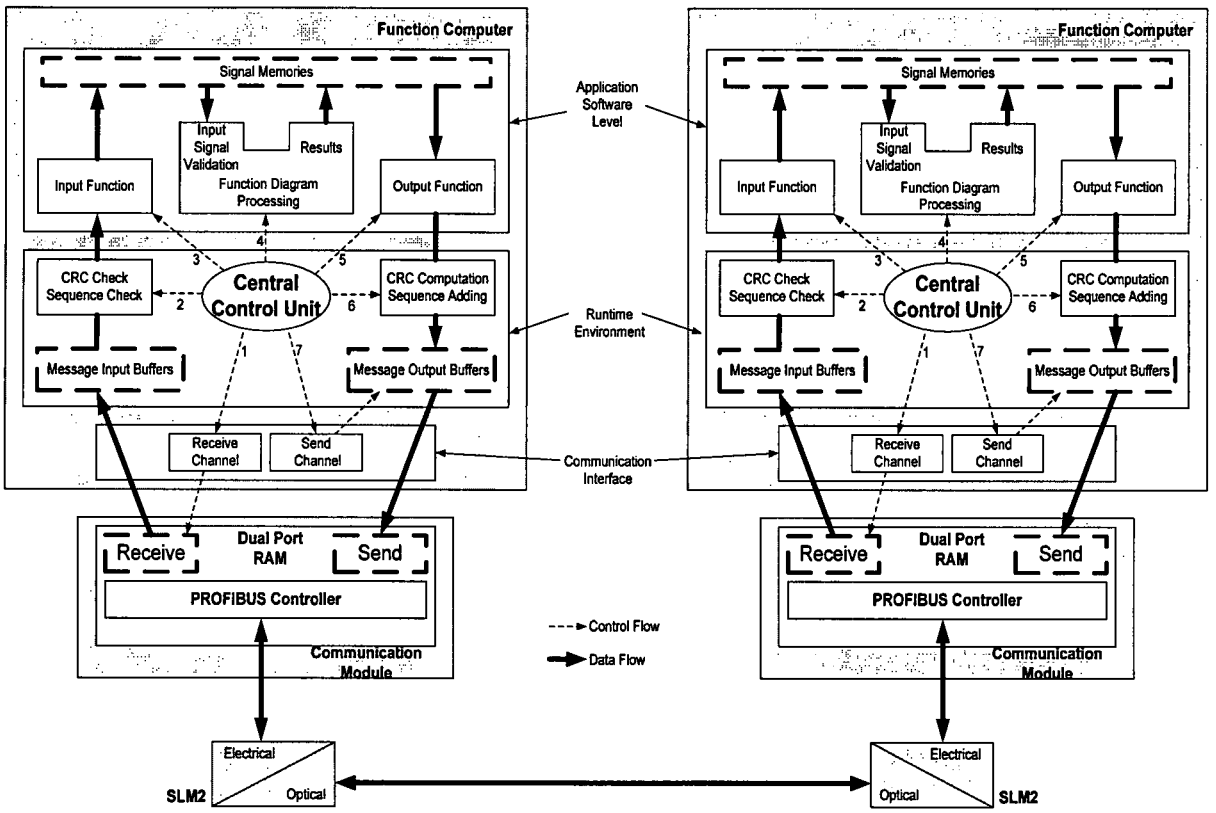


Figure 11-2—Communications Independence (IEEE Std 7-4.3.2)

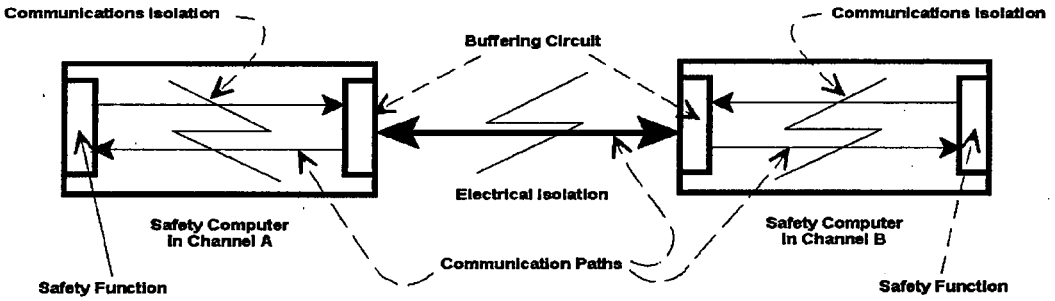
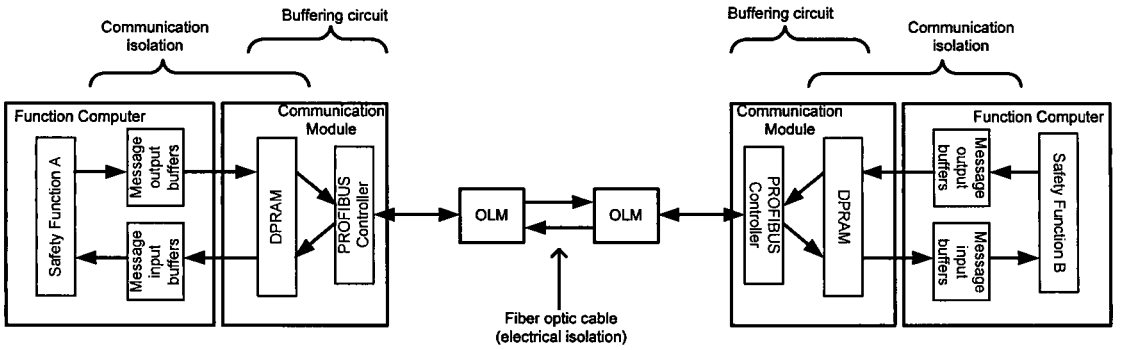


Figure 11-3—Communications Independence (U.S. EPR Implementation)



12.0 SAFETY TO NON-SAFETY-RELATED INTERFACE

12.1 *General Requirements for Interfaces*

The types of interfaces between PS and non-safety-related I&C systems are as follows:

- Information is exchanged between the SU and the PS for diagnostics, monitoring, and maintenance. This interface is normally disconnected and is made available only when an operator in the MCR enables the connection using a key switch.
- Information is transferred from the PS to the PICS. The PS transfers data to the PICS for display to the operator. Electrical isolation for this interface is achieved through Class 1E isolation devices.
- Information is transferred from the PS to the PAS for time stamping of reactor trips and ESFAS functions and to initiate non-safety-related partial cooldown via an isolated, hardwired connection.
- Information is transferred from the PS to the TG I&C system for the turbine trip function via an isolated, hardwired connection.
- Information is transferred from the PS to the (Qualified Display System) QDS. The PS transfers data to the QDS for display to the operator. Electrical isolation for this interface is achieved through Class 1E isolation devices.

These interfaces are accomplished in different ways, but the following requirements are consistently applied to the safety to non-safety-related interface:

- Independence is maintained so that failures in a non-safety-related system do not prevent the performance of a safety function.
- Data communication between the non-safety-related system and the PS does not prevent the performance of a safety function.

- The safety system does not rely on information from a non-safety-related system to perform its safety functions.

12.2 *Protection System – Service Unit Interface*

The SU provides functions needed for monitoring, testing, diagnostics, and modifying application software. The SU does not influence the automatic protective functions performed by the PS during normal operation. The SU accesses the system through the Class 1E MSI, which serves as the point of communication isolation between the SU and the PS units performing the safety-related protective functions. The connection between the PS and SU is normally disconnected using an isolation switch. This connection can be enabled only by an operator in the MCR using a key switch. Electrical isolation is provided through optical connections between the SU and the MSI.

12.3 *Protection System – PICS Interface*

In order to demonstrate independence between the PS and PICS, and SAS and PICS, communication will be unidirectional. To verify unidirectional behavior, the connection between the MSI and the gateway, within the PS and SAS, will consist only of a transmit segment between the two electrical to optical converters (EOC) connecting the MSI to the gateway (see Figure 6-13). There will be no physical segment connected that allows any transmittal of information from the gateway to the MSI.

The MSI provides Class 1E communication isolation for the PS – PICS interface. It acts as a qualified data transmission barrier and as a safety-related logical barrier. The MSI checks for, and uses data only from, expected messages that are defined during code generation. Additionally, the MSI checks configured communication channels only. Loss of the MSI does not lead to degradation of automatic protection channels because the MSI does not function as a part of those channels.

GW supports the exchange of information from the PS to the PICS. It acts as a protocol converter between the TXS communication protocol format and the specific protocol format required by the PICS. No direct physical network connection exists between GW

and the PS performing the protective functions. This connection is through the Class 1E MSI.

Separation of data flow is provided within the MSI and in the PS function processor. The interface between the MSI and the PS function processors is implemented in the same way as the inter-channel interfaces described in Section 11.0. Electrical isolation for this interface is achieved through optical connections between the GW and MSI and between the MSI and the PS function processor.

12.4 *Protection System — PAS Interface*

The interface between the PS and PAS is a hardwired interface used for time stamping reactor trips and ESFAS actuations. Electrical isolation for this interface is achieved through Class 1E isolation devices. A hardwired signal will be sent to PAS to initiate non-safety-related partial cooldown.

12.5 *Protection System – Turbine Generator I&C*

The interface between the PS and turbine generator I&C is a hardwired interface to trip the turbine upon a reactor trip. Electrical isolation for this interface is achieved through Class 1E isolation devices.

12.6 *Protection System – QDS*

In order to demonstrate independence between the PS and QDS, communication will be unidirectional. To verify unidirectional behavior, the connection between the two EOCs, and between the PS and QDS will consist only of a transmit segment. There will be no physical segment connected that allows any transmittal of information from the QDS to the PS (refer to U.S. EPR FSAR Tier 2, Figure 7.1-20).

The MSI provides Class 1E communication isolation for the PS – QDS interface. It acts as a qualified data transmission barrier and a safety-related logical barrier. The MSI checks for, and uses data only from, expected messages that are defined during code generation. Additionally, the MSI checks configured communication channels only.

Loss of the MSI does not lead to degradation of automatic protection channels because the MSI functions independently of those channels.

Separation of data flow is provided within the MSI and the PS function processor. The interface between the MSI and the PS function processors is implemented in the same way as the inter-channel interfaces described in Section 11.0. Electrical isolation for this interface is achieved through optical connections between the GW and MSI and between the MSI and the PS function processors.

Figure 12-1—Safety to Non-Safety-Related Communication Interface (IEEE Std 7-4.3.2)

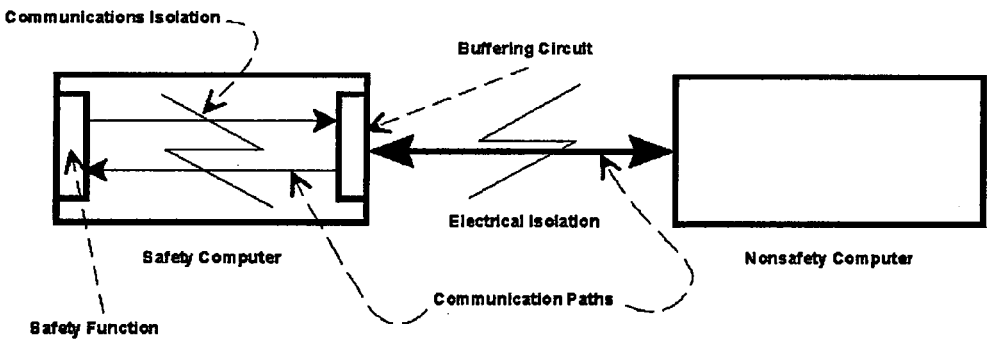
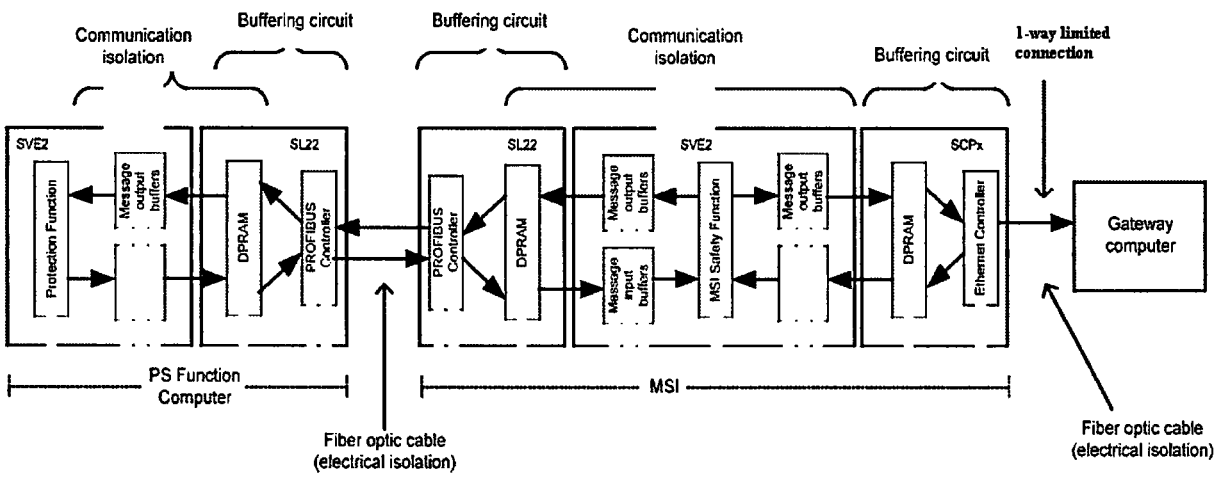


Figure 12-2—Safety to Non-Safety-Related Communication Interface (U.S. EPR Implementation)



13.0 COMPLIANCE TO THE SINGLE FAILURE CRITERION (CLAUSE 5.1 OF IEEE(603-1998)

The PS maintains the ability to perform the RT function in the presence of any credible single failure of an input sensor, functional unit of the PS, or RT device. The RT function is performed in a four-fold redundant manner from sensor to actuation device.

