



ANP-10309NP
Revision 0

**U.S. EPR Digital Protection System
Technical Report**

November 2009

AREVA NP Inc.

(c) 2009 AREVA NP Inc.

Non-Proprietary

Copyright © 2009

**AREVA NP Inc.
All Rights Reserved**

Nature of Changes

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

Contents

	<u>Page</u>
1.0 INTRODUCTION	1-1
2.0 BACKGROUND	2-1
2.1 NRC Approval of the TXS Platform	2-1
2.2 Plant Specific Action Items	2-2
3.0 DESCRIPTION OF THE U.S. EPR PROTECTION SYSTEM.....	3-1
3.1 System Role	3-1
3.2 System Organization.....	3-1
3.3 System Implementation	3-1
4.0 SYSTEM ARCHITECTURE.....	4-1
4.1 Overall System Architecture	4-1
4.2 System Architecture Features.....	4-1
5.0 PROTECTION SYSTEM UNITS.....	5-3
5.1 Remote Acquisition Units.....	5-3
5.2 Acquisition and Processing Units.....	5-3
5.3 Actuation Logic Units	5-4
5.4 Monitoring and Service Interfaces	5-4
5.5 Rod Control Cluster Assembly Units.....	5-5
5.6 Service Unit	5-5
5.7 Gateways.....	5-6
6.0 DETAILED SYSTEM ARCHITECTURE.....	6-8
6.1 General Network Concepts.....	6-8
6.2 RCCAU – APU Architecture	6-11
6.3 RAU – APU Architecture	6-11
6.4 APU – ALU Architecture (Subsystem A)	6-11
6.5 APU – ALU Architecture (Subsystem B).....	6-12
6.6 MSI-MU – APU Architecture	6-13
6.7 MSI-MU – RCCAU – RAU – ALU – MSI-AU Architecture	6-13
6.8 MSI-MU – GW – SU Architecture	6-13
7.0 REACTOR TRIP.....	7-1
7.1 Typical Automatic Reactor Trip Sequence.....	7-1
7.2 SPND Based Automatic Reactor Trip Sequence	7-2
7.3 Reactor Trip Voting Logic	7-3
7.4 Identification of Invalid Signals.....	7-4
7.5 Reactor Trip Outputs.....	7-5
7.6 Manual Reactor Trip	7-6
7.7 Reactor Trip Devices	7-6

7.8	Trip Breakers	7-7
7.9	Trip Contactors	7-7
7.10	Transistors of CRDM Operating Coils.....	7-7
8.0	ENGINEERED SAFETY FEATURES ACTUATION	8-1
8.1	Typical Automatic ESF Actuation Sequence.....	8-1
8.2	ESF Actuation Voting Logic	8-2
8.3	ESF Actuation Outputs	8-2
8.4	Divisional Assignments – ESF Actuation Outputs.....	8-3
8.5	System Level Manual ESF Actuations	8-4
9.0	PERMISSIVE SIGNALS.....	9-1
9.1	Definition.....	9-1
9.2	Design Rules for Implementation of Permissive Signals.....	9-2
10.0	SIGNAL DIVERSITY	10-1
10.1	Definition.....	10-1
10.2	Design Rules	10-1
11.0	INTERCHANNEL COMMUNICATION.....	11-3
11.1	Communication Interfaces	11-3
11.2	Communications Independence	11-3
12.0	SAFETY TO NON-SAFETY-RELATED INTERFACE.....	12-1
12.1	General Requirements for Interfaces.....	12-1
12.2	Protection System – Service Unit Interface.....	12-1
12.3	Protection System – PICS Interface	12-2
12.4	Protection System – Control System Interface	12-3
13.0	COMPLIANCE WITH IEEE STD 603.....	13-1
13.1	Use of IEEE Std 603-1998.....	13-1
14.0	SUMMARY/CONCLUSIONS.....	14-3
15.0	REFERENCES.....	15-4
APPENDIX A COMPARISON OF IEEE STD 603-1991 TO IEEE STD 603-1998		A-1

List of Tables

Table 1-1—Generic Hardware Equivalence	1-2
--	-----

List of Figures

Figure 6-1—Example of Redundant Point-to-Point Connection	6-15
Figure 6-2—Example of Redundant Ring Connection.....	6-16
Figure 6-3—RCCA – APU Architecture	6-17
Figure 6-4—RAU1 – Div 1 APU Architecture	6-18
Figure 6-5—RAU1 – Div 2 APU Architecture	6-19
Figure 6-6—RAU1 – Div 3 APU Architecture	6-20
Figure 6-7—RAU1 – Div 4 APU Architecture	6-21
Figure 6-8—RAU2 – APU Architecture	6-22
Figure 6-9—Subsystem A Div 1 APU – ALU Architecture.....	6-23
Figure 6-10—Subsystem A Div 2 APU – ALU Architecture.....	6-24
Figure 6-11—Subsystem A Div 3 APU – ALU Architecture.....	6-25
Figure 6-12—Subsystem A Div 4 APU – ALU Architecture.....	6-26
Figure 6-13—Subsystem B Div 1 APU – ALU Architecture.....	6-27
Figure 6-14—Subsystem B Div 2 APU – ALU Architecture.....	6-28
Figure 6-15—Subsystem B Div 3 APU – ALU Architecture.....	6-29
Figure 6-16—Subsystem B Div 4 APU – ALU Architecture.....	6-30
Figure 6-17—MSI-MU – APU Architecture.....	6-31
Figure 6-18—MSI-MU – RCCA – RAU – ALU – MSI-AU Architecture	6-32
Figure 6-19—MSI-MU – GW – SU Architecture	6-33
Figure 7-1—Typical Reactor Trip Sequence (One Division).....	7-8
Figure 7-2—SPND-Based Reactor Trip Sequence (One Division).....	7-9

Figure 7-3—Reactor Trip Outputs in One Division	7-10
Figure 7-4—Concept for Manual Reactor Trip (One Division).....	7-11
Figure 7-5—Reactor Trip Breakers and Reactor Trip Contactors	7-12
Figure 7-6—Reactor Trip Signals to Rod Control Transistors	7-13
Figure 8-1—Typical ESFAS Actuation Sequence (One Division).....	8-5
Figure 8-2—Example of PS Divisional Assignment to an ESF Actuation.....	8-6
Figure 11-1—TXS Communication Principle.....	11-7
Figure 11-2—Communications Independence (IEEE Std. 7-4.3.2).....	11-8
Figure 11-3—Communications Independence (U.S. EPR Implementation).....	11-8
Figure 12-1—Safety to Non-Safety Communication Interface (IEEE Std. 7-4.3.2).....	12-5
Figure 12-2—Safety to Non-Safety Communication Interface (U.S. EPR Implementation)	12-5

Nomenclature

Acronym	Definition
ALU	Actuation Logic Unit
APU	Acquisition and Processing Unit
CFR	Code of Federal Regulations
CRDM	Control Rod Drive Mechanism
DAC	Design Acceptance Criteria
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
I&C	Instrumentation and Control
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)
PICS	Process Information and Control System
PROFIBUS	Process Field Bus
PS	Protection System
RAU	Remote Acquisition Unit
RCCA(U)	Rod Control Cluster Assembly (Unit)
RPS	Reactor Protection System
RSS	Remote Shutdown Station
RT	Reactor Trip
SICS	Safety Information and Control System
SPACE	Specification and Coding Environment
SPND	Self-Powered Neutron Detector
SU	Service Unit
TXS	TELEPERM XS
V&V	Verification and Validation

1.0 INTRODUCTION

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

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

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

The PS provides signal diversity, as described in Section 10.0, "Signal Diversity." The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). AREVA NP takes credit for the signal diversity within the PS, as described in this report, in the U.S. EPR 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 heavily depend on I&C systems. The TXS platform is designed for use in safety-related automation applications and to meet safety-related I&C requirements. Typical uses include RPS and ESFAS functions, but the TXS platform can also perform a wide variety of functions (e.g., core monitoring and control, rod position monitoring, emergency diesel generator controls).

2.1 *NRC Approval of the TXS Platform*

As previously noted, the TXS platform is described in Reference 24, which has been reviewed and approved by the NRC (Reference 23). Reference 24 describes the TXS hardware and operating system software design, platform qualification testing, and application software capabilities. As noted in Reference 24, TXS is a qualified, 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.
 - Specification and coding environment (SPACE) tool for application software development.
- Equipment qualification methods.
- Operating system software development process, including verification and validation (V&V) methods.
- Processing principles:
 - Operating system operation.
 - Runtime environment operation.
 - Cyclic, deterministic, asynchronous operation.
- Inter-channel communication principles.
- Service unit (SU) maintenance interface.

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

2.2 *Plant Specific Action Items*

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

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

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

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

3.0 DESCRIPTION OF THE U.S. EPR PROTECTION SYSTEM

3.1 *System Role*

The PS is an 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 also processes manual commands and issues 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 signal diversity for RT functions. Each subsystem is divided into functional units based on the types of functionality required (e.g., signal acquisition, processing, voting, actuation). Descriptions of the PS functional units are provided in Section 5.0.

3.3 *System Implementation*

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

The TXS platform is applied to the PS design to obtain a 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 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 use self-powered neutron detectors (SPND) as inputs. For these functions, three layers of operation are used. Computers dedicated to the acquisition and distribution of 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 *Overall System Architecture*

The architecture of the PS is shown in U.S. EPR FSAR Tier 2, Figure 7.1-6. 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 Safeguard Building. The center of the figure represents the control complex shared between Safeguard Building 2 and 3. Within the quadrant representing each PS division, the upper portion represents Subsystem A and the lower portion represents Subsystem B.

In the PS architecture, the monitoring and service interface (MSI) serves as the safety to non-safety isolation point for networked connections. Those on the safety-related side of the MSI main unit (MSI-MU) are required to be Class 1E networks. Network connections on the non-safety side of the MSI-MU are non-Class 1E. Hardwired connections are used primarily for transmission of actuation orders.

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

4.2 *System Architecture Features*

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

4.2.1 *Physical Separation*

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

4.2.2 Power Supply

Each PS division is supplied by 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 24 Vdc feeds. To cope with loss of onsite and offsite power, the uninterruptible feeds to the PS cabinets are supplied with two-hour batteries.

4.2.3 Redundancy

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

4.2.4 Subsystems

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

5.0 PROTECTION SYSTEM UNITS

There are seven types of functional units that compose the PS: remote acquisition, acquisition and processing, actuation logic, monitoring and service interfaces, rod control cluster assembly, service, and gateways.

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

5.1 *Remote Acquisition Units*

The remote acquisition unit (RAU) primary functions are to acquire the signals from the SPND and 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 and distributes the signals to two APUs in each of the four divisions. Therefore, all 72 SPND measurements are processed by each APU.

