ANP-10281NP
Revision 0

U.S. EPR Digital Protection System
Topical Report

March 2007

AREVA NP Inc.

Non-Proprietary

For information address: AREVA NP Inc.
An AREVA and Siemens Company
3315 Old Forest Road
Lynchburg, VA 24506

U.S. Nuclear Regulatory Commission

Disclaimer

Important Notice Concerning the Contents and Application of This Report
Please Read Carefully

This report was developed based on research and development funded and conducted by AREVA NP Inc., and is being submitted by AREVA NP to the U.S. Nuclear Regulatory Commission (NRC) to facilitate future licensing processes that may be pursued by licensees or applicants that are customers of AREVA NP. The information contained in this report may be used by the NRC and, under the terms of applicable agreements with AREVA NP, those customers seeking licenses or license amendments to assist in demonstrating compliance with NRC regulations. The information provided in this report is true and correct to the best of AREVA NP's knowledge, information, and belief.

AREVA NP's warranties and representations concerning the content of this report are set forth in agreements between AREVA NP and individual customers. Except as otherwise expressly provided in such agreements with its customers, neither AREVA NP nor any person acting on behalf of AREVA NP:

- Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, nor the use of any information, apparatus, method, or process disclosed in this report.
- Assumes any liability with respect to the use of or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

ABSTRACT

This topical report describes the design of the U.S. EPR protection system and is provided to support the design certification application for the U.S. EPR.

The U.S. EPR protection system is a digital, integrated reactor protection and engineered safety features actuation system and is implemented using TELEPERM XS technology. The TELEPERM XS platform has been generically approved by the U.S. Nuclear Regulatory Commission for use in safety-related instrumentation and control applications in the United States. The primary purposes of the protection system are to: detect plant conditions that indicate the occurrence of a design basis event, and initiate the plant safety features required to mitigate the event. This purpose is fulfilled through the automatic actuation of reactor trips and the engineered safety features systems.

This report describes the application of TELEPERM XS technology to the U.S. EPR protection system design. It also presents the protection system architecture and the typical implementation of protective functions within this architecture. This report demonstrates compliance of the protection system design with applicable regulations and requirements, guidance documents, and industry standards. Key features of the protection system design are explained, such as functional diversity, interchannel communication, and safety to non-safety system interfaces.

Nature of Changes

Item	Section(s) or Page(s	Description and Justification

Contents

List of Tables

List of Figures

Nomenclature

Acronym	Definition
ALU	Actuation Logic Unit
APU	Acquisition and Processing Unit
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CFR	Code of Federal Regulations
CPU	Central Processing Unit
CRDM	Control Rod Drive Mechanism
DCD	Design Certification Document
DPRAM	Dual Port Random Access Memory
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Features Actuation System
GW	Gateway
HFE	Human Factors Engineering
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
MCR	Main Control Room
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
NRC	Nuclear Regulatory Commission
OLM	Optical Link Module
PAC(S)	Priority Actuation and Control (System)
PI	Panel Interface
PICS	Process Information and Control System
PROFIBUS	Process Field Bus
PS	Protection System
PWR	Pressurized Water Reactor
QDS	Qualified Display System

Acronym	Definition
RAU	Remote Acquisition Unit
RCCA(U)	Rod Control Cluster Assembly (Unit)
RPS	Reactor Protection System
RSS	Remote Shutdown Station
RT	Reactor Trip
RTM	Requirements Traceability Matrix
RTS	Reactor Trip System
SICS	Safety Information and Control System
SPACE	Specification and Coding Environment
SPND	Self-Powered Neutron Detector
SU	Service Unit
TMI	Three Mile Island
TXS	TELEPERM XS
V&V	Verification and Validation

1.0 INTRODUCTION

This topical report describes the design of the U.S. EPR protection system (PS) and is provided to support the design certification application for the U.S. EPR.

The PS is a digital, integrated reactor protection system (RPS) and engineered safety features actuation system (ESFAS) and 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 a design basis event and initiates the plant safety features required to mitigate the event. These actions are accomplished through the automatic actuation of reactor trips (RT) and engineered safety features (ESF) systems.

The PS utilizes 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.

This report describes the PS architecture and the typical implementation of functionality within this architecture. AREVA NP requests NRC approval of the following aspects of the PS design presented in this report:

- PS architecture
- Specific network configurations
- Typical RT concepts and sequences
- Typical ESFAS concepts and sequences
- Design rules for permissive signals
- Inter-channel communication independence
- Safety to non-safety system interfaces

- Conformance with relevant clauses of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603

AREVA NP is not requesting approval for a specific set of TXS hardware components or version of the software to be used in the PS. Therefore, generic terms for the PS equipment are used throughout this report (e.g., function computer, communication module, input module). Table 1-1 correlates the generic equipment references used to the equivalent specific equipment that was audited as part of the NRC review of the TXS topical report (References 23 and 24).

The PS provides for functional diversity, as described in Section 10.0, “Functional Diversity.” The functional diversity design rules described represent elements of diversity that correspond to the functional and signal diversity elements described in NUREG/CR-6303 (Reference 3). AREVA NP is also aware that the NRC is performing research to help develop criteria for what constitutes adequate diversity and what credit can be taken for designed-in robustness. AREVA NP intends to take credit for the functional diversity within the PS, as described in this report, in a defense-in-depth and diversity analysis.

Table 1-1—Generic Hardware Equivalence

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

2.0 BACKGROUND

The safety and reliability of nuclear installations depend in large measure 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).

Specific requirements for safety-related I&C systems in nuclear power plants are defined in national and international standards. Specific system properties, implemented in specially developed and qualified system software, are incorporated with the qualified TXS hardware to meet these requirements. TXS qualification is demonstrated by type-testing of hardware and software components.

TXS uses a specially designed engineering tool, SPACE, to implement the required nuclear power plant-specific I&C features. SPACE is an engineering tool, which generates the application software that satisfies safety-related requirements.

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, the TXS design is a qualified, generic digital 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, generic digital 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
  - 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. Newer versions of TXS hardware and software are being developed for use in safety-related nuclear applications. The generic approval of the TXS system design principles and methods eliminates the need for regulatory review of each individual TXS hardware or software upgrade. Instead, each applicant must demonstrate that the equipment and software used in the as-built system adheres to the approved TXS design principles and methods. Each applicant is also required to demonstrate that the qualification meets the plant license requirements and that plant-specific interface items are sufficiently addressed.

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 topical report does not apply to the installation of the TXS system; therefore, the resolution of the action items in Reference 23 is not within the scope of this report. For informational purposes, Appendix A identifies the documentation that AREVA NP anticipates will disposition each action item.

3.0 DESCRIPTION OF THE U.S. EPR PROTECTION SYSTEM

3.1 *System Role*

The PS is an integrated digital RPS and ESFAS. The purposes of the PS are to: detect plant conditions that indicate the occurrence of a design basis event, and initiate the plant safety features required to mitigate the event. 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 can also process manual commands and issue corresponding actuation orders.

3.2 *System Organization*

The PS is organized into four redundant divisions located in separate safeguards buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement functional diversity for 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 digital computer system distributed among four redundant divisions consisting of eight actuation paths (two subsystems per division). Each actuation path consists of two or three layers of

operation. The layers of operation include signal acquisition, data processing, and actuation signal voting.

The majority of the PS functions are performed in two layers. The acquisition and data processing layers are combined into one layer (i.e., acquisition and processing). The second layer is the actuation signal voting layer. The exceptions are the few functions that utilize the self-powered neutron detectors (SPND) as inputs. For these functions, three layers of operation are utilized. Computers dedicated to the acquisition and distribution of the SPND signals compose the acquisition layer, which for SPND-based functions is separate from the processing and actuation signal voting layers. Sections 7.0 and 8.0 describe the layers of operations in the PS design.

4.0 SYSTEM ARCHITECTURE

4.1 *Architecture Diagram Explanation*

The architecture of the PS is shown in Figure 4-1. The quadrants of the figure represent the four physically separated, redundant PS divisions. The equipment assigned to each PS division is located in the corresponding safeguards building. The center of the figure represents the control room complex shared between safeguards buildings two and three. Within the quadrant representing each PS division, the upper portion represents subsystem A and the lower portion represents subsystem B.

Figure 4-1 shows the distinctions between Class 1E networks, non-Class 1E networks, and hardwired connections. For networked connections, the monitoring and service interface (MSI) serves as the safety to non-safety isolation point. Network connections 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 primarily for transmission of actuation orders.

The networks shown in Figure 4-1 are intended to represent functional connections only, and are not representative of the detailed network topologies as implemented. Examples of the detailed individual network topologies are provided in Section 6.0.

4.2 *System Architecture Features*

The system architecture features are described in Sections 4.2.1 through 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, safeguards 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 an independent Class 1E, uninterruptible electrical bus. These busses 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 24VDC 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 is 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 does not prevent performance of the safety functions. 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 the other divisions; the same is true of subsystem B. The primary purpose of this arrangement is to provide functional diversity for RT functions. Section 10.0 presents the design rules for assigning PS functions to the subsystems. Implementation of these design rules supports the effectiveness of the functional diversity concept and optimization of the entire system.

Figure 4-1—Protection System Architecture

5.0 PROTECTION SYSTEM UNITS

This section describes the different functional units that compose the PS. The description of each unit type 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.

This section also describes the priority actuation and control (PAC) units, the panel interfaces (PI), and the qualified display system (QDS), whose primary functions include interfacing with the PS, although they are not part of the PS.

5.1 *Remote Acquisition Units*

The remote acquisition unit's (RAU) primary functions are to acquire the signals from the SPND and to distribute these signals to the acquisition and processing units (APU) for processing. Each RAU consists of a function computer, input and output modules, and communication modules.

Each PS division contains two redundant RAUs; both are assigned to subsystem A. Each PS division acquires 18 of the 72 SPNDs. Each RAU acquires all 18 of the SPND signals assigned to its division. **[**

]

5.2 *Acquisition and Processing Units*

The APU's primary functions are:

- Acquire the signals from the process sensors, RAU, and rod control cluster assembly units (RCCAU)
- 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 computer, 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 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.

5.3 *Actuation Logic Units*

The ALU's 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 unlatch actuation outputs. Each ALU consists of a function computer, 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 (Section 7.5) and in a hardwired 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.

5.4 *Monitoring and Service Interfaces*

Each PS division contains two MSIs; the main unit (MSI-MU) and the auxiliary unit (MSI-AU). The MSI performs functions related to both subsystems; therefore, they are

not assigned to a particular subsystem. Each MSI consists of a function computer, input and output modules, and communication modules.

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

The MSI-MU's primary functions are status monitoring and data transfer. The MSI-MU facilitates monitoring for conditions, such as communication failures between other PS units and for protection channel status information. The MSI-MU's data transfer functions include the transfer of manual commands to the APU and ALU, transfer of information for display to the operators, and transfer of information needed by other I&C systems. The MSI-MU provides the required Class 1E isolation to prevent non-safety-related systems from affecting the performance of the PS.

5.5 *Rod Control Cluster Assembly Units*

The RCCAU's primary function is the acquisition and digital processing of the analog rod position measurements. Each RCCAU consists of a function computer, input and output modules, specialized TXS signal conditioning modules, and communication modules.

The PS contains four RCCAUs; one assigned to each division. The RCCAU of each division communicates with two APUs in its division. The RCCAU performs functions related to both subsystems; therefore, they are not assigned to a particular subsystem. The RCCAU receives analog signals from the measurement devices, digitizes them, and performs temperature compensation algorithms. The digitized and compensated rod position measurements are sent to one APU in each subsystem.

5.6 *Service Unit*

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

- System diagnosis

- Monitoring the system's functional status
- Performing periodic tests of the system
- Modifying the changeable software parameters
- Loading new software versions

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

5.7 *Gateways*

5.8 *Panel Interfaces*

The PI's primary function is to interface the PS to the safety information and control system (SICS), including the QDS. Each PI consists of a function computer, input and output modules, and communication modules. The PI is part of the SICS.

5.9 *Qualified Display System*

The QDS's primary function is to provide a digital display of safety-related information and variables to the operator. The QDS also serves as an interface for the operator to perform safety-related manual commands. Each QDS consists of the monitor and a QDS computer. The QDS is part of the SICS.

The SICS contains four QDS to display PS information; one assigned to each PI. The QDS receives the information to be displayed from the PI and sends manual commands to the PI for distribution to the appropriate MSI-MU.

5.10 *Priority Actuation and Control Modules*

The primary functions of the PAC modules are:

- Receive actuation orders from the PS and other I&C systems
- Prioritize the various signals

- Issue the order of highest safety significance to the actuator

The PAC modules also receive checkback signals from the actuators for distribution to the appropriate I&C systems. The PAC modules are part of the PACS.

A PAC module is assigned to each ESF actuator that receives commands from the PS. Each PAC module receives orders from the ALU that performs the function related to the actuator. RT actuators receive orders directly from the PS; they do not have an associated PAC module.

Section 11.2 provides a more detailed description concerning the interface between the PAC modules and the PS. AREVA NP topical report ANP-10273P, “AV42 Priority Actuation and Control Module Topical Report,” (Reference 25) provides further information on the PAC module.

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 6-20) showing network connections between the different units of the PS. These figures represent the conceptual system design and may be modified in the detailed system design phases.

In general, two types of Class 1E network topologies are utilized 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 toplogy 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 configurations, 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 configuration of the network, through the features designed into the TXS platform for interference-free communication. Communication independence is addressed further in Section 12.0.

6.1.4 *Network Operation Concepts*

[

] Additional information on the echo and segmentation functions is provided in Sections 6.1.4.1 through 6.1.4.4.

6.1.4.1 *Send Echo*

[redacted]

6.1.4.2 *Monitor Echo*

[redacted]

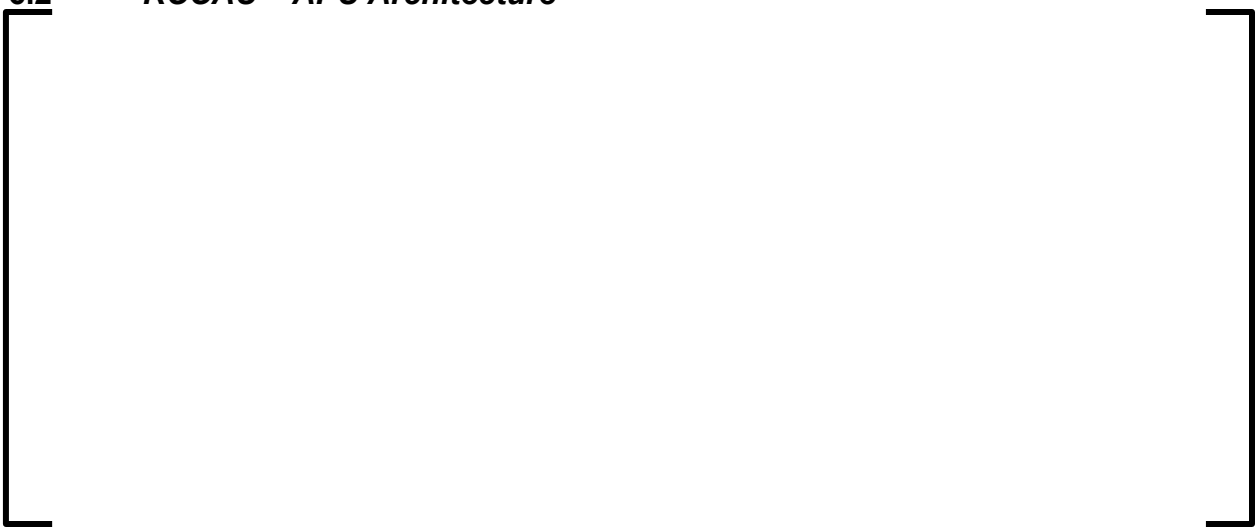
6.1.4.3 *Suppress Echo*

[redacted]

6.1.4.4 *Segmentation*

[redacted]