Single failures upstream of the voting logic (sensor or APU failure) are accommodated by the voting logic. The two-out-of-four vote in each division becomes either two-out-of-three or one-out-of-three, depending on the nature of the failure automatically detected or not. In either case, the ability to perform RT when required is retained. Certain exceptional failures that can occur upstream of the voting logic are accommodated in other ways. For example, single failures of SPND or RCCA position measurements are accommodated by either signal selection (2nd MIN or 2nd MAX) or through automatic use of a more conservative trip setpoint.

Single failures at the voting logic level are accommodated by either redundancy within each division or redundancy across the four divisions. In case of a detected or an "undetected–spurious" failure of an ALU, the redundant ALU in the same division performs the RT function, and RT orders are still generated in each of the four divisions. In case of an "undetected–blocking" failure of an ALU, the affected division cannot issue RT orders, but any two of the remaining three divisions can actuate the RT function. Single failures of RT devices are accommodated by the two-out-of-four arrangement of the devices. A spurious opening of an RT device does not result in either spurious trip or loss of ability to trip. A failure of a single RT device to open is accommodated by the opening of any two of the other three redundant devices. A system level failure modes and effects analysis (FMEA) is performed to verify compliance with the single failure criterion.

The architecture of the PS is used as the basis for the analysis. The FMEA considers each major part of the system, how it might fail, and the effect of the failure on the system.

Because the PS is an integrated RT and 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 results of the FMEA are described in Appendix A.

14.0 RESPONSE TIME METHODOLOGY

A response time methodology is performed to determine the response time of the DCS portions of a protective function. The DCS architecture is used as the basis for the analysis. The response time methodology considers the different signal paths from the output of the sensor or black box signal conditioning components to the input of the actuator, and assumes conservative response times. The response time methodology is described in Appendix B.

15.0 SUMMARY/CONCLUSIONS

The U.S. EPR PS is an RPS and ESFAS implemented using the TXS technology. The TXS platform is a qualified, generic I&C platform that has been found acceptable for use in safety-related applications by the NRC.

The application-specific implementation of the TXS platform in the U.S. EPR design consists of a robust, four-fold redundant structure with two independent subsystems in each division. The PS and SICS provide manual RT and ESF actuation capability at the system level.

Where data communication exists between divisions of the PS (interchannel communication), the communication and isolation techniques used are consistent with regulatory and industry guidance. Independence is maintained between redundant portions of the system.

Where data communication exists between the PS and non-safety-related I&C systems, the communication and isolation techniques used are consistent with regulatory and industry guidance. A failure in another I&C system does not prevent the PS from performing its safety-related functions.

Extensive self-surveillance, fault detection, and fault accommodation measures are inherent in the TXS platform design. When coupled with engineered, application specific monitoring configurations, the PS detects, identifies, and mitigates failures with a high degree of confidence.

In addition to the redundant PS system architecture, two independent subsystems allow the use of signal diversity that further increases overall system reliability. A high-quality software design process contributes to system reliability by precluding failures due to software design errors.

16.0 REFERENCES

U.S. Regulations

1. 10 CFR Part 50 Appendix A, "General Design Criteria for Nuclear Power Plants."

2. 10 CFR Part 50.55a, "Codes and Standards."

U.S. Regulatory Guidance

3. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

4. Regulatory Guide 1.153, "Criteria for Safety Systems," Revision 1, June 1996.

5. Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," Revision 2, January 2006.

6. NUREG-0800, Section 7A, Branch Technical Position 7-14, "Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems," Revision 5, March 2007.

7. Regulatory Guide 1.75, "Physical Independence of Electrical Systems," Revision 3, February 2005.

8. Regulatory Guide 1.22, "Periodic Testing of PS Actuation Functions," Revision 0, February 1972.

9. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995.

10. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 0, May 1973.

11. NUREG-0800, Section 7A, Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions," Revision 5, March 2007.

12. Regulatory Guide 1.62, "Manual Initiation of Protective Actions," Revision 0, October 1973.

13. NUREG-0800, Section 7.9, "Data Communication Systems," Revision 5, March 2007.

U.S. Industry Standards

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

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

16. IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

17. IEEE Standard 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."

18. EPRI-TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," Revision 2, 2000.

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

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

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

22. Deleted.

Regulatory Review Precedent

23. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, "Acceptance for Referencing of Licensing Topical Report," EMF-2110 (NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System" (TAC NO. MA1983)," and associated Safety Evaluation Report.

AREVA NP Documents

24. EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," May 2000 Enclosure to letter, James F. Mallay (Siemens Power Corporation) to Document Control Desk (NRC), "Publication of EMF-2110(NP)(A) Revision 1, TELEPERM XS: A Digital Reactor Protection System," NRC:00:033, Siemens Power Corporation, July 12, 2000).

25. Deleted.

26. Deleted.

27. Deleted.

28. Deleted.

29. Deleted.

30. ANP-10304, Revision 5, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP, May 2012.

APPENDIX A
PROTECTION SYSTEM FAILURE MODES AND EFFECTS ANALYSIS

A.1 Purpose

A failure modes and effects analysis (FMEA) is a systematic procedure used to analyze the protection system (PS) in order to identify potential failures and their consequences. The purposes of an FMEA according to IEEE Std 352-1987 (Reference 1) are as follows:

- To assist in selecting design alternatives with high reliability and high safety potential during early design phases
- To verify that each conceivable failure mode and their effects on the operational success of the system has been considered
- To list potential failures and identify the magnitude of their effects
- To develop early criteria for test planning and the design of test and check out systems
- To provide a basis for quantitative reliability and availability analysis
- To provide historical documentation for future references to aid in the analysis of field failure and consideration of design changes
- To provide input data for tradeoff studies
- To provide a basis for establishing corrective action priorities
- To assist in objective evaluation of design requirements related to redundancy, failure detection systems, fail-safe characteristics, and automatic and manual override

A.1.1 Scope and Methods

Scope

A system-level FMEA is performed on the PS to identify potential single point failures and their consequences. The architecture of the PS, as shown in U.S EPR FSAR Tier 2, Figure 7.1-6, as well as the functional requirements for the system, defined in U.S.

EPR FSAR Tier 2, Section 7.2 and Section 7.3, are used as the bases for the analysis. This FMEA follows the guidance of the U.S. EPR general engineering guideline for failure modes and effects analysis. After detailed hardware layout and application specific software documentation are produced, the performance of a detailed FMEA is required to confirm the results of the system-level FMEA.

Per Reference 1, the essential function of an FMEA is to consider each major part of the system, how it may fail (the mode of the failure) and what the effect of the failure on the system would be (the failure effect). 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 Section 5.0. The PS consists of four identical divisions, so the definition of functional units is the same for each division. In general, a single failure of the same unit in any of the four PS divisions has the same effect on every function processed by that unit, regardless of which division has the failed unit. Therefore, the failure of each functional unit in one division is analyzed and considered representative of the effects of the same failure in any other division. Any exceptions are identified.

The FMEA contained herein is prepared in support of the U.S. EPR Design Certification Document submittal. It consists of an FMEA of the parts of the system that participate in the generation of automatic reactor trip (RT), engineered safety features actuation system (ESFAS), and permissive signals. The functional units that are analyzed are the following:

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

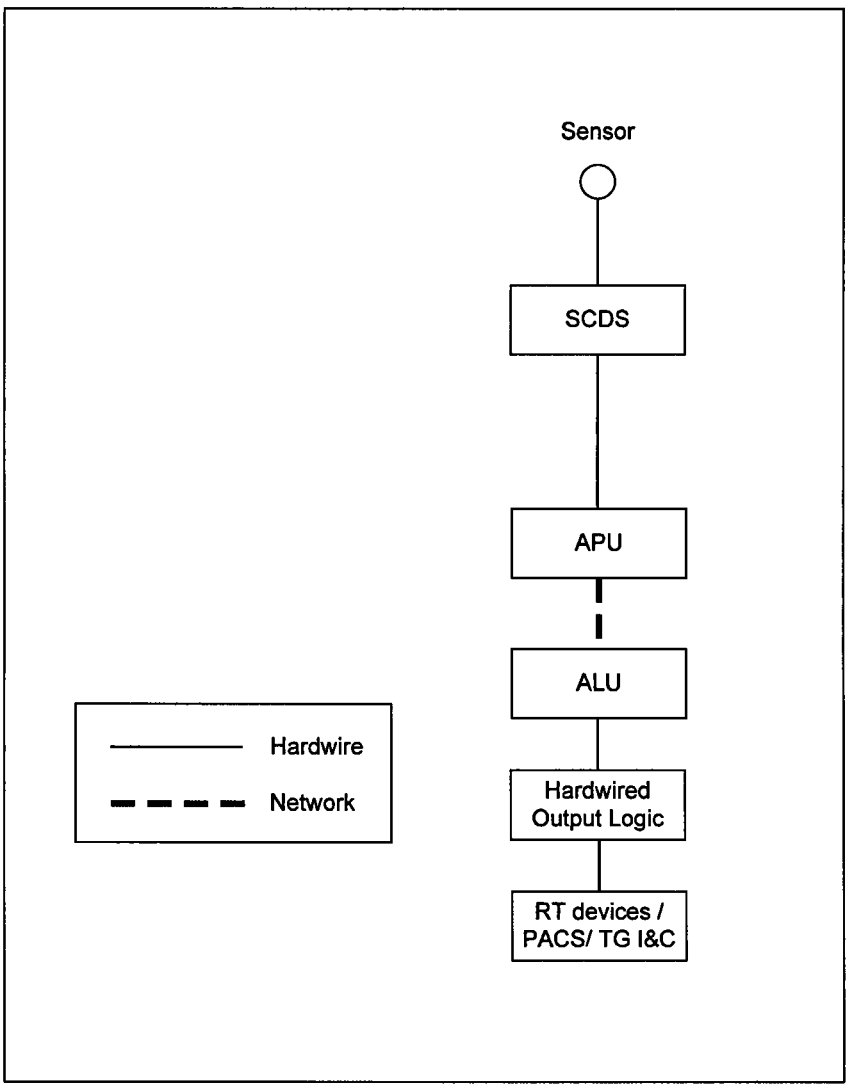
In addition to the equipment defined as functional units of the system, certain other equipment also contributes to the automatic RT, ESFAS, and permissive functions and is analyzed as part of the system-level FMEA:

- Sensor input measurements from the SCDS
- Hardwired output logic

- Reactor trip devices
- Priority and actuator control (PAC) modules

A simplified interface diagram for the aforementioned components is shown in Figure A.1.

Figure A.1—PS Component Interface



Consideration of Maintenance

GDC 21 (Reference 2) requires, in part, that "removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated." For this reason, the FMEA of the PS is performed considering inoperable (see U.S. EPR FSAR Tier 2, Table 7.1-6, for functional processor operational states) components due to preventative or corrective maintenance. The

bounding approach would be to consider an entire PS division inoperable for maintenance; however, due to mechanical system redundancy limitations, the single failure criterion cannot always be satisfied with an entire PS division inoperable. Therefore, plant Technical Specifications (U.S. EPR FSAR Tier 2, Chapter 16) are used to identify components that do not need to be considered in a maintenance condition while assuming a single failure elsewhere within the system. If the Technical Specifications prevent a component from being in maintenance for more than an allowable outage interval, then that component is considered operable when performing the single failure analysis. This results in the following configuration used as the worst-case maintenance condition to be assumed when performing the single failure analysis.