5.2 *Acquisition and Processing Units*

The APU primary functions are to:

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

5.3 Actuation Logic Units

The ALU primary functions are to perform voting of processing results from the redundant APU in the various divisions and to issue actuation orders based on voting results. The ALU also contains the logic used to latch and either manually or automatically unlatch actuation outputs. Each ALU consists of a function 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. 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 (i.e., MSI-MU), and the auxiliary unit (i.e., MSI-AU). The MSI performs functions related to both subsystems; therefore, they

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

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

The MSI-MU primary functions are to provide status monitoring and data transfer. The MSI-MU facilitates monitoring for conditions, such as communication failures between other PS units, and for protection channel status information. The MSI-MU data transfer functions include transferring manual commands to the APU and ALU, information for display to the operators, and 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 primary function is to acquire and process 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 transferred 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 functional status.

- Performing periodic tests of the system.
- Modifying the changeable software parameters.
- Loading new software versions.

The PS contains one SU; the SU communicates with the units in the four PS divisions. The SU serves both subsystems in every division; therefore, it is not assigned to a particular subsystem. The SU communicates with the PS units through each division's MSI-MU and can be accessed through a service terminal in the I&C service center, a computer within each Safeguard Building, and a location in the main control room (MCR).

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

5.7 Gateways

The gateway (GW) primary function is to perform the exchanges between the PS and the process information and control system (PICS). The GW transfers information from the PS to the PICS for display and archival storage and receives operator orders (e.g., function resets, permissive validations) from the PICS. The GW converts TXS communication mechanisms into those used by the PICS, and vice versa.

The PS contains two GWs; one assigned to Division 2 and one assigned to Division 3. Each GW is divided into two sub-units (GW1 and GW2), for a total of four sub-units. Each sub-unit communicates with the MSI-MU in the four PS divisions through a switching unit. During operation, a GW1 sub-unit and a GW2 sub-unit (possibly from different divisions) are in the active operational mode (master), and together they fulfill the requirements of the PS-PICS interface. The remaining two sub-units remain in the standby operational state and have the same internal image as their respective master. During switchover between master and standby, the operation of the GW continues undisturbed and the information remains consistent.

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

6.0 DETAILED SYSTEM ARCHITECTURE

6.1 *General Network Concepts*

The detailed system architecture is represented through a series of figures (Figure 6-3–Figure 6-19) showing network connections between the different units of the PS. These figures represent the intended PS network design. They are provided to assist in understanding the general network concepts described in this section, but are subject to modification during the U.S. EPR detailed design process.

In general, two types of Class 1E network topologies are used within the PS. These are redundant point-to-point and redundant ring topologies. A given network topology includes optical link modules (OLM) and the connections between them. Multiple PS units can access a network through the same OLM; therefore, the OLMs are considered part of the network and are not part of any PS unit.

6.1.1 *Redundant Point-to-Point Network Topology*

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

6.1.2 *Redundant Ring Network Topology*

A redundant ring network topology consists of at least three OLMs and their corresponding double fiber optical links. A given redundant ring network topology can contain only a finite number of OLMs. Each network in the PS contains fewer OLMs than the maximum allowed. Each double fiber optical link consists of a separate

transmit and receive channel. In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of one OLM, does not affect network availability. If an OLM is lost, only the unit(s) directly connected to the failed OLM is affected. The remaining units accessing the ring network can still communicate with one another. The redundant ring topology is shown in Figure 6-2.

6.1.3 Network Topologies – Independence of PS Divisions

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

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

6.1.4 Network Operation Concepts

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

6.1.4.1 *Send Echo*

When an OLM receives a message via any channel, the message is forwarded to the other channels for transmission. If the receiving channel is an optical channel, the module also returns the message to the sending OLM as an echo. Accordingly, a message is propagated to the other OLMs on a network, and the echo is sent to the sending OLM to verify the integrity of the optical segment. The echo is terminated when received by the OLM and is not allowed to propagate to the connected PS function computers.