6.2 *RCCAU – APU Architecture*



6.3 *RAU – APU Architecture*

6.4 *APU – ALU Architecture (Subsystem A)*

6.5 *APU – ALU Architecture (Subsystem B)*

6.6 *MSI-MU – APU Architecture*

6.7 *MSI-MU – RCCAU – RAU – ALU – MSI-AU Architecture*

6.8 *MSI-MU – PI Architecture*

6.9 *MSI-MU – GW – SU Architecture*

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

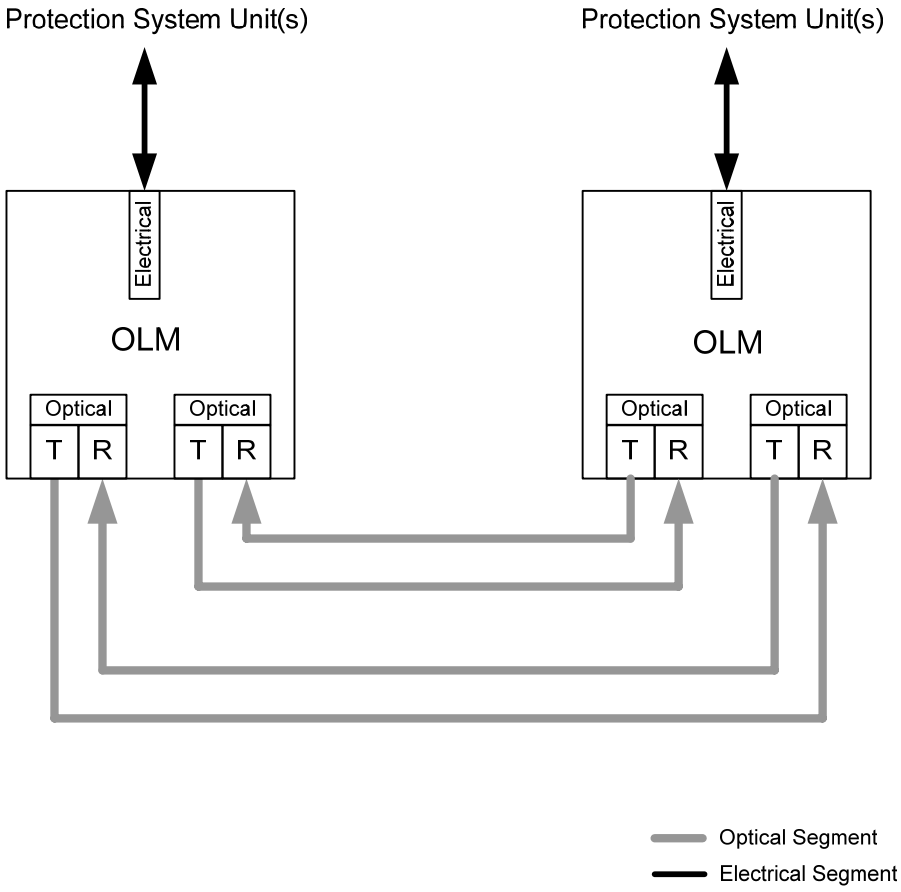


Figure 6-2—Example of Redundant Ring Connection

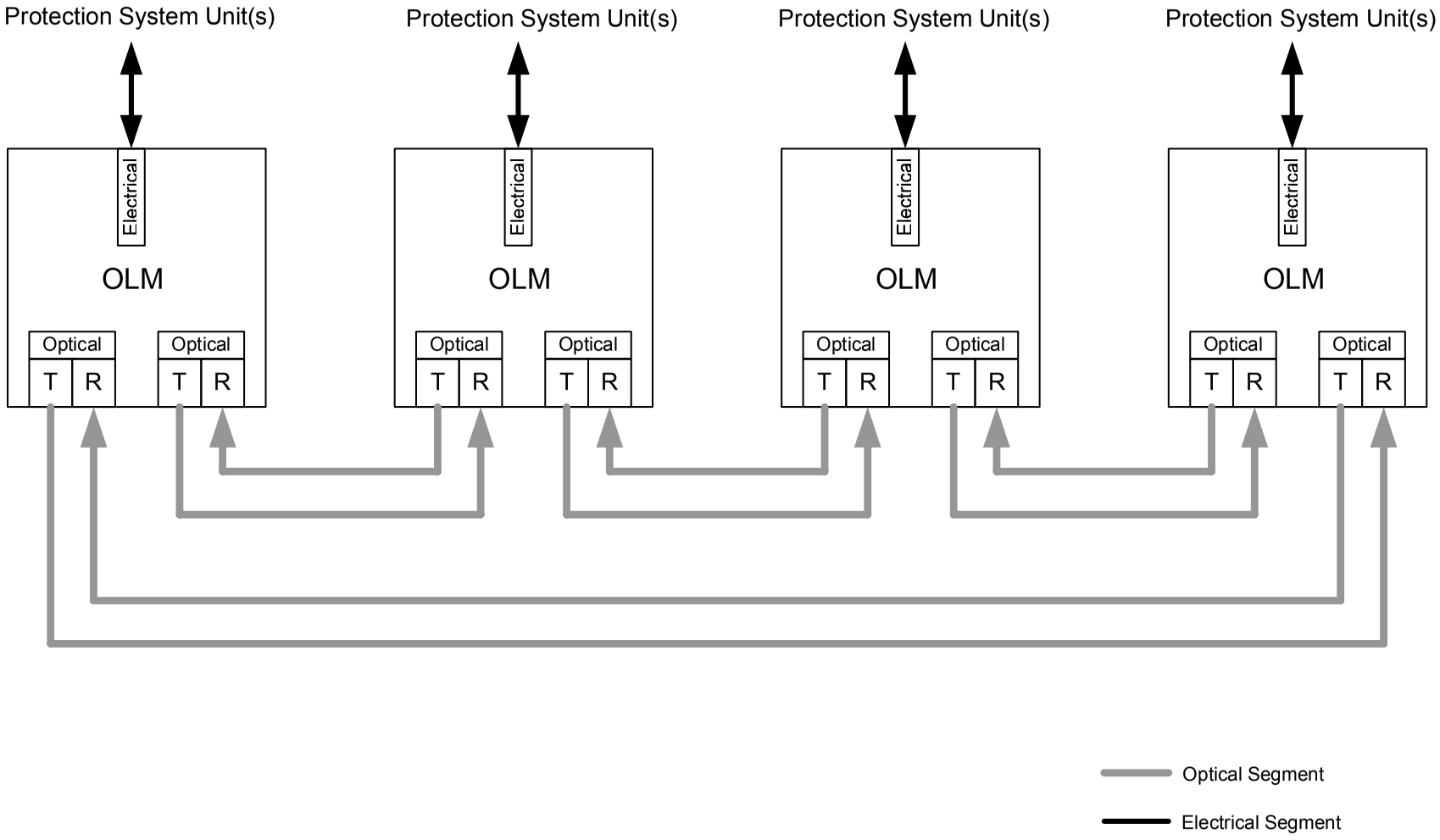


Figure 6-3—RCCAU – APU Architecture

Figure 6-4—RAU1 – Div 1 APU Architecture

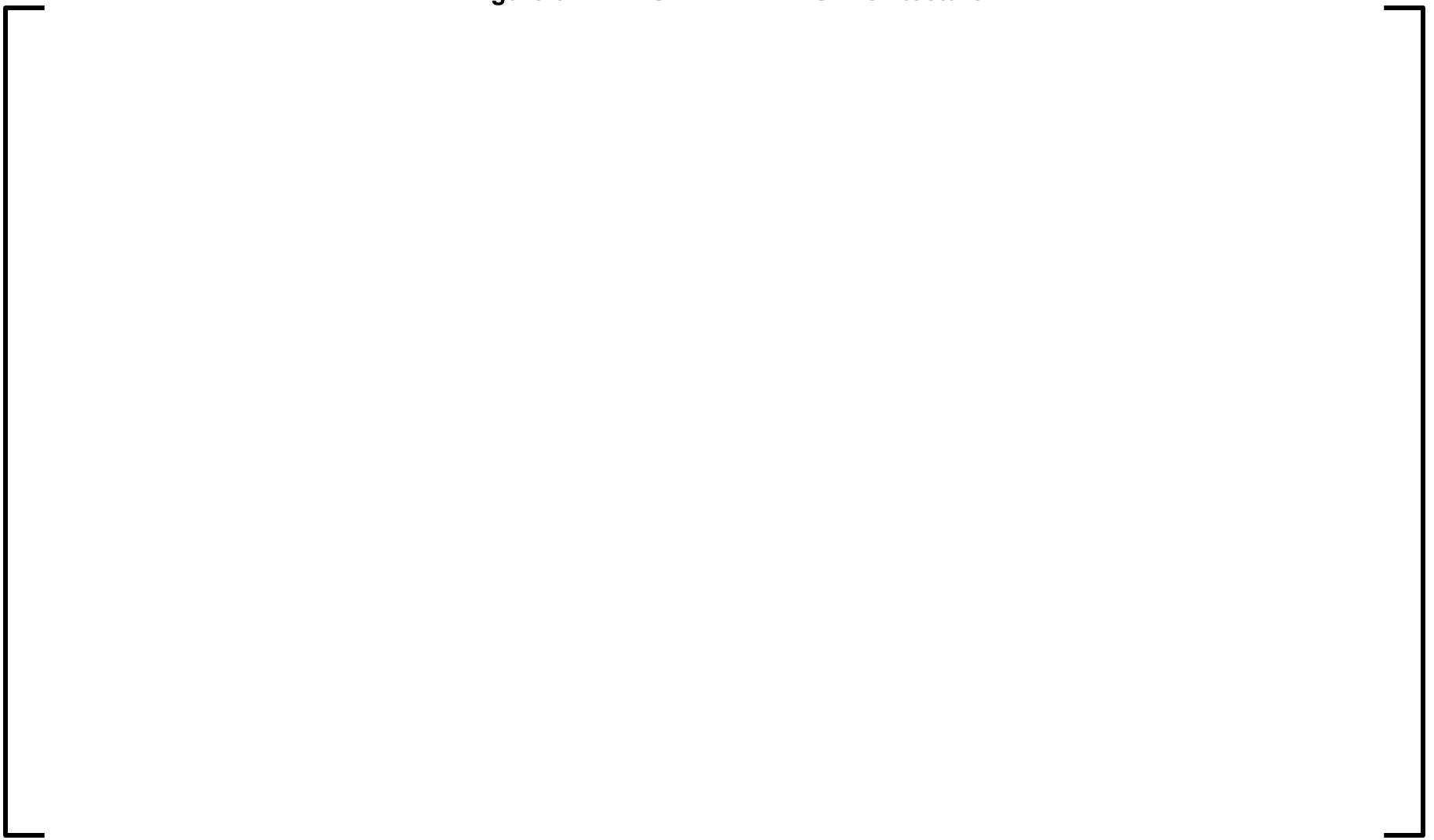


Figure 6-5—RAU1 – Div 2 APU Architecture

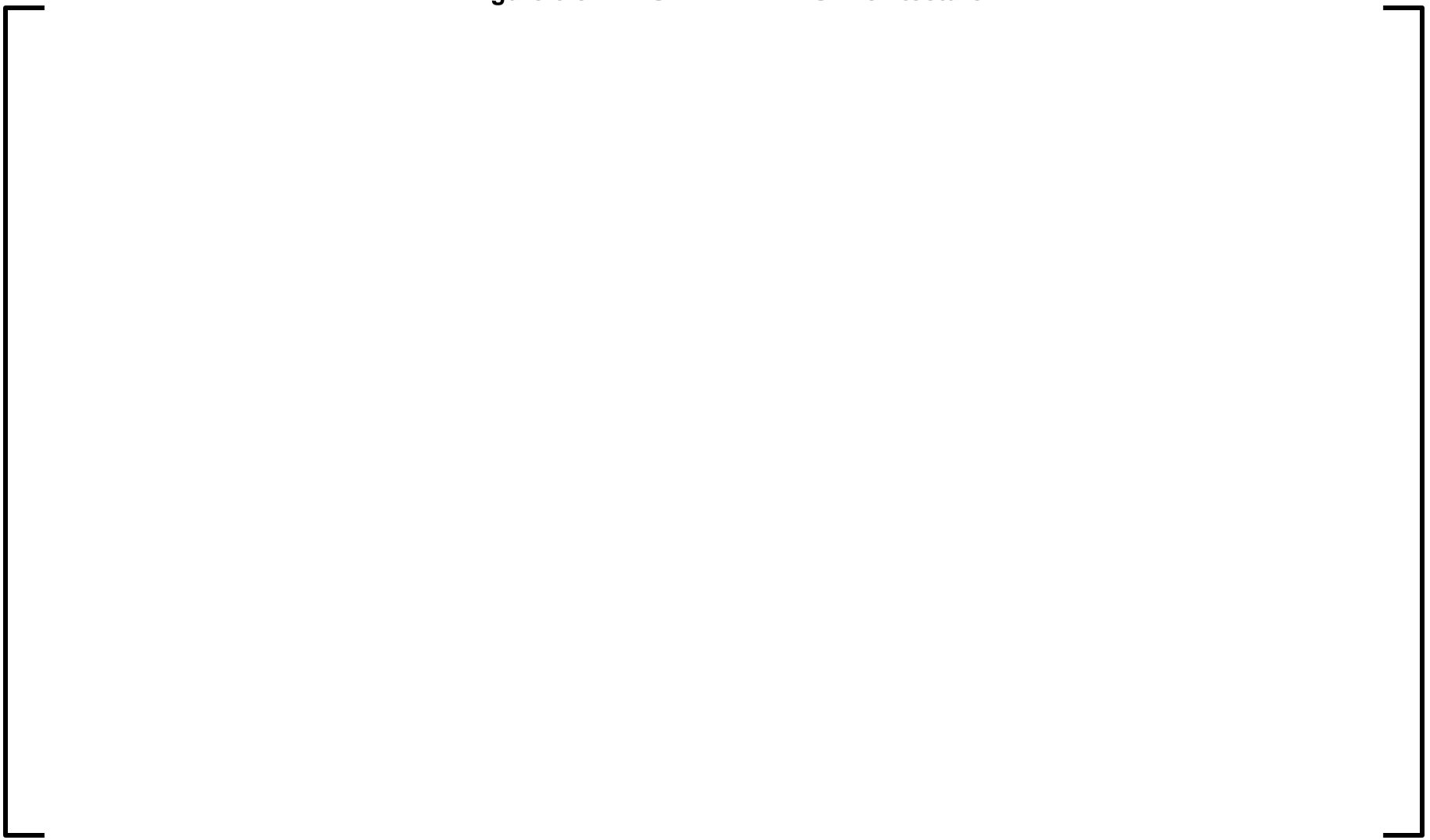


Figure 6-6—RAU1 – Div 3 APU Architecture

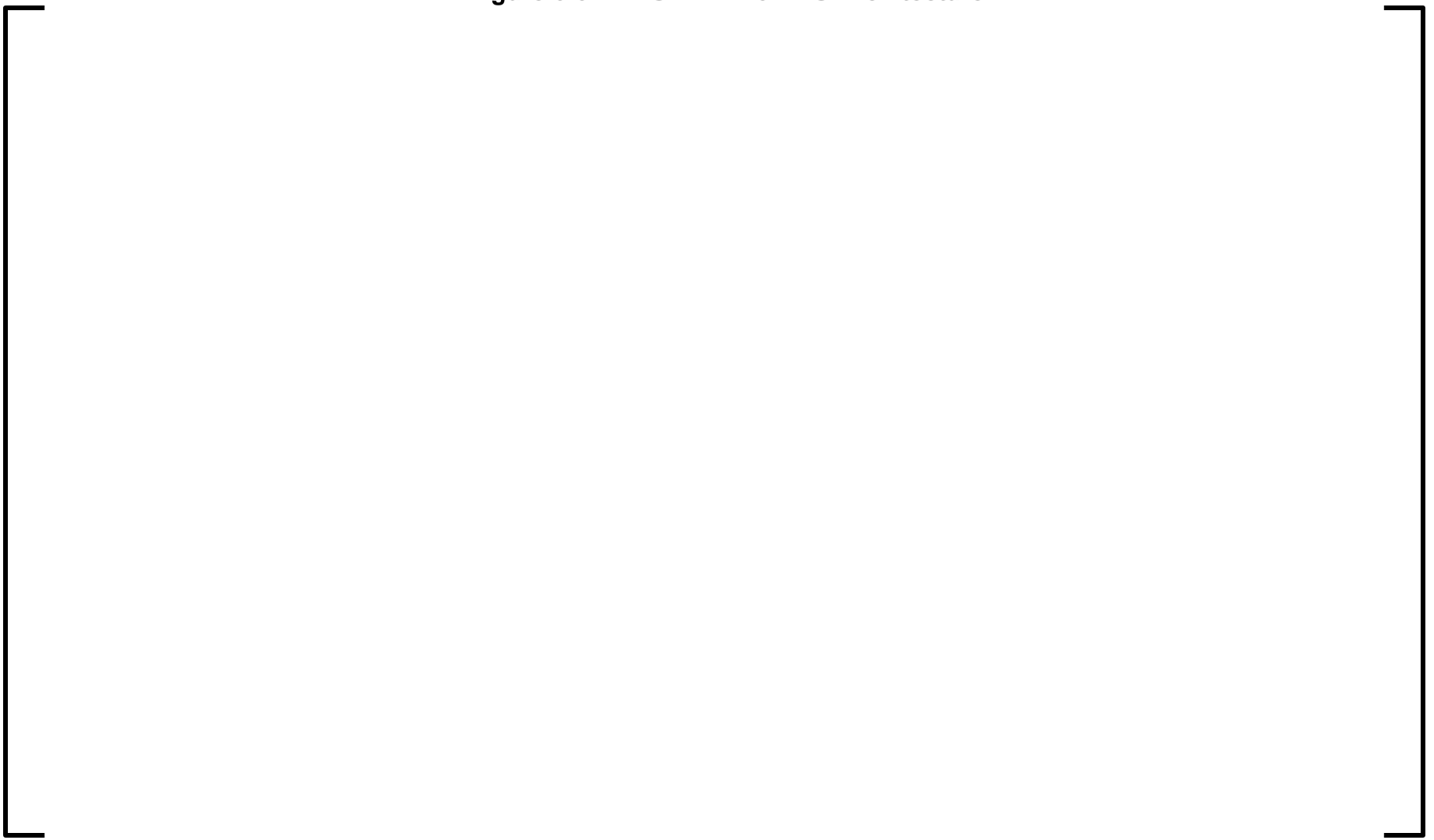


Figure 6-7—RAU1 – Div 4 APU Architecture

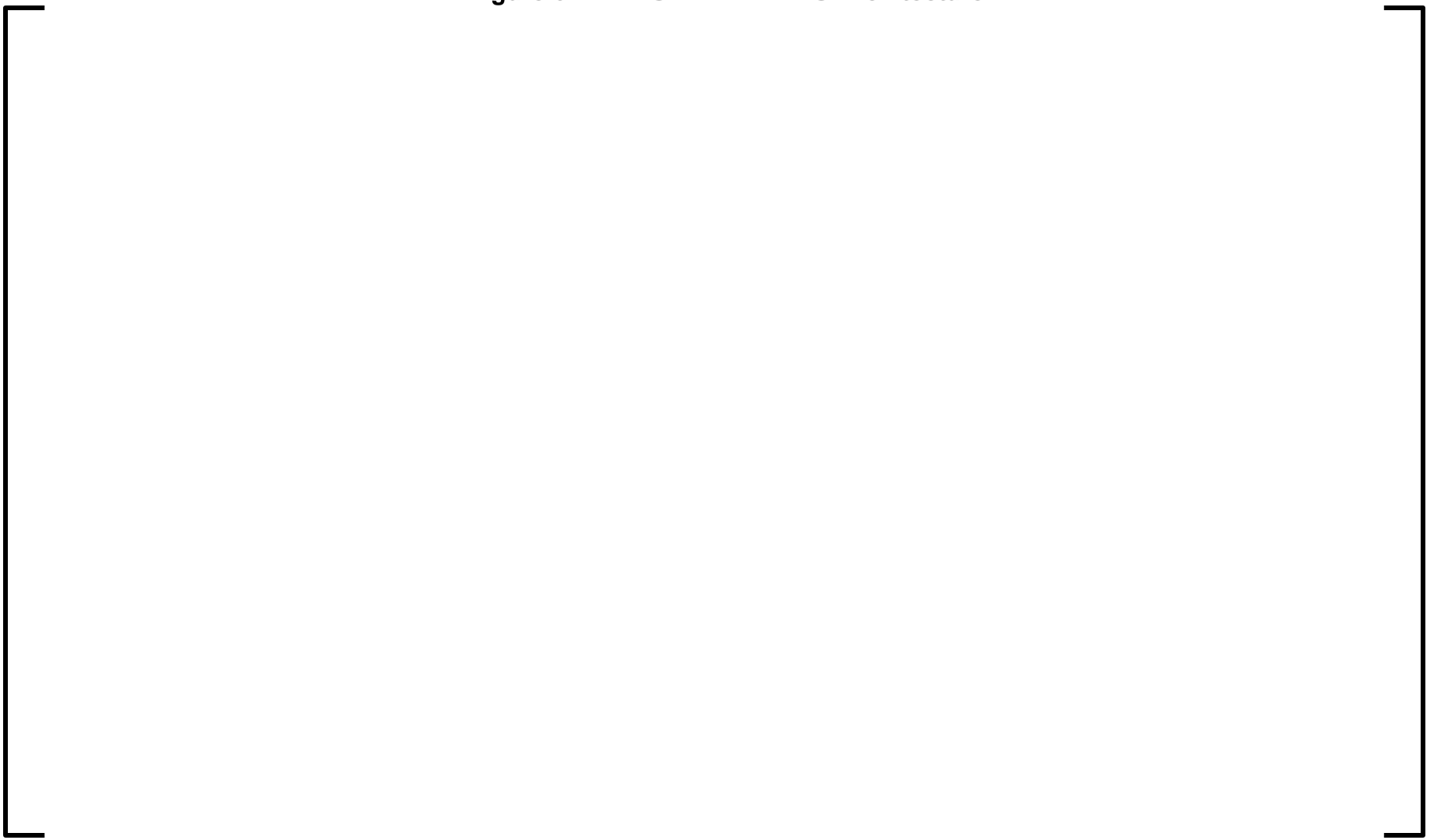


Figure 6-8—RAU2 – APU Architecture

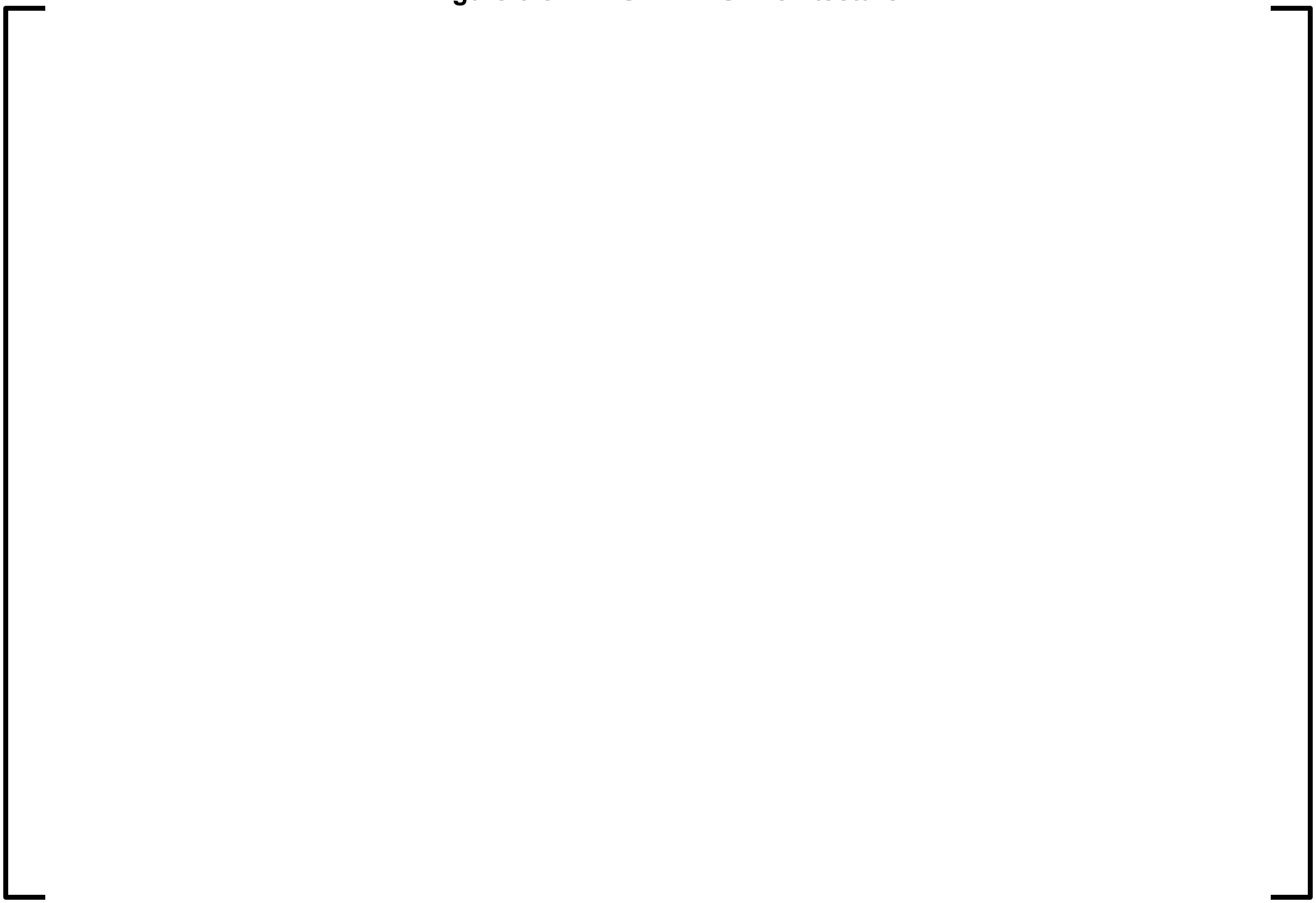


Figure 6-9—Subsystem A Div 1 APU – ALU Architecture

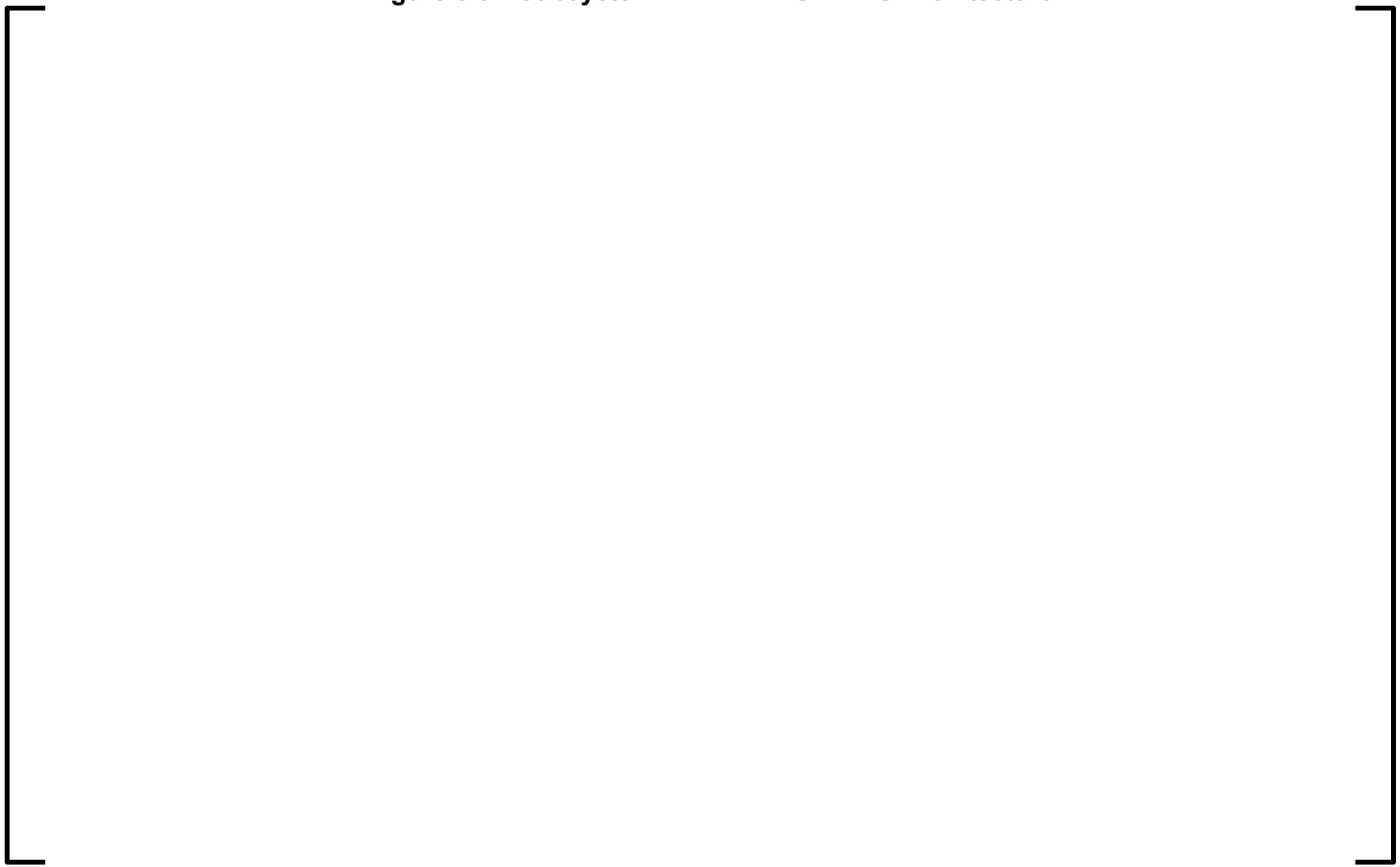


Figure 6-10—Subsystem A Div 2 APU – ALU Architecture

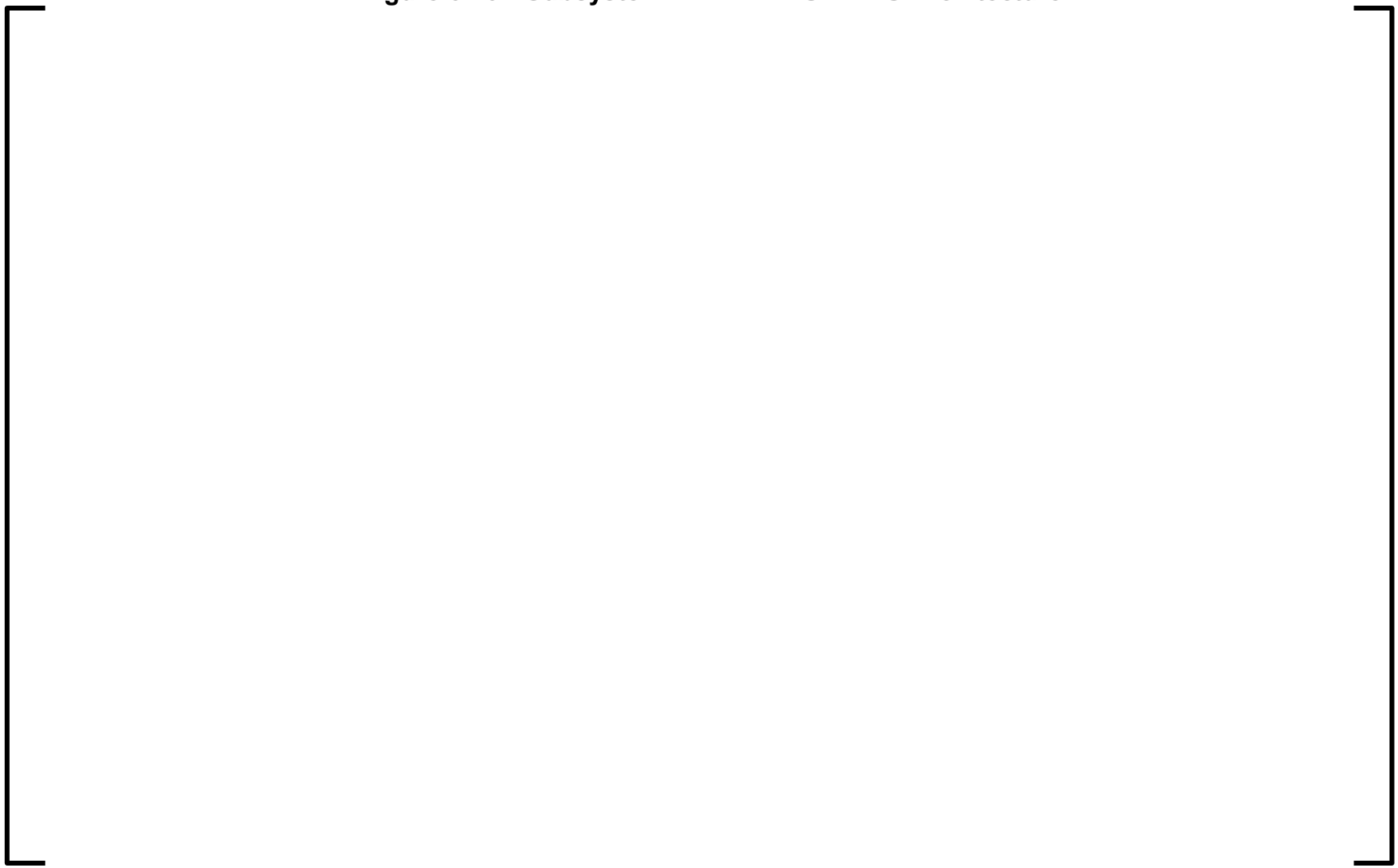


Figure 6-11—Subsystem A Div 3 APU – ALU Architecture

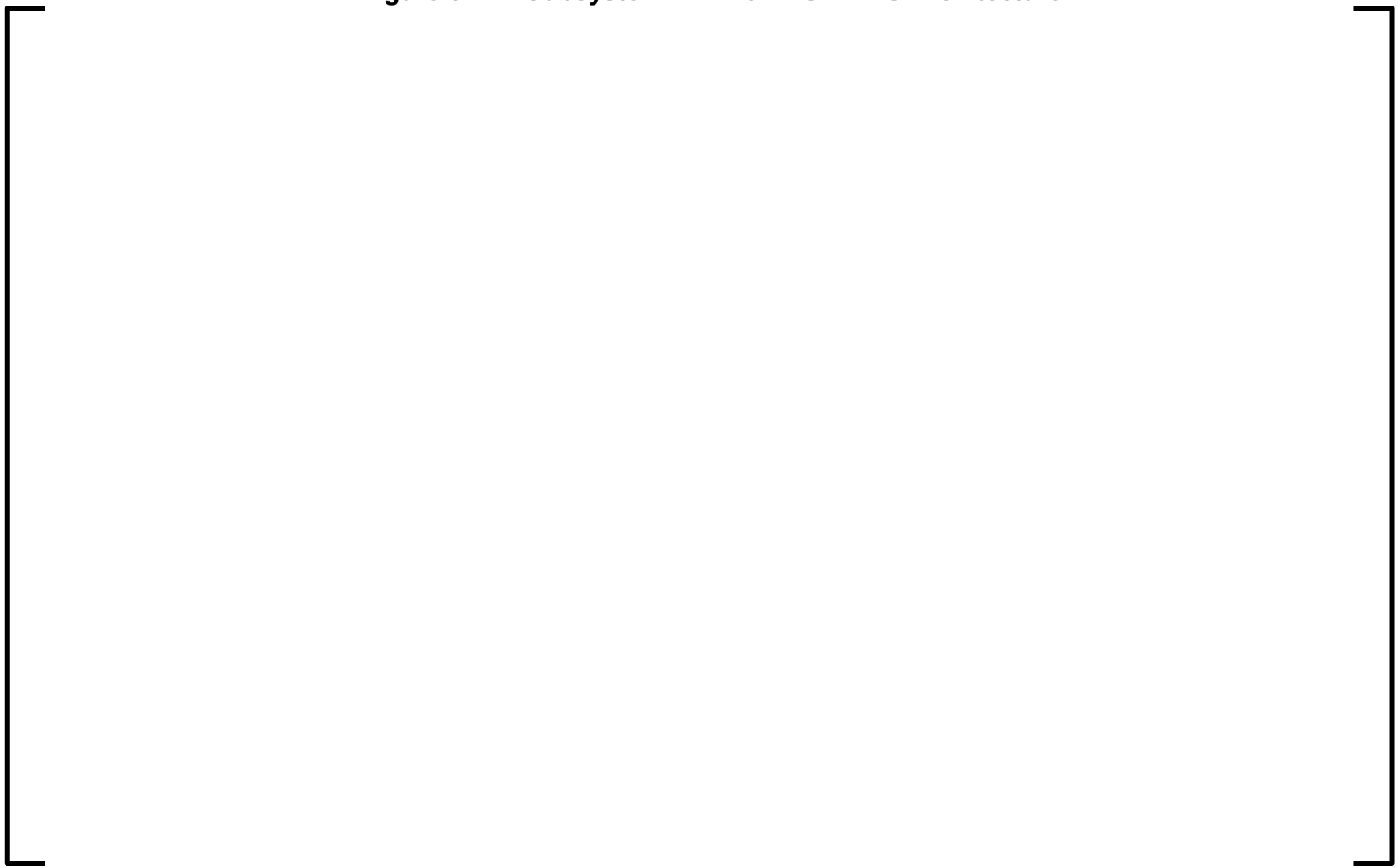


Figure 6-12—Subsystem A Div 4 APU – ALU Architecture

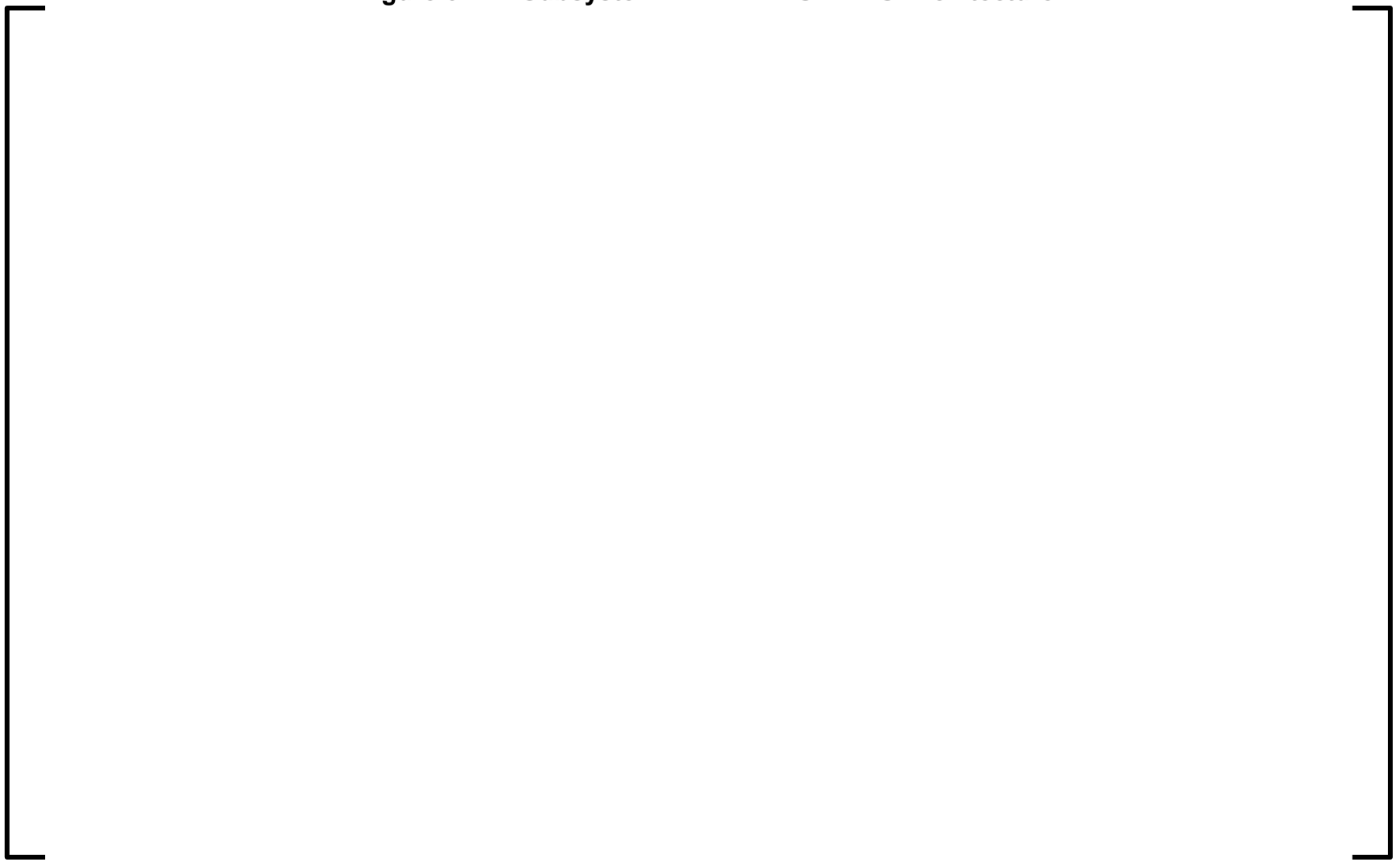


Figure 6-13—Subsystem B Div 1 APU – ALU Architecture

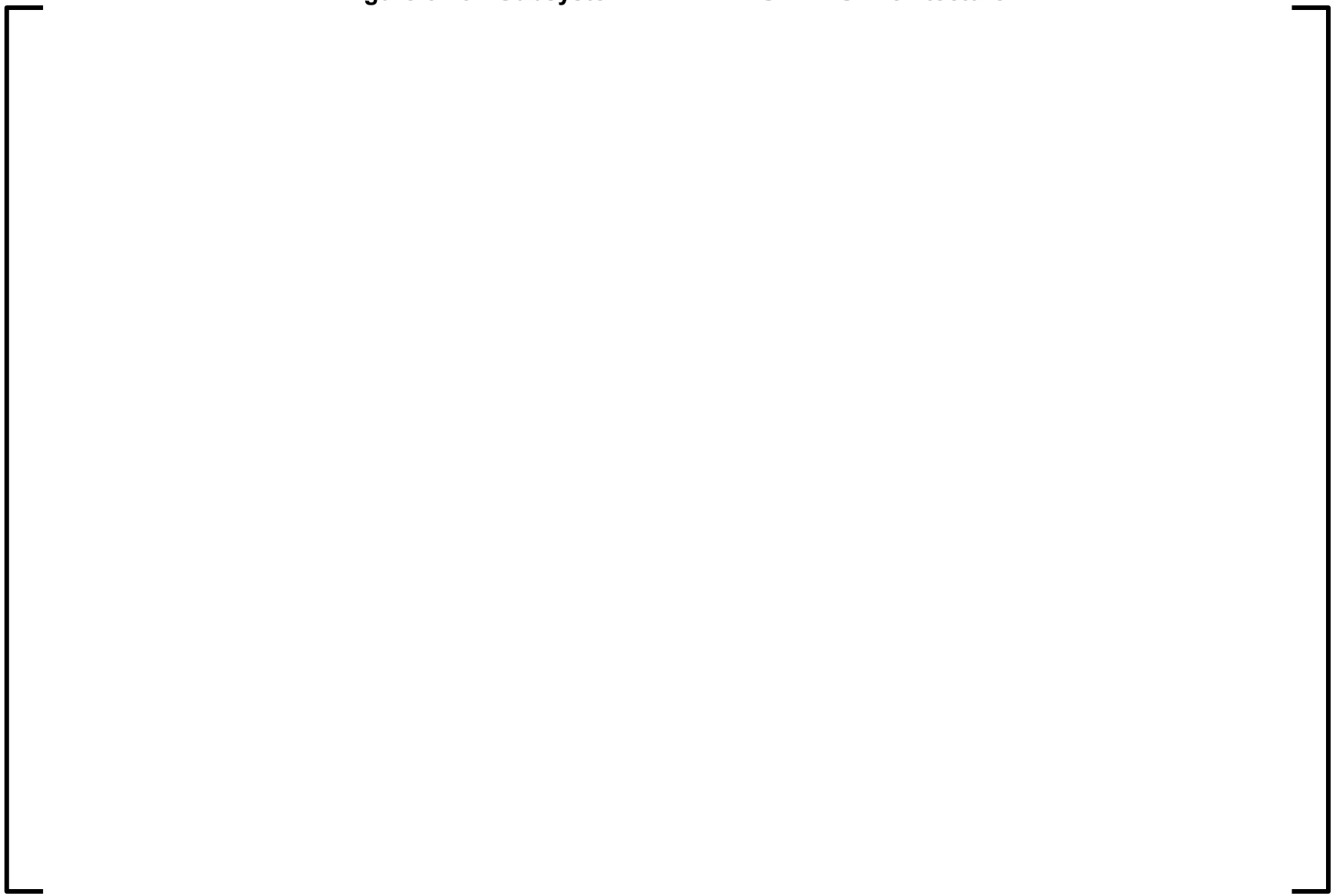


Figure 6-14—Subsystem B Div 2 APU – ALU Architecture

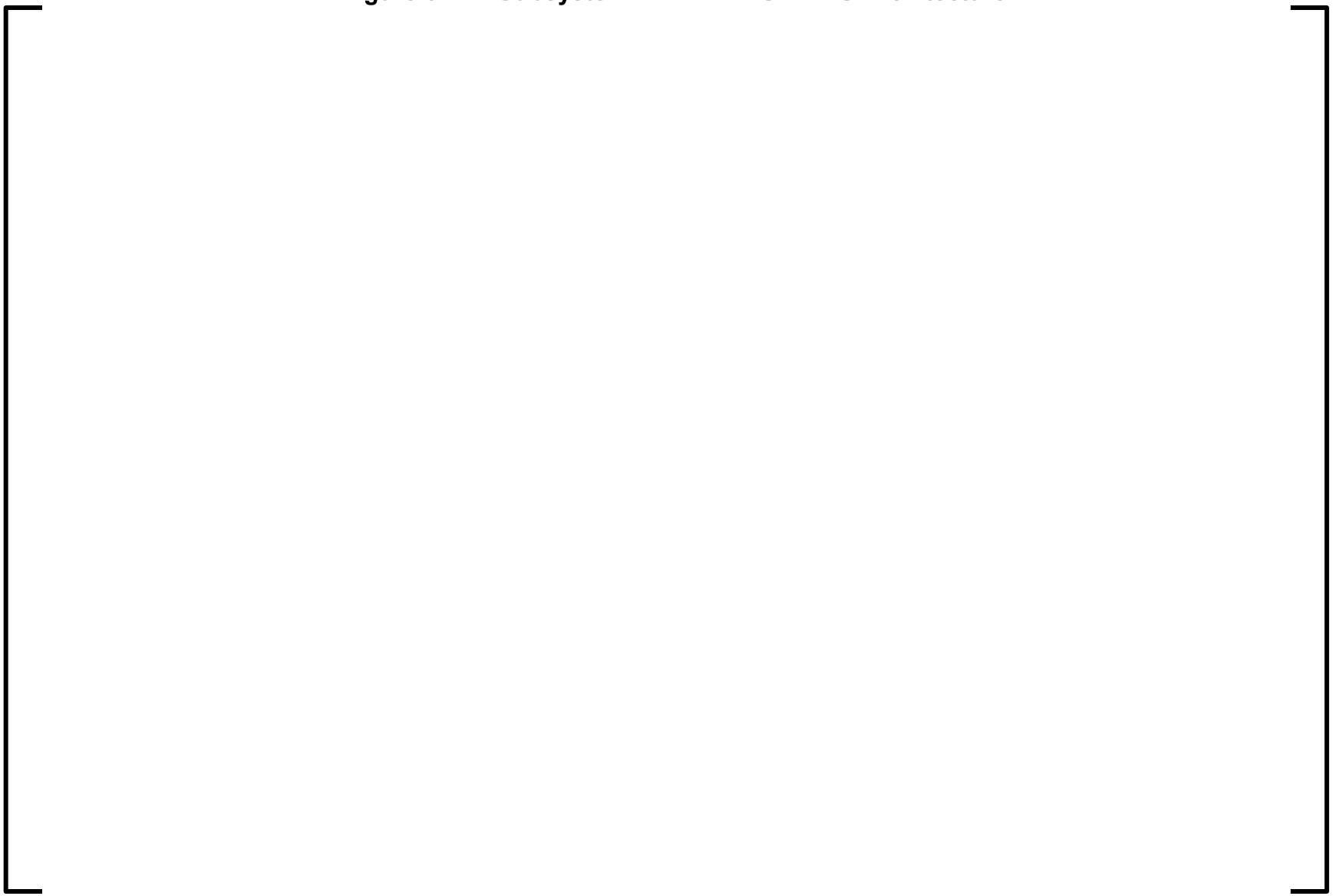


Figure 6-15—Subsystem B Div 3 APU – ALU Architecture

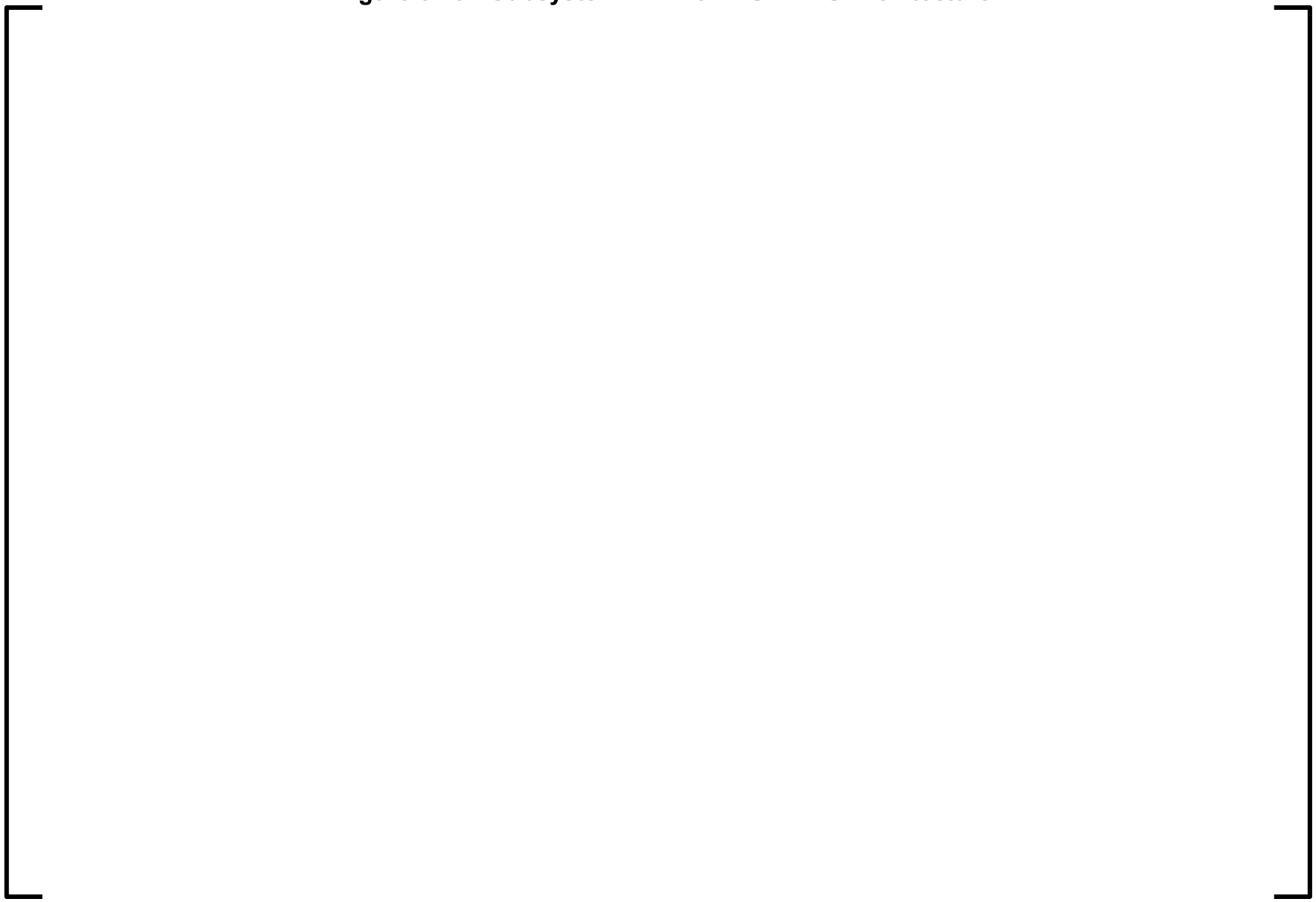


Figure 6-16—Subsystem B Div 4 APU – ALU Architecture