Components in one division are inoperable, with the exception of the following:

- SPND – A total of 67 SPND are operable in any combination. For simplicity, it is considered that 13 SPND are operable in one division, and 18 are operable in each of the other three divisions. This condition is controlled by LCO 3.3.1, Table 3.3.1-1, Sensors.
- ALU – Three ALUs are operable in each component. Therefore one ALU in one subsystem is considered inoperable. This condition is controlled by LCO 3.3.1, Table 3.3.1-1, Signal Processors.
- System level manual actuation mechanisms for the following functions are operable:
  - Reactor Trip (LCO 3.3.1, Table 3.3.1-1, Manual Actuation Switches)
  - SIS Actuation (LCO 3.3.1, Table 3.3.1-1, Manual Actuation Switches)
  - SG Isolation (LCO 3.3.1, Table 3.3.1-1, Manual Actuation Switches)
- Hardwired logic and PAC modules for the following actuators are operable:
  - CVCS Charging Isolation Valve (LCO 3.4.9)
  - CVCS Auxiliary Spray Isolation Valve (LCO 3.4.9)
  - CVCS Charging Containment Isolation Valve (LCO 3.6.3)

- Volume Control Tank Isolation Valve 1 (LCO 3.1.8)
- Volume Control Tank Isolation Valve 2 (LCO 3.1.8)
- Letdown Line Isolation Valve (LCO 3.1.8)
- Pressurizer Safety Relief Valves (LCO 3.4.10)
- RCP trip breakers (LCO 3.3.1, Table 3.3.1-1, Sensors)
- All Containment Isolation Valves (LCO 3.6.3)
- Emergency Feedwater Trains (LCO 3.7.5)
- Annulus Ventilation Accident Filtration Trains (LCO 3.6.7)

Each APU within a division is considered inoperable for maintenance, therefore, a global effect is modification of the downstream voting logic in the ALUs. This effect is taken into account and noted in Table A.3-1 through Table A.3-14. An exception is made for the EDG actuation function because LCO 3.3.1 requires the four divisions to be operable. For the EDG actuation function only one APU is considered in maintenance per division.

Methods

In order to bound the possible failures, both detected and undetected failures of sensors and 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: undetected-spurious and undetected-blocking. A failure denoted "undetected–spurious" is a failure not automatically detected, which results in a spurious partial trigger or actuation. A failure denoted "undetected–blocking" is 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. Specific communication failures are analyzed in Table A.1-1. Table A.1-1 applies to all TXS systems.

Table A.1-1—Communication Failures

Postulated Communication Failure	TXS Network Mitigation Techniques
Messages may be corrupted due to errors in communication modules, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.	• Messages are checked for correct addressing, length, and content (CRC check). • If corruption results in invalid addressing, all functional units on the network ignore the message. • If corruption results in invalid message length, all functional units on the network ignore the message. • If corruption results in incorrect content, all individual signals in the message are flagged with a faulty status before being used in processing
Messages may be repeated at an incorrect point in time.	• Each time a message is sent from the same function processor, a value is incremented and attached to the message; the receiving function processor uses this information to determine message age. • In a TXS system there is no correct time to repeat a message; messages are not repeated for any reason. New messages with an incremented message age are generated every cycle. • If a message was spuriously repeated, all functional units on the network recognize from the message age that the message is old; and it is ignored.

Postulated Communication Failure	TXS Network Mitigation Techniques
Messages may be sent in the incorrect sequence.	• New messages with incremented message age are generated every cycle. If the message received has a message age out of sequence, it is ignored. • Information within a message that is not in the correct place or sequence is detected by the receiving functional unit (CRC check), and the message is ignored.
Messages may be lost, resulting in both failures receiving an uncorrupted message or acknowledging receipt of a message.	• Messages are checked for age when they are received. • One message is allowed to be missed; if the message age indicates that two or more messages have been missed, a fault is indicated. • TXS communication techniques do not rely on the receiving function processor to acknowledge receipt of messages.
Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or buffered messages.	• Messages are checked for age when they are received; old messages are ignored. • There is no "permitted arrival time window" associated with the TXS communication techniques. • In a TXS system this type of fault would be treated the same as a lost message.
Messages may be inserted into the communication medium from unexpected or unknown sources.	• Messages contain information about the sender and receiver location. • These locations are pre-defined at code generation. • Messages from unexpected or unknown sources are ignored.

Postulated Communication Failure	TXS Network Mitigation Techniques
Messages may be sent to the wrong destination, which could be treated as a valid message.	• Messages contain information about the sender and receiver location. • These locations are pre-defined at code generation. • Only messages addressed to the receiver are used; all other messages are ignored.
Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.	• Messages are a pre-determined, fixed length. • Messages contain information indicating the message length. • Messages of incorrect length are ignored.
Messages may contain data outside of the expected range.	• The individual data within a message are validated by CRC check. • Analog data contained within a message receive a "not-a-number" check.
Messages may appear valid, but data may be placed in incorrect locations within the message.	• Messages use standard frames; messages that do not conform are ignored. • The receiving function processor detects this type of individual bit error by CRC check.
Messages may occur at a high rate that degrade or cause the system to fail (i.e., broadcast storm).	• Each function processor on a network operates with a deterministic cycle. • Each possible message is generated and sent every cycle to verify a constant bus load. • The function processor accesses received messages from the dual port RAM of its communication module independently of the communication module access to the network. • Postulated communication events that overload a network do not affect other separate networks.

Postulated Communication Failure	TXS Network Mitigation Techniques
Message headers or addresses may be corrupted.	• Message headers are checked for validity when received. • Addresses are pre-defined at code generation; messages with invalid addresses are ignored.

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, each function of the system is considered affected, as every function is processed by at least one APU and two ALUs in a division. Considering the effect on every function of the system bounds all cases of specific APU and ALU single failures.

Certain ESF actuation functions are performed uniquely within the PS architecture. For these cases, exceptions to the typical FMEA results are annotated within the FMEA Table in Section A.3.

When referring to the nature of a single failure, the terms "detected" and "undetected" as used in the context of the PS FMEA do not correspond with the definition of a detectable failure in IEEE Std 603-1998. 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. As defined by IEEE Std 603-1998, the PS has only detectable failures and no identifiable, but non-detectable failures.

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.

Assumptions

The following assumptions are considered in the PS system-level FMEA. The validity of these assumptions shall be verified in the course of performing a detailed FMEA

following equipment selection, equipment layout, functional allocation, and application software development:

- Network failures defined as undetected-spurious, and undetected-blocking are bounded by the similar failure of the sending functional unit. Therefore, only detected network failures need to be analyzed.
- No single failure in the electrical supply systems upstream of the PS cabinets can result in loss of power to an entire cabinet. This assumption is reasonable considering the electrical supply requirements defined for the PS in Section 4.2.2 and U.S. EPR FSAR Tier 2, Chapter 7.
- Distribution of power within a single PS cabinet prevents single failure in the electrical distribution from causing loss of function of more than one ALU functional unit.
- No single failure in the electrical supply systems upstream of the PACS cabinets can result in loss of power to an entire cabinet.
- Distribution of power within a single PACS cabinet prevents single failure in the electrical distribution from causing loss of function of more than one of a group of PAC modules that are redundant to each other.
- Failure of a functional unit where all outputs are "1" is not a postulated single failure mode. This type of failure results from an output module failing with all outputs "1." This assumption is especially relevant to the RCP trip function. The two RCP trip outputs from any given ALU (to two different RCP) shall be through different output modules. This precludes a single failure from resulting in multiple spurious RCP trips.
- Plant actuators which, if spuriously actuated, can challenge plant safety require actuation signals from more than one division of the PS to actuate (e.g., more than one pilot operator actuated from different divisions are required to change the state of the main valve).

- The EDG actuation function is performed in both subsystems within each division of the PS. Each division of the PS actuates only the EDG associated with the same electrical division. There is no sharing of information between the divisions for the EDG actuation function.
- A single SPND can not fail due to effects of an AOO or PA. Because of their close locations within the core, if conditions exceeded the qualification parameters of the SPND, many detectors would fail.
- For those components that the U.S. EPR™ Technical Specifications (U.S. EPR FSAR Tier 2, Chapter 16) limits the time for component inoperability to less than 72 hours for ECCS, the FMEA analyzes for a single failure without taking an additional component or division out for maintenance. This assumption is based on the reliability of the available components, given the limited time of inoperability by the U.S. EPR™ Technical Specifications.
- PS cannot automatically detect a failure of a system level manual actuation mechanism. Therefore, only undetected-spurious and undetected-blocking failures shall be considered for system-level manual actuation mechanisms.
- Failures of manual inputs to permissive functions are not considered for each individual function. All manual inputs to these functions are dispositioned as follows:
  - Spurious input from SICS - The manual input is only allowed to influence the permissive status when the plant conditions are appropriate, as determined by PS voting logic, independent of the SICS signal.
  - Blocking input from SICS – Accommodated by redundant divisions. The permissive in the affected division may be in the incorrect state. This is bounded by the results of ALU failure for each permissive function.
- The Turbine Trip and MFW Isolation – Full load functions are initiated from an RT initiation signal. The FMEA for the Turbine Trip and MFW Isolation – Full Load on a RT initiation will be covered by the FMEA for the RT functions.

- The P18 permissive is validated from an RT initiation signal. The FMEA for the P18 permissive validation on an RT initiation will be covered by the FMEA for the RT functions.

- The P6 permissive and P13 permissive are unique in that the inhibited state of the permissive enables the associated protective functions. It is, therefore, desirable to have the permissive fail into the inhibited state. Therefore, the voting logic used in the P6 and P13 permissives is modified toward inhibition (state is "0") of the permissive in case of invalid input signals as follows:

Table A.1-2—Voting Logic for P6 and P13 Permissives

		Initial Voting Logic
		3/4
# of invalid inputs	1	2/3
	2	2/2
	3	Output = "0"
	4	Output = "0"

The voting logic for all permissives, other than P6 permissive and P13 permissive, is modified toward validation (state is "1") in case of invalid input signals as follows:

Table A.1-3—Voting Logic for other Permissives

		Initial Voting Logic		
		2/3	2/4	3/4
# of invalid inputs	1	1/2	2/3	2/3
	2	Output = "1"	1/2	1/2
	3	Output = "1"	Output = "1"	Output = "1"
	4		Output = "1"	Output = "1"

- AND logic and OR logic use passive status processing. That is, if one input is invalid, the output is invalid regardless of the status of the remaining inputs.

- There are two general cases where multiple sensors are used as inputs to a calculation:
  - The multiple inputs are redundant measurements of the same process parameter.
    - In this case, if any one input has an invalid status, that input is disregarded and the calculation is performed using the remaining inputs.
  - The multiple inputs are not redundant to one another and measure different process parameters.
    - In this case, if any one input has an invalid status, the output of the calculation is invalid.

A.2 System Description

Section A.2 provides basic information pertinent to understanding the results of the FMEA. The automatic RT and ESFAS functions performed by the system are described in U.S. EPR FSAR Tier 2, Section 7.2 and Section 7.3.

A.2.1 Protection System Architecture

The architecture of the U.S. EPR™ Protection System can be found in U.S. EPR FSAR Tier 2, Figure 7.1-6. The four partitions on the figure represent the four physically separated, redundant PS divisions. The equipment assigned to each PS division is located in the corresponding Safeguard Building. Each PS division is further divided into subsystems A and B. The following sections identify features of the PS design that prevents a single failure from impairing the ability of the system to perform its safety functions.

Physical Separation

The four redundant divisions of the PS are physically separated within their respective Safeguard Buildings. In addition to the spatial separation features, Safeguard Building 2 and 3 are designed to protect against external hazards. The four divisionally separated rooms containing the PS equipment are in different fire zones. Therefore, the consequences of internal hazards (e.g., fire) would impact only one PS division.

Power Supply Independence

Each PS division is supplied by the independent Class 1E emergency uninterruptible power supply (EUPS). The EUPS are backed by the emergency diesel generators to cope with loss of offsite power. Inside a division, the PS cabinets are supplied by two redundant, uninterruptible 24 VDC feeds. To cope with loss of onsite and offsite power, the uninterruptible feeds to the PS cabinets are supplied with two-hour batteries.

Loss of Power

In case of loss of offsite power, each PS division is supplied with its own battery until the emergency diesel generators are started and connected to the EUPS. A single failure of a divisional battery could result in loss of power to a PS division. In that case, all function processors in the division shutdown (no data communication is sent from the division) and all outputs go to a "0" state. This results in opening that divisions RT devices (the tripped state), and no actuation of ESFAS components controlled by that division. The other 3 PS divisions remain capable of performing their protective functions. Upon restoration of power to a PS division, all function processors go through a reset and start-up self-test mode, during which the outputs remain in a "0" state. Upon successful completion of the start-up self-test, each function processor enters its normal cyclic operation mode. The RT outputs will transition from the "0" state (trip) to their normal "1" state (no-trip). This alone does not return the affected RT breaker to its normal state. Manual action is required locally (re-rack the breaker) to return to its closed position. Upon successful completion of the start-up self-test, when each function processor enters its normal cyclic operation mode, ESFAS outputs remain in their normal "0" state. If an AOO or PA is in progress during restoration of power, a change of state of the ESFAS outputs (to the actuate state) occur to respond to the event.

Redundancy

The PS architecture is generally four-fold redundant for both RT and ESFAS functions. A single failure during corrective or periodic maintenance (maintenance bypass), or a

single failure and the effects of an internal hazard do not prevent performance of the safety functions. Where there are exceptions because of limited redundancy of plant systems actuated by the PS, plant technical specifications are used to strictly limit the amount of time the related components can be out of service for maintenance. The plant technical specification controls preclude the need to consider a single failure concurrent with a maintenance condition for these cases.

For RT functions, each PS division actuates one redundancy of the RT devices based on redundant processing performed in four divisions. For ESFAS functions, the redundancy of the safety function as a whole is defined by the redundancy of the ESF system mechanical trains. In general, this results in one PS division actuating one mechanical train of an ESF system based on redundant processing performed in four divisions. The PS not only supports the redundancy of the mechanical trains, but also enhances this redundancy through techniques (e.g., redundant actuation voting).