6.1.4.2 *Monitor Echo*

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

6.1.4.3 *Suppress Echo*

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

6.1.4.4 *Segmentation*

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

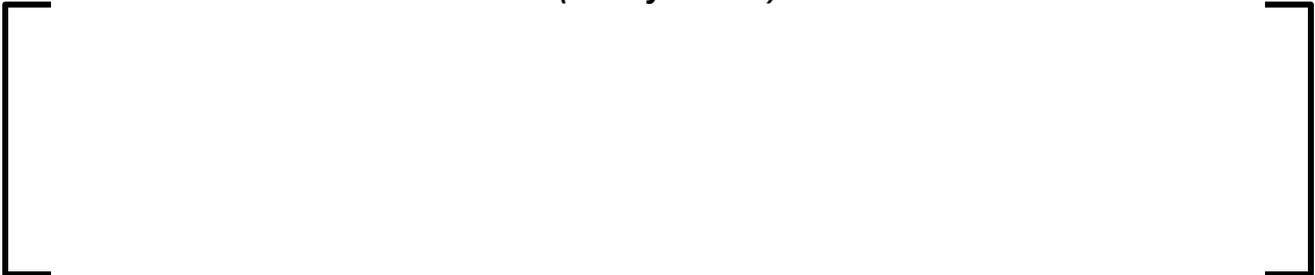
6.2 *RCCAU – APU Architecture*



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 – GW – SU Architecture





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

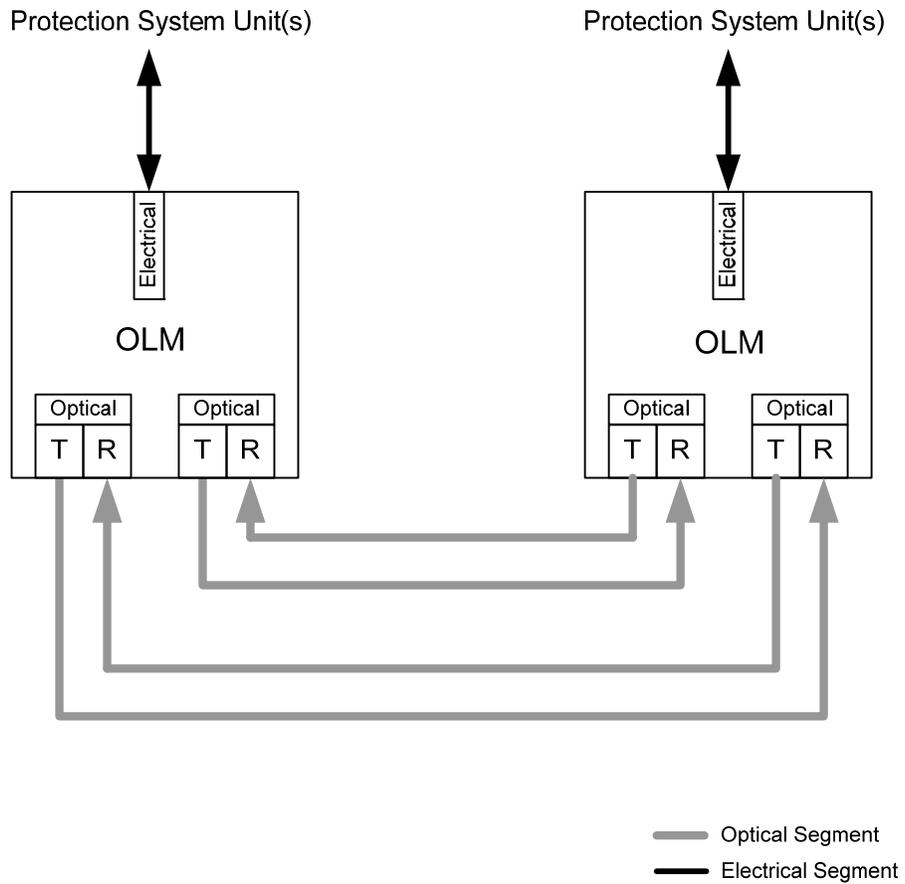


Figure 6-2—Example of Redundant Ring Connection

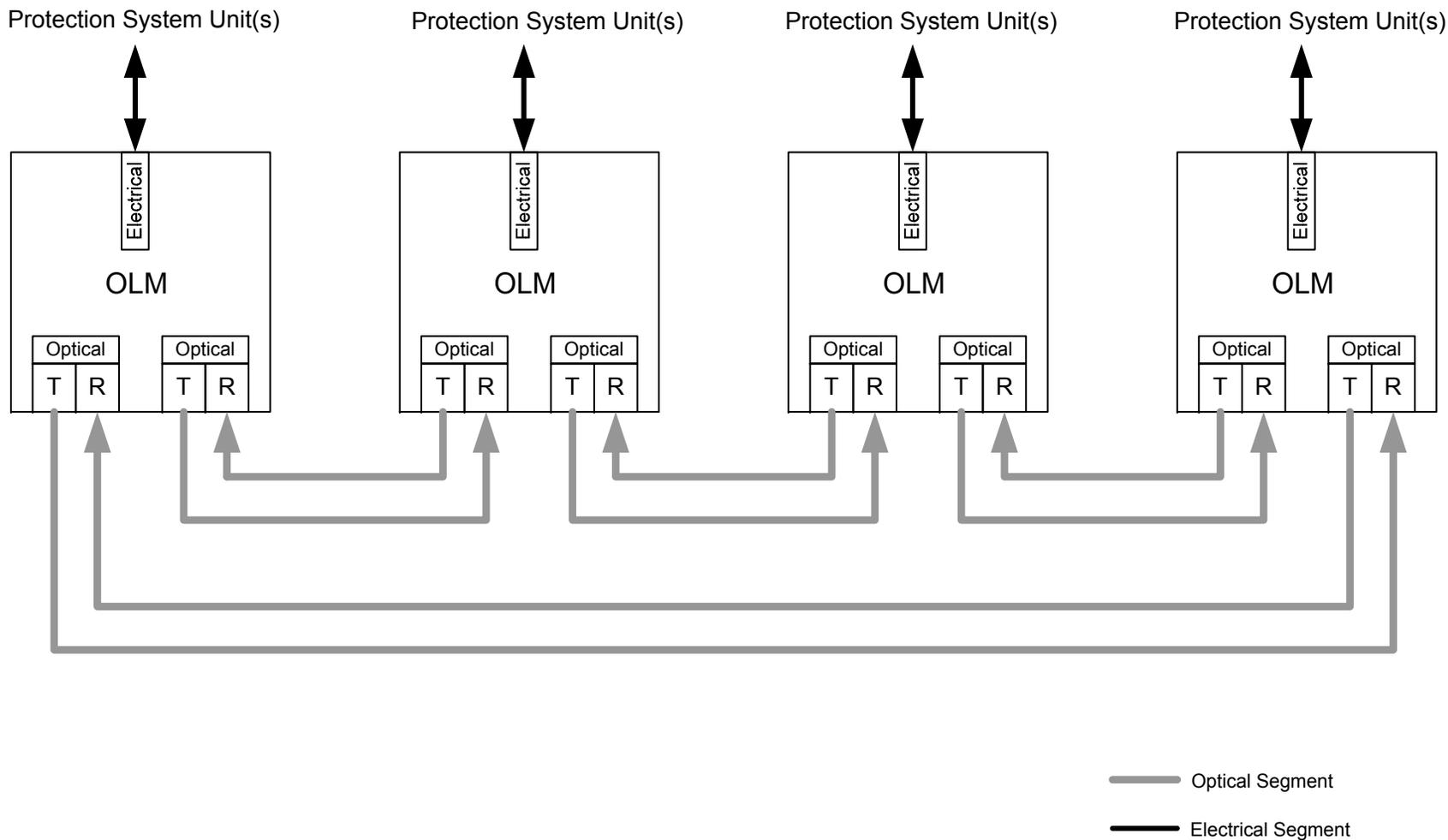