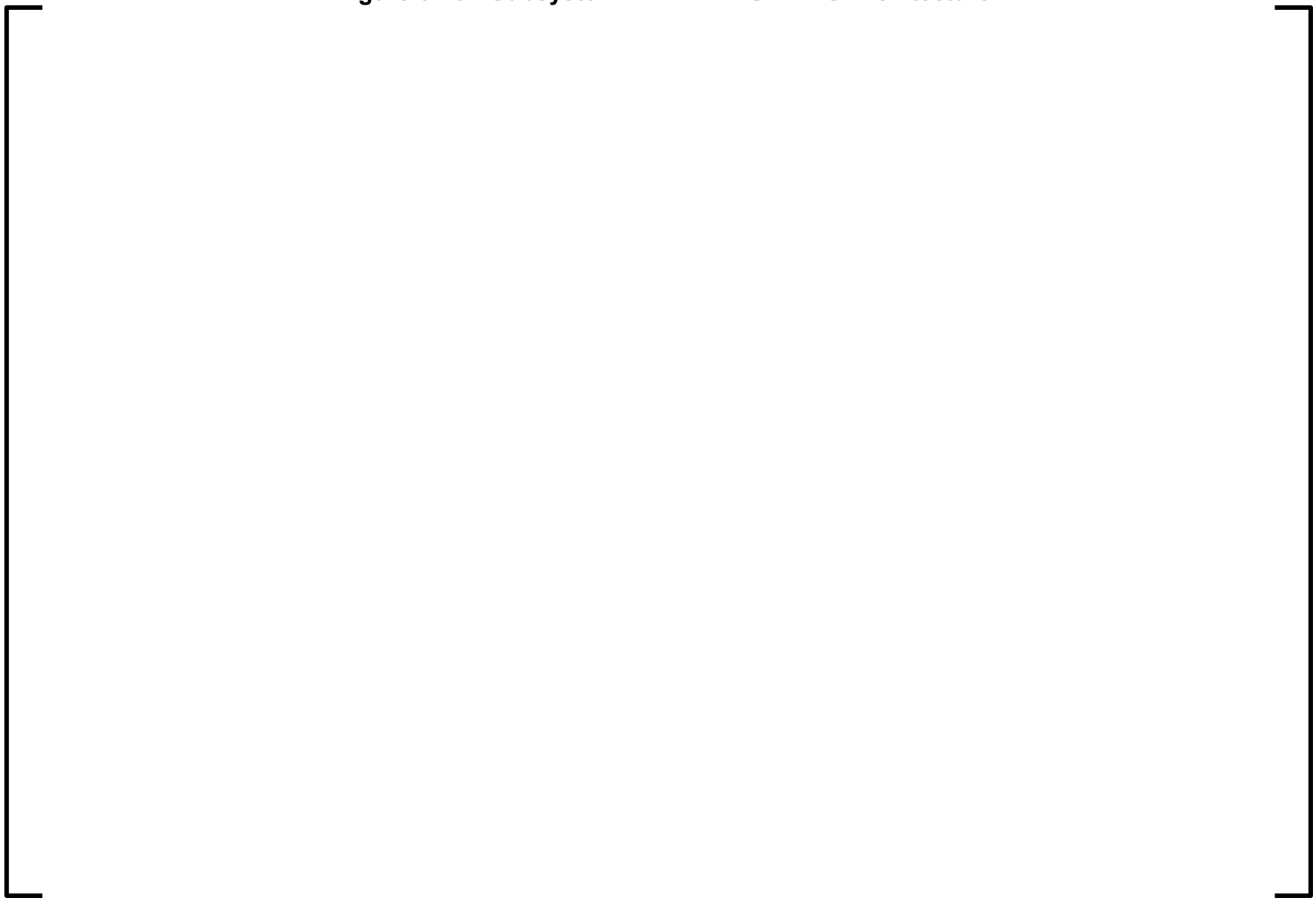


Figure 6-17—MSI-MU – APU Architecture

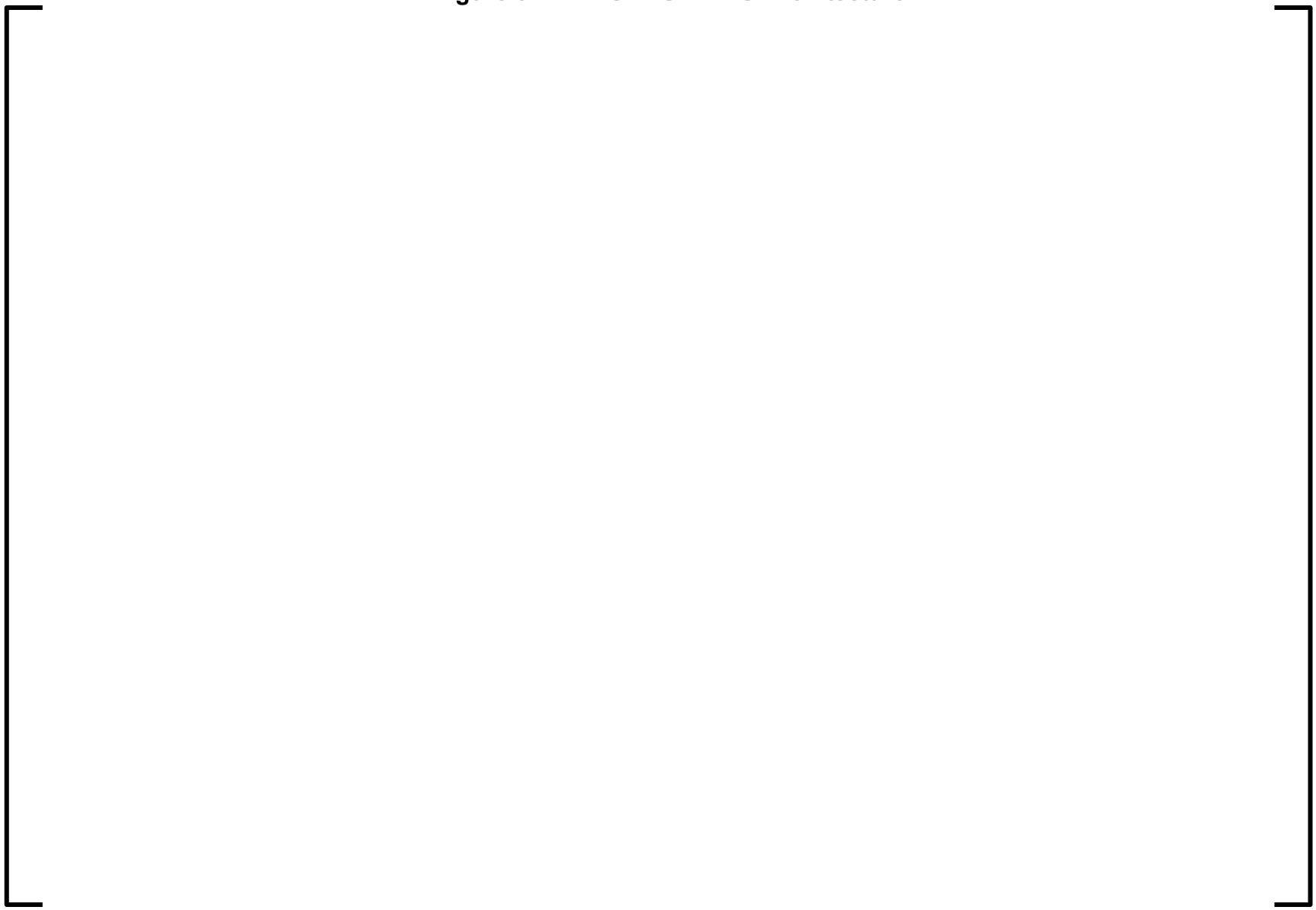


Figure 6-18—MSI-MU – RCCA – RAU – ALU – MSI-AU Architecture

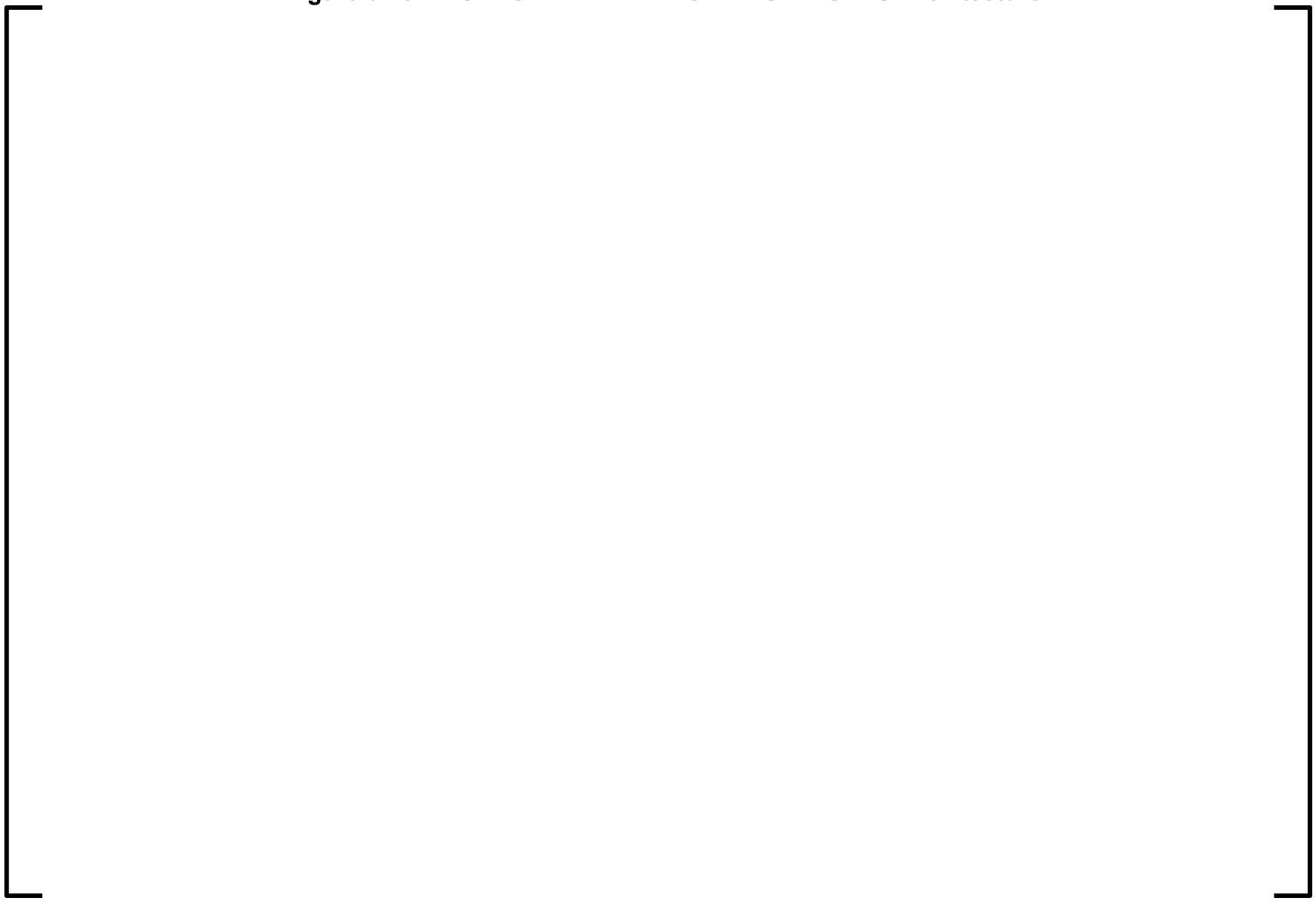


Figure 6-19—MSI-MU – PI Architecture

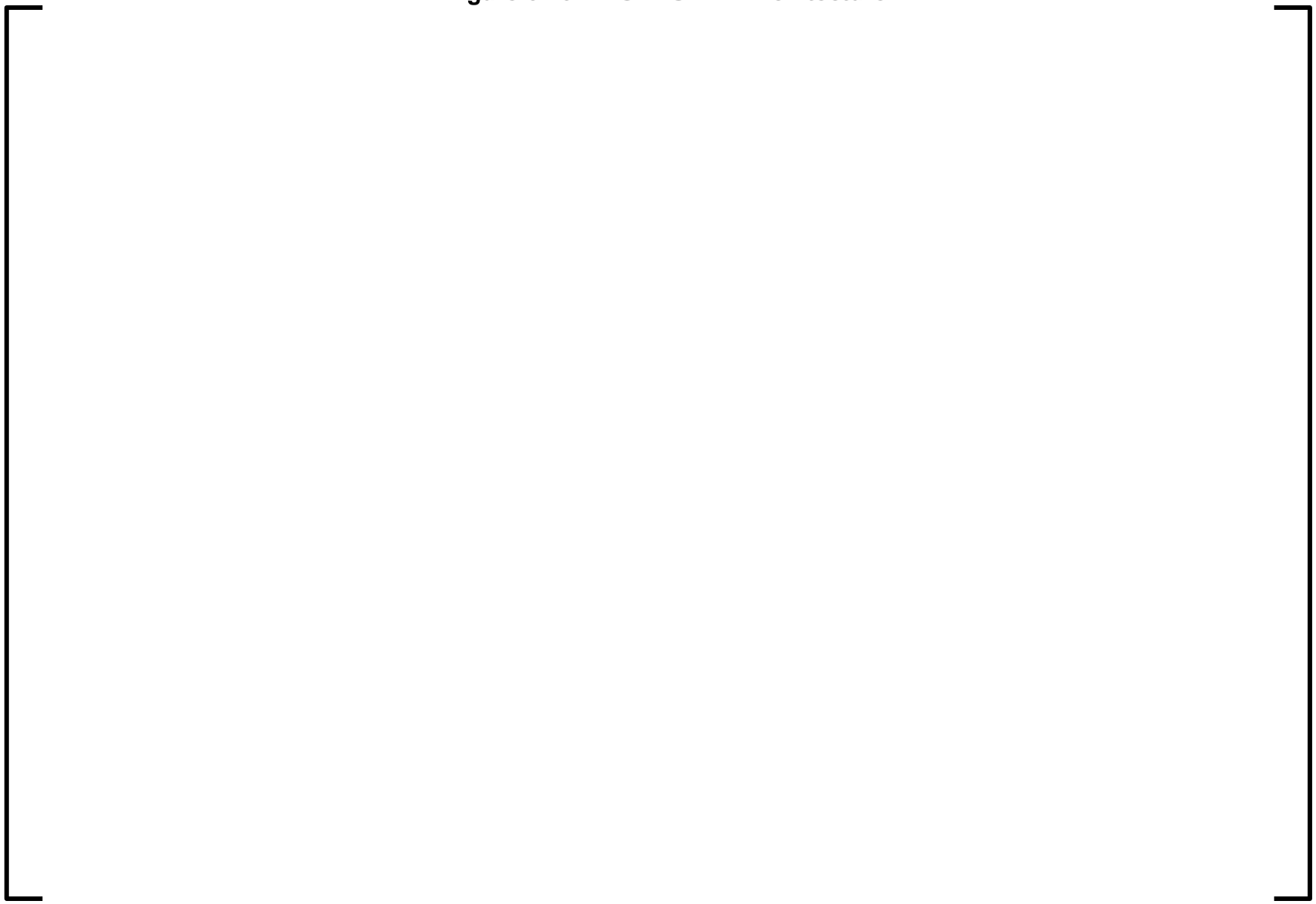
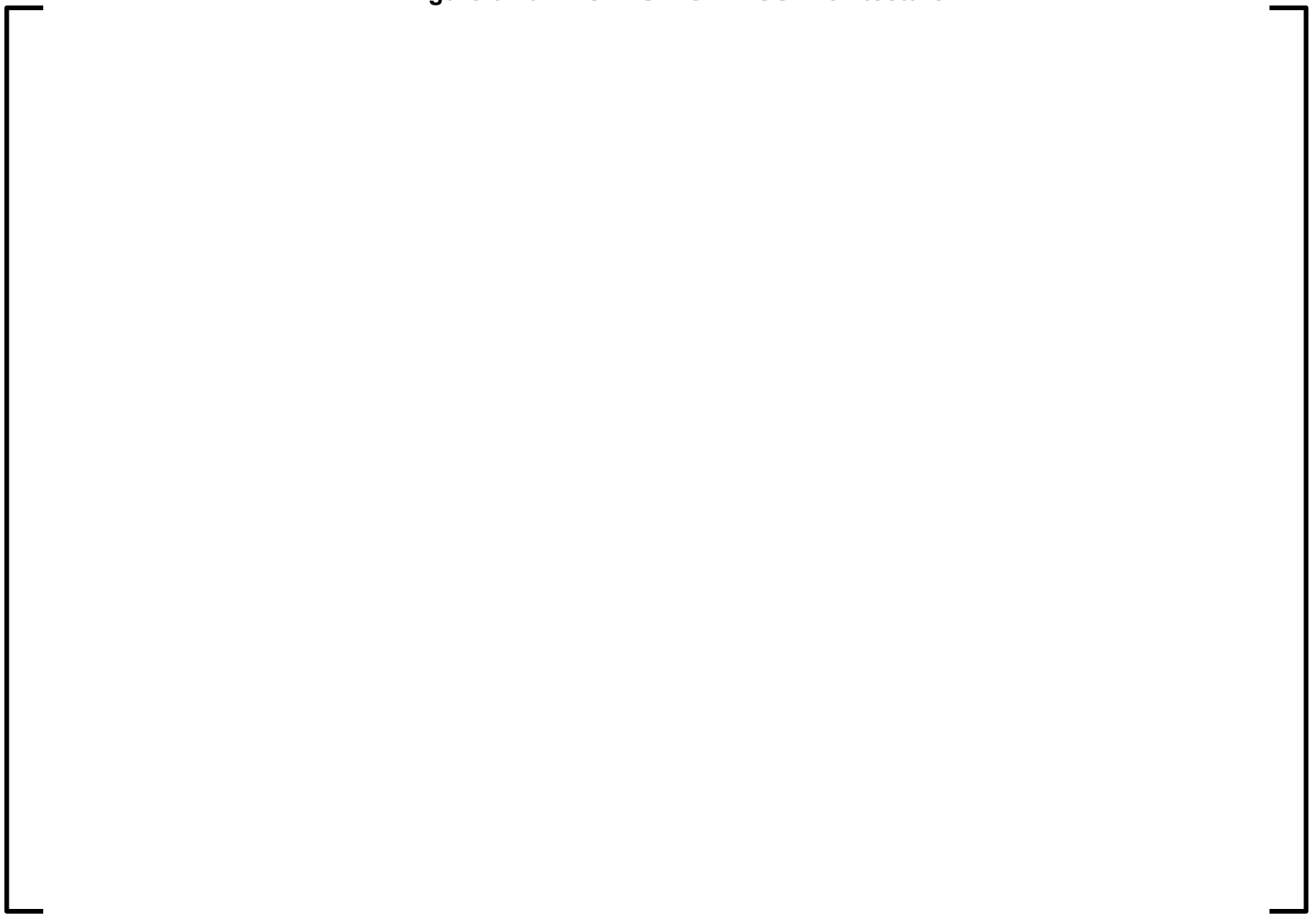


Figure 6-20—MSI-MU – GW – SU Architecture



7.0 REACTOR TRIP

7.1 *Typical Automatic Reactor Trip Sequence*

Figure 7-1 represents a typical RT sequence, excluding functions using the SPND as inputs. The typical sequence utilizes only safety related sensor inputs 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 typical 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 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 sent 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 7.5), resulting in an RT output.

- The RT outputs from each subsystem within a division are then combined in a hardwired “functional OR” logic (Section 7.5), resulting in a divisional RT order. The divisional RT order is propagated to the corresponding divisional trip devices.

7.2 *SPND Based Automatic Reactor Trip Sequence*

7.3 *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 ensure that an invalid signal is marked with a faulty status before reaching the voting function are described in Section 7.4.

7.4 *Identification of Invalid Signals*

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

7.5 *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 7-3.

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 digital outputs of the ALU being 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.