Subsystems

Each PS division is divided into two functionally independent subsystems: A and B. Subsystem A in each division is redundant to subsystem A of the other divisions; the same is true of subsystem B. The primary purpose of this arrangement is to provide functional diversity for RT functions; however, in some cases redundancy within a division is achieved by implementing the same function in each subsystem

Environment

PS equipment is located in a mild environment. The mild environment is protected by safety-related building structures and safety-related HVAC systems. No single failure results in adverse environmental conditions for the PS equipment.

A.2.2 Protection System Processing Components

The following sections describe the main functionality of the APU and ALU.

Acquisition and Processing Units (APU)

The APU primary functions are:

- Acquire the signals from the process sensors through the signal conditioning and distribution system (SCDS) (see Figure A.1).
- Perform processing (e.g. calculations, setpoint comparisons) using the input signals.
- Distribute the results to the actuation logic units (ALU) for voting.
- Contain a function processor for each APU consisting of input and output modules, and communication modules.

Each PS division contains five APUs; three assigned to subsystem A, two assigned to subsystem B. Each APU communicates its results to the ALU within its subsystem in each division. Each APU of a division is redundant to the corresponding APU of the other divisions. For example, APU A1 in each division acquires one of four redundant input signals, and each APU A1 performs identical processing. The four redundant results undergo voting in all divisions by the ALU.

Actuation Logic Units (ALU)

The ALU primary functions are to perform voting of the processing results from the redundant APU in the different divisions and to issue actuation orders based on the voting results. The ALU also contains the logic used to latch and either manually or automatically un-latch actuation outputs. Each ALU consists of a function processor, input and output modules, and communication modules.

Each PS division contains four ALUs; two assigned to each subsystem. The two ALUs of the same subsystem within a division are redundant and perform the same processing using the same inputs. The outputs of two redundant ALUs are combined in a hardwired "functional AND" logic for RT outputs and in a hardwired "functional OR" logic for ESFAS outputs. This avoids both unavailability of ESFAS actuations and

spurious RT actuations. The actuation orders from the ALU are sent to the PACS for ESFAS actuations, or to the trip devices for RT actuations.

A.2.3 Diversity of Reactor Trip Mechanism

The PS uses two diverse, safety-related means of initiating a reactor trip: trip breakers and trip contactors. Automatic RT orders issued by the PS act on these two different safety-related components of the control rod drive power supply system, each independent and capable of actualizing the full RT.

The automatic orders to the trip devices from the PS are de-energize to actuate. This removes the power to the control rod grippers and allows the rods to drop and initiate the reactor trip.

Trip Breakers

Each PS division is assigned to one of four trip breakers; each divisional RT order acts on the under-voltage coil of the assigned breaker (de-energize to open). PS divisions 1 and 2 open trip breakers located in division 2. PS divisions 3 and 4 open trip breakers located in division 3. The trip breakers are arranged in a "1 out of 2 taken twice" configuration that withstands single failure and requires the following logical combination of PS divisional RT orders to actuate an RT: (1 or 2) and (3 or 4).

Trip Contactors

There are 23 sets of four trip contactors. Each set can remove power to four CRDM power supplies. Eleven sets of contactors are in division 1, and 12 sets are in division 4. Each PS division is assigned to one contactor in each of the 23 sets. Each set of four contactors is arranged in a 2 out of 4 configuration. Together the trip breakers and trip contactors withstand single and double failures. Additionally, the trip contactors are diverse from the trip breakers to add reliability to the reactor trip function as a whole.

A.3 Results

A.3.1 FMEA Results Definitions

The following are definitions for the items listed in Table A.3-1 through A.3-14:

1. Name of Sensor, Functional Unit, or Equipment – Each item in the PS is identified by name. The analysis was conducted at this level.

2. Associated RT – The associated reactor trip function(s) affected by the failure.

3. Associated ESFAS – The associated engineered safety features function(s) affected by the failure.

4. Failure Mode – Significant failure modes, including both random and degradation failures of the PS, are identified and evaluated.

   - Detected Failure – A failure that is automatically detected by the inherent and engineered monitoring mechanisms of the system. Detected failures of sensors or APUs result in the downstream voting logic being modified.

   - Undetected Failure – A failure that is not automatically detected by the system. Undetected failures are detectable through periodic testing. An undetected failure of a sensor or APU results in the downstream voting logic inherently becoming different.

5. Effect of a Division out for Maintenance (Tables A.3-2 through A.3-14 only) – The effects on the PS from a division taken out for maintenance, and all of the components within that division made inoperable.

6. Failure Cause – The failure cause is not identified in the system-level analysis. The failure modes are selected to bound the results of any specific failure cause. Specific failure causes can be identified only after specific equipment is selected and application software is developed.

7. Method of Detection – For the system-level FMEA, the method of detection (for detectable failures) is always inherent or engineered monitoring mechanisms. Specific methods of detection cannot be identified until specific equipment is selected and application software is developed.

8. Inherent Compensating Provision(s) – This entry lists the existing provisions within the system that compensates for the failure mode at the level being analyzed.

9. Effect on the Protection System – This entry lists the ultimate effect on the PS.

10. Comments – This entry lists any other effects, outcomes or general information related to the failure.

A.3.2 RT and ESF Functions Results

The results of the U.S. EPR™ PS FMEA for RT and ESFA functions are shown in Table A.3-1.

Table A.3-1—FMEA Results Table

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
1	Incore Detector (SPNDs)	RT-HLPD RT-Low DNBR	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed SPND marked invalid	For a detected failure of 1 to 5 SPNDs, the PS degrades the setpoint to compensate for the failure. On 6th invalid SPND, technical specifications dictate reduction in power to mode where SPND are not required. 7 or more invalid SPND result in automatic RT.	The undetected failure of the most limiting SPND signal is analyzed as a credible single failure in the Chapter 15 safety analyses (U.S. EPR FSAR Tier 2, Chapter 15).
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Specific consideration as a single failure in the safety analyses	No effects on the system level.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Safety analysis credits the undetected failure of an SPND.	No effects on the system level.	
2	Excore Detector (PRDs)	RT-High neutron Flux rate of change	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
3	Excore Detector (IRDs)	RT- High Neutron Flux RT- Low Doubling Time	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
4	PZR P (NR)	RT- High or Low PZR Pressure RT-Low DNBR	SI Actuation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
5	PZR L (NR)	RT- High PZR Level	CVCS Charging Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
6	CLEG T (NR)	RT - Low DNBR	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
7	CLEG T (WR)	RT - High Core Power Level RT - Low Saturation Margin	CVCS Isolation for Anti-dilution	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	CVCS Isolation for Anti-Dilution function only requires either Div. 1 or Div. 4 to achieve its function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
8	HLEG T (NR)	RT - High Core Power Level RT - Low Saturation Margin	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
9	HLEG T (WR)	None	SIS Actuation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
10	HLEG P (NR)	None	PSRV Opening	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
11	HLEG P (WR)	RT - High Core Power Level RT - Low Hot Leg Pressure RT - Low Saturation Margin	SIS Actuation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
12	HLEG Loop Level	None	SIS Actuation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
13	RCP Speed	RT - Low DNBR RT - Low RCP Speed	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	Note that this is credited for the complete loss of flow (4 RCPs stopped simultaneously). Loss of partial flow is credited to the Low-low RCS flow function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
14	RCS loop flow	RT - Low RCS Flow Rate RT - Low Low RCS Flow Rate RT - Low DNBR	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
15	ΔP Over RCP	None	RCP Trip	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Two redundant channels on each pump; Three pumps treated as three redundant channels	APU voting logic modified to 1/1 on affected pump; Downstream voting logic remains 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels on each pump; Three pumps treated as three redundant channels	APU voting logic becomes 1/1 on affected pump; Downstream voting logic remains 2/2	
16	SG L (NR)	RT - High or Low SG Level	SG Isolation, MFW Isolation – Full Load	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
17	SG Pressure	RT - Low or High SG Pressure RT - SG Pressure Drop	MSRIV Opening, MSRT Isolation, Main Steam Isolation, MFW Isolation-SSS, EFW Actuation, EFW Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2 for RTs and 2/2 for ESF functions.	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
18	Containment Service Compartment Pressure (NR)	RT - High Containment Pressure	Hydrogen Mixing Dampers Opening	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
19	Containment Service Compartment Pressure (WR)	None	Containment Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
20	Containment Equipment Compartment Pressure	RT - High Containment Pressure	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
21	Equipment Room/Containment Service Compartment Room dP	None	Hydrogen Mixing Dampers Opening	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/5	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/6 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/5	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/6 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/5	
22	Containment High Range Activity	None	Containment Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
23	SG L (WR)	None	EFW Actuation, EFW Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels; Redundant ALUs and PAC modules per division.	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting; Redundant ALUs and PAC modules per division.	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting; Redundant ALUs and PAC modules per division.	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
25	RCCA Analogy Position Indication	RT - Low DNBR	None	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; DNBR setpoint selection	Failed sensor marked invalid. Low DNBR setpoint value is adequate for single undetected rod insertion; Inadvertent bank insertion detected by other 2 divisions	Safety analysis (U.S. EPR FSAR Tier 2, Chapter 15) credits only one rod insertion or a bank insertion. The setpoint value is adequate for a single undetected rod drop. A bank drop shall be sensed by all divisions. Therefore if a single failure occurs with a division out for maintenance, then the remaining 2 divisions shall detect a bank drop.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Failure is toward the safe state	Rod drop (1/4) signal is generated; More conservative DNBR setpoint value is used	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	DNBR setpoint selection	Low DNBR setpoint value is adequate for single undetected rod insertion; Inadvertent bank insertion detected by other 2 divisions	
26	6.9kV Bus Voltage	None	EDG Actuation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Failed sensor marked invalid. Downstream 2/3 voting logic modified to 1/2	If a division was taken out for maintenance, then that corresponding EDG cannot be started. Each division of the EDG Actuation function does not communicate to other divisions. Therefore other divisions are not affected by a division out for maintenance or a single failure.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	APU issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	2/3 voting; Three redundant channels	Downstream voting logic becomes 2/2.	
27	Main Steam Line Activity	None	SG Isolation	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effects on the system level
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
28	Boron Concentration	None	CVCS Isolation for Anti-dilution	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	CVCS Isolation for Anti-Dilution function only requires either Div. 1 or Div. 4 to achieve its function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
29	Temp. Downstream Boron Measurement	None	CVCS Isolation for Anti-dilution	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	CVCS Isolation for Anti-Dilution function only requires either Div. 1 or Div. 4 to achieve its function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
30	CVCS Charging Flow	None	CVCS Isolation for Anti-dilution	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	CVCS Isolation for Anti-Dilution function only requires either Div. 1 or Div. 4 to achieve its function.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
31	MCR Intake Activity	None	MCR Air Conditioning System Isolation and Filtering	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	The MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake). This is a safe state for the system.	The MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake) if a radiation monitor fails or is put into maintenance.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/3 voting	Affected division issues spurious partial trigger; the MCR Air Intake System shall go into filtration mode (Reconfigure Air Intake). This is a safe state for the system.	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 1/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 1/2	
36	APU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting (For EDG actuation function: Redundant APU in same division)	All signals sent from affected APU marked invalid; Downstream voting logic modified (For EDG actuation, function is performed by redundant APU in same division)	Undetected - spurious failure of 1 APU can result in spurious EDG actuation Spurious failure of 1 APU and an APU out for maintenance (See Assumption Section) causes a spurious Turbine Trip. A spurious turbine trip is described in the safety analysis Section 15.2.2 (U.S. EPR FSAR Tier 2, Chapter 15).
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting (For EDG actuation, failure is in the safe direction)	Downstream voting logic becomes 1/2. (For EDG actuation, APU issues multiple spurious actuation signals.) (This condition causes a spurious Turbine Trip)	
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	2/3 voting (For EDG actuation function: Redundant APU in same division)	Downstream voting logic becomes 2/2. (For EDG actuation, function is performed by redundant APU in same division)	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
37	Network APU - ALU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting (For EDG actuation function: Redundant APU in same division)	All signals sent from affected APU marked invalid; Downstream voting logic modified (For EDG actuation, function is performed by redundant APU in same division)	Undetected - spurious failure of 1 APU can result in spurious EDG actuation. An inoperable APU results in a MCR Isolation and Filtering trigger. Spurious failure of 1 APU and an APU out for maintenance (See Assumption Section) causes a spurious Turbine Trip. A spurious turbine trip is described in the safety analysis Section 15.2.2 (U.S. EPR FSAR Tier 2, Chapter 16).
38	ALU	All	All	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Redundant ALU in each subsystem. (For EDG actuation, redundant subsystem in same division)	ALU fails into state requesting RT, no ESF actuation; RT order generated in one division, RT devices voting logic becomes 1/3. One division unable to perform an ESF actuation. (For EDG actuation, redundant subsystem performs the function)	Undetected - spurious failure of 1 ALU can result in spurious ESF actuation (with the exception of EDG actuation). ESF Plant actuators which, if spuriously actuated can challenge plant safety require actuation orders from more than one division. For RCP trip function, failure of a functional unit such that all outputs are "1" is not postulated. This would be the failure of an output module. Therefore, the two RCP trip outputs from the same ALU (to two different RCP) must be through different output modules to prevent multiple spurious RCP trip.
				b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem; ESF spurious actuations in the safe direction	ALU fails into state requesting RT or EDG actuation, RT order generated in one division, RT devices voting logic becomes 1/3. For EDG actuation, redundant subsystem performs the EDG actuation. For ESF actuations, spurious actuation order is generated	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions for RT; Redundant ALU for ESF actuations; Redundant sub-system for EDG actuation	One division unable to issue RT order, function performed by other 3 divisions; For ESF actuation, redundant ALU in same subsystem performs the function; For EDG actuation, affected subsystem unable to issue actuation, redundant subsystem in same division performs the function.	If both ALUs in a division are inoperable (one ALU in maintenance and one single failure) then the EFW Actuation and Isolation functions cannot be triggered in one division. For the event that an EFW actuation has occurred and both ALUs are inoperable for one division (one single failure and one for maintenance) the Safety Automation System (SAS) shall control the level for the EFW function. For the SG tube rupture event with both ALUs inoperable for one division (one single failure and one for maintenance), the SG Isolation function is still fulfilled by the containment isolation check valve on the EFW line.