Figure 6-3—RCCAU – APU Architecture

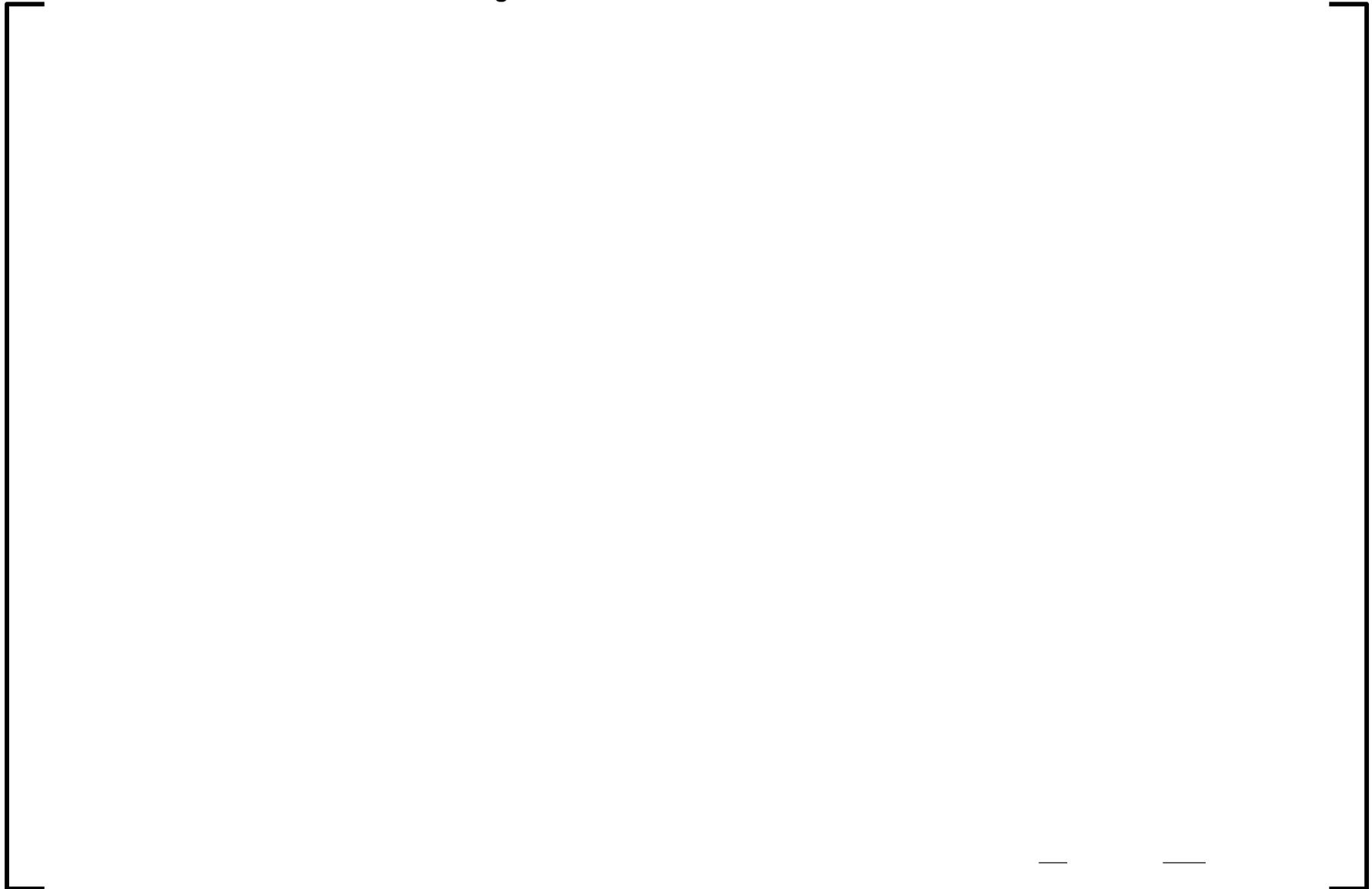


Figure 6-4—RAU1 – Division 1 APU Architecture

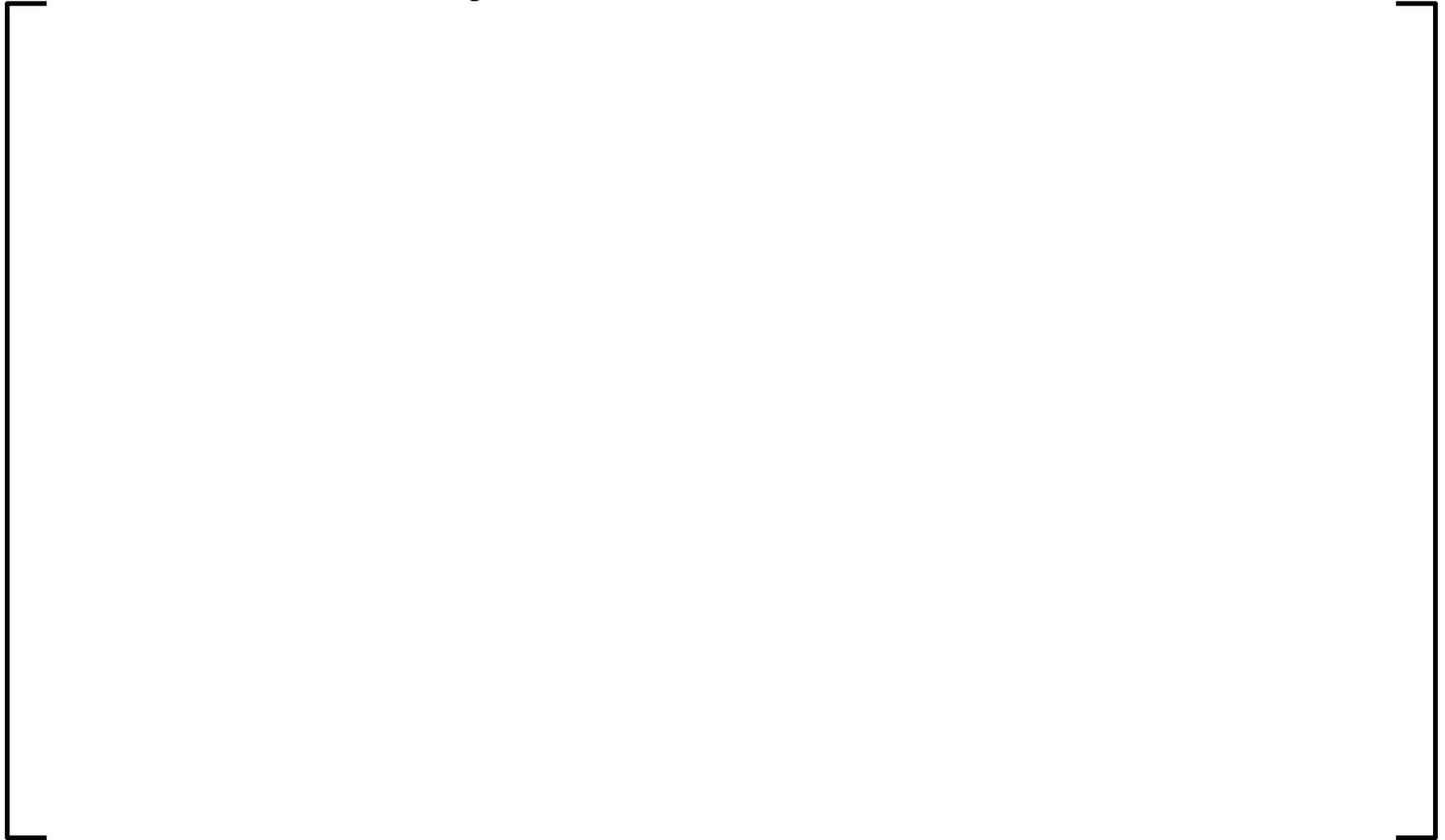


Figure 6-5—RAU1 – Division 2 APU Architecture

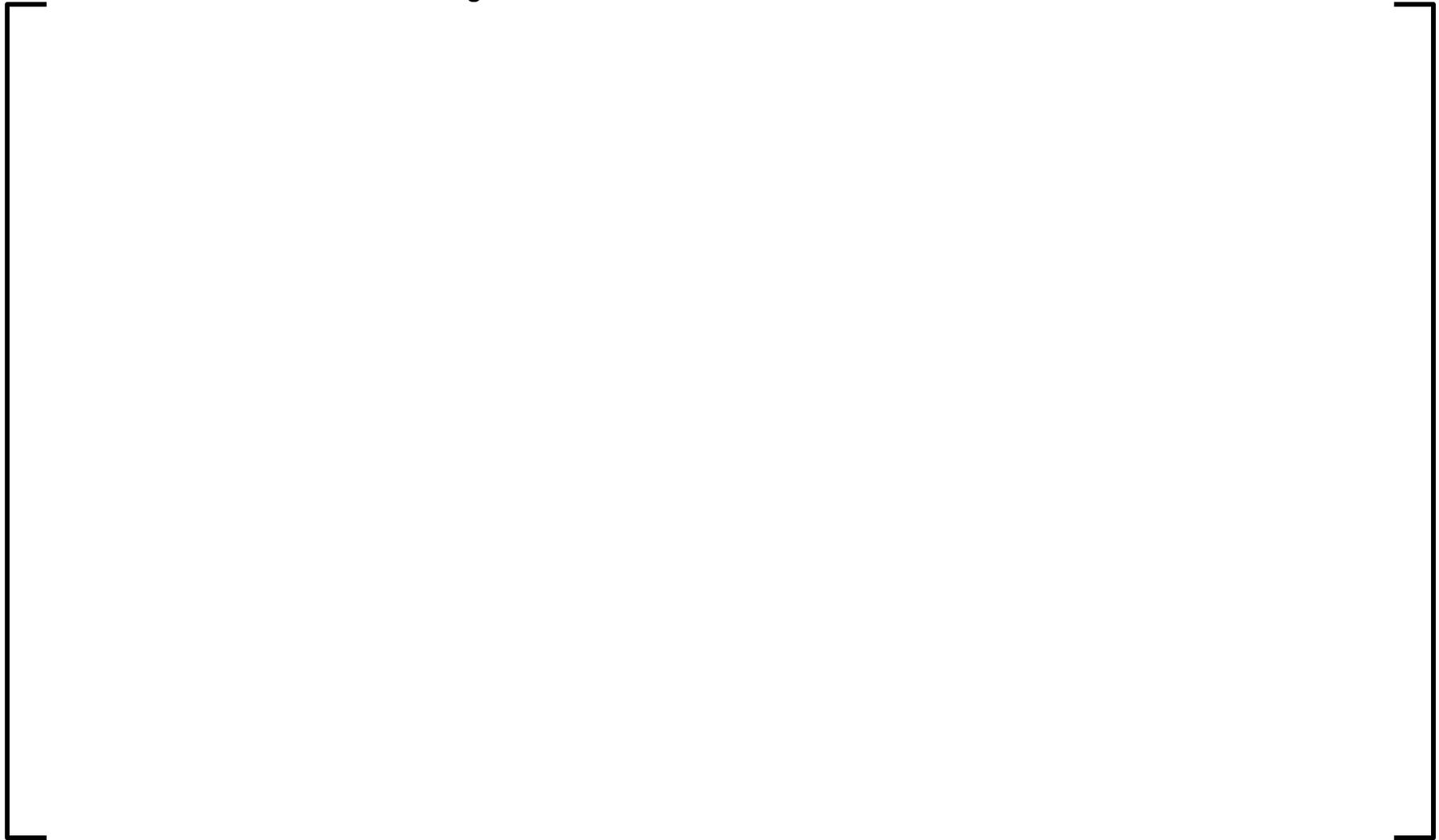


Figure 6-6—RAU1 – Division 3 APU Architecture

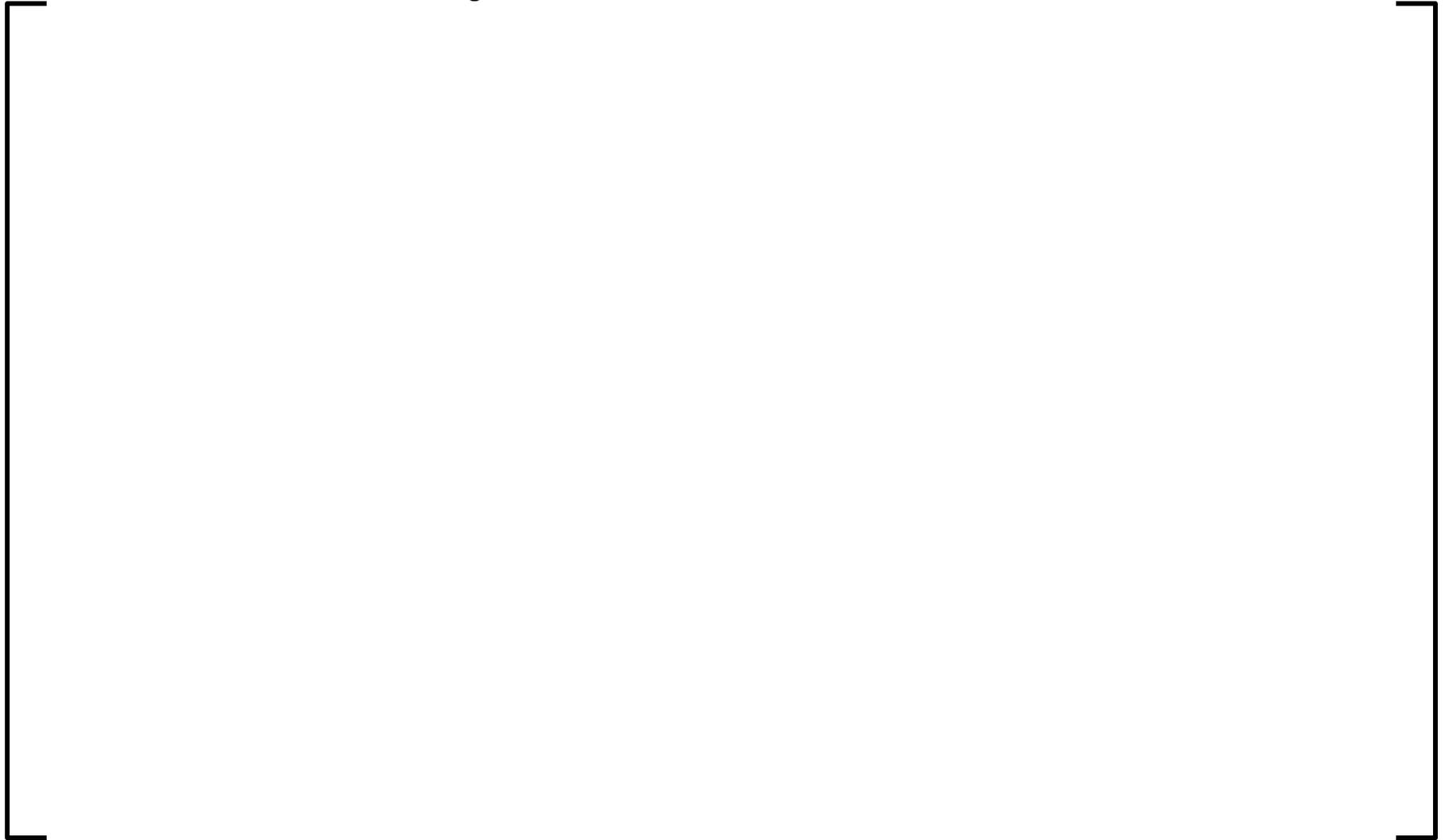


Figure 6-7—RAU1 – Division 4 APU Architecture

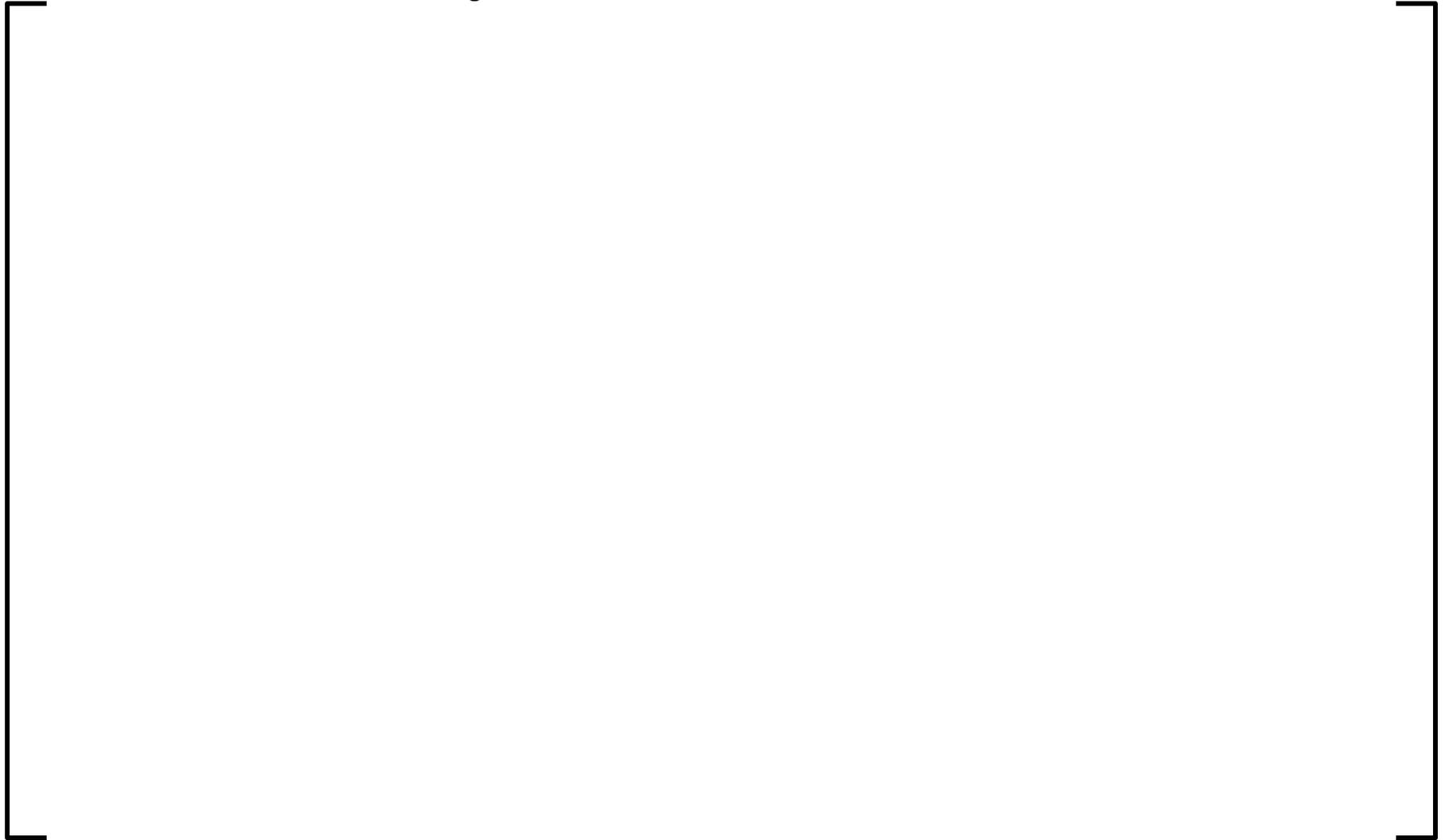


Figure 6-8—RAU2 – APU Architecture



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