7.6 *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, 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) to bypass 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's automatic RT functions.

There are four dedicated RT buttons in the remote shutdown station (RSS), one for each division. These buttons are hardwired to the shunt trip coils of the RT breakers, and are not included in the logic of the PS. Figure 7-4 illustrates the manual RT concept.

7.7 *Reactor Trip Devices*

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

- Trip breakers (safety-related)
- Trip contactors (safety-related)
- Transistors that control power to the control rod drive mechanisms (CRDM) operating coils (non-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 7-5 and Figure 7-6 show the arrangement of the various RT actuators.

7.8 *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)

7.9 *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.

7.10 *Transistors of CRDM Operating Coils*

The transistors that control power to the CRDM operating coils are not safety-related trip devices. However, they are the fastest acting of the trip devices and allow the safety-related trip breakers and contactors to open under unloaded conditions. Each transistor that controls power to a CRDM is de-energized based on the result of 2 out of 4 voting on the divisional RT orders from the four divisions of the PS.

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

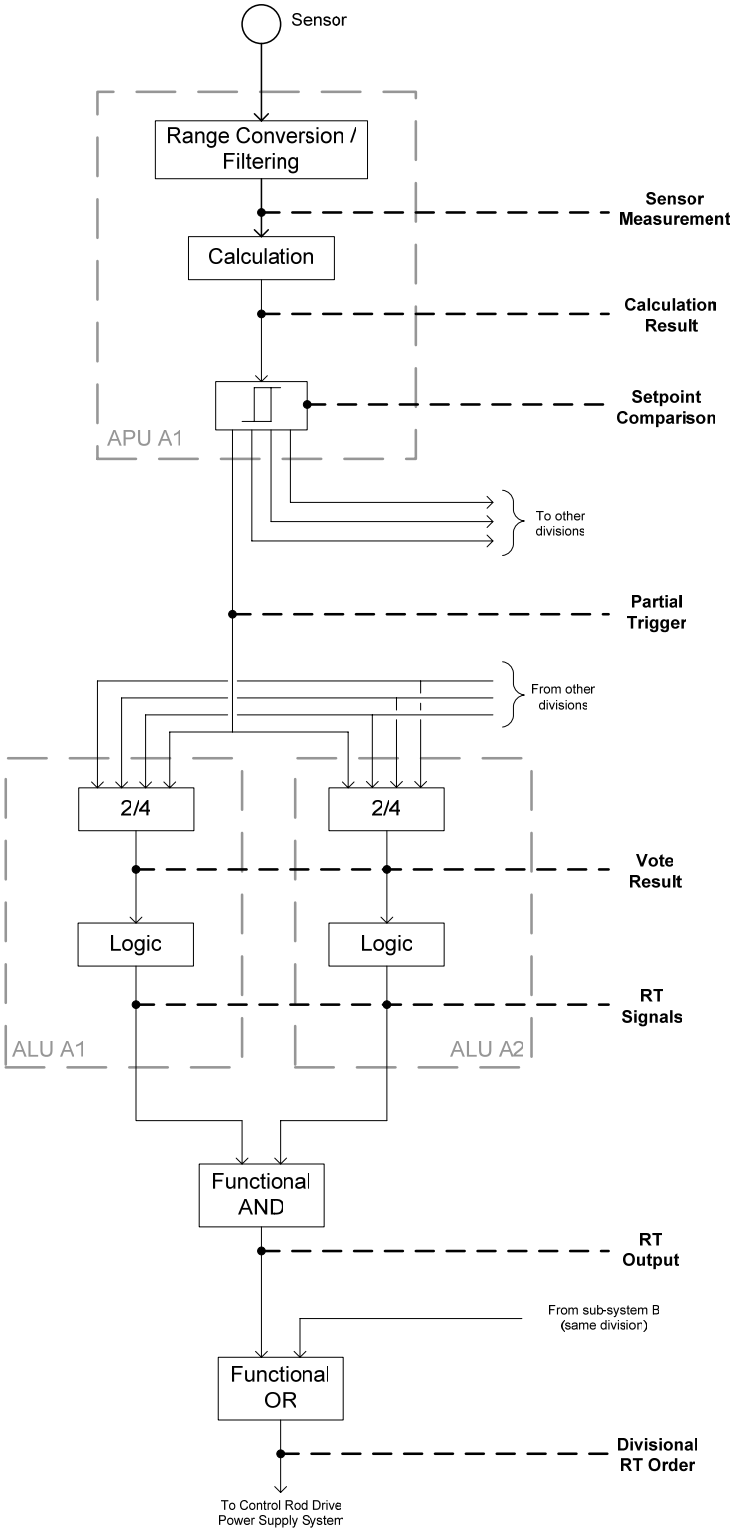


Figure 7-2—SPND-Based Reactor Trip Sequence (One Division)

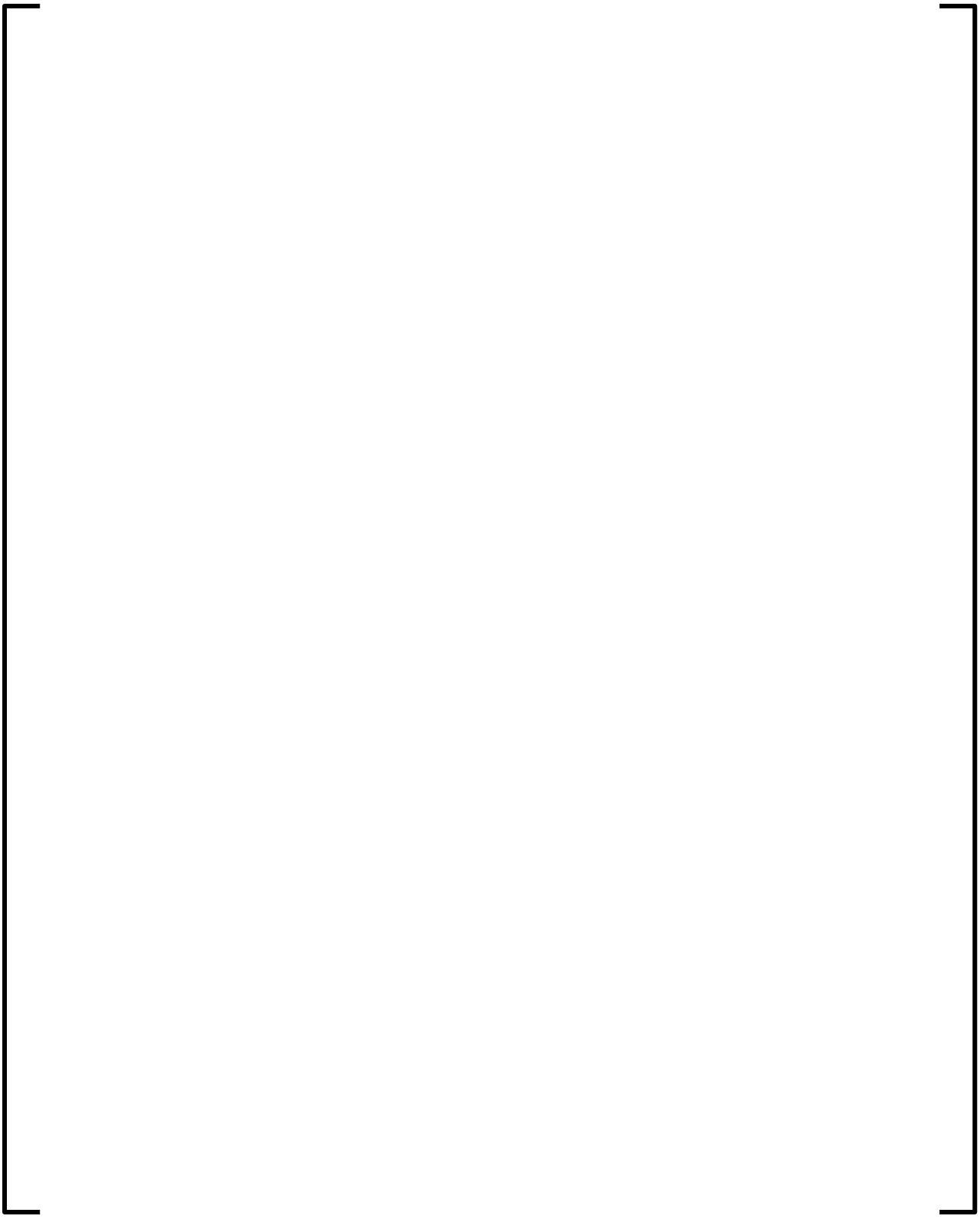


Figure 7-3—Reactor Trip Outputs in One Division

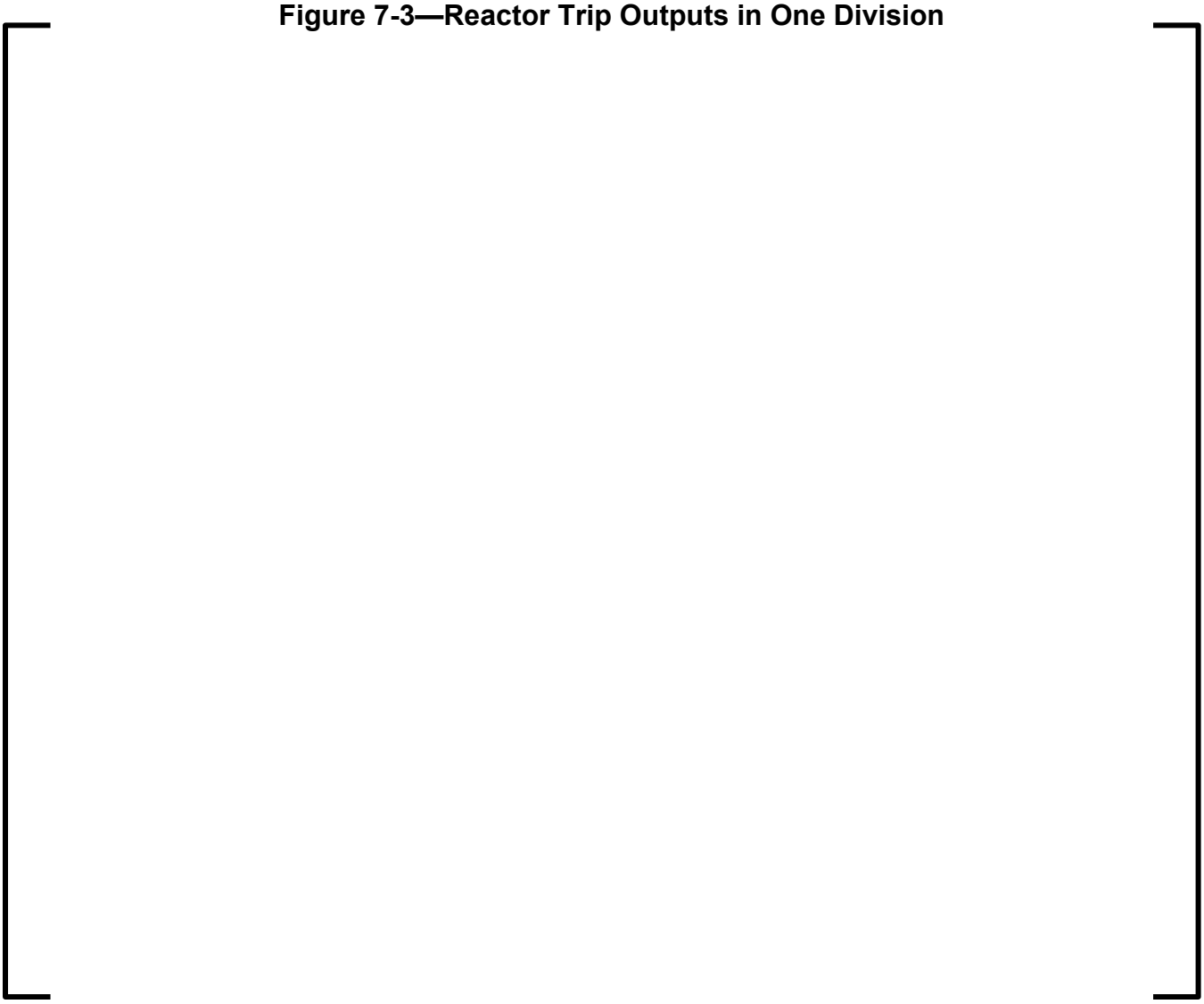


Figure 7-4—Concept for Manual Reactor Trip (One Division)