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
39	Hardwired Output Logic	All	All	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Three redundant divisions for RT; For ESF (including EDG actuation) failure is toward the safe state	Spurious RT order generated in one division. RT devices voting logic becomes 1/2; Spurious actuation of a single ESF actuator.	ESF plant actuators which, if spuriously actuated can challenge plant safety require actuation orders from more than one division.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant divisions for RT; Redundant divisions for ESF; Redundant hardwired logic within division for EFW isolation and EDG actuation.	One division unable to issue RT order, function performed by other 2 divisions; For ESF actuation, redundant divisions remain operable; For EDG actuation, affected subsystem unable to issue actuation, redundant subsystem in same division performs the function. For EFW isolation, redundant hardwired logic in same division performs the function	
40	Reactor Trip Device	All	None	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Three redundant divisions of RT devices; 2/3 actuation.	Spurious RT order generated in one division. RT devices voting logic becomes 1/2	No effects on the system level.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant divisions of RT devices; 2/3 actuation.	One RT device fails to open; Remainder of RT devices function in 2/2 configuration.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
41	PAC Module	None	All	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Failure is toward the safe state.	Spurious actuation signal given to the attached actuator.	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 state of the main valve). *For the RCP Trip function if a spurious PAC Module failure occurs, one RCP shall trip. This event is described in the safety analysis Section 15.3.1 (U.S. EPR FSAR Tier 2, Chapter 15).

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Redundant divisions of ESF actuation; For EFW isolation and EDG actuation redundant PAC module in same division;	Failure to actuate attached actuator, redundant divisions remain operable; Redundant PAC module in same division performs EDG actuation or EFW isolation function.	Safety Analysis Section 15.1.5 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for a main steam line break upstream of the MSIV, but outside of the Reactor Building. This analysis can also be used to credit a spurious MSRT Opening. *For the MSIV Isolation function, if one pilot valve is in maintenance (open pilot valve) then a spurious failure of the second pilot valve (via PAC Module) in the series could cause a spurious MSIV closure. Safety analysis Section 15.2.4.1 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the inadvertent Main Steam Isolation Valve closure. For the Turbine Trip function a spurious turbine trip is described in the safety analysis Section 15.2.2 (U.S. EPR FSAR Tier 2, Chapter 15).
42	System Level Manual Actuation Mechanism	All		b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/4 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/3	No effects on the system level.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant channels and 2/4 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/3	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
			SIS	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/4 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/3	No effects on the system level.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/4 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/3	
			EFW Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting; Redundant ALUs and PAC modules per division.	Spurious actuation occurs in the affected division	Safety Analysis Table 15.0-11 (U.S. EPR FSAR Tier 2, Chapter 15) assumes the single failure of an EFW train during accidents requiring EFW actuation. The EFW system is inactive during normal operation.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/1 voting; Redundant ALUs and PAC modules per division.	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			EFW Actuation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting; Redundant ALUs and PAC modules per division.	Spurious actuation occurs in the affected division	Safety Analysis Section 15.1.2 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the increase in feedwater flow. This analysis can be used to credit a spurious EFW actuation.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/1 voting; Redundant ALUs and PAC modules per division.	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			Partial Cooldown	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	No effects on the system level.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
			MSRIV Opening	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	Safety Analysis Section 15.1.4 (U.S. EPR FSAR Tier 2, Sections 15.1.5 and 15.5.3) describes the analysis for the inadvertent opening of the MSRT.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			MSRT Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	For normal operation the MSRT is normally closed. For overpressure events in Safety Analysis U.S. EPR FSAR Tier 2, Sections 15.2.2, 15.2.4, 15.2.6, 15.5.1, and 15.5.2, Safety Analysis Table 15.0-11 (U.S. EPR FSAR Tier 2, Chapter 15) assumes the loss of one train of the MSRT.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			Main Steam Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	No effect on the system level
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
			MFW Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	Safety Analysis Section 15.2.7 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the inadvertent isolation of the MFW.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			Containment Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	No effect on the system level
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
			CVCS Charging Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	A spurious CVCS Isolation would provide letdown, but no charging. This is can be considered a SBLOCA (low end of the break spectrum). Safety Analysis Section 15.6.1 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the inadvertent opening of a PSRV. This analysis can be used to credit a spurious CVCS Isolation.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
			CVCS Isolation on Anti-dilution	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	A spurious CVCS Isolation would provide letdown, but no charging. This is can be considered an SBLOCA (low end of the break spectrum). Safety Analysis Section 15.6.1 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the inadvertent opening of a PSRV. This analysis can be used to credit a spurious CVCS Isolation.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			EDG Actuation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	A spurious EDG actuation would not challenge plant safety. The EDGs would not be connected to the plant bus, unless a LOOP has occurred.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			PSRV Opening	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/2 voting per PSRV	Spurious actuation occurs in the affected division; Downstream voting logic becomes 1/1 for the affected PSRV.	No effect on the system level
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	2/2 voting per PSRV	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	

No	Name of Sensor, Functional Unit, or Equipment	Associated RT	Associated ESFAS	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System	Comments
			SG Isolation	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/4 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/3	No effect on the system level
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant channels and 2/4 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/3	
			RCP Trip	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	Safety Analysis Section 15.3.1 and 15.3.2 (U.S. EPR FSAR Tier 2, Chapter 15) describes the analysis for the inadvertent RCP trip.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			MCR Air Conditioning System Isolation and Filtering	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	1/1 voting	Spurious actuation occurs in the affected division	A spurious actuation of the MRC Isolation and Filtering function will fail into the safe state.
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Two redundant channels and 1/1 voting	Affected division unable to issue an actuation. The automatic function shall perform the actuation when necessary.	
			HMD Opening	b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	No effect on the system level
				c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

A.3.3 Permissive Functions Results

The results of the U.S. EPR™ PS Permissive Functions FMEA are shown in Tables A.3-2 through A.3-14.

Permissive P8

The Permissive P8 function has failure modes that allow the permissive to be in the incorrect state during certain plant conditions.

These failure modes have been reviewed by safety analysis to verify that they force the affected protection functions in the conservative direction. The results of this assessment are as follows:

The worst case failure results in one half of the sensors not providing input into the permissive status. This does not result in the permissive having the incorrect state during operation with rods out. However, when rods are in the process of inserting, a situation may occur when the P8 validated signal is sent (indicating all shutdown RCCA are in), but some shutdown RCCA are not fully inserted.

Permissive P8 provides input to the selection of the setpoint for the CVCS isolation for anti-dilution isolation function. In this case it selects between power and shutdown conditions based on rod insertion. Based on the above FMEA result, it is possible to have a situation where not all rods are in but the appearance is given to enable the anti-dilution shutdown state. The anti-dilution shutdown state setpoint is further selected based on RCPs running or not running (see permissive P7). With the RCPs running (at power and shutdown) the anti-dilution setpoint is based on assuming the most reactive rod is stuck out of the core. At power, the setpoint is based on when shutdown margin is lost and the rods can no longer shutdown the reactor. In the shutdown mode, the setpoint is based on the approach to critical. If rods are in the process of being inserted then the reactor is actually in the shutdown state. As long as no more than one rod is out of the core the analysis remains valid and the failure mode results in an acceptable

condition. Furthermore, the shutdown anti-dilution setpoint is more conservative than the setpoint for at-power.

Table A.3-2—Permissive P2

Permissive P2 is representative of PRD neutron flux measurements higher than low-power setpoint value (10 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	Excore Detector (PRDs)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels.	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level

Permissive P2 is representative of PRD neutron flux measurements higher than low-power setpoint value (10 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-3—Permissive P3

Permissive P3 is representative of PRD neutron flux measurements higher than an intermediate power setpoint value (70 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	Excore Detector (PRDs)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level

Permissive P3 is representative of PRD neutron flux measurements higher than an intermediate power setpoint value (70 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-4—Permissive P5

Permissive P5 is representative of IRD neutron flux measurements above a low-power setpoint value (10-5 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	Excore Detector (IRDs)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level

Permissive P5 is representative of IRD neutron flux measurements above a low-power setpoint value (10-5 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-5—Permissive P6

Permissive P6 is representative of core thermal power above a low-power setpoint value (10 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	CLEG T (NR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	HLEG T (NR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
3	HLEG P (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

Permissive P6 is representative of core thermal power above a low-power setpoint value (10 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	RCS Loop Flow	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
5	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
6	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 2/2	No effect on the system level

Permissive P6 is representative of core thermal power above a low-power setpoint value (10 percent power)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
7	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-6—Permissive P7

Permissive P7 defines when reactor coolant pumps (RCPs) are no longer in operation

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	RCP Speed	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	RCP Breaker Position (Including Bus Breaker)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
3	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	

Permissive P7 defines when reactor coolant pumps (RCPs) are no longer in operation

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
5	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-7—Permissive P8

Permissive P8 defines the shutdown state with all rods in (ARI)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	RCCA Position of Shutdown RCCA (48 total)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	Failures result in one half of the sensors not providing input into the permissive status. This does not result in the permissive having the incorrect state during operation with rods out. However, when rods are in the process of inserting, a situation may occur when the P8 validated signal is sent, but some shutdown RCCA are not fully inserted.
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Remainder of signals into AND logic do not allow AND to be satisfied; Downstream voting logic remains 2/3	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	Failures result in one half of the sensors not providing input into the permissive status. This does not result in the permissive having the incorrect state during operation with rods out. However, when rods are in the process of inserting, a situation may occur when the P8 validated signal is sent, but some shutdown RCCA are not fully inserted.
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes 1/2	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	Failure results in one half of the sensors not providing input into the permissive status. This does not result in the permissive having the incorrect state during operation with rods out. However, when rods are in the process of inserting, a situation may occur when the P8 validated signal is sent, but some shutdown RCCA are not fully inserted.

Permissive P8 defines the shutdown state with all rods in (ARI)

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-8—Permissive P12

Permissive P12 defines the transition from hot shutdown to cold shutdown with respect to RCS pressure

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	PZR P (NR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-9—Permissive P13

Permissive P13 defines when steam generator draining and filling operations are allowed

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	HLEG T (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 2/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 2/2	No effect on the system level
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-10—Permissive P14

Permissive P14 defines when the residual heat removal system is allowed to be connected to the RCS

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	HLEG T (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	HLEG P (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
3	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
4	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to ½	No effect on the system level

Permissive P14 defines when the residual heat removal system is allowed to be connected to the RCS

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
5	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-11—Permissive P15

Permissive P15 defines when SI actuation due to ΔPsat is disabled and SI actuation due to low loop level is enabled

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	RCP Speed	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	RCP Breaker Position (Including Bus Breaker)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
3	HLEG T (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	

Permissive P15 defines when SI actuation due to ΔPsat is disabled and SI actuation due to low loop level is enabled

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	HLEG P (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
5	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
6	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
7	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-12—Permissive P16

Permissive P16 defines when the SIS may be aligned from cold leg injection to hot leg injection

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	HLEG P (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to ½	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes ½	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-13—Permissive P17

Permissive P17 corresponds to the temperature conditions where brittle fracture protection is required

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	CLEG T (NR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes 1/2	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

Table A.3-14—Permissive P18

Permissive P18 prevents unsafe positioning of the SG transfer valves

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
1	HLEG T (WR)	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Three redundant channels (excluding channel out for maintenance)	Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected – Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger; Downstream voting logic becomes 1/2	
			c) Undetected – Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger; Downstream voting logic becomes 2/2	
2	APU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	2/3 voting	Affected division issues spurious partial trigger. Downstream voting logic becomes 1/2	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Three redundant channels and 2/3 voting	Affected division unable to issue partial trigger. Downstream voting logic becomes 2/2	
3	Network APU-ALU	Loss of components for affected division; Voting logic in other divisions modified to 2/3	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Three redundant channels and 2/3 voting	All signals received from affected APU marked invalid; Downstream voting logic modified to 1/2	No effect on the system level

Permissive P18 prevents unsafe positioning of the SG transfer valves

No.	Name of Sensor, Functional Unit, or Equipment	The Effect of One Division Out for Maintenance	Failure Mode	Failure Cause	Method of Detection	Inherent Compensating Provision	Effect on the Protection System with One Division Out for Maintenance	Comments
4	ALU	One ALU per division is considered inoperable. This condition is controlled by LCO 3.3.1 (Table 3.3.1-1, Component C.2.)	a) Detected Failure	See Definition 6, Section A.3.1	TXS inherent or engineered fault detection mechanism	Four redundant divisions	ALU fails into state requesting RT, No ESF actuation; Status of permissive in failed ALU is irrelevant. Permissive is correctly calculated based on 4 divisions of input information in redundant ALU	Incorrect permissive status can result in either spurious actuation, or failure to actuate of the functions affected by the permissive. These results are bounded by the FMEA for the PS RT and ESF functions, which considers both spurious actuation and fail to actuate of all functions performed by a single ALU.
			b) Undetected - Spurious	See Definition 6, Section A.3.1	None	Redundant ALU in each subsystem	Permissive has incorrect validated status in affected ALU	
			c) Undetected - Blocking	See Definition 6, Section A.3.1	None	Four redundant divisions	Permissive has incorrect inhibited status in affected ALU	

A.4 Appendix A References

1. IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems."

2. 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."