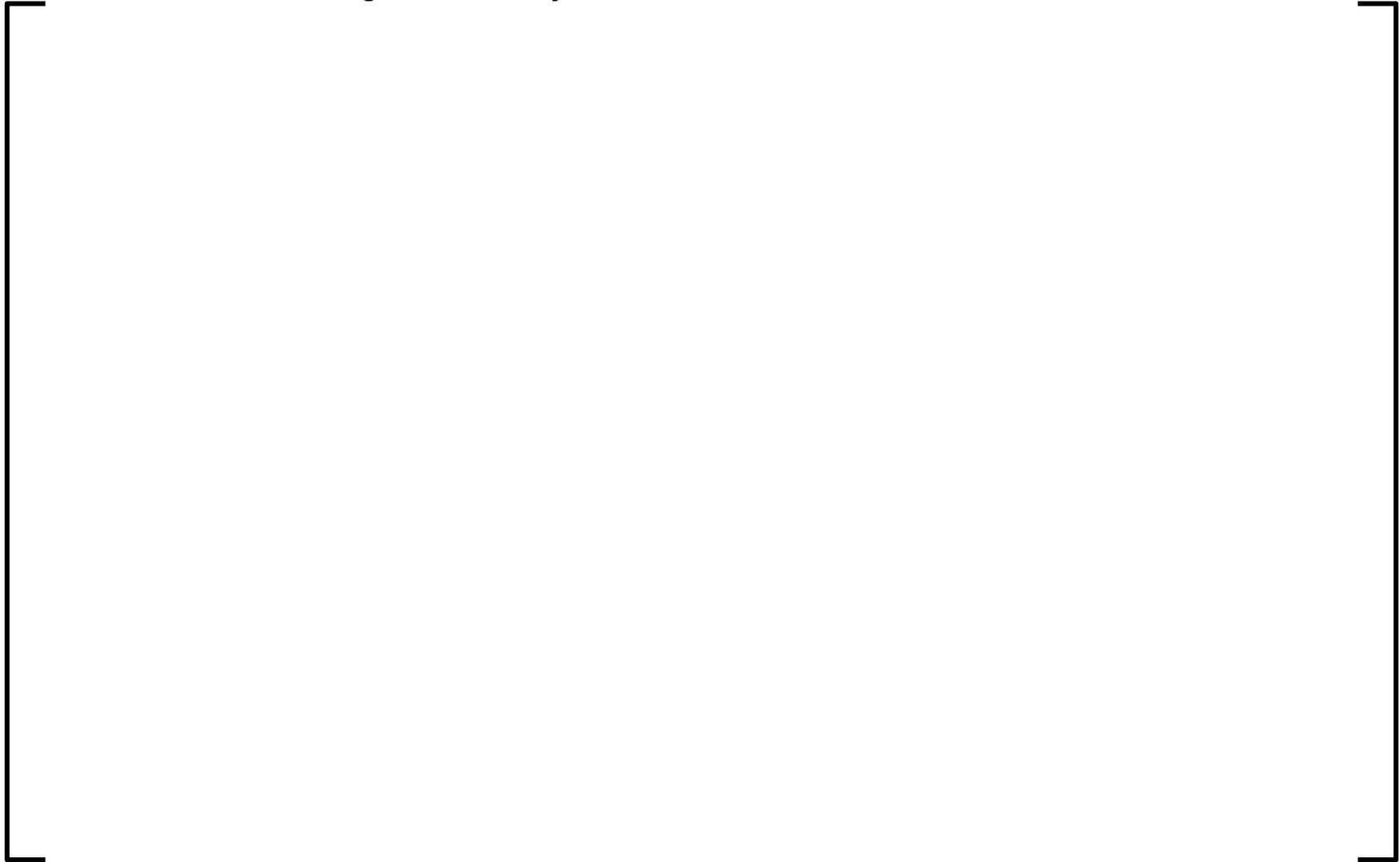


Figure 6-10—Subsystem A Division 2 APU – ALU Architecture

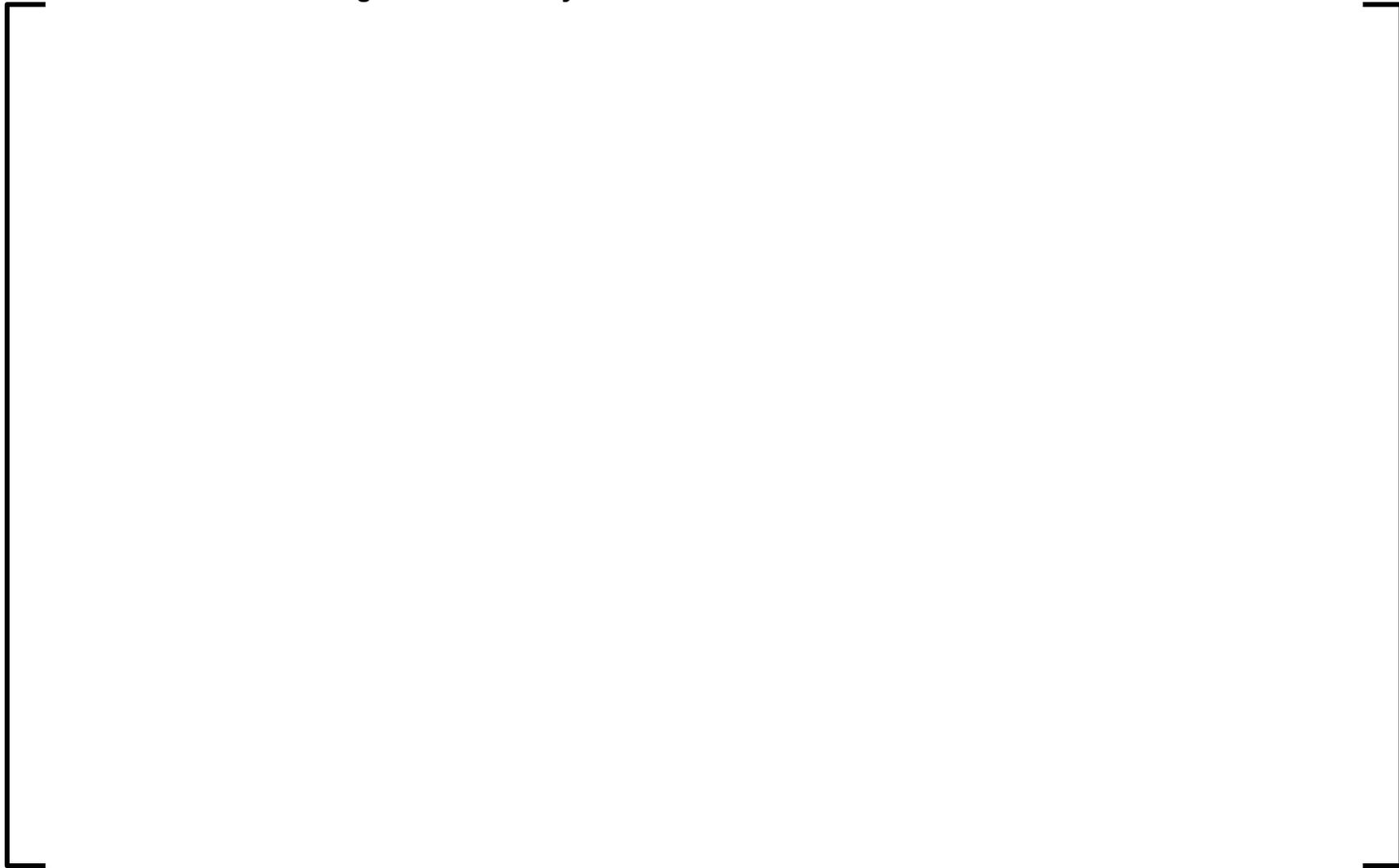


Figure 6-11—Subsystem A Division 3 APU – ALU Architecture

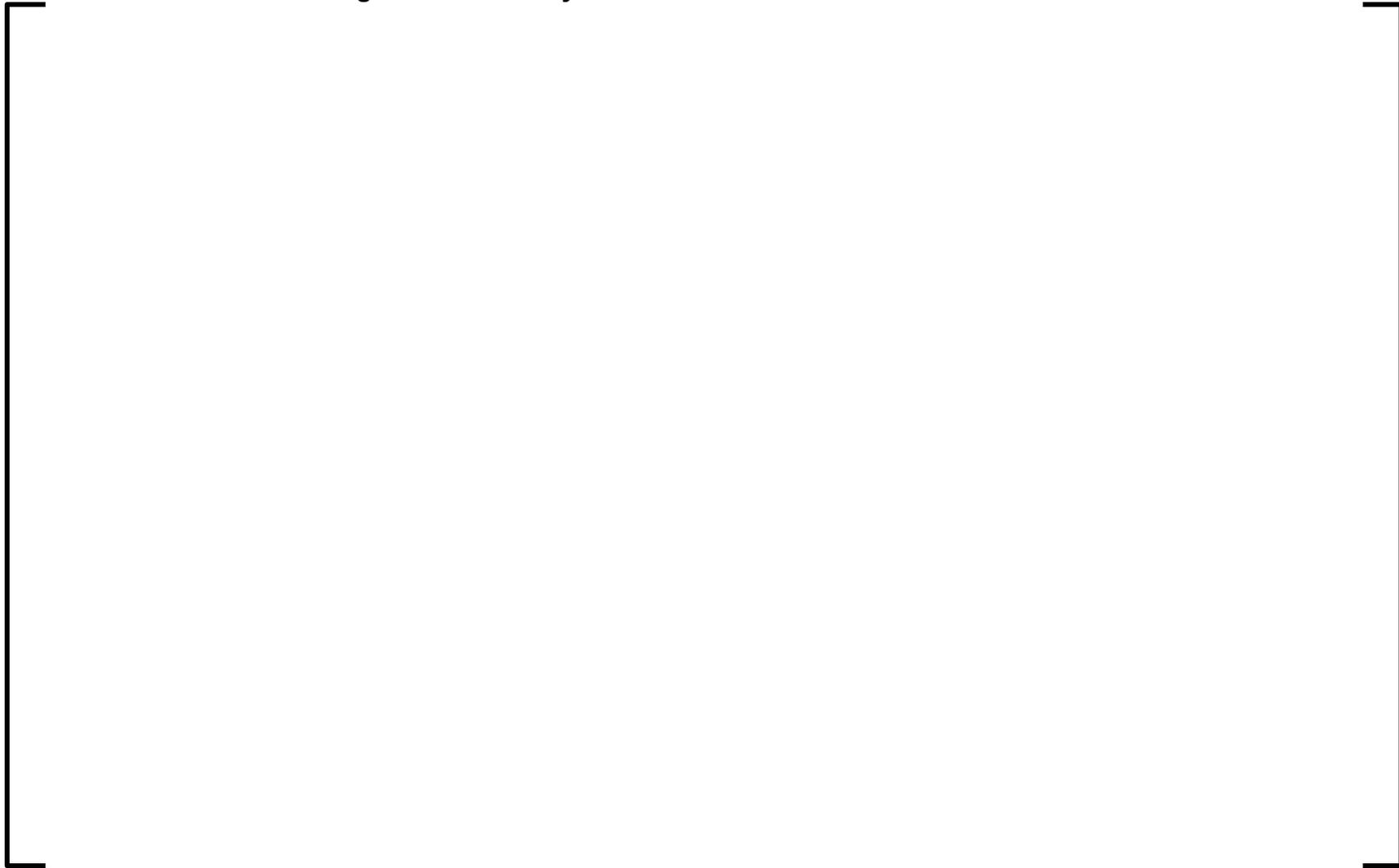


Figure 6-12—Subsystem A Division 4 APU – ALU Architecture

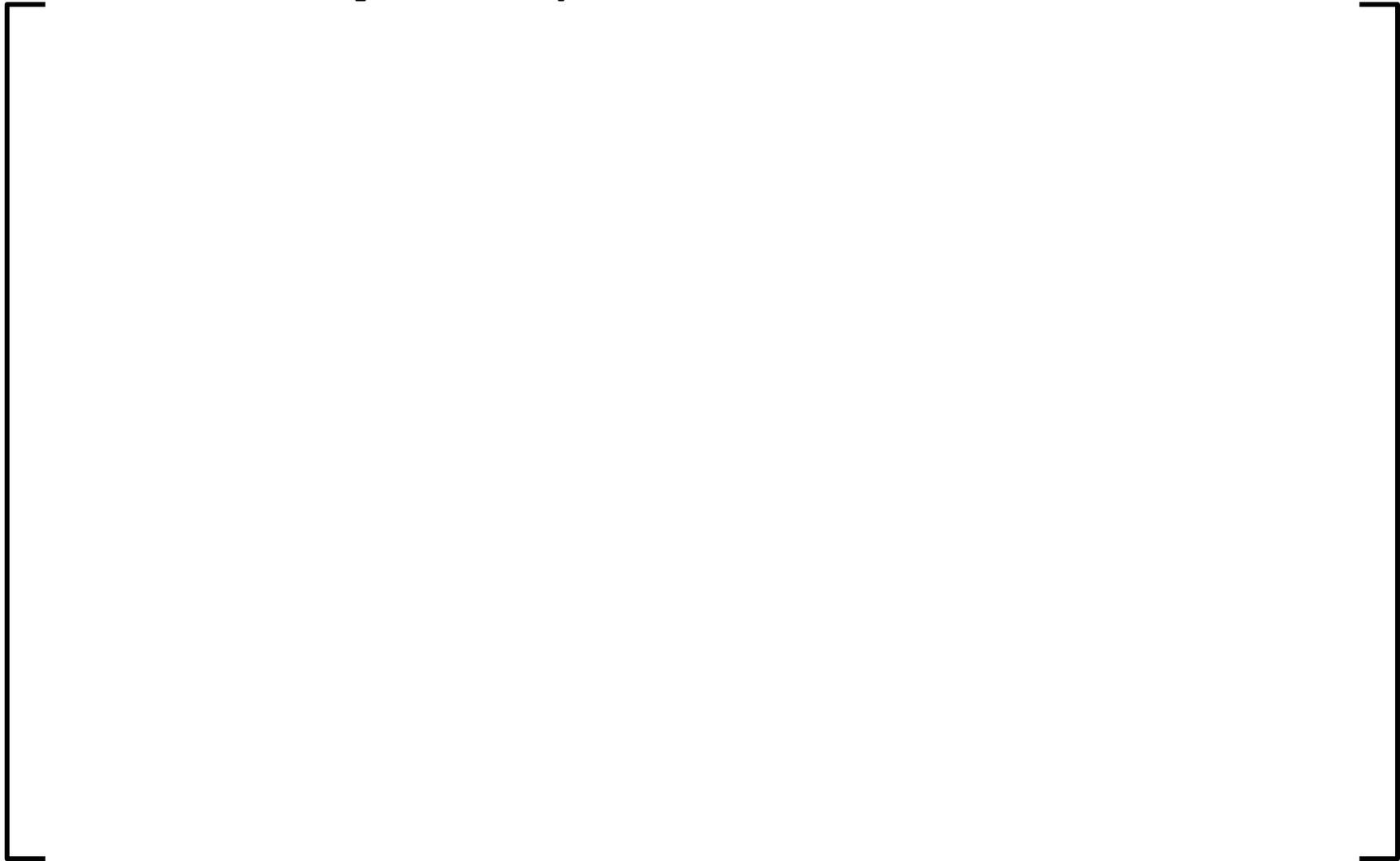


Figure 6-13—Subsystem B Division 1 APU – ALU Architecture

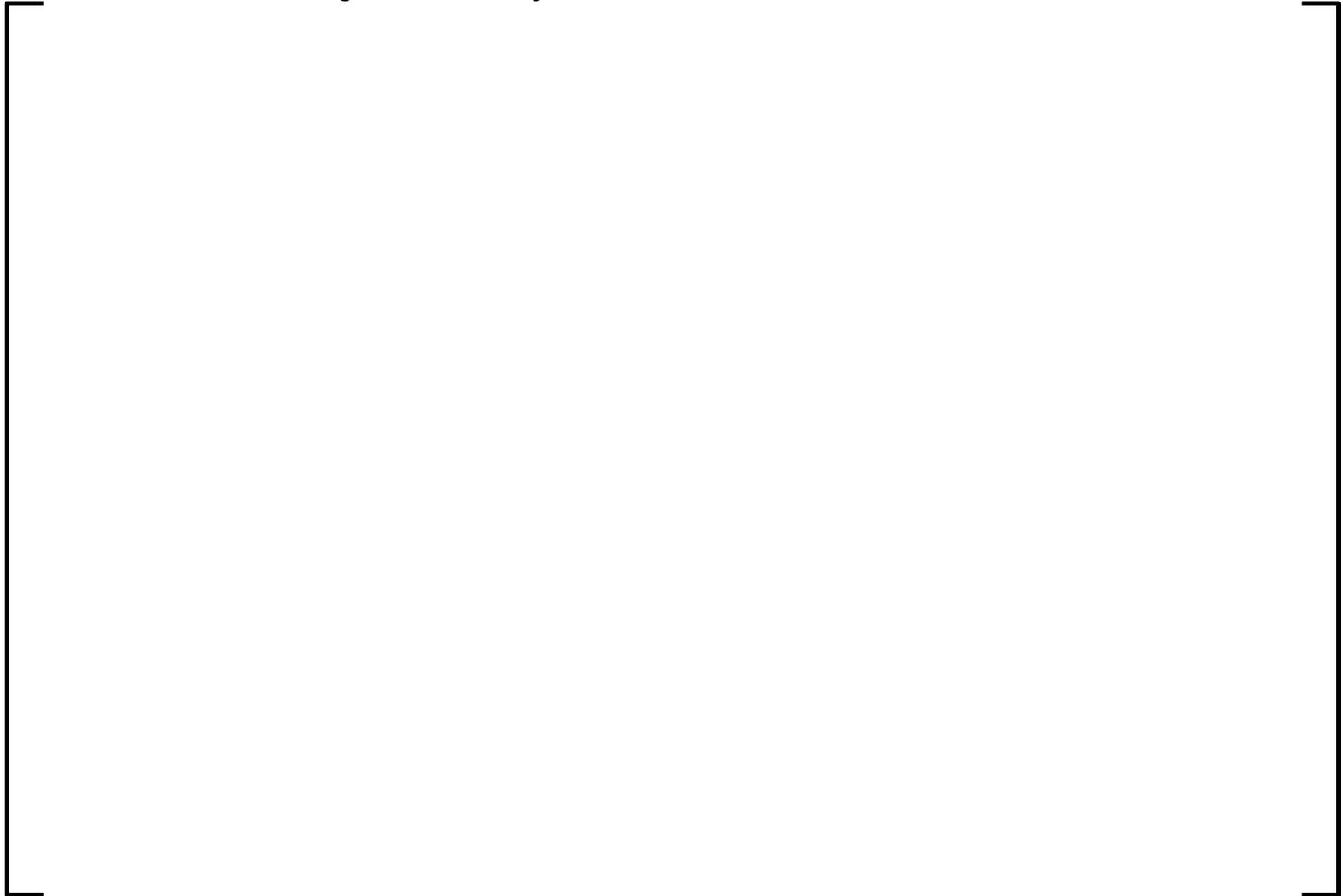


Figure 6-14—Subsystem B Division 2 APU – ALU Architecture

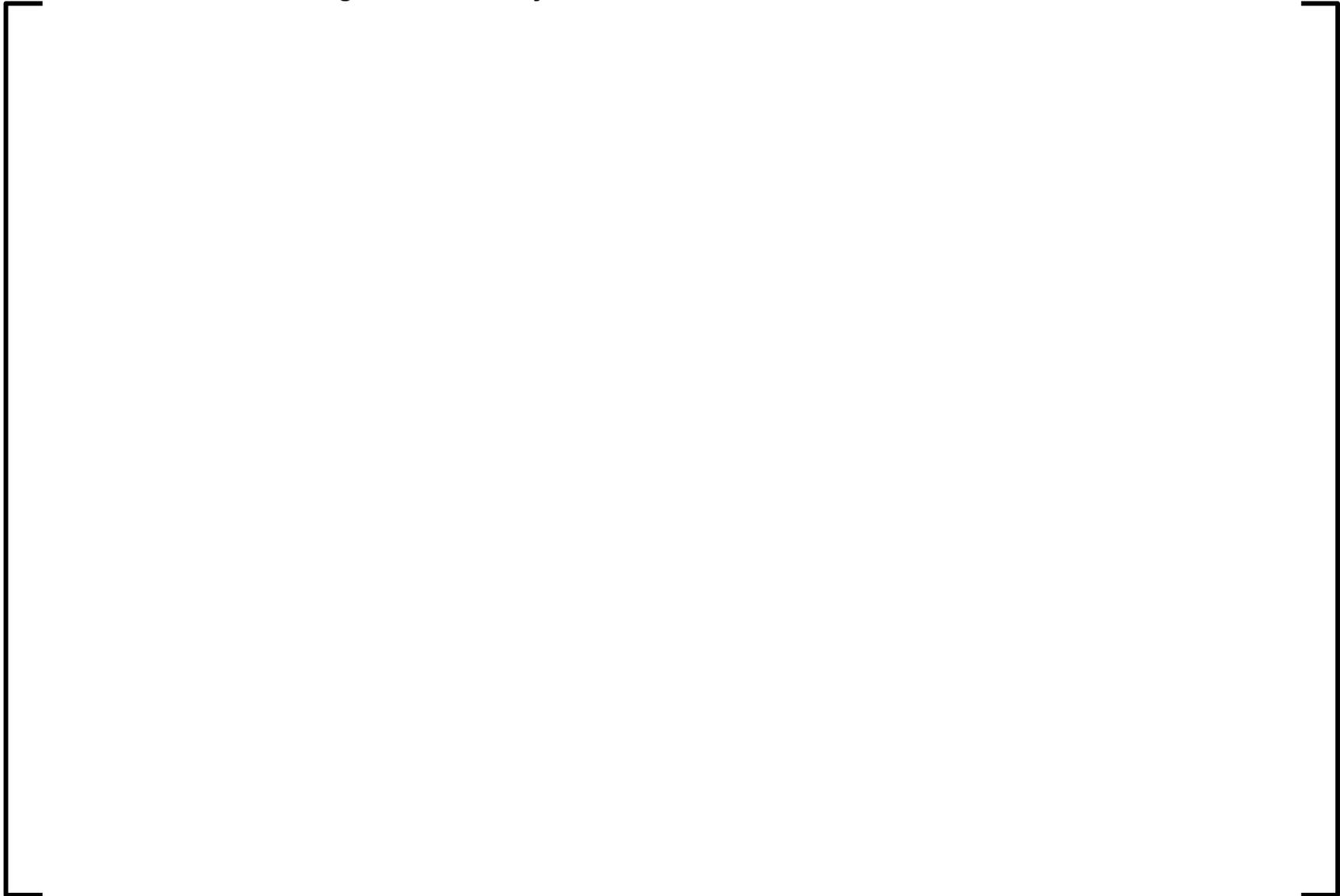


Figure 6-15—Subsystem B Division 3 APU – ALU Architecture