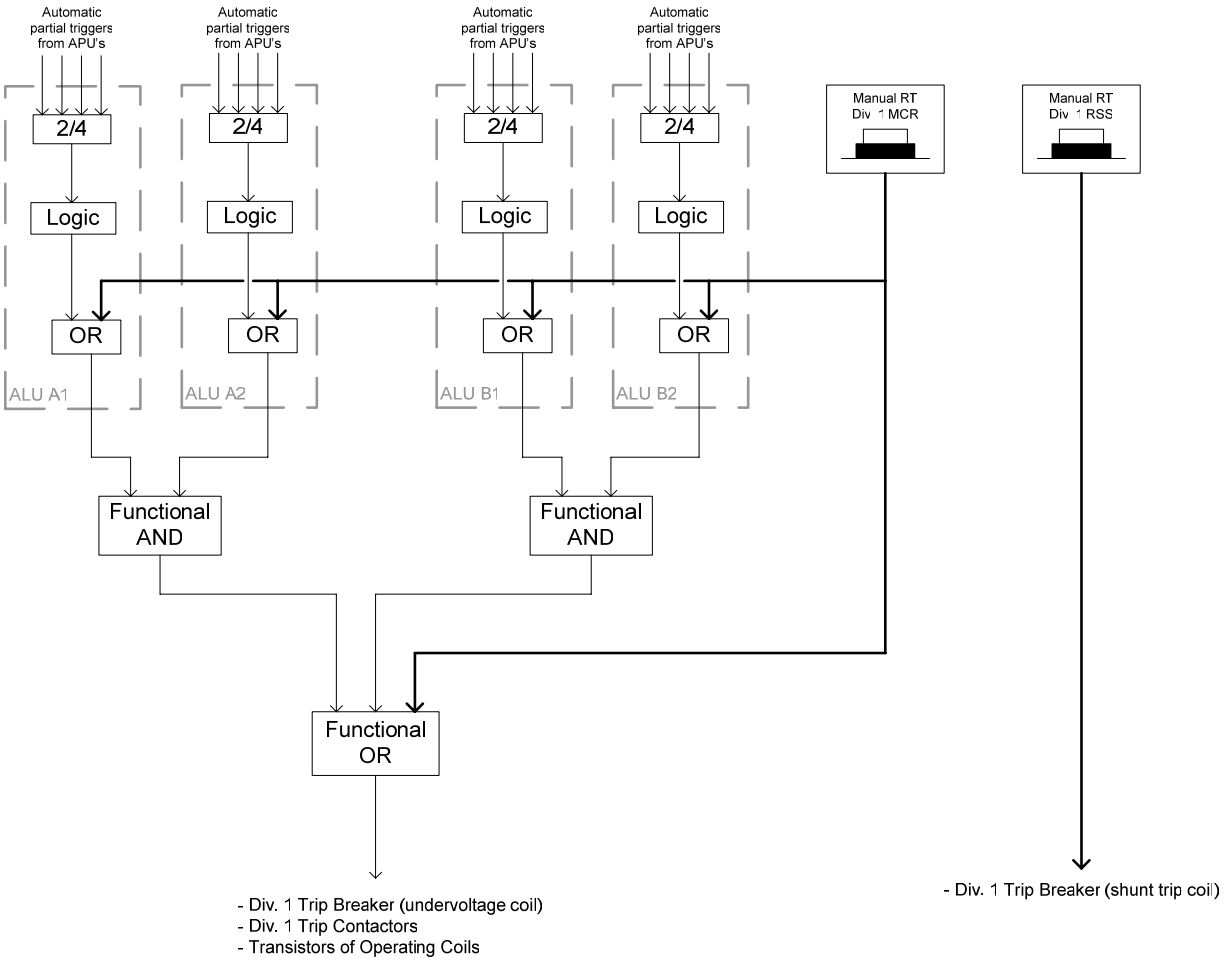


Figure 7-5—Reactor Trip Breakers and Reactor Trip Contactors

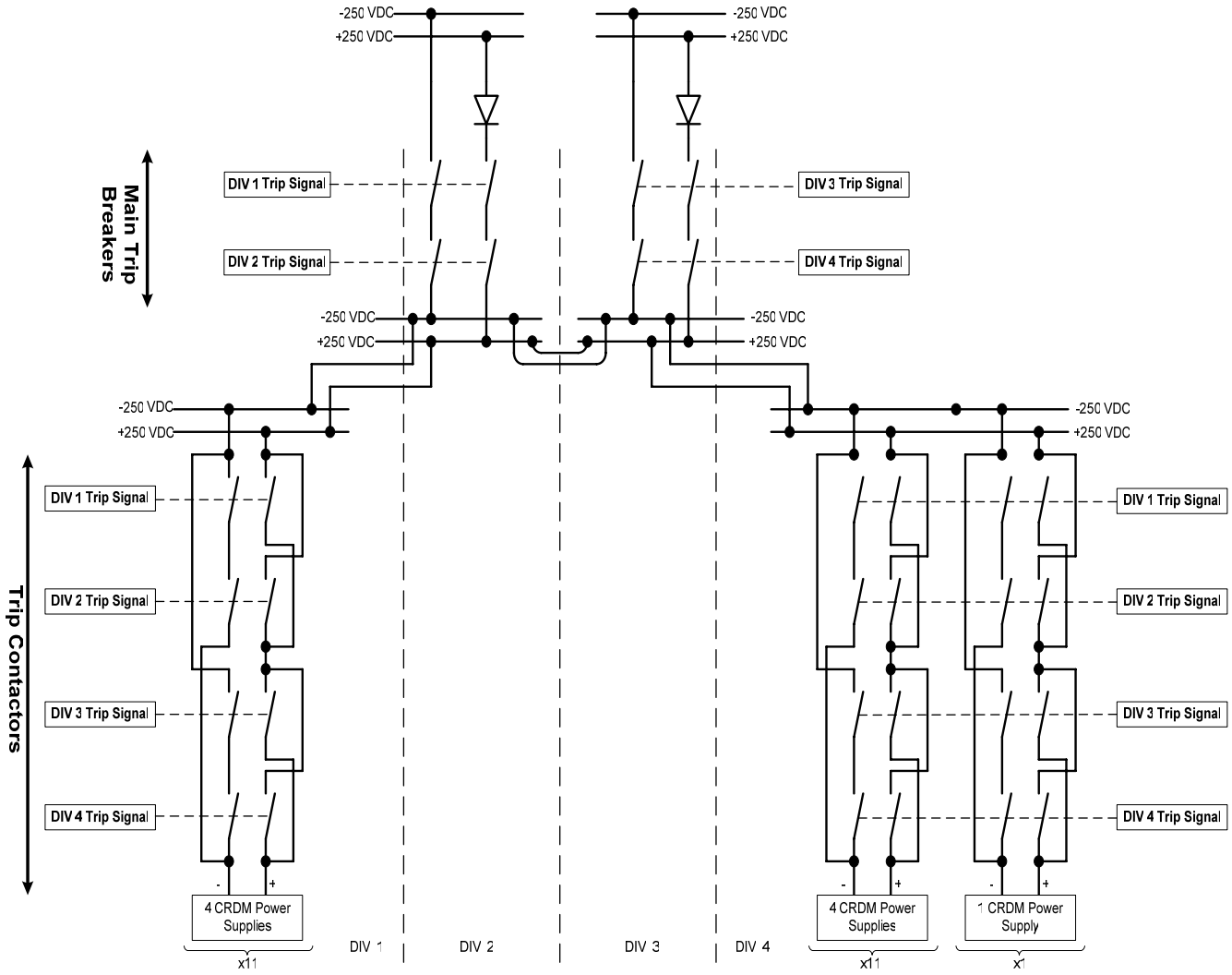
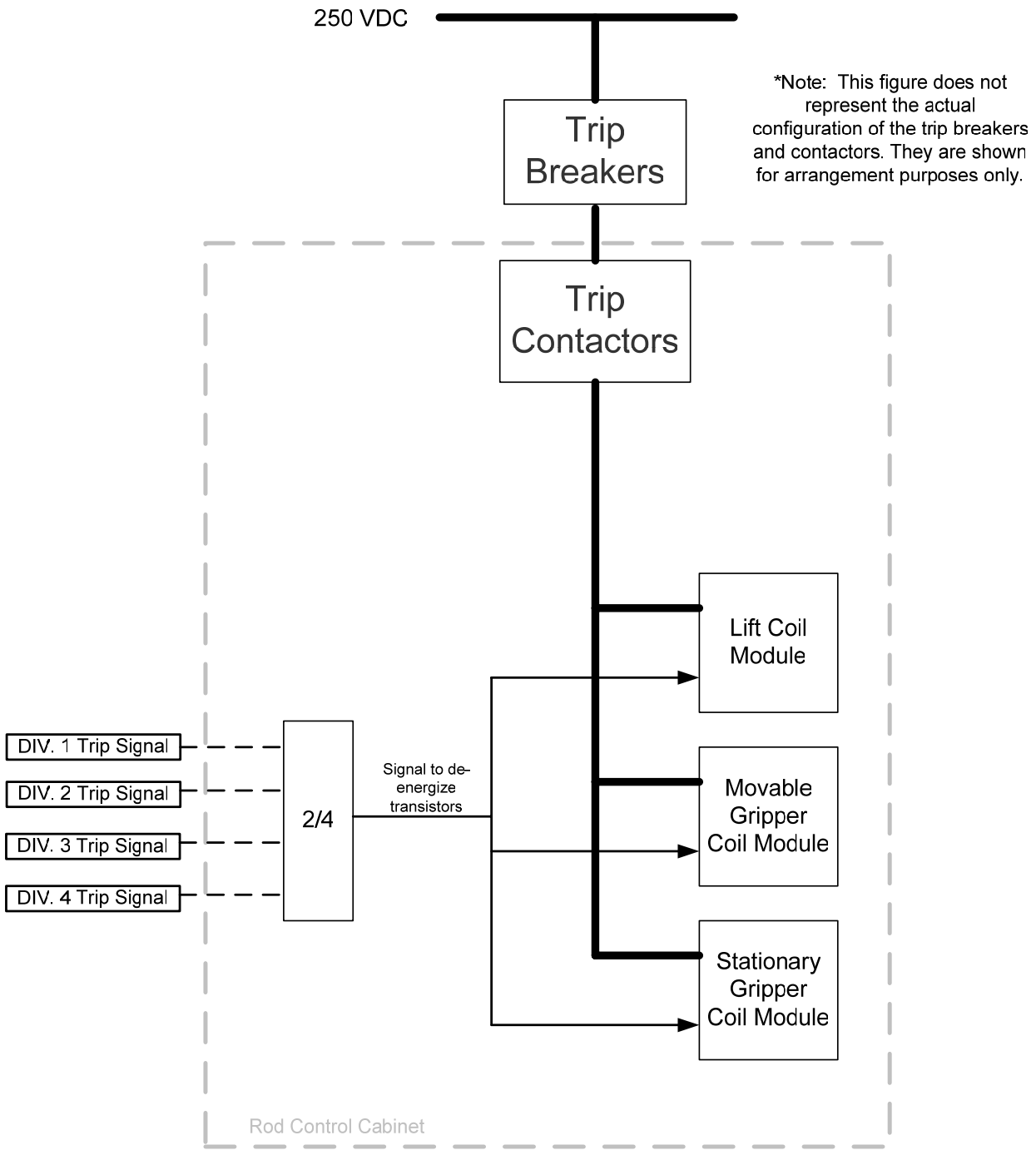


Figure 7-6—Reactor Trip Signals to Rod Control Transistors



8.0 ENGINEERED SAFETY FEATURES ACTUATION

8.1 *Typical Automatic ESF Actuation Sequence*

The typical ESF actuation sequence is represented by Figure 8-1, and is similar to the typical RT sequence. The typical ESF actuation is performed in two layers (i.e., 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 typical ESF actuation sequence is as follows:

- One APU in each division of the PS acquires one-fourth of the redundant sensors that are inputs to 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 sent 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 ensure completion of the function.

- The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired logical OR; therefore, either of the redundant ALU can actuate an ESF function. The result of the logical 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. The concept of modification toward actuation is described in Section 7.3. The concept of modification toward no-actuation is 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 2/2
- 3 faulty input signals: No actuation
- 4 faulty input signals No actuation

Section 7.4 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, each ESF actuator is assigned a dedicated PAC module. This module collects the actuation signals from multiple I&C systems and sends the proper actuation order to the actuator according to pre-defined priority assignments.

The ESF actuation signals are latched in the ALU, so that the actuation order remains until the actuation signal is reset. When this actuation order is present as an input to the PAC module, the associated actuator cannot be influenced by conflicting commands

of lower priority from other I&C systems. When the ESF actuation signal is reset in the ALU, the actuation order is removed from the input of the PAC module. Once the PS actuation order is removed, orders of lower priority are then allowed to influence the actuator.

8.4 *Divisional Assignments – ESF Actuation Outputs*

The determination of 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 the 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 two redundant ALU within the PS division can actuate the same ESF function.

Overall plant safety may dictate that special attention is paid to preventing 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 is closure of the MSIV. There are two redundant mechanical paths (one on each side of the valve in Figure 8-2); either can realize 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 *Manual ESF Actuations*

In addition to the automatic ESF actuation functions performed by the PS, the capability to manually initiate these functions is provided in the MCR. These manual functions are implemented at the system level and perform the same actions as the automatic functions. The U.S. EPR design includes the ability to manually manipulate these actuators at the individual component level from the non-safety-related HMI; however, the system level actuations discussed in this section are implemented completely through Class 1E actuation paths.

The implementation of manual system level actuation of ESF functions is determined on a case-by-case basis. Each manual ESF actuation function is unique because of the number and types of actuators involved, the level of sequencing required, and the number of associated actions required (e.g., auxiliary or support systems). The implementation of these functions also takes into account diversity requirements imposed by defense-in-depth and diversity concepts. Therefore, several typical implementation designs are identified and applied to the manual initiation functions to satisfy the requirements imposed on each individual function.

At the level of the PAC modules, priority between the automatic functions of the PS and the manual system level initiation functions is determined on a case-by-case basis. In some cases, the automatic and manual functions could be combined in a hardwired OR logic to give them equal priority at the PAC level. The manual system level initiation functions have priority over actuation requests from non-safety-related control functions or individual component control from the non-safety-related HMI.

8.5.1 *Typical Manual ESF Actuation 1*

Figure 8-3 illustrates the implementation of a manual system level initiation function that utilizes Class 1E hardwired technology and bypasses the PS units. A button in the

MCR or RSS simultaneously closes contacts related to the required actuators. The closed contacts provide actuation signals to the PAC modules attached to the required actuators. This implementation is used for functions that require no sequencing logic. Manual initiation functions that are credited in a defense-in-depth and diversity analysis can be implemented this way because the actuation path is diverse from the automatic functions of the PS.

8.5.2 *Typical Manual ESF Actuation 2*

Figure 8-4 illustrates the implementation of a manual system level initiation function that utilizes a Class 1E logic device and bypasses the PS units. This logic device is diverse from the PS units, uses no software during operation, and is fully testable. A button in the MCR or RSS sends the actuation signal to the logic device to begin the actuation sequence. Feedback from the individual PAC modules can be utilized as inputs to the logic device, which satisfies any sequencing or interlocking requirements. This implementation is used for manual initiation functions that require sequencing or interlocks and are credited in a defense-in-depth and diversity analysis.

8.5.3 *Typical Manual ESF Actuation 3*

Figure 8-5 illustrates the implementation of a manual system level initiation function utilizing the PI. The function bypasses the PS units. A button in the MCR or RSS sends the actuation signal to the PI to begin the actuation sequence. TXS function blocks can be used in the PI to perform any timing, sequencing, or interlocking required for the initiation function. Although the PI operating system and hardware is not diverse from that of the PS, the application software is significantly different. AREVA NP has not yet determined how this actuation path will be credited in a defense-in-depth and diversity analysis.

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

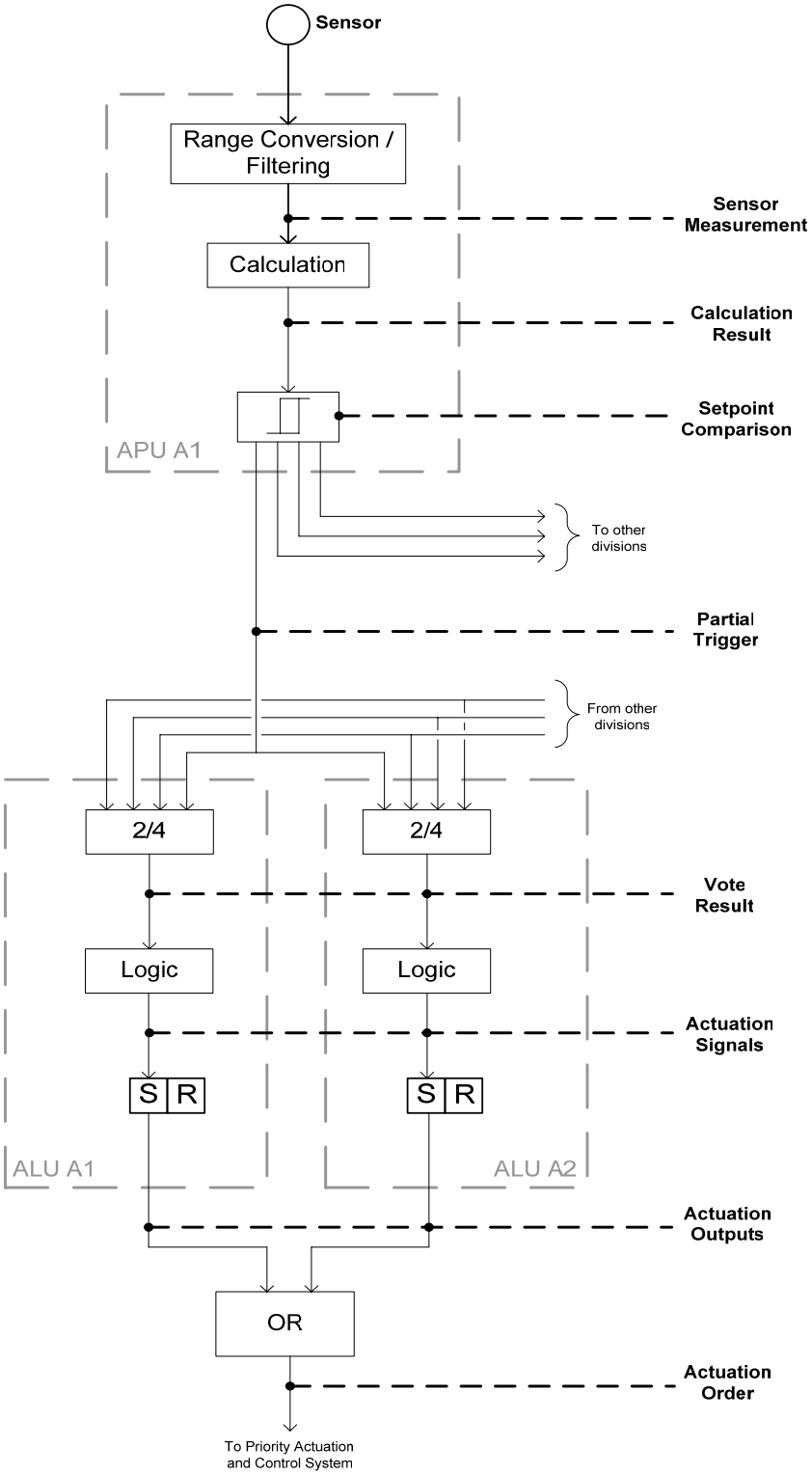


Figure 8-2—Example of PS Divisional Assignment to an ESF Actuation

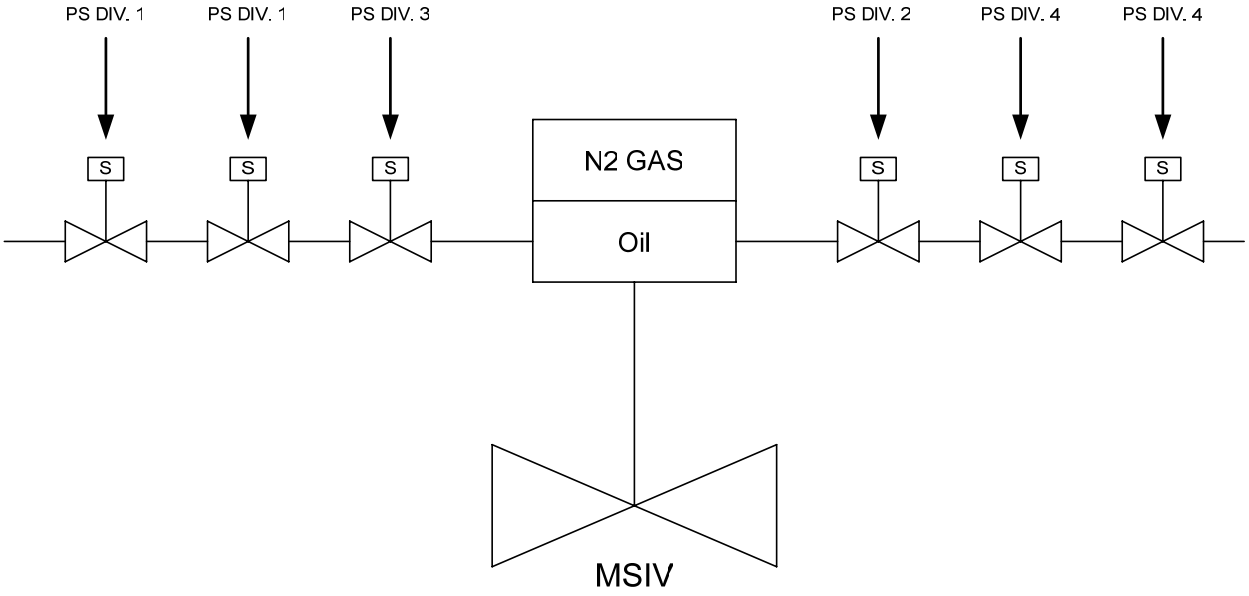


Figure 8-3—Typical #1 for Manual System Level Initiation

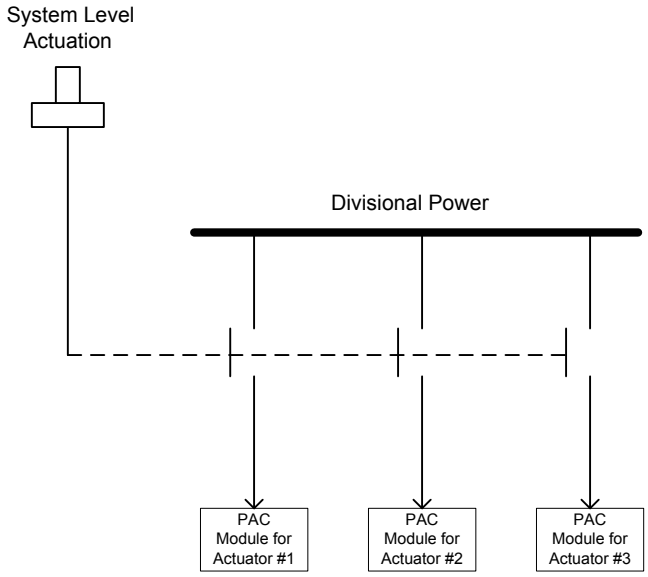


Figure 8-4—Typical #2 for Manual System Level Initiation

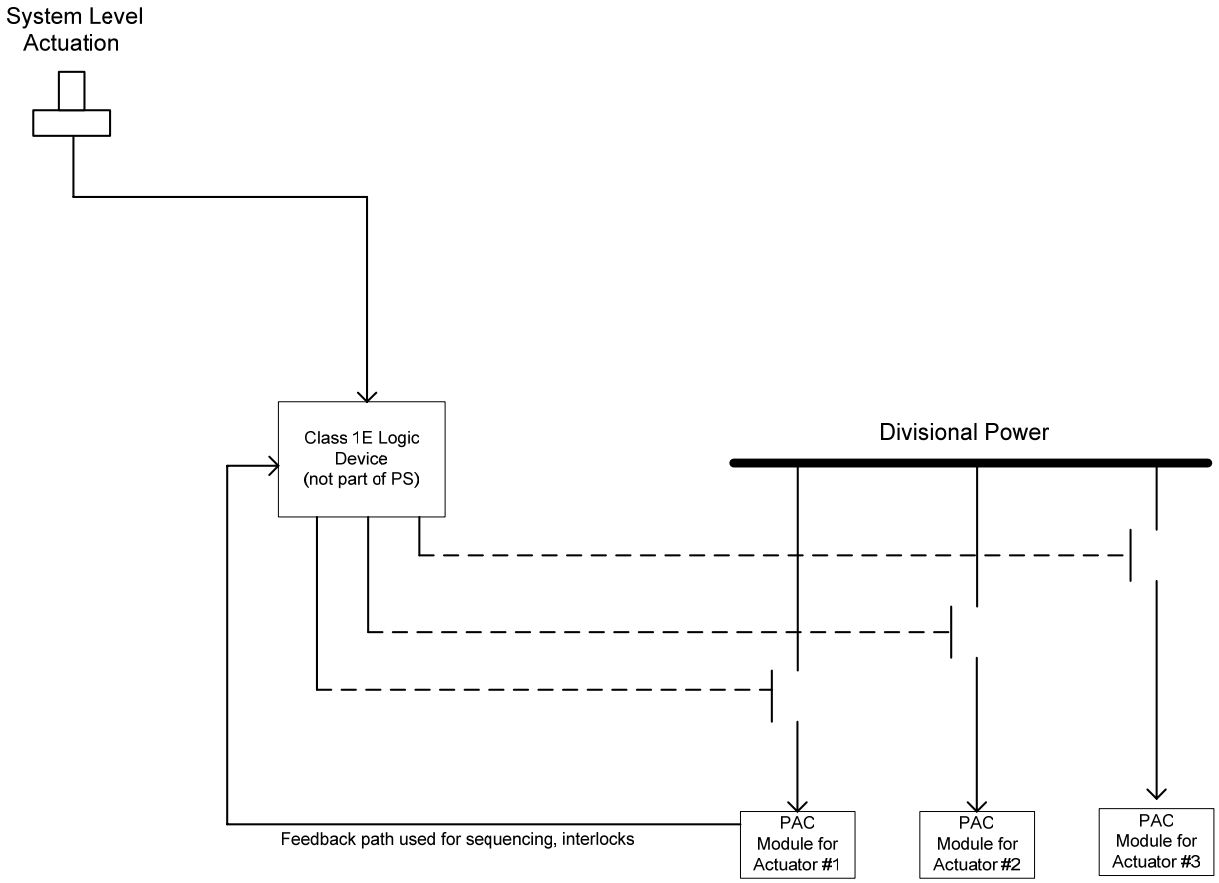
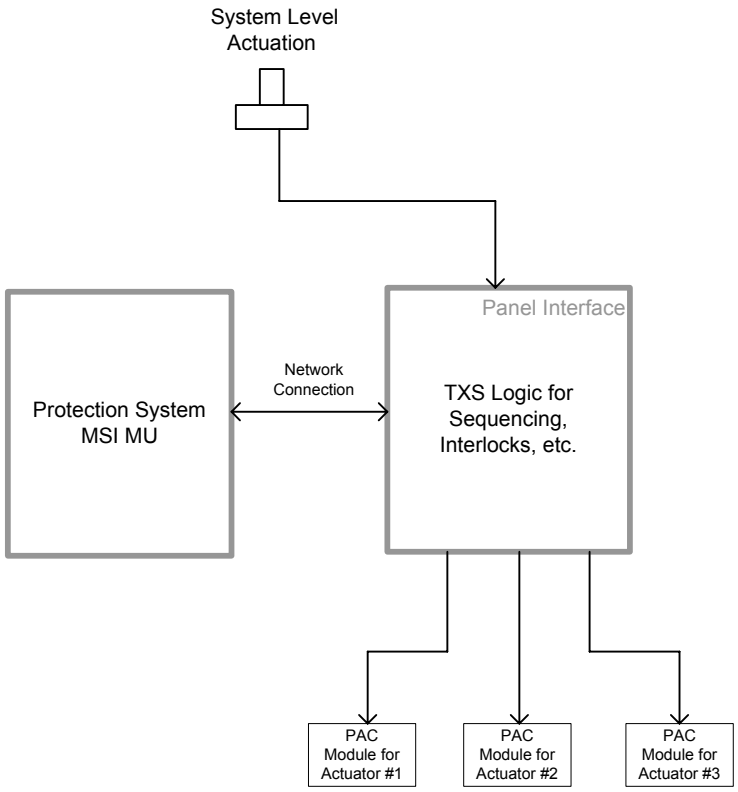