APPENDIX B
PROTECTION SYSTEM RESPONSE TIME

B.1 Basis

Branch Technical Position 7-21 (Reference 1) provides guidance for the NRC staff review of digital computer real-time performance. The following passages are stated as review acceptance criteria in BTP 7-21:

> "Limiting response times should be shown to be consistent with safety requirements (e.g., suppress power oscillations, prevent fuel design limits from being exceeded, prevent a non-coolable core geometry). Setpoint analyses and limiting response times should also be shown to be consistent."
>
> "Digital computer timing should be shown to be consistent with the limiting response times and characteristics of the computer hardware, software, and data communications systems."
>
> "The level of detail in the architectural description should be sufficient that the staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available."
>
> "The means proposed, or used, for verifying a system's timing should be consistent with the design."
>
> "Testing and/or analytic justification should show that the system meets limiting response times for a reasonable, randomly selected subset of system loads, conditions, and design basis events."

It is therefore necessary to establish limiting time response calculation methods for typical PS functions to validate:

- Time response assumptions used as inputs to the plant safety analysis.
- Consistency of setpoint calculations with the PS design.
- The sufficiency of the PS architecture with respect to time response.

B.2 Scope

The total response time for a given function consists of several sub-intervals that span from a process variable exceeding a pre-defined limit to completion of the function (e.g., complete valve closure or required flow rate established). The scope of this document is limited to only the DCS portion of the total response time of any given protective function and excludes time intervals such as sensor response times and valve closure times.

This document applies only to the automatic protective functions identified in U.S. EPR FSAR Tier 2, Chapter 7.

B.3 Contents

The remainder of this document is organized as follows:

Section B.4 defines the basic principles relevant to response time calculations. These basic principles are based on the generic TXS platform properties that are architecture independent.

Section B.5 describes how the basic principles of Section B.4 are applied to verify that the response times calculated are the limiting (maximum) response times for the system.

Section B.6 defines the assumed cycle times used in the calculations. Both function processor cycle times and communication cycle times are considered. The principles defined in Sections B.4 and B.5 are then applied to the specific architecture of the PS

and systems interfacing with the PS to obtain limiting response times for the typical function types.

B.4 Basic Response Time Principles

B.4.1 Definition of Response Time T2

The total response time for a given function consists of several sub-intervals that span from a process variable exceeding a pre-defined limit to completion of the protective function. The sub-interval addressed in this document is known as T2. T2 accounts for the DCS portion of the protection channel, and is defined as the time from sensor or black box signal conditioning output to RT breaker input terminals for RT functions, or to output of the PACS for ESF actuation functions.

B.4.2 TELEPERM XS Timing Concepts

The PS is composed of TXS function processors which run asynchronously to each other and exchange signals using network links. Therefore, when calculating response time, function processor cycle times and communication times for data exchange must both be taken into account.

Each TXS function processor uses a cyclic execution model. Each processing task is performed at a pre-defined time during each processing cycle. For the purpose of response time calculations, three processing tasks are of interest:

1. Function Diagram Groups: The function diagrams executed by a TXS function processor can be organized into one or two function diagram groups (FDG). Each FDG is assigned a cycle time: T_{fg1} for the first FDG and T_{fg2} for the second FDG. The results of the first FDG will be available every T_{fg1} milliseconds, and the results of the second FDG will be available every T_{fg2} milliseconds. The longer of the two FDG cycle times must be evenly divisible by the shorter cycle time to verify that the end of a cycle of the longer FDG coincides with the end of a cycle of the shorter FDG. This is necessary to facilitate signal exchange between the two FDGs within the same function processor.

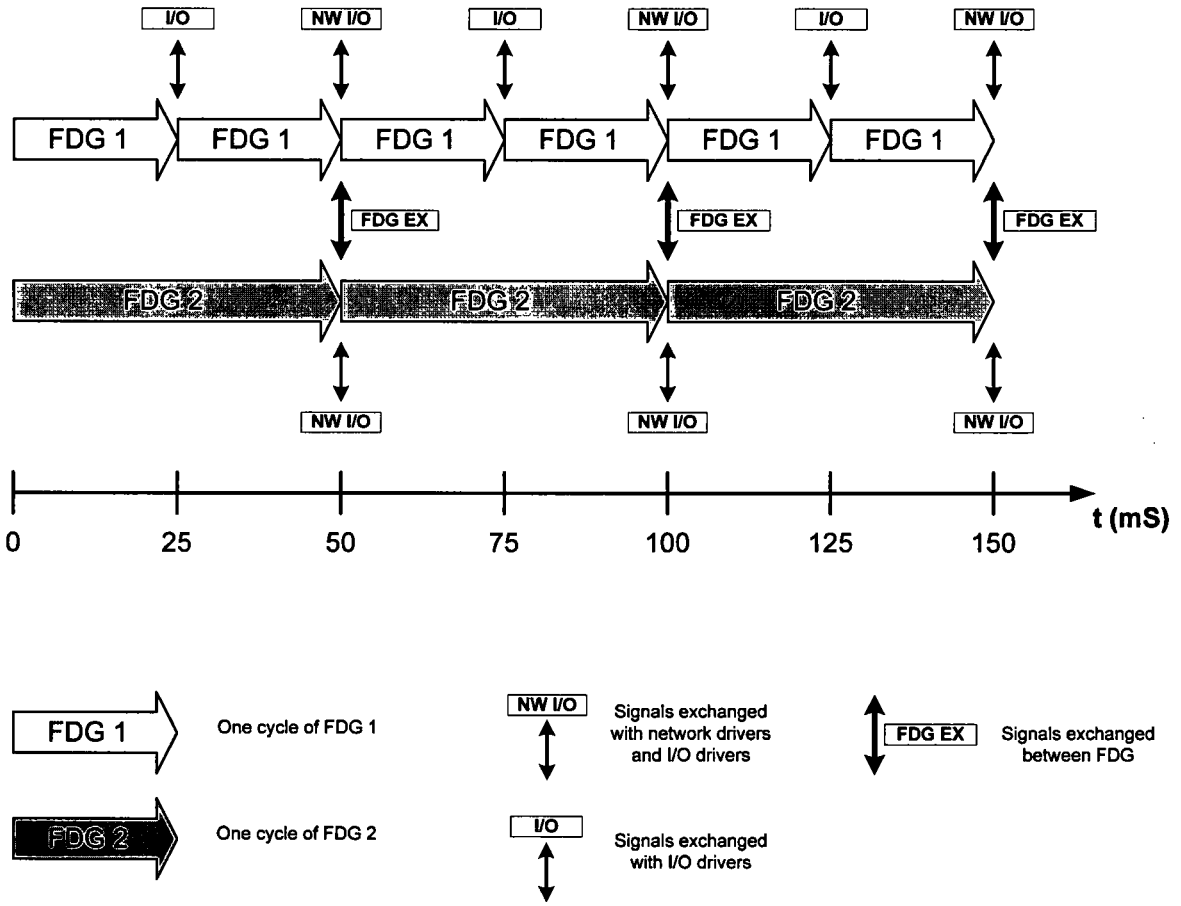
Within an FDG, all required signal exchanges between individual function diagrams can be performed during one FDG cycle time. However, signal exchanges between the two FDGs can only occur at the beginning or end of the longer of the two FDG cycle times.

2. Communication Drivers: Drivers for network communication modules are executed cyclically with a cycle time, T_N, which is common for all TXS function processors in a system. A common cycle time does not imply that the communications are synchronized between different functional processors; different functional processors can start their communication cycles at different times. For all function processors, the time that elapses between the start of two communication cycles is the same. Every T_N milliseconds, each function processor reads the messages received during the previous communication cycle, and writes the messages to be sent during the next communication cycle.

3. Input / Output (I/O) Drivers: The drivers for the input and output modules attached to a TXS function processor are executed with a cycle time corresponding with the faster of the two FDG cycle times. This results in acquired values (inputs) and generated signals (outputs) being updated at least at the beginning or end of both FDG cycles.

Figure B.4-1 provides an example of the timing relative to the three processing tasks described above. The example assumes a TXS function processor with two FDGs and cycle times of $T_N = T_{fg2} = 50$ and $T_{fg1} = 25$.

Figure B.4-1—Example of 2 FDG Timing Principles



B.5 Application of Principles

B.5.1 Limiting Response Time

The exact response time of a PS function can not be calculated due to:

- The different function processors of the system operate asynchronously. This is a desirable characteristic for a safety-related system, but it complicates the response time determination. The time delays introduced by asynchronous operation are not constant; for example, they may change after restarting an individual function processor.
- The load of the function processor and networks can not be calculated exactly.

Therefore, the approach followed in this methodology is to determine the worst case, or limiting, response time for each typical function type. The limiting time delays possible due to asynchronisms are taken into account, and full loading of function processors and networks is assumed. This verifies that the limiting response time for each function type is obtained.

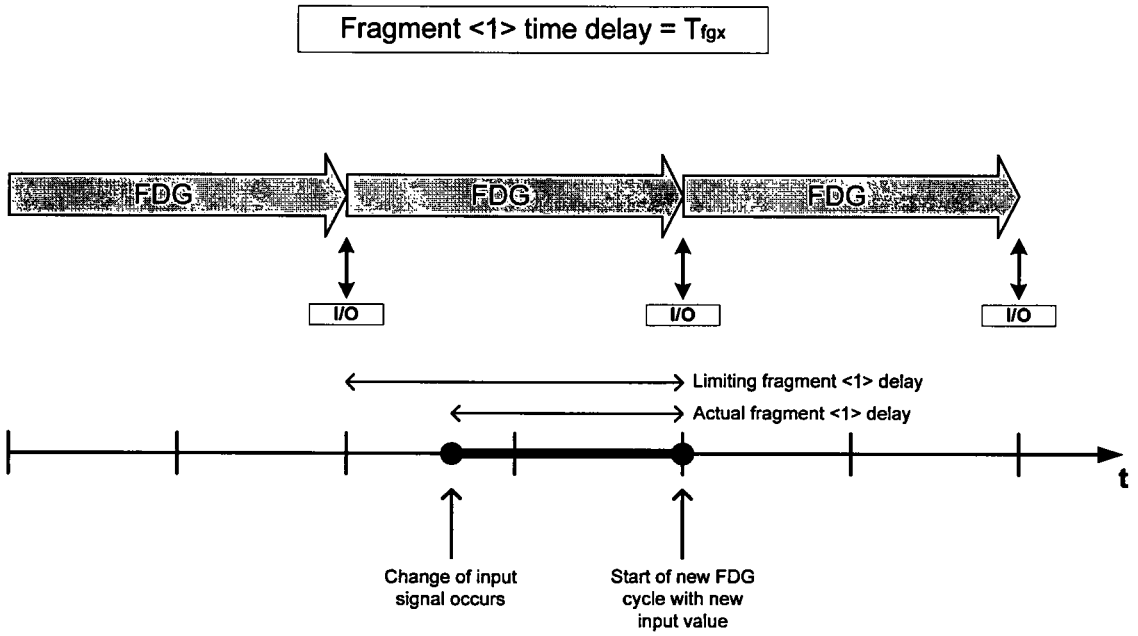
The remainder of Section B.5 is dedicated to defining the fragments of time to be considered in a limiting response time calculation. The following time fragments are defined:

- Acquisition of an input signal
- Processing within one FDG
- Exchange of a signal between FDGs of the same function processor
- Exchange of a signal between different function processors over network links
- Generation of an output signal

B.5.2 Acquisition of an Input Signal (Time Fragment <1>)

Fragment <1> corresponds with the time between an input signal changing and the time the new input value is used in FDG processing. A FDG reads input signals from the I/O driver at the beginning of every FDG cycle. In the limiting case, the input signal changes just after the beginning of an FDG cycle. This results in a limiting fragment <1> time delay equal to the FDG cycle time. Figure B.5-1 shows the fragment <1> time delay.