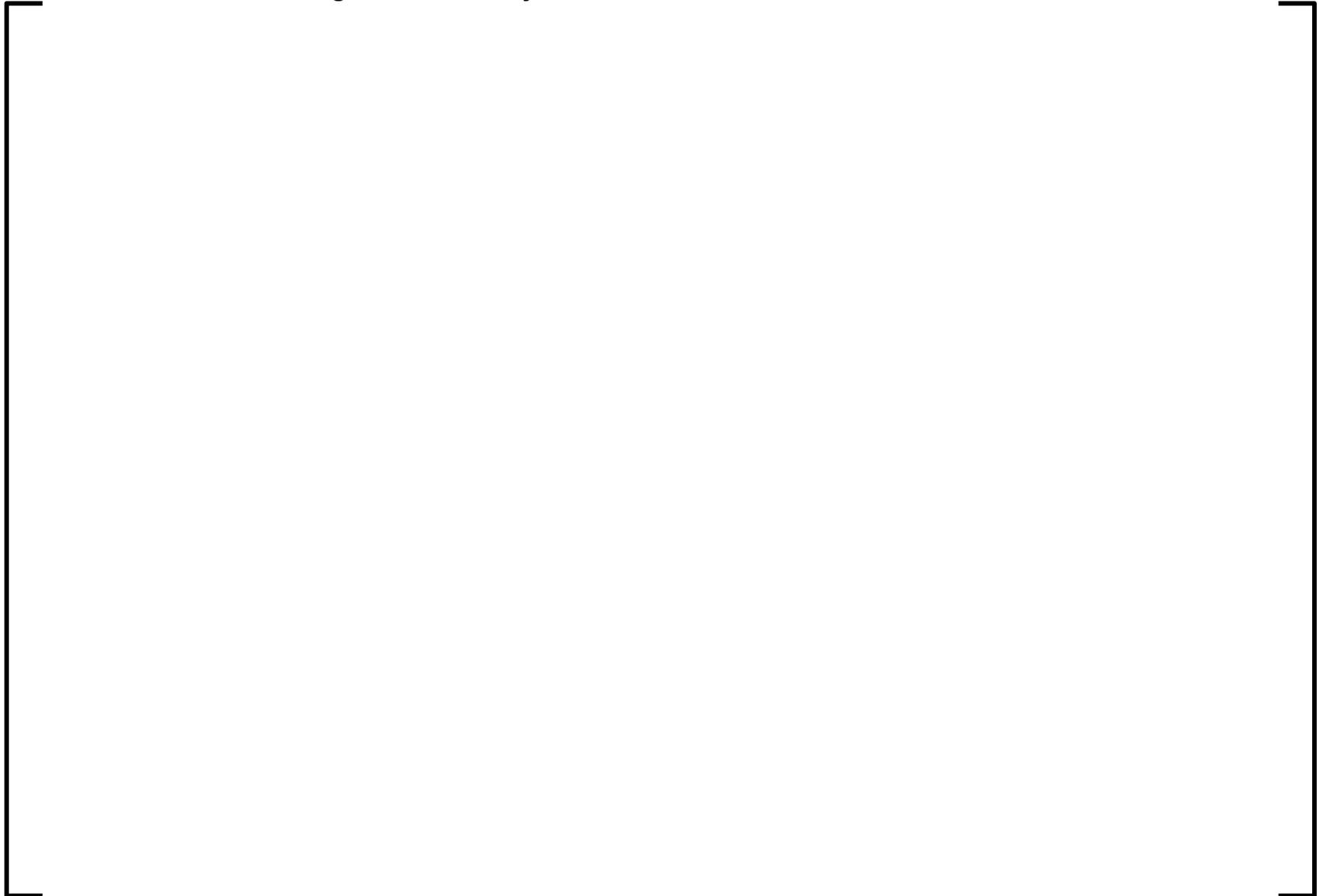


Figure 6-16—Subsystem B Division 4 APU – ALU Architecture

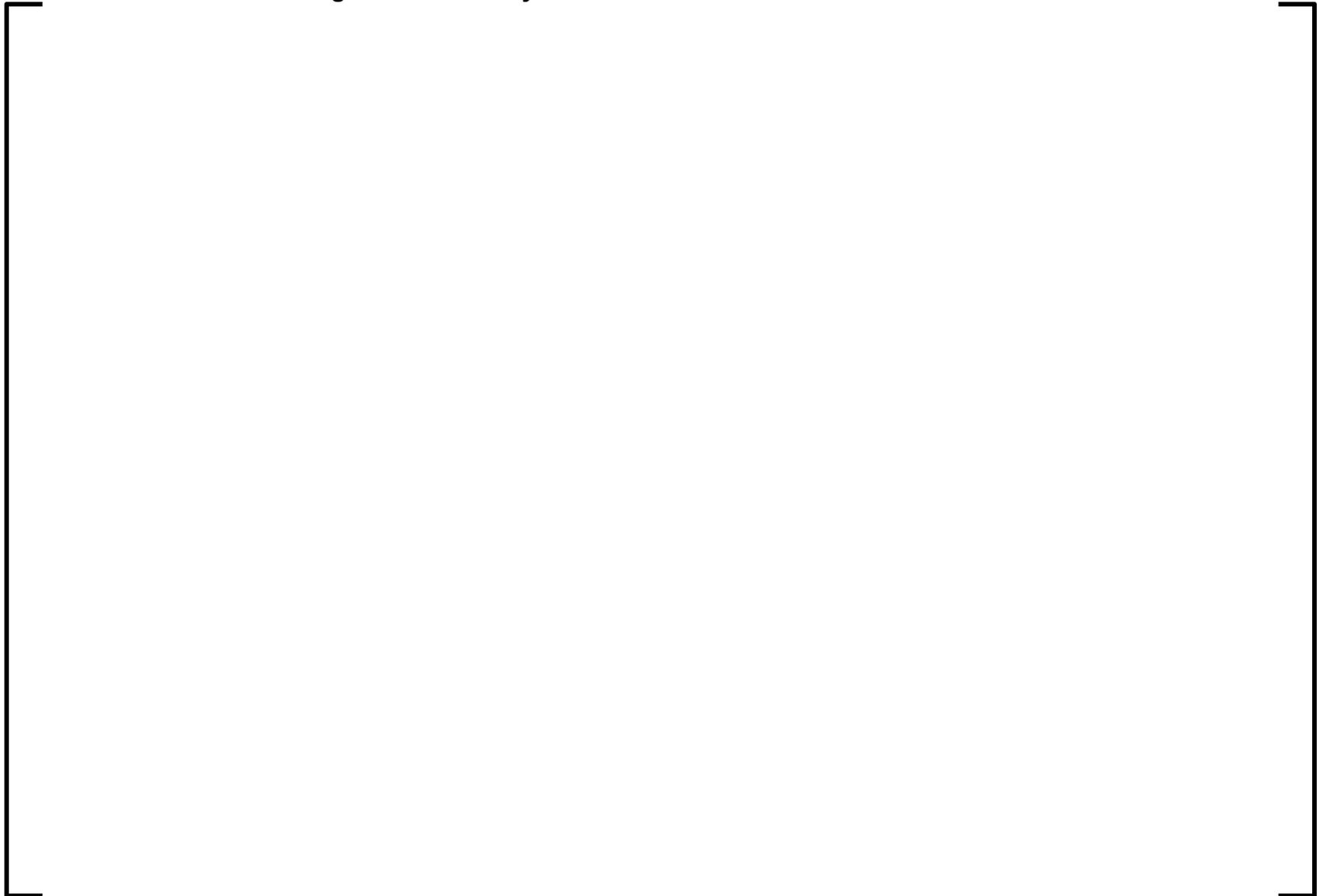


Figure 6-17—MSI-MU – APU Architecture

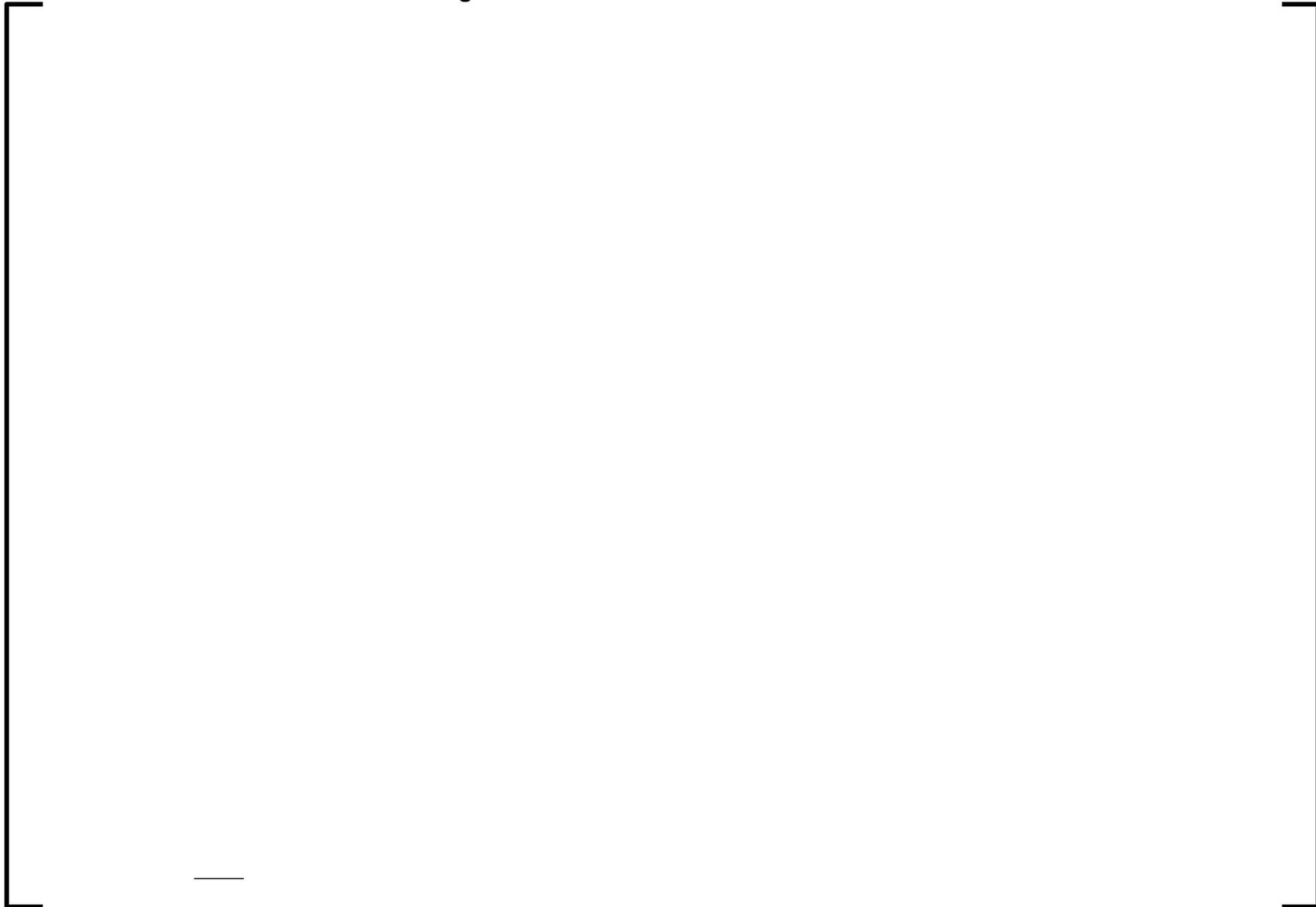


Figure 6-18—MSI-MU – RCCA – RAU – ALU – MSI-AU Architecture

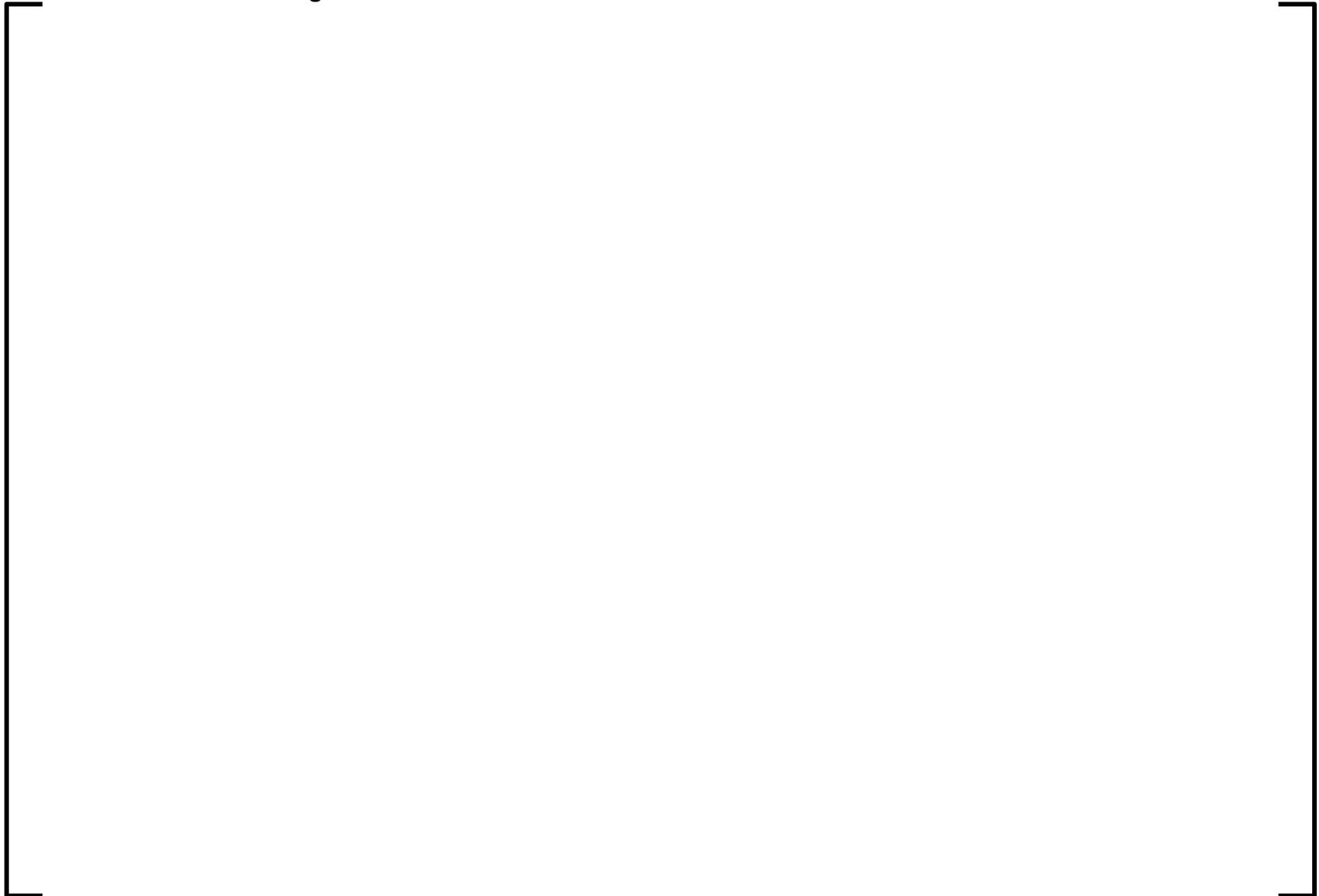


Figure 6-19—MSI-MU – GW – SU Architecture



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 uses 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 transferred to redundant ALU in each PS division.