Figure 8-5—Typical #3 for Manual System Level Initiation



9.0 PERMISSIVE SIGNALS

9.1 *Definition*

The PS uses permissive signals to enable or disable certain 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 and/or disable protective functions. Likewise, an inhibited permissive can enable and/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 APU layer 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:

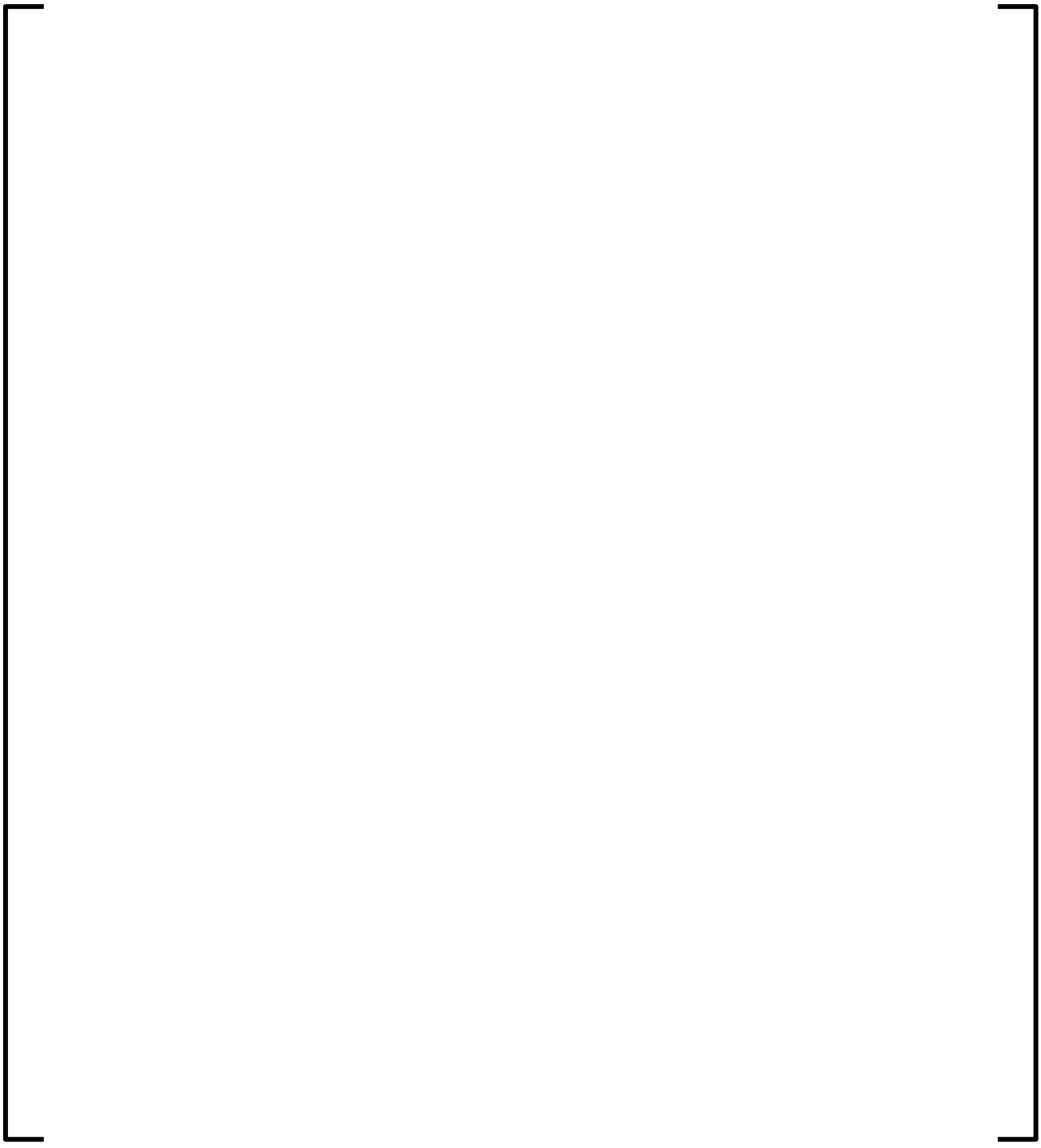
- P-AUTO for both validation and inhibition
- P-MANU for both validation and inhibition
- P-AUTO for validation and P-MANU for inhibition
- P-MANU for validation and P-AUTO for inhibition

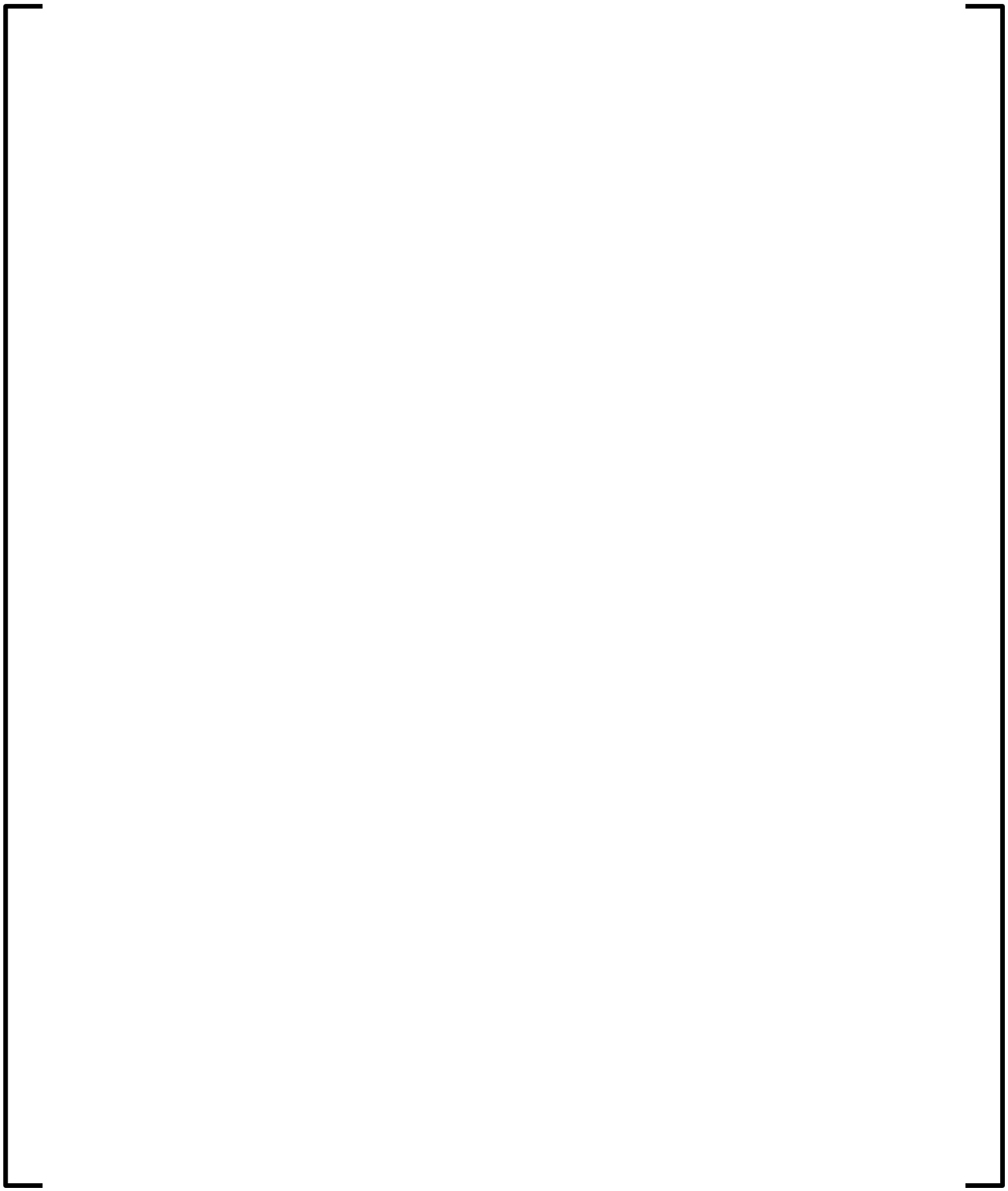
9.2 *Design Rules for Implementation of Permissive Signals*

10.0 FUNCTIONAL DIVERSITY

10.1 *Definition*

10.2 *Design Rules*





11.0 USE OF PAC IN ESFAS FOR U.S. EPR

11.1 *PAC Module Operation*

As noted in Reference 25, the PAC module prioritizes the various sense and command inputs and executes an output that reflects the plant licensing requirements and operational preferences. Additionally, the PAC module monitors the checkback signals from the actuators; it also drives and initiates the appropriate action. Each actuator or drive to be controlled requires one PAC module. The PAC module can process commands from multiple sources (e.g., inputs received from safety-related and non-safety-related I&C systems, automatic and manual portions of systems, and the MCR and RSS panels). Further description of the PAC module is provided in Reference 25.

11.2 *PAC Concept*

In the U.S. EPR design, the PAC modules are used for motor drive actuators, solenoids, and open and closed loop controlled actuators. Each PAC module organizes the priority of actuation signals issued by multiple I&C systems toward a given actuator.

As described in Section 8.3, when an actuation order is present as an input to the PAC module, the associated actuator cannot be influenced by any conflicting commands of lower priority from other I&C systems. When an ESF actuation signal is reset in the ALU, the actuation order is removed from the input of the PAC module. Once the PS actuation order is removed, orders of lower priority are then allowed to influence the actuator.

11.3 *Typical Application*

Within the PS, only the ESFAS utilizes the PAC modules. Each component controlled as part of an ESF system includes a PAC module in series with its control logic. The module is responsible for determining the priority of its input signals and for placing the actuator in the correct state.

For protection against unavailability of ESFAS orders, the two redundant ALUs are connected in a hardwired OR configuration. The output of this hardwired OR serves as the input to the appropriate PAC module. Therefore, if one ALU is lost the function remains available.

If an actuator is used by several protective actions, the actuation outputs are hardwired in an OR configuration. If needed, one PAC module can receive ESFAS signals from both subsystems.

The PAC modules also provide checkback signals. These checkback signals are collected from the PACS and processed by the MSI-AU. This functionality facilitates periodic testing of the PS.

12.0 INTERCHANNEL COMMUNICATION

12.1 *Communication Interfaces*

The use of interchannel communication in the PS is demonstrated by the communication between two function computers belonging to two different divisions of the PS (Figure 12-1). The typical hardware configuration includes a function computer 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 computer initiates sending activities and the messages are addressed to the receiving function computer. 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 computer by the message input and message output buffers. The function computer accesses the DPRAM independently of access by the communication module's PROFIBUS controller, which sends and receives data to and from the network.

12.2 *Communications Independence*

The TXS platform is designed using principles to provide communication independence. These 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:

- Processing and communication actions are controlled in a discrete, cyclic manner.
- Using a communication module that serves as a buffering circuit consistent with the guidance of IEEE Std. 7-4.3.2-2003, Annex E (Reference 14).

- Individual memory locations for each message, allowing separation between the send and receive data paths.

- Checks on the status of individual signals that provide valid input data to function processing.

Communications independence is the ability of computers in redundant divisions to exchange data without adverse interaction. Independence requirements of IEEE Std. 603 are supplemented by guidance contained in IEEE Std. 7-4.3.2.

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

The TXS communication techniques provide communications independence between redundant divisions and are consistent with the guidance of Reference 14. The related figure from Reference 14 is duplicated in Figure 12-2. An equivalent figure describing the TXS communication is shown in Figure 12-3. Figure 12-3 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 contained in the communication module. The communication module provides buffering so the function computers can read and write to the DPRAM independently of the PROFIBUS controller, which transfers data between the network and the DPRAM. Therefore, the function computer in one division operates independent of the operation of a function computer in a redundant division.

The DPRAM also begins the separation of data flow, which continues inside the function computer. Within the function computer, 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 safety function processor to operate independently from the PROFIBUS controller.
- It establishes separation of data flow by containing separate memory locations for messages to be sent and those that are received.

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

Figure 12-1—TXS Communication Principle

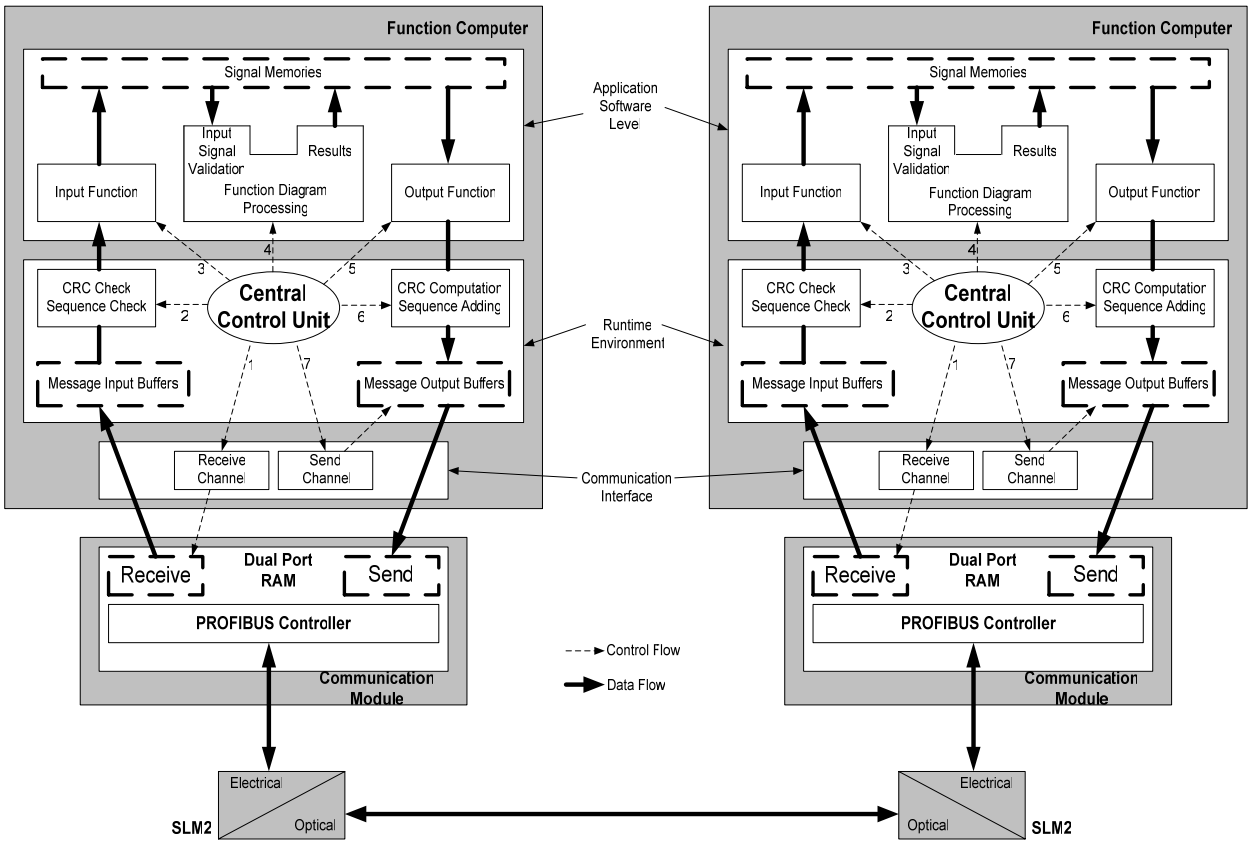


Figure 12-2—Communications Independence (IEEE Std. 7-4.3.2)

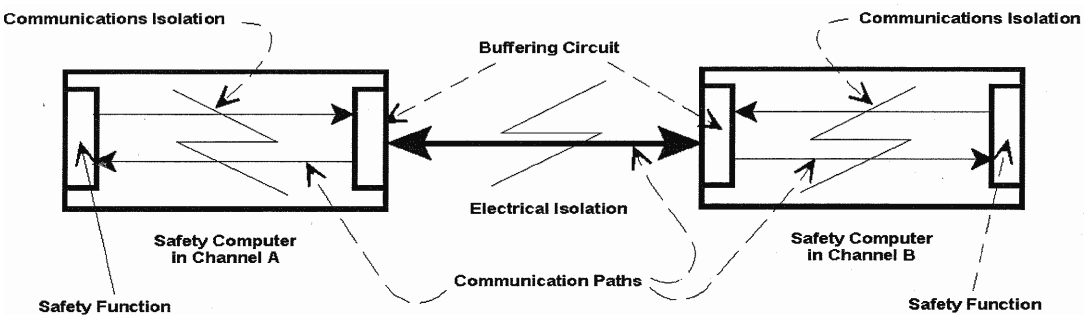
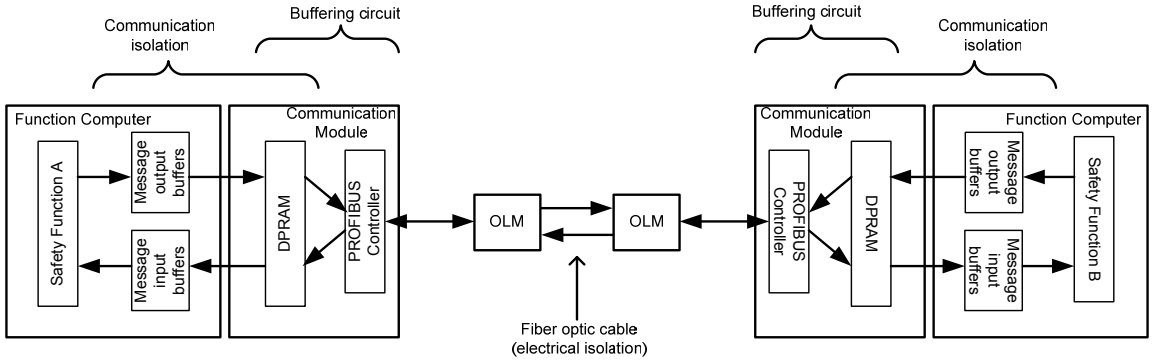


Figure 12-3—Communications Independence (U.S. EPR Implementation)



13.0 SAFETY TO NON-SAFETY INTERFACE

13.1 *General Requirements for Interfaces*

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

- Information is exchanged between the SU and the PS for diagnostics, monitoring, and maintenance.
- Information is exchanged between the PS and the PICS. Manual commands are sent from PICS to the PS during the course of normal operation and as part of post-accident management. The PS sends data to the PICS for display to the operator.
- Information is sent from the PS to a non-safety-related automation system for use in processing of control functions.

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

- Independence is maintained so that failures in a non-safety system do not prevent the performance of a safety function.
- Data communication between the non-safety 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 system to perform its safety functions.
- For commands from the PICS that are required on the safe shutdown path, the same command is also available from the Class 1E SICS.

13.2 *Protection System – Service Unit Interface*

The SU provides the 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 access to the system

is 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. Electrical isolation is provided through the use of optical connections between the SU and the MSI. This interface was reviewed and approved in Reference 23.

13.3 *Protection System – PICS Interface*

The PICS is the primary operator interface to the U.S. EPR I&C systems and is to be used in all plant conditions as long as it can be verified to be functioning correctly. Therefore, it is required that the operator be able to perform some functionality related to the PS from the PICS. Information from the PS is also required to be displayed on the PICS. The following are examples of the required functionality:

- Periodic testing of RT functionality on a division-by-division basis
- Reset of ESFAS initiation signals to allow manual operation of actuators in a post-accident management capacity
- Manual validation or inhibition of permissive signals needed during normal operation and for post-accident management
- Display of information (e.g., sensor measurements, discrepancy monitoring results, actuation vote status)

Information exchange between the PS and PICS is accomplished through the MSI-MU and GW.

Annex E of Reference 14 describes an acceptable method of implementing the safety to non-safety interface. The related figure from that annex is reproduced in Figure 13-1. Figure 13-2 is an equivalent figure depicting the PS implementation. The PS design conforms to the guidance of Reference 14, and incorporates additional layers of communications isolation between the GW and the PS function computers that use the data from the GW. In addition to the buffering circuit used on the GW side of the MSI, buffering circuits are also used on the PS side of the MSI and on the PS function computer. Separation of data flow is provided within the MSI and in the PS function computer. The interface between the MSI and the PS function computers is implemented in the same way as the inter-channel interfaces described in Section 12.0.

Electrical isolation for this interface is achieved through optical connections between the GW and MSI and between the MSI and the PS function computers.

13.4 *Protection System – Control System Interface*

The non-safety-related I&C automation systems require information from the PS during normal operation (e.g., permissive signals, sensor information). This signal exchange is realized primarily through electrically isolated, hardwired connections from the PS to the system that requires the information. In some cases, this interface may be realized by the PS sending information to the control system through the GW.

If a sensor is shared between the PS and another system, the sensor is acquired in the signal conditioning of the PS. The signal is multiplied and electrically isolated, then routed to the non-safety-related system. If the non-safety I&C system needs the result of PS processing, an electrically isolated, hardwired output is used from the appropriate PS function computer to the non-safety system.

Figure 13-1—Safety to Non-Safety Communication Interface (IEEE Std. 7-4.3.2)

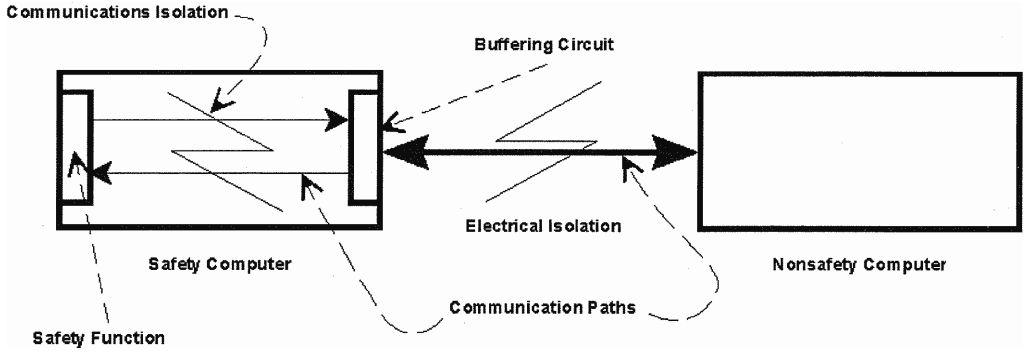
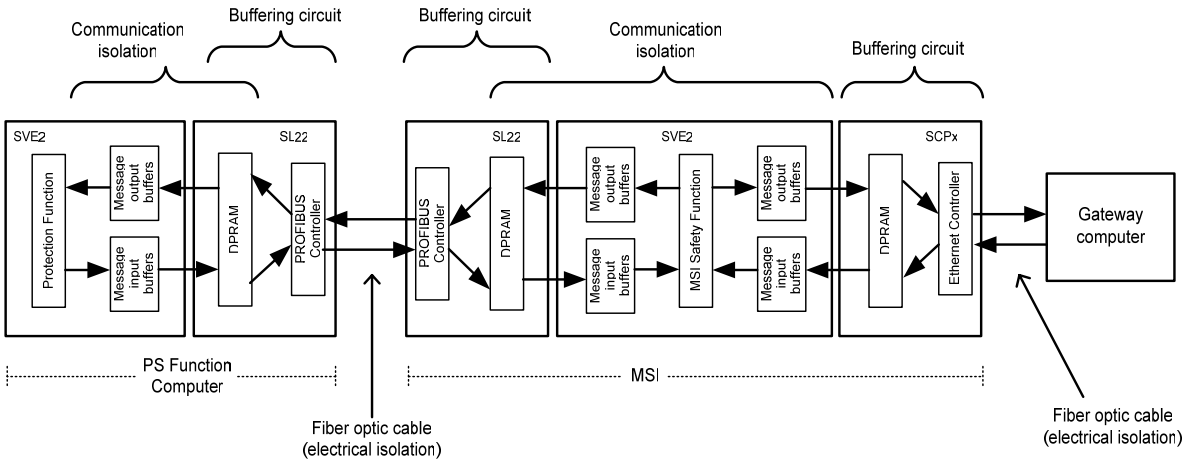


Figure 13-2—Safety to Non-Safety Communication Interface (U.S. EPR Implementation)



14.0 COMPLIANCE WITH IEEE STD. 603

14.1 *Background*

10 CFR 50.55a(h) (Reference 2) requires protection and safety systems to meet the guidance of IEEE Std. 603-1991 (Reference 15), which is endorsed by Regulatory Guide 1.153 (Reference 4). The 1991 version of this IEEE standard has been revised to IEEE Std. 603-1998 (Reference 16). The purpose of this revision was to "clarify the application of this standard to computer-based safety systems and to advanced nuclear power generating station designs."