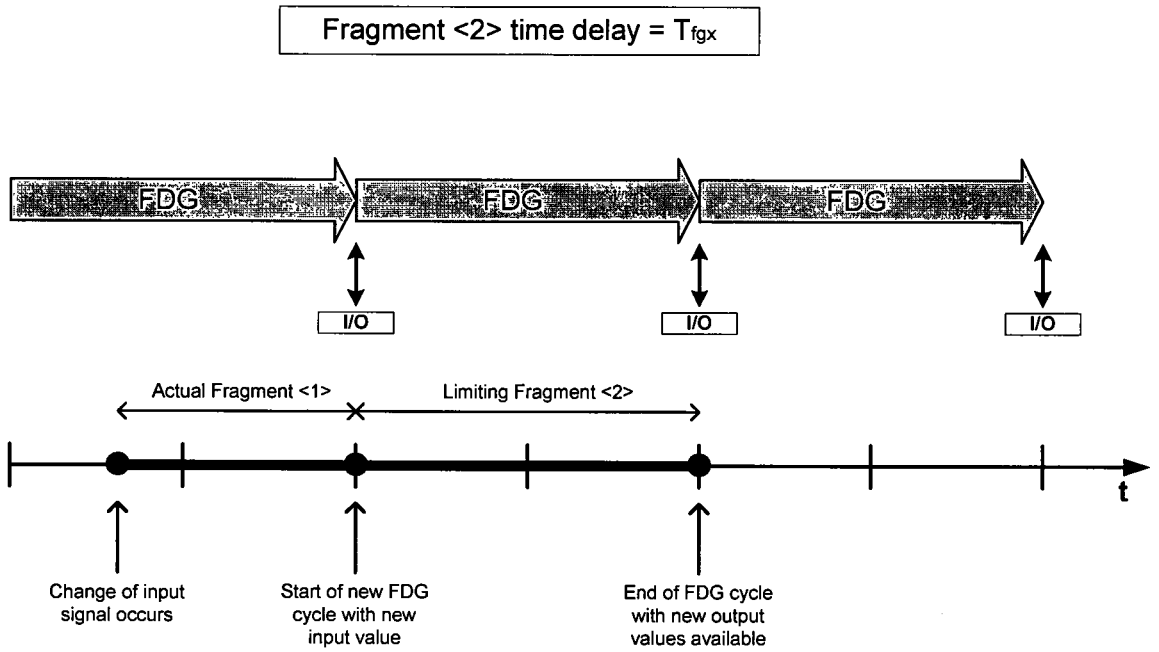
Figure B.5-1—Acquisition of Input Signal



B.5.3 Processing Within One FDG (Time Fragment <2>)

Fragment <2> corresponds with the time between the start of an FDG cycle with refreshed input values, and the end of the FDG cycle when new FDG outputs are available. The limiting fragment <2> time delay is equal to the cycle time of the FDG itself. Figure B.5-2 shows the fragment <2> time delay.

Figure B.5-2—Processing Within One FDG



B.5.4 Signal Exchange between FDGs within the Same Function Processor (Time Fragment <3>)

Fragment <3> corresponds with the time between the source FDG making a signal available, and the destination FDG being ready to accept the signal. Two cases are possible for fragment <3> depending on the relative cycle time of the source FDG and the destination FDG:

- If the source FDG has a slower cycle time than the destination FDG, then a cycle of the destination FDG starts exactly at the end of the source FDG. In this case, the limiting fragment <3> time delay is equal to zero.
- If the source FDG has a faster cycle time than the destination FDG, then one or more cycles of the source FDG must elapse before the beginning of the next cycle of the destination FDG. In this case, the limiting fragment <3> time delay is equal to $T_{fg\ dest} - T_{fg\ source}$.

This results in an overall limiting fragment <3> time delay equal to max(0, $T_{fg\ dest} - T_{fg\ source}$). Figure B.5-3 and Figure B.5-4 show the fragment <3> time delay for both cases.

Figure B.5-3—Signal Exchange from Slow FDG to Fast FDG

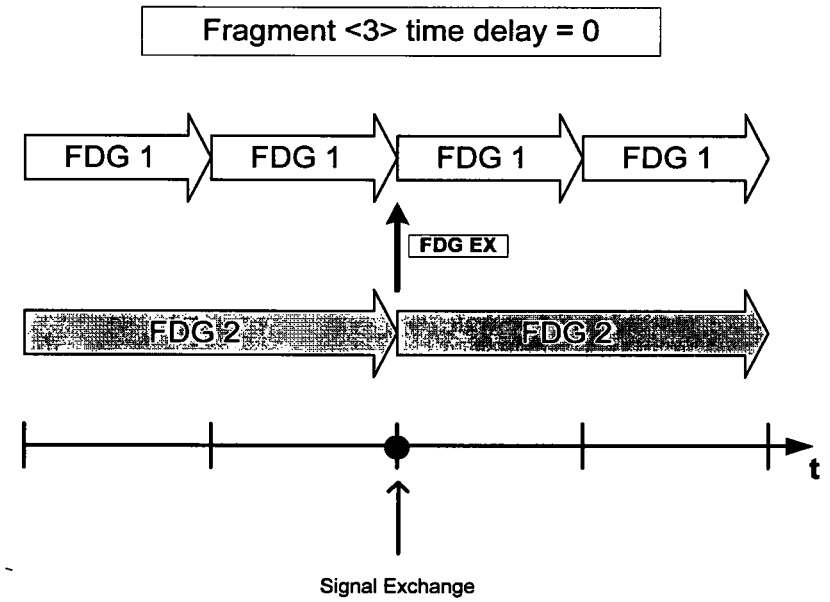
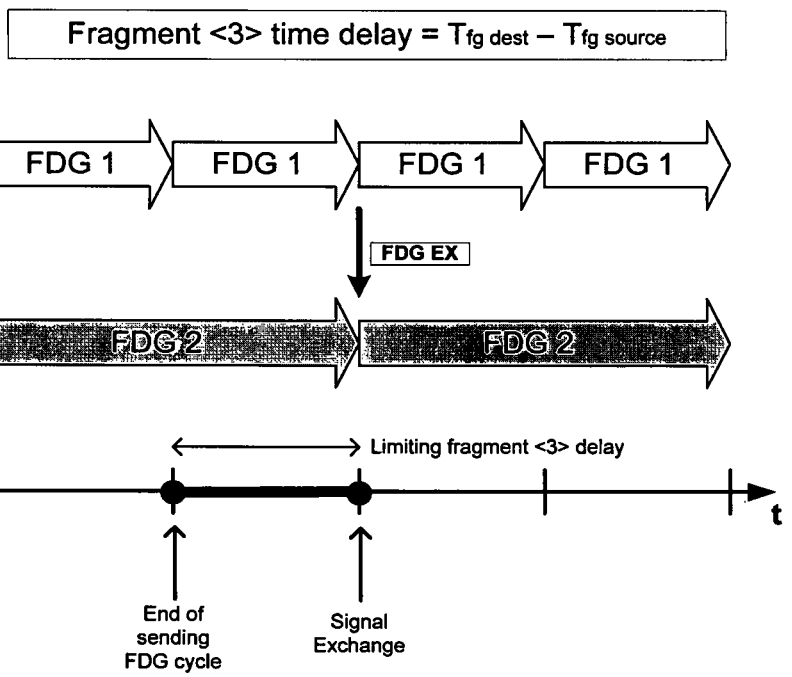


Figure B.5-4—Signal Exchange from Fast FDG to Slow FDG



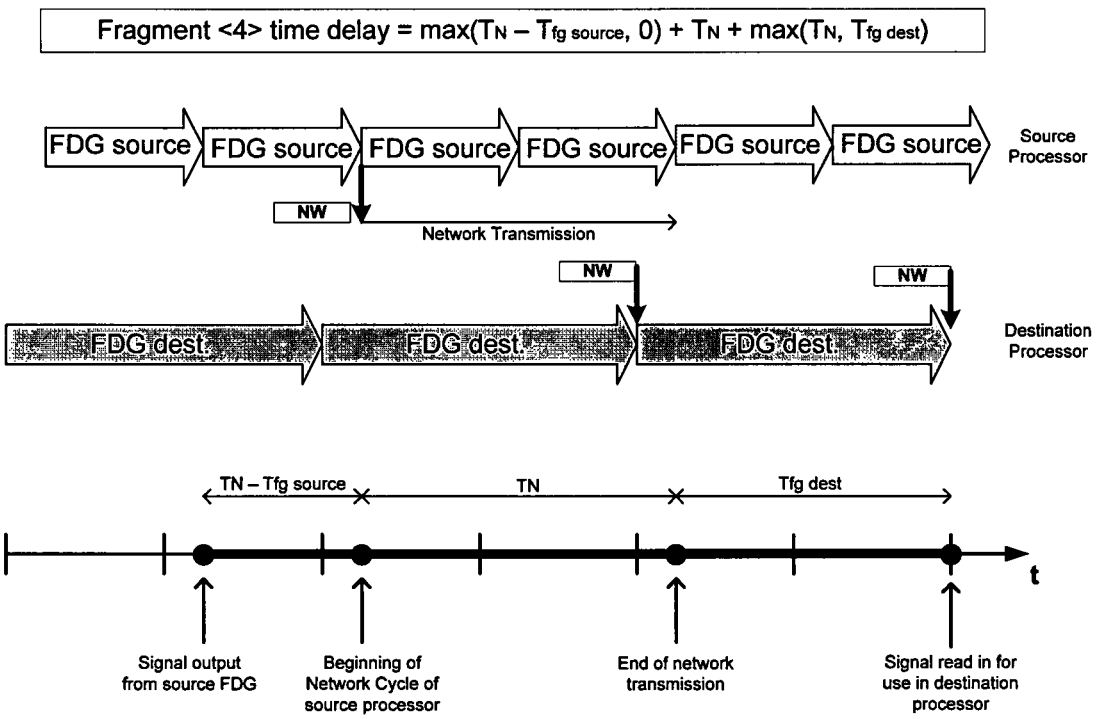
B.5.5 Signal Exchange between Function Processors over Network Link (Time Fragment <4>)

Fragment <4> corresponds with the time between the source function processor writing its output signals to be sent on the network, and the destination function processor reading in those signals. Three time delays must be considered:

- If the source FDG has a cycle time faster than the network cycle time, it must wait for the beginning of the next network cycle time. This introduces a limiting time delay equal to $\max(0, T_N - T_{fg\ source})$ for the sending portion of message transfer.
- The assumption is made that the full network bandwidth is used. This means that the serial data transmission occurs during the entire network cycle time and the last piece of information is sent just before the end of the cycle. This introduces a limiting network transmission delay time equal to T_N.
- The message may arrive at the destination function processor just after the beginning of a communication cycle. If the communication cycle time is longer than the FDG cycle time, a limiting time delay is introduced equal to T_N. If the destination FDG cycle time is longer than the communication cycle time, it must be considered that the message arrives just after the beginning of an FDG cycle. This introduces a limiting time delay equal to $T_{fg\ dest}$. Therefore, the limiting time delay for the receive portion of message transfer is equal to $\max(T_N, T_{fg\ dest})$.

Taking into account the three time delays involved in network communication, the overall limiting fragment <4> time delay is equal to $\max(0, T_N - T_{fg\ source}) + T_N + \max(T_N, T_{fg\ dest})$. Figure B.5-5 shows the fragment <4> time delay.

Figure B.5-5—Signal Exchange over Network Link

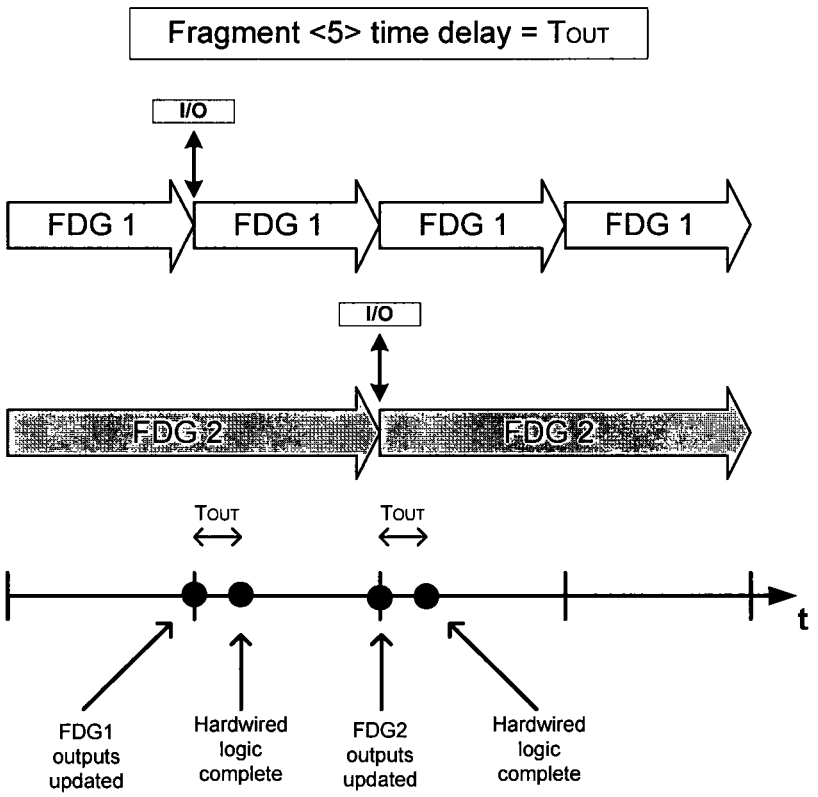


Note: In this example, TN = Tfg dest = 2Tfg source

B.5.6 Generation of an Output Signal (Time Fragment <5>)

Fragment <5> corresponds with the time between the output signals being updated, and the completion of the hardwired logic downstream of the ALUs. Output signals are updated at the end of every FDG. Opto-coupler modules are used to implement the hardwired logic, and their time delay is annotated as T_{OUT}. Figure B.5-6 shows the limiting fragment <5> delay which is equal to T_{OUT}.