The U.S. EPR is an evolutionary nuclear plant design and contains computer based safety systems; therefore, it is appropriate to apply the guidance of IEEE Std. 603-1998 to the U.S. EPR design. Furthermore, IEEE Std. 7.4.3.2 (Reference 14), which has been endorsed by Regulatory Guide 1.152 (Reference 5) also refers to the 1998 version of IEEE Std. 603. Additionally, draft NUREG-0800 Appendix 7.1-D, "Guidance for the Evolution of the Application of IEEE Std. 7-4.3.2" states:

> IEEE Std 603-1998, was evolved from IEEE Std 603-1991. The 1998 version of IEEE Std 603, was revised to clarify the application of the standard to computer-based safety systems and to advanced nuclear power generating station designs. IEEE Std. 603-1998 provides criteria for the treatment of electromagnetic and radio frequency interferences (EMI/RFI) and includes common-cause failure of digital computers in the single failure criterion. However, IEEE Std 603-1998 has neither been incorporated into the regulations nor endorsed by a regulatory guide. Therefore, the use of criteria from IEEE Std 603-1998 by licensees and applicants may be acceptable, if appropriately justified, consistent with current regulatory practice.

AREVA NP has performed a comparison of IEEE Std. 603-1991 to IEEE Std. 603-1998 (see Appendix B of this report). As shown in Appendix B, the requirements contained in IEEE Std. 603-1998 meet or exceed the requirements contained in the 1991 version. Specifically, the 1998 version of IEEE Std. 603-1998 primarily incorporates other IEEE Standards that have been reviewed by the NRC and endorsed by Regulatory Guides

(e.g., Regulatory Guide 1.152). Therefore, it is appropriately justified, from both a design and regulatory perspective, to apply the guidance of IEEE Std. 603-1998 to the U.S. EPR Protection System design.

Accordingly, AREVA NP's position is that compliance with IEEE Std. 603-1998 constitutes compliance with IEEE Std. 603-1991, and therefore satisfies the requirement contained in 10 CFR 50.55a(h).

The U.S. EPR PS design conformance with the clauses in IEEE Std. 603-1998 are described in the following sections.

14.2 *Clause 4 – Safety System Design Basis*

The functional design of the PS is based on a set of specific design bases established for the nuclear power generating station. These bases are documented in accordance with items A through L of Clause 4.

For the PS, the specific design bases (items A through L of Clause 4) will be addressed in the U.S. EPR Design Control Document (DCD).

14.3 *Clause 5.0 – Safety System Criteria*

The PS initiates automatic protective actions so that plant parameters are maintained within acceptable limits and so that the criteria for each design basis event are satisfied.

The PS has a four-fold redundant structure; each redundancy is allocated to a different electrical division and located in different safeguard buildings. Inside a division, the PS is separated into two independent subsystems, A and B, to incorporate functional diversity. RT functions are distributed between the subsystems, so that if the main signal is provided in one subsystem, a second diverse initiating signal, if necessary, is provided in the other subsystem. If a signal is needed for processing in both subsystems, it is implemented twice, once in each subsystem. ESFAS channels are also distributed between different subsystems. All elements of one ESFAS channel are implemented in the same subsystem.

14.4 *Sub-Clause 5.1 – Single-Failure Criterion*

The PS maintains the ability to perform all required safety functions at the system level in the presence of a credible single failure. If one redundancy within the PS is bypassed for testing or maintenance, and a credible single failure occurs in another redundancy, the ability to perform the required protective actions is maintained.

The single failure criterion is satisfied through redundancy implemented in all levels of the PS architecture. The process sensor level, the acquisition and processing level, and the voting/actuation level contain sufficient redundancy so that a credible single failure within the PS does not prevent a safety function from being performed.

Other system features, (e.g., physical separation, electrical and communication independence, voting logic), also contribute to single failure tolerance.

The redundant divisions of the PS are located in different safeguards buildings and are powered by separate Class 1E busses. Therefore, a single failure caused by an external hazard or a single power supply failure does not affect more than one redundancy of the system.

Electrical isolation and communications independence are employed on communication links between redundant divisions within the PS. Therefore, a credible single electrical failure in one redundancy, or a communication failure in one redundancy or between redundancies, does not affect the ability of the other redundancies to perform a safety function.

Electrical isolation and communications independence are employed on connections between the PS and non-safety systems. Therefore, a credible single electrical or communication failure in the non-safety system does not affect the ability of the PS to perform a safety function.

The voting logic utilized in the PS is designed so that a credible single failure in the PS does not prevent a protective action from being performed, and does not result in a

spurious actuation. If a failure is detected upstream of the voting logic, the vote is automatically modified to disregard the invalid input resulting from the single failure.

14.5 *Sub-Clause 5.2 – Completion of Protective Action*

Once initiated by the PS, protective actuations proceed to completion. Return to normal operation requires deliberate operator intervention. Once open, RT breakers require manual closure and cannot be manually closed until the RT signal is automatically cleared by the PS. The RT signal is only cleared when the initiating plant variable returns to within an acceptable range. System level ESF actuation signals can be reset by specific operator action or, in certain cases, by the initiating plant variable returning to within an acceptable range. This system level reset does not stop the ESF actuators. Further operator actions are required to stop the actuators on a component-by-component basis after the system level signal is reset.

14.6 *Sub-Clause 5.3 – Quality*

Components and modules used in the PS are evaluated to provide a quality consistent with minimum maintenance requirements and low failure rates. The PS is designed, manufactured, and tested in accordance with a rigorous quality assurance program that satisfies the requirements of 10 CFR 50, Appendix B. The PS software development process is implemented in accordance with the guidance of Reference 14 and Branch Technical Position (BTP) 7-14 (Reference 6). Qualification of software tools is performed in accordance with the guidance presented in Reference 6. Additional details about the software development and qualification process are presented in Reference 24 and AREVA NP Topical Report ANP-10272, “Software Program Manual for TELEPERM XS Safety System Topical Report” (Reference 26).

14.7 *Sub-Clause 5.4 – Equipment Qualification*

The PS equipment is environmentally and seismically qualified; therefore, the system is capable of performing its designated safety functions while exposed to normal, abnormal, test, event and post-event environmental conditions. Mild environment qualification conforms to the guidance of IEEE Std. 323-1974 (Reference 17). The TXS

Equipment Qualification Program is described in further detail in Reference 24. Upgraded modules and new equipment qualification will follow the same methodology (e.g., design review, type-testing, quality verification). In addition to equipment qualification, the corresponding section in the TXS Topical Report (i.e., Section 7.4 of Reference 24) also addresses electromagnetic interference (EMI). EMI qualification of the PS is consistent with the guidance of EPRI TR-102323 (Reference 18).

14.8 *Sub-Clause 5.5 – System Integrity*

The PS is designed and tested to confirm that the equipment components and the system as a whole demonstrate performance adequate for completion of protective actions over the range of transient and steady-state conditions of both the energy supply and the environment. The PS response times will be demonstrated to be consistent with those dictated by the plant accident analysis acceptance criteria. Failure modes are taken into account in the system design and are discussed in Reference 24.

14.8.1 *Cyber Security*

The TXS system design provides multiple, diverse levels of protection against cyber intrusion. These include administrative/procedural controls, TXS hardware controls, and TXS software controls. These security measures have multiple levels of defense (Reference 24).

14.9 *Sub-Clause 5.6 – Independence*

The PS consists of four separate and independent divisions, each with multiple processing and actuation channels. Redundant processing and actuation channels are assigned to separate divisions so that they are physically separated and electrically isolated. Separation of redundant channels begins at the process sensors and is maintained in the field wiring, containment penetrations and system cabinets.

The PS is designed to provide physical and electrical independence in accordance with the guidance of Regulatory Guide 1.75 (Reference 7) and IEEE Std. 384-1992

(Reference 19). Communications independence is provided consistent with the guidance of Reference 14.

Where redundant equipment communicates via data links (i.e., interchannel communication), communication independence is demonstrated by the system features discussed in Section 12.2.

Electrical isolation devices are employed on connections between the PS and non-safety systems. Where the PS communicates with a non-safety system via data links, communication independence is demonstrated by the system features discussed in Sections 13.2 and 13.3.

14.10 *Sub-Clause 5.7 – Capability for Testing and Calibration*

The PS is designed to provide capability for test and calibration consistent with the guidance provided in Regulatory Guide 1.22 (Reference 8), Regulatory Guide 1.118 (Reference 9), and IEEE Std. 338-1987 (Reference 20).

PS periodic testing duplicates, as closely as practical, the overall performance required of the system. The capability exists to permit testing during power operation. The PS design does not require modifications of the installed equipment for testing (e.g., disconnecting wires, installing jumpers).

The PS is also designed to provide numerous self-diagnostic test capabilities. These self-diagnostic test capabilities are described in detail in Reference 24.

14.11 *Sub-Clause 5.8 – Information Displays*

The U.S. EPR design does not credit manually controlled actions for safety systems to accomplish their safety functions. However, if the results of the safety analysis dictate the need for a manually controlled action for which no automatic action is provided, the required information display will be implemented consistent with the guidance provided in IEEE Std. 497-2002 (Reference 21).

If the PS is operated in a “bypassed” mode, an output for indication of the bypass is provided. Indication and identification of protective actions are provided to the operator at the system and divisional levels. The PS minimizes the possibility of ambiguous indications to the operator and provides bypassed and inoperable status information consistent with the guidance of Regulatory Guide 1.47 (Reference 10).

The relevant displays are provided to the operator in the MCR.

14.12 *Sub-Clause 5.9 – Control of Access*

Access to the PS hardware is in multiple layers. Access to the PS cabinets is controlled via front and rear mounted cabinet doors. During normal operation, the cabinet doors are closed and locked. Door positions are monitored, allowing operators to investigate any unexpected open cabinet doors.

The SU is the only access method to the software of the safety function processors. The SU and the PS units have multiple features to control access to the safety function computers and prevent unauthorized access. The control mechanisms include:

[ ]

Additional details regarding control of system access are provided in Reference 24.

14.13 *Sub-Clause 5.10 – Repair*

The U.S. EPR system is designed with self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities. The PS self-test features are designed consistent with the guidance of BTP 7-17 (Reference 11). The TXS platform self-diagnostic test capabilities are addressed in detail in Reference 24.

14.14 *Sub-Clause 5.11 – Identification*

Redundant divisions of the PS carry distinctive markings in the form of color-coded identification plates. These markings are distinct from identifying markings placed on any other equipment. Any PS components that may be too small to carry an identification plate are housed in equipment clearly labeled as being part of a single redundant division of the PS. Configuration management is used for maintaining the identification of PS software.

14.15 *Sub-Clause 5.12 – Auxiliary Features*

Auxiliary supporting features that are required for the PS to operate are classified as safety-related and are designed to satisfy applicable criteria.

Electrical power is supplied to the PS from Class 1E busses that satisfy applicable criteria. These busses provide battery backed, uninterruptible power supplies for the safety-related I&C systems.

Heating, ventilation, and air conditioning (HVAC) service is supplied to the I&C rooms that house the PS equipment by the safety-related HVAC system. The HVAC system is organized into four trains that are redundant, physically separated, and comply with applicable safety criteria.

Auxiliary supporting features that are not required for the PS to perform its safety functions are designed so that they do not degrade the PS below an acceptable level.

14.16 *Sub-Clause 5.13 – Multi-Unit Stations*

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

14.17 *Sub-Clause 5.14 – Human Factors Considerations*

Human factors are considered throughout the design of the PS in accordance with the U.S. EPR Human Factors Engineering (HFE) Program. The HFE program is described in AREVA NP topical report ANP-10279, "U.S. EPR Human Factors Engineering Program Topical Report" (Reference 27).

14.18 *Sub-Clause 5.15 – Reliability*

The PS is designed to accomplish its safety functions in a reliable manner to support overall plant reliability. The following design features demonstrate the reliability of the PS at the system level:

- Highly redundant architecture
- Highly reliable equipment
- Independent subsystems within each division for functional diversity concept
- Extensive fault detection and accommodation abilities
- High quality software design process

The deterministic nature of the TXS operating system is described in Reference 24. The following features are used in the TXS application software development to obtain deterministic behavior:

- The use of a standard function block library provides a large experience base for the standard modules.
- The use of the automatic code generator eliminates an important human error source. By eliminating the human interface between I&C function development

and code generation, both errors of translation and the introduction of complexity by engineers trying to optimize application coding can be eliminated.

- Software component testing is specifically designed to validate the development of the I&C functionality, verifying behavior at the range limits for input parameters and proper logic response to input parameters marked invalid.

The PS is analyzed in the U.S. EPR probabilistic risk assessment to support the overall U.S. EPR probabilistic design objectives, which are described in AREVA NP report ANP-10274 “U.S. EPR Probabilistic Risk Assessment Methods Report” (Reference 28).

The reliability of the TXS platform is demonstrated by its operating experience. Section 15.0 contains a summary of the TXS operating experience.

14.19 *Sub-Clause 5.16 – Common Cause Failure Criteria*

The U.S. EPR I&C architecture is designed so that plant parameters are maintained within the acceptable limits established for each design basis event in the presence of a single, credible common cause failure. Specific features that minimize or eliminate the potential for common cause failures are discussed in Sections 14.2, 14.4, 14.6, 14.7, 14.8, 14.9, 14.12, and 14.18.

Features of the PS that minimize common mode failures include:

- Use of functional diversity in the design of the PS.
- Minimization of the number of processors (e.g., use common processors), since hardware failures are the dominant contributor to unavailability.
- Design capabilities of the TXS system software and V&V measures taken in the application software engineering process are oriented on making software common mode failure highly improbable.
- In the unlikely event that a software common mode failure occurs, an RT occurs with ESF in the fail-safe state.

- TXS processor lock-up is sensed by the CPU watchdog (hardware device), which resets the processor and result in a trip state for each processor. In the limit, a lock-up of all the TXS processors results in an RT with ESF in the fail-safe state.

The PS is analyzed for credible common cause failures as part of the diversity and defense-in-depth analysis. If this analysis identifies a credible common cause failure that could prevent the PS from performing a safety function, one or more of the following are implemented:

- Performance of the function automatically by a diverse, software-based system
- Performance of the function manually through a diverse, software-based system
- Performance of the function manually through a non-software-based actuation path

14.20 *Clause 6.0 – Sense and Command Features*

The sense and command features present in the PS satisfy the requirements of Clause 5 and the requirements of Clause 6 as described below.

14.21 *Sub-Clause 6.1 – Automatic Control*

The PS is designed to automatically initiate required RT and ESF functions required to mitigate the effects of design basis events. These automatic initiations are performed with precision and reliability when the associated plant variable measured by the PS exceeds a predefined setpoint. The setpoints used by the PS and the associated margins, errors, and response times are bounded by the plant safety analysis assumptions.

14.22 *Sub-Clause 6.2 – Manual Control*

The design of the PS provides for system level manual initiation of protective functions from the MCR. The system level manual initiations perform all actions performed by the related automatic actuations and are implemented consistent with the guidance of

Regulatory Guide 1.62 (Reference 12). Details concerning the implementation of manual protective functions are described in Sections 7.6 and 8.5.

14.23 *Sub-Clause 6.3 – Interaction between Sense and Command Features and Other Systems*

The U.S. EPR I&C systems contain design features to prevent a single credible event that could result in a non-safety system action causing a condition requiring protective action and concurrently preventing the protective action in those channels designated to provide protection against the condition. These design features include:

- Isolation of the PS from channel failure by providing additional redundancy
- Isolation of the control system from channel failure by using data validation techniques to select a valid signal for control system actuation
- Electrical isolation techniques to prevent credible electrical faults from propagating to redundant divisions
- Communication isolation techniques to prevent credible communication faults from propagating to redundant divisions
- Allocation of functionally diverse RT functions to two independent sub-systems with no connections between them

The redundancy designed into the PS, along with the design features listed above, allows the PS to conform to the requirements of Sub-Clause 6.3, even if a protective channel is in a maintenance bypass condition.

14.24 *Sub-Clause 6.4 – Derivation of System Inputs*

To the extent feasible and practical, inputs to the PS are derived from signals representing direct measurements of the desired variables. When direct variable measurement is not feasible, the desired variable is calculated based on the minimum possible number of direct measurements. The PS inputs will be included as part of the PS design bases documentation in the U.S. EPR DCD.

14.25 *Sub-Clause 6.5 – Capability for Testing and Calibration*

Means are provided for checking, with a high degree of confidence, the operational availability of each PS input sensor during reactor operation. This is accomplished in one of the following ways:

- Perturbing the monitored variable
- Introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable
- Cross-checking between channels that bear a known relationship to each other and that have readouts available

The TXS platform provides self-monitoring and periodic testing features to check the operational availability of the PS computers that process the input sensors.

14.26 *Sub-Clause 6.6 – Operating Bypasses*

The PS implements operating bypasses in the form of permissive signals. When the plant conditions associated with allowing the operating bypass are not met, the PS automatically prevents the activation of the operating bypass. If plant conditions change, and an activated operating bypass is no longer permissible; the PS automatically removes the appropriate active operating bypass. When an operating bypass is in effect, indication of this condition is provided to the operator. A discussion of implementation of permissive signals is presented in Section 9.0.

14.27 *Sub-Clause 6.7 – Maintenance Bypass*

For periodic testing and diagnostic activities, individual function computers of the PS can be placed into a special testing and diagnostic mode via the SU. The function computer that is being tested behaves like a computer with a detected fault for the system. In this testing mode, the signal outputs via the input/output (I/O) modules are disabled and signals sent via communication links are marked with the status “TEST.” Accordingly, communication from the unit under test is disregarded by the remainder of the system.

When any single unit of the system is bypassed for testing or maintenance, the PS maintains the ability to perform its safety functions. The sense and command features of the PS still satisfy the single failure criteria in this condition.

14.28 *Sub-Clause 6.8 – Setpoints*

For the setpoints used by the PS, the allowance for uncertainties between the process analytical limit and the setpoint used in the protective function is determined using a documented methodology. The U.S. EPR instrument setpoint methodology is described in AREVA NP topical report ANP-10275 “U.S. EPR Instrument Setpoint Methodology” (Reference 29). This methodology is developed to provide adequate assurance that the plant safety limits are not exceeded.

Where a protective action requires the use of multiple setpoints corresponding to different plant conditions, the PS design uses the more restrictive setpoint when required.

14.29 *Clause 7.0 – Execute Features*

The execute features associated with the PS satisfy the requirements of Clause 5 and the requirements of Clause 7 as described below.

14.30 *Sub-Clause 7.1 – Automatic Control*

The execute features associated with the PS are capable of receiving and acting upon the automatic actuation signals generated by the PS consistent with the design bases of the system.

14.31 *Sub-Clause 7.2 – Manual Control*

Manual control of each individual component acted on by the PS is provided to the operator. Manual control at the component level is implemented so it does not interfere with manual system level actuation. Individual component control does not prevent the PS from satisfying the single failure criteria.

14.32 *Sub-Clause 7.3 – Completion of Protective Action*

The design of the execute features associated with the PS is such that once initiated, protective actions go to completion. When the actuation signals generated by the sense and command features are reset, the execute features do not automatically return to normal. Deliberate operator action is required to return the execute features to normal after the sense and command features are reset, as described in Section 14.5.

14.33 *Sub-Clause 7.4 – Operating Bypass*

Operating bypasses of protective actions are implemented in the sense and command features of the PS. Compliance to the requirements concerning operating bypasses is addressed in Section 14.26.

14.34 *Sub-Clause 7.5 – Maintenance Bypass*

The capability of the PS to accomplish its safety functions is retained while execute features equipment is in maintenance bypass. This capability is established by redundancy designed into the system and by administrative controls placed on reduction of redundancy due to maintenance. Portions of the execute features with a redundancy of one are designed so that when a portion is placed in maintenance bypass, temporarily reducing its degree of redundancy to zero, the remaining portions provide acceptable reliability.

14.35 *Clause 8.0 – Power Source Requirements*

Electrical power is supplied to the PS from battery-backed, uninterruptible power supplies. The electrical power sources for the PS satisfy the applicable requirements of Clause 5 and are discussed in further detail below.

14.36 *Sub-Clause 8.1 – Electrical Power Sources*

Those portions of the power systems that provide electrical power to the PS are classified as safety-related and satisfy the criteria applicable to Class 1E power systems

described in IEEE Std. 603-1998 (Reference 16) and IEEE Std. 308-2001 (Reference 22).

14.37 *Sub-Clause 8.2 – Non-Electrical Power Sources*

The PS does not rely on non-electrical power sources for operation.

14.38 *Sub-Clause 8.3 – Maintenance Bypass*

The capability of the PS to perform its safety functions is retained while its power sources are in maintenance bypass. The aspects of the electrical power system that fulfill this capability will be described in the U.S. EPR DCD.

15.0 TELEPERM XS OPERATING EXPERIENCE

NUREG-0800, Section 7.9, “Data Communication Systems,” subsection III, “Review Procedures,” in the paragraph titled “Reliability” states that “the reviewer should determine that the operating history of the DCS in similar applications is known and that it has been satisfactory” (Reference 13). While the information provided in this section is not directly related to the scope of this topical report, it provides information demonstrating the reliability and satisfactory operation of the TXS platform.

The TXS platform is a proven, reliable, technology that has been in operation for over ten years both domestically and internationally. Observed failure rates of TXS platform equipment currently in operation have been much lower than the theoretically calculated failure rates (Figure 15-1). The experience gained with this product through development, implementation, and operation guides future development efforts.

During the design and prototype phase of a product, the expected failure rate is calculated to determine the lifetime of this product. This calculation is based on experience values for the failure rates of the different components (e.g., capacitors, integrated circuits, circuit boards). The result, the expected failure rate, provides data for reliability examinations, warranty questions, spare parts management, and other operational considerations. Together with the field failure rate, the expected failure rate is the basis for the recognition of design errors, production errors and other errors.

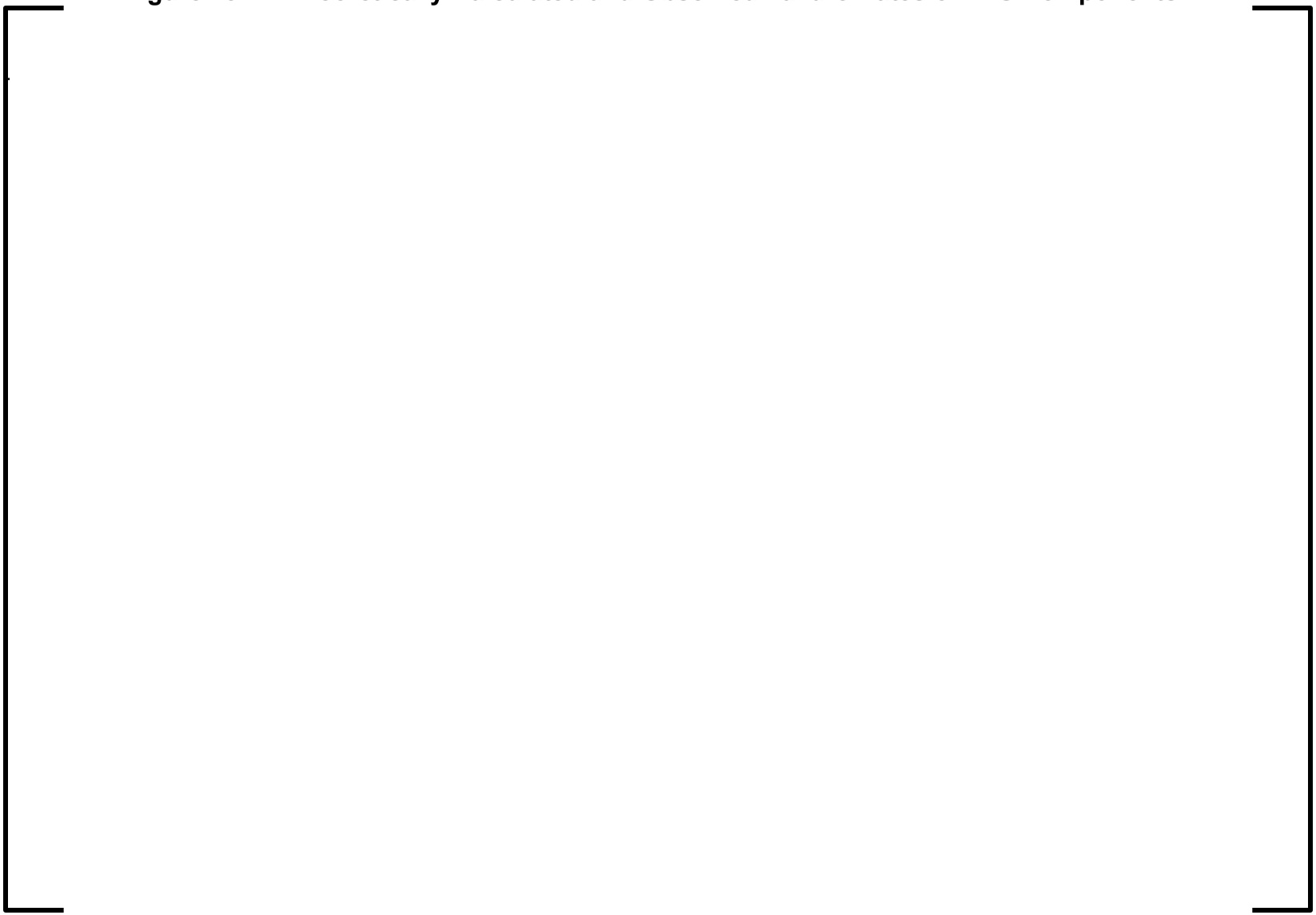
There are over 22,000 first generation TELEPERM XS components in service today. TXS systems in operation have experienced far fewer failures than statistically calculated and expected. **[**

] Second generation hardware is currently in development following the established TXS design principles, including qualification and testing methods, and is expected to operate in the same reliable manner.

Examples of TXS systems currently operating as reactor protection systems include:

- The 4-channel reactor protection system of the Westinghouse PWRs Beznau 1 and 2 (Switzerland)
- The 3-channel reactor protection system in the VVER440 plants Paks 1–4 (Hungary)
- The 2 x 2-out-of-3 structured supplementary reactor protection system in the BWR Philippsburg 1 (Germany)

Figure 15-1—Theoretically Calculated and Observed Failure Rates of TXS Components



16.0 SUMMARY/CONCLUSIONS

The U.S. EPR PS is a digital, integrated 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 provides for manual RT and ESF actuation capability at the system and component level, independent of the TXS computers when required.

Where data communication exists between divisions of the PS (interchannel communication), the communication and isolation techniques utilized 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 utilized 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 exhibits the ability to detect, identify, and mitigate failures with a high degree of confidence.

In addition to the redundant PS system architecture, two independent subsystems allow for the use of functional 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. The architecture of the PS and the implementation of protective functions within this architecture, complies with the relevant regulatory requirements.

This report describes the PS architecture and the typical implementation of functionality within this architecture. AREVA NP requests NRC approval of the following aspects of the PS design presented in this report:

- PS architecture
- Specific network configurations
- Typical RT concepts and sequences
- Typical ESFAS concepts and sequences
- Design rules for permissive signals
- Inter-channel communication independence
- Safety to non-safety system interfaces
- Conformance with relevant clauses of IEEE Std. 603

17.0 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 4, 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 7B-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 323-1974, “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. IEEE Standard 308-2001, “IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.”

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. Siemens Topical Report 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, July 12, 2000).

25. AREVA NP Topical Report ANP-10273P, Revision 0, “AV42 Priority Actuation and Control Module Topical Report,” November 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report," NRC:06:054, November 28, 2006).

26. AREVA NP Topical Report ANP-10272, Revision 0, “Software Program Manual for TELEPERM XS Safety System Topical Report,” December 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10272, "Software Program Manual TELEPERM XS Tm Safety Systems Topical Report," NRC:06:061, December 21, 2006).

27. AREVA NP Topical Report ANP-10279, Revision 0, “U.S. EPR Human Factors Engineering Program Topical Report,” January 2007, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10279, "U.S. EPR Human Factors Engineering Program Topical Report," NRC:07:004, January 29, 2007).

28. AREVA NP Report ANP-10274NP, Revision 0, “U.S. EPR Probabilistic Risk Assessment Methods Report,” December 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review of ANP-10274NP, "Probabilistic Risk Assessment Methods Report," NRC:06:055, December 15, 2006).

29. AREVA NP Topical Report ANP-10275P, Revision 0, “U.S. EPR Instrument Setpoint Methodology,” March 2007

Appendix A
Plant Specific Action Items

Plant Specific Open Item	Documentation
1.) The licensee must demonstrate that the generic qualification bounds the plant specific condition (e.g., temperature, humidity, seismic, and electromagnetic compatibility) for the location(s) in which the TXS equipment is to be installed. The generic qualification data must comply with EPRI qualification requirements specified in EPRI TR-107330 and TR-102323 R1.	Plant-specific Combined License item.
2.) The licensee's plant-specific software development V&V activities and configuration management procedures must be equivalent to industry standards and practices endorsed by the NRC (as referenced in SRP BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems").	AREVA NP Topical Report ANP-10272, "Software Program Manual for TELEPERM XS Safety System Topical Report" (Reference 26)
3.) If the licensee develops a TXS auxiliary feedwater control system, the licensee must include automatic initiation and flow indication (TMI Action Plan Item II.E.1.2). The licensee needs to confirm that the plant-specific application conforms to the requirements of 10 CFR 50.34 (f)(2)(xii).	U.S. EPR DCD
4.) If the licensee replaces existing accident monitoring instrumentation (TMI Action Plan Item II.F.1) display capabilities with a TXS system, including the bypass and inoperable status information, the licensee needs to confirm that the new system provides equivalent sampling and analyzing features, and meets the requirement of 10 CFR 50.34(f)(2)(xvii).	U.S. EPR DCD
5.) If the licensee installs a TXS inadequate core cooling detection system, the licensee needs to confirm that the new system conforms to the requirements of 10 CFR 50.34(f)(2)(xviii).	U.S. EPR DCD
6.) If the licensee installs a TXS containment isolation system (TMI Action Plan Item I II.E.4.2), the licensee must verify that the plant-specific application conforms to the requirement of 10 CFR 50.34(f)(2)(xiv).	U.S. EPR DCD

Plant Specific Open Item	Documentation
7.) For monitoring plant conditions following core damage, the licensee must verify that the TXS system meets the processing and display portions of the requirements of 10 CFR 50.34(f)(2)(xix).	U.S. EPR DCD
8.) If the licensee installs a TXS system for monitoring reactor vessel water level during post-accident conditions, the licensee must provide plant-specific verification of the ranges, and confirm that human factors issues have been adequately addressed, as required by 10 CFR 50.34(f)(2)(xxiv).	Not applicable to the U.S. EPR since 10 CFR 50.34(f)(2)(xxiv) only applies to BWRs.
9.) If the licensee installs a TXS reactor protection system, the licensee must provide confirmation that the TXS system is diverse from the system for reducing the risk from anticipated transients without scram (ATWS), as required by 10 CFR 50.62. If the licensee installs a TXS ESFAS, the licensee must provide confirmation that the diversity requirements for plant systems (feedwater, auxiliary feedwater, turbine controls, etc.) are maintained.	U.S. EPR DCD
10.) Setpoints will be evaluated on a plant-specific basis. The licensee must ensure that, when the TXS system is installed, overly conservative setpoints that may occur due to the elimination of analog system drift are not retained, as this would increase the possibility that the TXS equipment may be performing outside the vendor specifications. The licensee must provide the staff with a revised setpoint analysis that is applicable to the installed TXS system(s).	AREVA NP Topical Report ANP-10275P, "U.S. EPR Instrument Setpoint Methodology Report" (Reference 29)
11.) The licensee must evaluate plant-specific accident analyses to confirm that a TXS RT system (RTS) includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with the accident analysis presented in Chapter 15 of the plant safety analysis report.	U.S. EPR DCD

Plant Specific Open Item	Documentation
12.) The staff requires that each licensee ensure that the plant-specific TXS application complies with the criteria for defense against common-mode failures in digital instrumentation and control systems.	U.S. EPR DCD AREVA NP U.S. EPR Diversity and Defense-in-Depth Analysis Methodology Topical Report (scheduled to be submitted to NRC in June 2007)
13.) The licensee should propose plant-specific Technical Specifications including periodic test intervals.	U.S. EPR DCD
14.) The licensee should demonstrate that the power supply to the TXS system complies with EPRI TR-107330 requirements.	U.S. EPR DCD
15.) The licensee should demonstrate that the qualification of the isolation devices were performed in accordance with EPRI TR 107330 requirements.	Plant-specific Combined License item.
16.) The licensee should demonstrate that Siemens TXP (control systems) or other manufacturer's control systems satisfy the acceptance guidance set forth in Section 4.1 of this safety evaluation.	U.S. EPR DCD AREVA NP U.S. EPR Diversity and Defense-in-Depth Analysis Methodology Topical Report (scheduled to be submitted to NRC in June 2007)
17.) The licensee should address the need for a requirement traceability matrix (RTM) for enumerating and tracking each system requirement throughout its lifecycle, particularly as part of making future modifications.	AREVA NP Topical Report ANP-10272 (Reference 26)

Appendix B
Comparison of IEEE Std. 603-1991 to IEEE Std. 603-1998

The following table identifies and assesses the differences between IEEE Std. 603-1991 and IEEE Std. 603-1998

IEEE 603-1991	IEEE 603-1998	Comment
2. Definitions detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. NOTE: Identifiable, but nondetectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1988.	**3. Definitions** 3.13 detectable failures. Failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. NOTE-Identifiable, but nondetectable, failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Refer to IEEE Std 379-1994.	Only definitions with differences are listed. Regulatory Guide (RG) 1.53 Rev. 2 now endorses IEEE Std. 379-2000.
division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.	3.14 division. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components. NOTE - A division can have one or more channels.	Makes allowance for interchannel communication, used in some digital applications.
NOTE: The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.	NOTES: 1 -The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E. 2-This definition of "safety system" agrees with the definition of "safety-related systems" used by the American Nuclear Society (ANS) and IEC 60231A.	Note 2 adds clarification on definition that has no impact on requirements.

IEEE 603-1991	IEEE 603-1998	Comment
4. Safety System Designation A specific basis shall be established for the design of each safety system of the nuclear power generating station, The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:	**4. Safety system design basis** A specific basis shall be established for the design of each safety system of the nuclear power generating station. The design basis shall also be available as needed to facilitate the determination of the adequacy of the safety system, including design changes. The design basis shall be consistent with the requirements of ANSI/ANS 51.1-1983 or ANSI/ANS 52.1-1983 and shall document as a minimum:	No difference.
4.1 The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.	a) The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.	No difference.
4.2 The safety functions and corresponding protective actions of the execute features for each design basis event.	b) The safety functions and corresponding protective actions of the execute features for each design basis event.	No difference.
4.3 The permissive conditions for each operating bypass capability that is to be provided.	c) The permissive conditions for each operating bypass capability that is to be provided.	No difference.
4.4 The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.	d) The variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured.	No difference.
4.5 The following minimum criteria for each action identified in 4.2 whose operation may be controlled by manual means initially or subsequent to initiation. See IEEE Std 494-1974.	e) The protective actions identified in item b) that may be controlled by manual means initially or subsequently to initiation. See IEEE Std 497-1981. The proactive actions are as follows:	RG 1.97 Rev. 4 now endorses IEEE Std. 497-2002.

IEEE 603-1991	IEEE 603-1998	Comment
4.5.1 The points in time and the plant conditions during which manual control is allowed.	1) The points in time and the plant conditions during which manual control is allowed.	No difference.
4.5.2 The justification for permitting initiation or control subsequent to initiation solely by manual means.	2) The justification for permitting initiation or control subsequent to initiation solely by manual means.	No difference.
4.5.3 The range of environmental conditions imposed upon the operator during normal, abnormal, and accident circumstances throughout which the manual operations shall be performed.	3) The range of environmental conditions imposed upon the operator during normal, abnormal, and accident conditions throughout which the manual operations shall be performed.	No difference.
4.5.4 The variables in 4.4 that shall be displayed for the operator to use in taking manual action.	4) The variables in item d) that shall be displayed for the operator to use in taking manual action.	No difference.
4.6 For those variables in 4.4 that have a spatial dependence (that is, where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.	f) For those variables in item d) that have a spatial dependence (i.e., where the variable varies as a function of position in a particular region), the minimum number and locations of sensors required for protective purposes.	No difference.
4.7 The range of transient and steady-state conditions of both motive and control power and the environment (for example, voltage, frequency, radiation, temperature, humidity, pressure, and vibration) during normal, abnormal, and accident circumstances throughout which the safety system shall perform.	g) The range of transient and steady-state conditions of both motive and control power and the environment (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference) during normal, abnormal, and accident conditions throughout which the safety system shall perform.	No difference.
4.8 The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).	h) The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
4.9 The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design.	i) The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design	No difference.
4.10 The critical points in time or the plant conditions, after the onset of a design basis event, including:	j) The critical points in time or the plant conditions, after the onset of a design basis event, including:	No difference.
4.10.1 The point in time or plant conditions for which the protective actions of the safety system shall be initiated.	1) The point in time or plant conditions for which the protective actions of the safety system shall be initiated.	No difference.
4.10.2 The point in time or plant conditions that define the proper completion of the safety function.	2) The point in time or plant conditions that define the proper completion of the safety function.	No difference.
4.10.3 The points in time or the plant conditions that require automatic control of protective actions.	3) The point in time or the plant conditions that require automatic control of protective actions.	No difference.
4.10.4 The point in time or the plant conditions that allow returning a safety system to normal.	4) The point in time or the plant conditions that allow returning a safety system to normal.	No difference.
4.11 The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.	k) The equipment protective provisions that prevent the safety systems from accomplishing their safety functions.	No difference.
4.12 Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).	l) Any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria).	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5. Safety System Criteria The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Appendix A for an illustrative example.)	**5. Safety system criteria** The safety systems shall, with precision and reliability, maintain plant parameters within acceptable limits established for each design basis event. The power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function. (See Annex A for an illustrative example.)	No difference.
5.1 Single-Failure Criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of:	5.1 Single-failure criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of	No difference.
(1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures;	a) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures.	No difference.
(2) all failures caused by the single failure; and	b) All failures caused by the single failure.	No difference.
(3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.	c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.	No difference.
The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 provides guidance on the application of the single-failure criterion.	The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1994 provides guidance on the application of the single-failure criterion. IEEE Std 7-4.3.2-1993 addresses common cause failures for digital computers.	The additional clarification on single failure does not affect requirements. RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000. Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std.7-4.3.2-2003.

IEEE 603-1991	IEEE 603-1998	Comment
This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probable assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probable assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion, IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.	This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.	No difference.
Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probable assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.	Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in Clause 4, item i) of the design basis, a probabilistic assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.2 Completion of Protective Action. The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal, This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.	5.2 Completion of protective action. The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required.	No difference.
5.3 Quality. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989).	5.3 Quality. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994).	Updates quality assurance guidance reference. No impact on digital I&C requirements.
(Not included in IEEE Std. 603-1991)	Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.
5.4 Equipment Qualification, Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.	5.4 Equipment qualification. Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
(Not included in IEEE Std. 603-1991)	Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.
5.5 System Integrity. The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.	5.5 System integrity. The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.	No difference.
(Not included in IEEE Std. 603-1991)	Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 74.3.2-1993.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE STd. 7-4.3.2-2003.
5.6 Independence 5.6.1 Between Redundant Portions of a Safety System. Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring, that' safety function.	5.6 Independence 5.6.1 Between redundant portions of a safety system. Redundant portions of a safety system provided for a safety function shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design basis event requiring that safety function.	No difference.
5.6.2 Between Safety Systems and Effects of Design Basis Event. Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.	5.6.2 Between safety systems and effects of design basis event. Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the degree necessary to retain the capability of meeting the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.6.3 Between Safety Systems and Other Systems. safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.	5.6.3 Between safety systems and other systems. The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4, item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.	No difference.
5.6.3.1 Interconnected Equipment (1) Classification: Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems, Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.	5.6.3.1 Interconnected equipment a) Classification. Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.	No difference.
(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.	b) Isolation. No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.6.3.2 Equipment in Proximity (1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981.	5.6.3.2 Equipment in proximity a) *Separation.* Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1992.	RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.
(2) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.	b) *Barrier.* Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in Clause 4, items g) and h) of the design basis.	No difference.
5.6.3.3 Effects of a Single Random Failure. Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 for the application of this requirement.	5.6.3.3 Effects of a single random failure. Where a single random failure in a nonsafety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1994 for the application of this requirement.	RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.
5.6.4 Detailed Criteria. IEEE Std 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits.	5.6.4 Detailed criteria. IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits.	RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.

IEEE 603-1991	IEEE 603-1998	Comment
(Not included in IEEE Std. 603-1991)	IEEE Std 74.3.2-1993 provides guidance on the application of this criteria for the separation and isolation of the data processing functions of interconnected computers.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.
5.7 Capability for Test and Calibration. Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case: (1) appropriate justification shall be provided (for example, demonstration that no practical design exists), (2) acceptable reliability of equipment operation shall be otherwise demonstrated, and (3) the capability shall be provided while the generating station is shut down.	5.7 Capability for testing and calibration. Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case: - Appropriate justification shall be provided (e.g., demonstration that no practical design exists), - Acceptable reliability of equipment operation shall be otherwise demonstrated, and - The capability shall be provided while the generating station is shut down.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.8 Information Displays 5.8.1 Displays for Manually Controlled Actions. The display instrumentation provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.	5.8 Information displays 5.8.1 Displays for manually controlled actions. The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator.	No difference.
5.8.2 System Status Indication. Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.	5.8.2 System status indication. Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status. This information shall include indication and identification of protective actions of the sense and command features and execute features. The design shall minimize the possibility of ambiguous indications that could be confusing to the operator. The display instrumentation provided for safety system status indication need not be part of the safety systems.	No difference.
5.8.3 Indication of Bypasses. If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.	5.8.3 Indication of bypasses. If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.	No difference.
5.8.3.1 This display instrumentation need not be part of the safety systems.	a) This display instrumentation need not be part of the safety systems.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.8.3.2 This indication shall be automatically actuated if the bypass or inoperative condition (a) is expected to occur more frequently than once a year, and (b) is expected to occur when the affected system is required to be operable.	b) This indication shall be automatically actuated if the bypass or inoperative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable.	No difference.
5.8.3.3 The capability shall exist in the control room to manually activate this display indication.	c) The capability shall exist in the control room to manually activate this display indication.	No difference.
5.8.4 Location. Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.	5.8.4 Location. Information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to affect the actions.	No difference.
5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.	5.9 Control of access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.	No difference.
5.10 Repair. The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.	5.10 Repair. The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.11 Identification. In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:	5.11 Identification. In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:	No difference.
(1) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 and IEEE Std 420-1982.	a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.	RG 1.75 Rev. 3 now endorses IEEE Std. 384-1992.
(2) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.	b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.	No difference.
(3) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification of fire protection equipment, phase identification of power cables).	c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).	No difference.
(4) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.	d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.	No difference.
(5) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974.	e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974.	No difference.
(Not included in IEEE Std. 603-1991)	f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993.	Added reference to IEEE 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.

IEEE 603-1991	IEEE 603-1998	Comment
5.12 Auxiliary Features 5.12.1 Auxiliary supporting features shall meet all requirements of this standard.	5.12 Auxiliary features. Auxiliary supporting features shall meet all requirements of this standard.	No difference.
5.12.2 Other auxiliary features that (1) perform a function that is not required for the safety systems to accomplish their safety function and (2) are part of the safety systems by association (that is, not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade. the safety systems below an acceptable level. Examples of these other auxiliary features shown in Figure 3 and an illustration of the application of this criteria is contained in Appendix A.	Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A.	No difference.
5.13 Multi-Unit Stations. The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1980. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1988.	5.13 Multi-unit stations. The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379- 1994.	RG 1.32 Rev. 3 now endorses IEEE Std. 308-2001. RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.
5.14 Human Factors Considerations. Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer (s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.	5.14 Human factors considerations. Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
5.15 Reliability. For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.	5.15 Reliability. For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis.	No difference.
(Not included in IEEE Std. 603-1991)	Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.
(Not included in IEEE Std. 603-1991)	5.16 Common cause failure criteria. Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure (See IEEE 379-1994).	RG 1.53 Rev. 2 now endorses IEEE Std. 379-2000.
(Not included in IEEE Std. 603-1991)	IEEE Std 7-4.3.2-1993 provides guidance on performing an engineering evaluation of software common cause failures, including use of manual action and non-safety-related systems, or components, or both, to provide means to accomplish the function that would otherwise be defeated by the common cause failure.	Added reference to IEEE Std. 7-4.3.2, which addresses digital I&C applications. RG 1.1.52 Rev. 2 now endorses IEEE Std. 7-4.3.2-2003.

IEEE 603-1991	IEEE 603-1998	Comment
6. Sense and Command Features - Functional and Design Requirements. In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:	6. Sense and command features-functional and design requirements. In addition to the functional and design requirements in Clause 5, the requirements listed in 6.1 through 6.8 shall apply to the sense and command features.	No difference.
6.1 Automatic Control. Means shall be provided to automatically initiate and control all protective actions except as justified in 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in 4.5 following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of 4.5.	6.1 Automatic control. Means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4, item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e).	No difference.
6.2 Manual Control 6.2.1 Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.	6.2 Manual control. Means shall be provided in the control room to a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.	No difference.
6.2.2 Means shall be provided in the control room to implement manual initiation and control of the protective actions identified in 4.5 that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.	b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
6.2.3 Means shall be provided to implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in 4.10. The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.	c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action.	No difference.
6.3 Interaction Between the Sense and Command Features and Other Systems 6.3.1 Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:	6.3 Interaction between the sense and command features and other systems 6.3.1 Requirements Where a single credible event, including all direct and consequential results of that event, can cause a nonsafety system action that results in a condition requiring protective action, and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:	No difference.
(1) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:	a) Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
(a) Channels that sense a set of variables different from the principal channels.	1) Channels that sense a set of variables different from the principal channels.	No difference.
(b) Channels that use equipment different from that of the principal channels to sense the same variable.	2) Channels that use equipment different from that of the principal channels to sense the same variable.	No difference.
(c) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.	3) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.	No difference.
Both the principal and alternate channels shall be part of the sense and command features.	4) Both the principal and alternate channels shall be part of the sense and command features.	No difference.
(2) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.	b) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.	No difference.
See Fig 5 for a decision chart for applying the requirements of this section.	See Figure 5 for a decision chart for applying the requirements of this clause.	No difference.
6.3.2 Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	6.3.2 Provisions. Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.	No difference.
6.4 Derivation of System Inputs. To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.	6.4 Derivation of system inputs. To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
6.5 Capability for Testing and Calibration 6.5.1 Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation, This may be accomplished in various ways; for example:	6.5 Capability for testing and calibration 6.5.1 Checking the operational availability. Means shall be provided for checking, with a high degree of confidence, the operational availability of each sense and command feature input sensor required for a safety function during reactor operation. This may be accomplished in various ways; for example:	No difference.
(1) by perturbing the monitored variable,	a) By perturbing the monitored variable,	No difference.
(2) within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or	b) Within the constraints of 6.6, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable, or	No difference.
(3) by cross-checking between channels that bear a known relationship to each other and that have readouts available.	c) By cross-checking between channels that bear a known relationship to each other and that have readouts available.	No difference.
6.5.2 One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:	6.5.2 Assuring the operational availability. One of the following means shall be provided for assuring the operational availability of each sense and command feature required during the post-accident period:	No difference.
(1) Checking the operational availability of sensors by use of the methods described in 6.5.1.	a) Checking the operational availability of sensors by use of the methods described in 6.5.1.	No difference.
(2) Specifying equipment that is stable and retains its calibration during the post-accident time period.	b) Specifying equipment that is stable and the period of time it retains its calibration during the post-accident time period.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
6.6 Operating Bypasses. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:	6.6 Operating bypasses. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:	No difference.
(1) Remove the appropriate active operating bypass(es).	a) Remove the appropriate active operating bypass(es).	No difference.
(2) Restore plant conditions so that permissive conditions once again exist.	b) Restore plant conditions so that permissive conditions once again exist.	No difference.
(3) Initiate the appropriate safety function(s).	c) Initiate the appropriate safety function(s).	No difference.
6.7 Maintenance Bypass. Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of 5.1 and 6.3.	6.7 Maintenance bypass. Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3.	No difference.
EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).	NOTE - For portions of the sense and command features that cannot meet the requirements of 5.1 and *6.3* when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability).	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
6.8 Setpoints 6.8.1 The allowance for uncertainties between the process analytical limit documented in Section 4.4 and the device setpoint shall be determined using a documented methodology. Refer to ISA S67.040-1987.	6.8 Setpoints. The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.	RG 1.105 Rev. 3 now endorses ANSI/ISA S67.04-1994.
6.8.2 Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.	Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features.	No difference.
7. Executive Features - Functional and Design Requirements In addition to the functional and design requirements in Section 5, the following requirements shall apply to the execute features:	7. Execute features (functional and design requirements) In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features.	No difference.
7.1 Automatic Control, Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with 4.4 of the design basis.	7.1 Automatic control. Capability shall be incorporated in the execute features to receive and act upon automatic control signals from the sense and command features consistent with Clause 4, item d) of the design basis.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
7.2 Manual Control. If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.	7.2 Manual control. If manual control of any actuated component in the execute features is provided, the additional design features in the execute features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2. Capability shall be provided in the execute features to receive and act upon manual control signals from the sense and command features consistent with the design basis.	No difference.
7.3 Completion of Protective Action. The design of the execute features shall be such that once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in 4.11 of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (that is, cycling) of specific equipment to maintain completion of the safety function.	7.3 Completion of protective action. The design of the execute features shall be such that, once initiated, the protective actions of the execute features shall go to completion. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. When the sense and command features reset, the execute features shall not automatically return to normal; they shall require separate, deliberate operator action to be returned to normal. After the initial protective action has gone to completion, the execute features may require manual control or automatic control (i.e., cycling) of specific equipment to maintain completion of the safety function.	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
7.4 Operating Bypass. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:	7.4 Operating bypass. Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:	No difference.
(1) Remove the appropriate active operating bypass(es).	a) Remove the appropriate active operating bypass(es).	No difference.
(2) Restore plant conditions so that permissive conditions once again exist.	b) Restore plant conditions so that permissive conditions once again exist.	No difference.
(3) Initiate the appropriate safety function(s).	c) Initiate the appropriate safety function(s).	No difference.
7.5 Maintenance Bypass. The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.	7.5 Maintenance bypass. The capability of a safety system to accomplish its safety function shall be retained while execute features equipment is in maintenance bypass. Portions of the execute features with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.	No difference.
8. Power Source Requirements 8.1 Electrical Power Sources. Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1980.	8. Power source requirements 8.1 Electrical power sources. Those portions of the Class 1E power system that are required to provide the power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std 308-1991.	RG 1.32 Rev. 3 now endorses IEEE Std. 308-2001.

IEEE 603-1991	IEEE 603-1998	Comment
8.2 Non-electrical Power Sources. Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.	8.2 Non-electrical power sources. Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.	No difference.
8.3 Maintenance Bypass. The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.	8.3 Maintenance bypass. The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.	No difference.