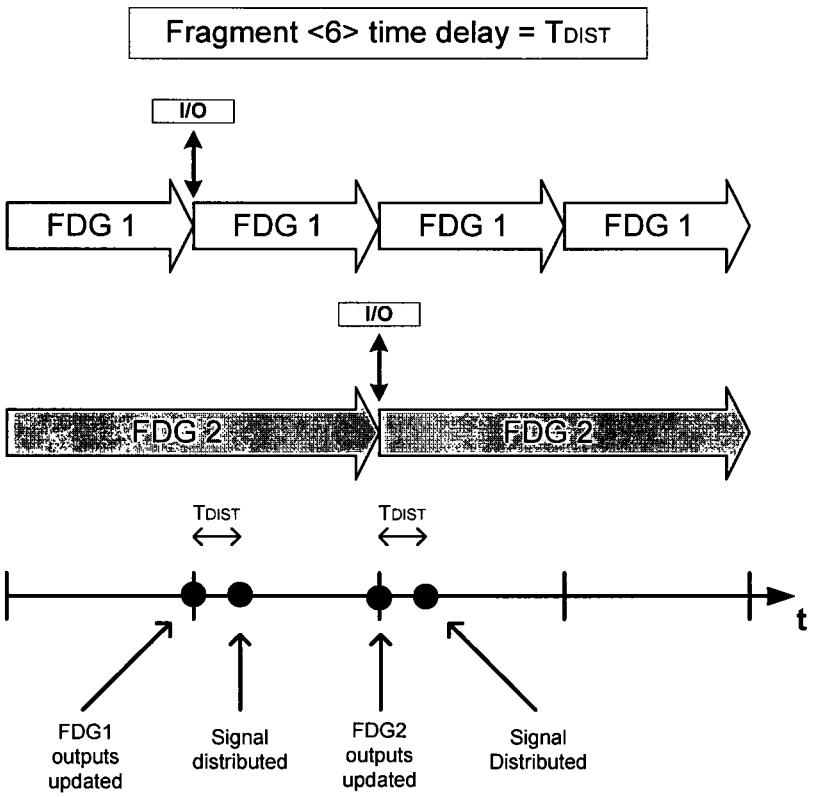
Figure B.5-6—Distribution of Signal



B.5.7 Signal Distribution through the SCDS (Time Fragment <6>)

Fragment <6> corresponds with the time necessary to distribute sensor input signals through the signal conditioning and distribution system (SCDS). Outputs are sent from the sensor or black box signal conditioning equipment and distributed through the SCDS to the APU. Output signals are updated at the end of every FDG. Non-processor based components are used to distribute the signal, and their time delay is denoted as T_{DIST}. Figure B.5-7 shows the limiting fragment <6> delay, which is equal to T_{DIST}.

Figure B.5-7—Generation of Output Signal



B.5.8 Priority Module of the Priority and Actuator Control System (PACS) (Time Fragment <7>)

Fragment <7> corresponds with the time necessary for the priority module of the PACS to send an actuation signal upon request from the PS. The priority module of the PACS time delay is denoted as T_{PACS}. This time delay will be added after the generation of an PS output signal (Time Fragment <5>) (See Section B.5.6).

B.6 Timing Assumptions

[
]

must be used if they are different than those assumed for the typical function. The following assumptions are made:

- All function processors use a communication cycle time of T_N = 50mS.
- Priority Module of the PACS is T_{PACS} = 24 mS.
- Signal distribution by SCDS is T_{DIST} = 10mS.
- APUs A1, A2, B1, B2 use one FDG with a cycle time of T_{fg1} = 25mS.
- APU A3 uses one FDG with a cycle time of T_{fg1} = 50mS.
- All ALUs use two FDG with cycle times T_{fg1} = 25mS and T_{fg2} = 50mS. For ALUs, FDG1 processes all automatic actuations. FDG2 is used only to process permissive and manual commands. Only T_{fg1} must be accounted for in limiting time response determination for typical PS functions.
- Opto-coupler output response times are T_{out} = 10mS.

B.6.1 Response times for typical PS functions

Given the special case of APU A3 having a different cycle time than the other APUs, each typical implementation must be considered two ways. First a limiting response time is calculated for each typical function assuming any APU, other than APU A3, is used. Second, the limiting response time is calculated for each typical function assuming that APU A3 is used.

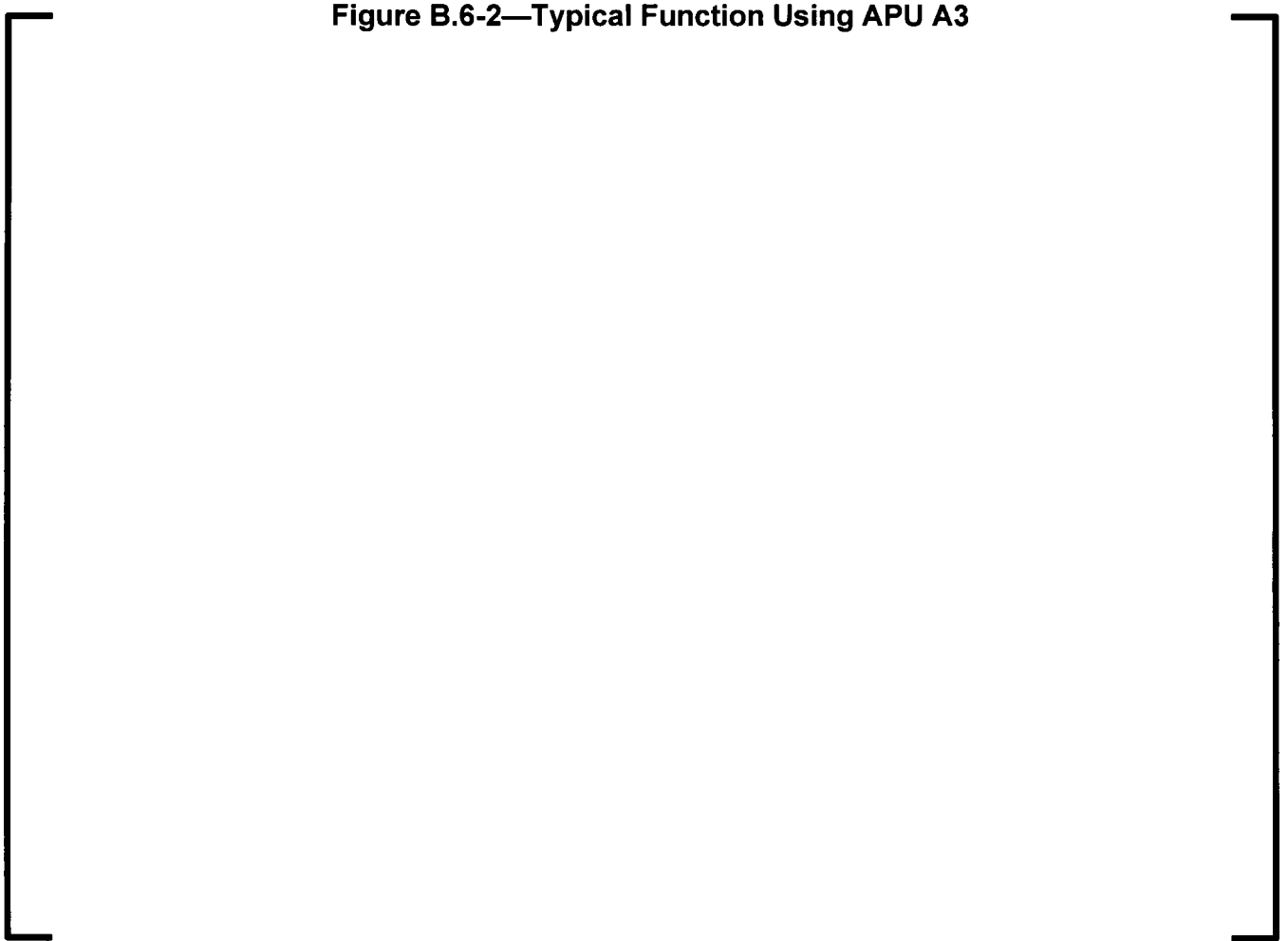
B.6.2 Function Type 1—Typical Function Not Using APU A3

[
]

Figure B.6-1—Typical Function Not Using APU A3

B.6.3 Function Type 2—Typical Function Using APU A3

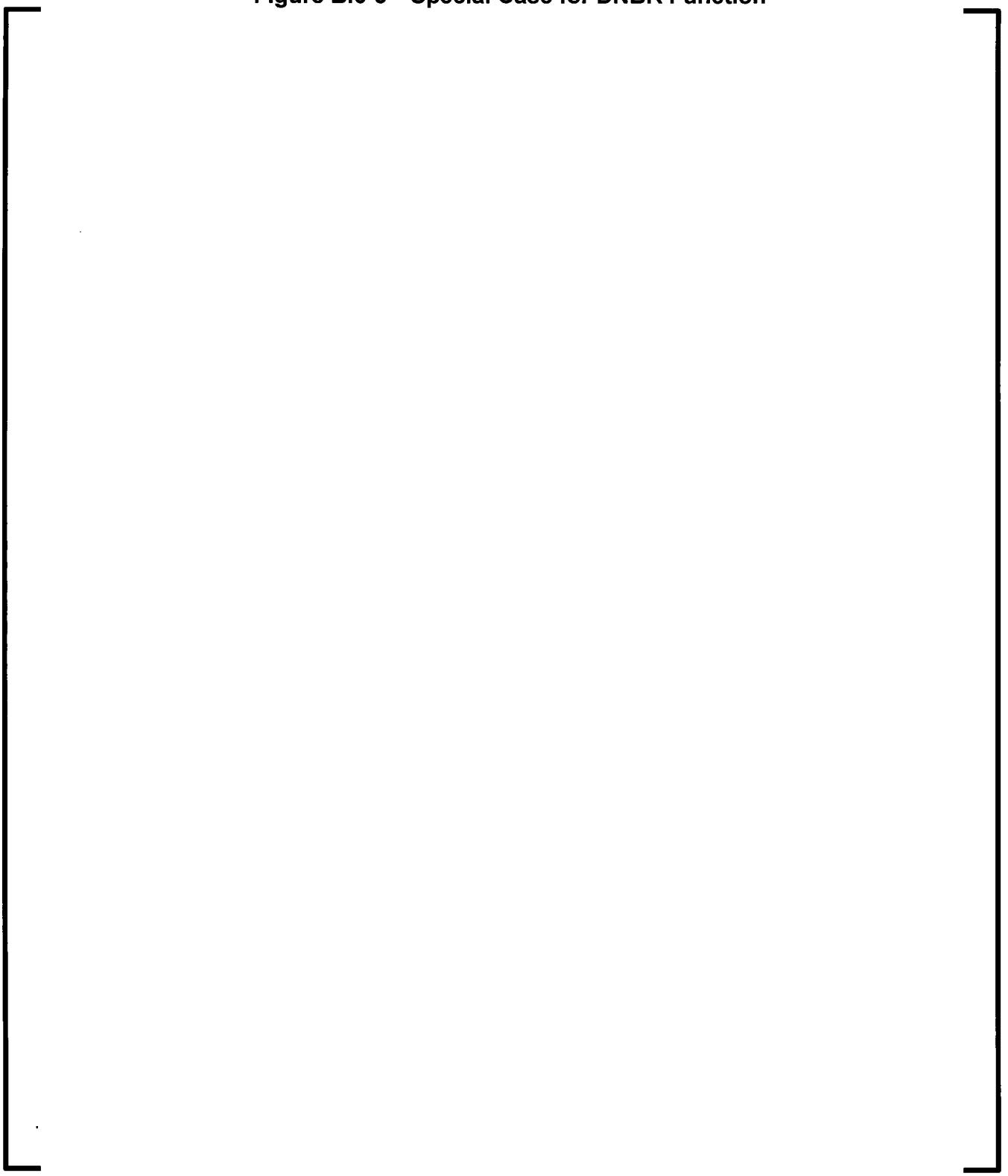
Figure B.6-2—Typical Function Using APU A3



B.6.4 Function Type 3—Special Case for DNBR Function

2. The processing path involving APU A3 has the same structure as function type 2. In this special case, the DNBR function requires processing of all the self-powered neutron detectors (SPND) fingers. Only one finger over the 12 is processed in APU A3 at every cycle. So, the complete processing requires 12 FDG cycles.

Figure B.6-3—Special Case for DNBR Function



B.7 Appendix B References

1. NUREG-0800, Branch Technical Position 7-21, Rev. 5, "Guidance on Digital Computer Real-Time Performance," March 2007.