- Two out of four voting is performed on the partial trigger signals in each ALU. If additional logic is needed (e.g., comparison to permissive conditions), the ALU performs this logic.
- If the vote result is TRUE and the actuation logic (if any) is satisfied, the ALU generates an RT signal.
- The RT signals of the redundant ALU in each subsystem are combined in a hardwired functional AND logic (Section 7.5), resulting in an RT output.

- The RT outputs from each subsystem within a division are then combined into a hardwired “functional OR” logic (Section 7.5), 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

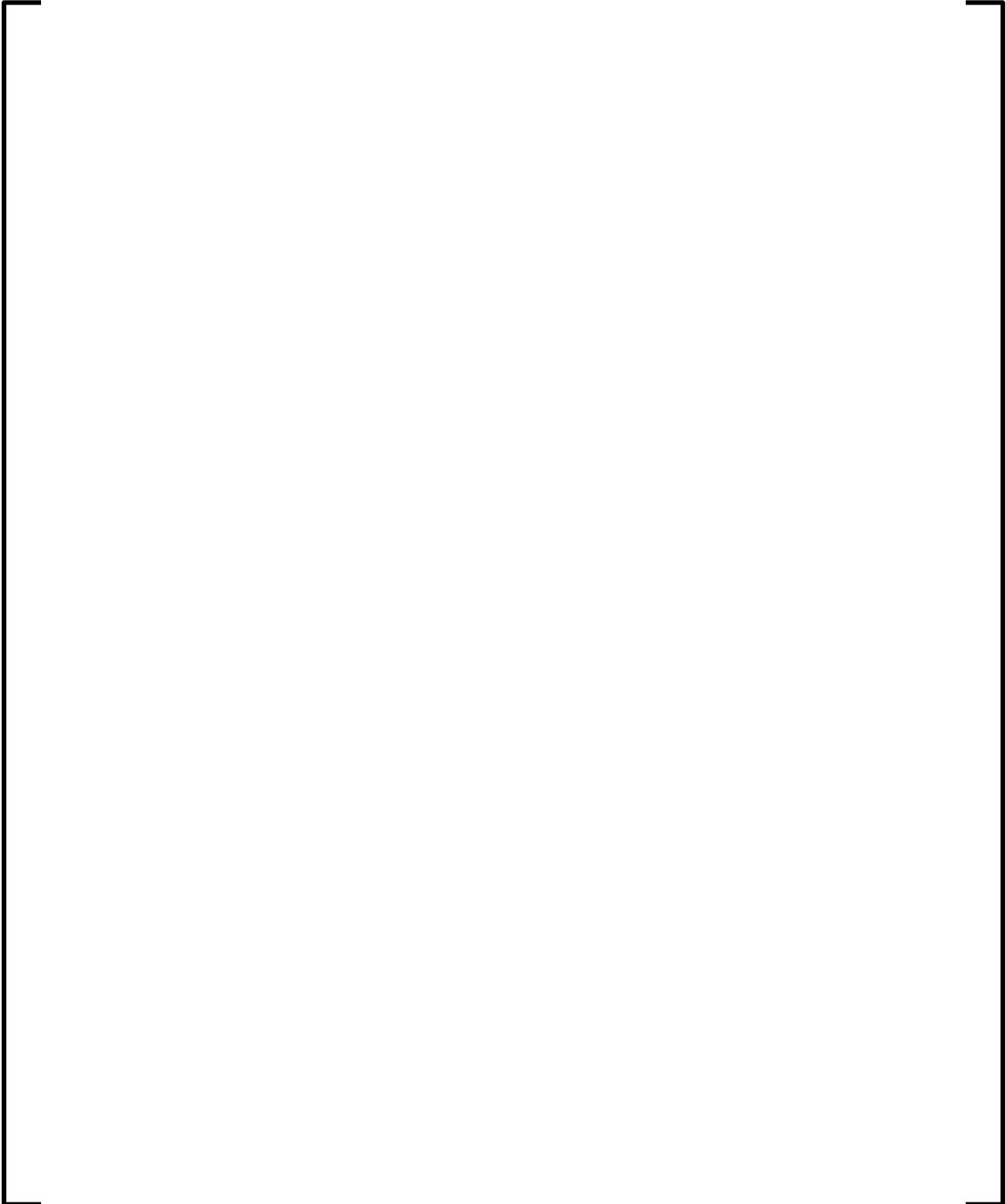
7.3 *Reactor Trip Voting Logic*

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 confirm 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 in a zero-voltage state.

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

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

7.6 *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) that bypasses the electronics of the PS. For added reliability and operational purposes, each button is also hardwired to a digital input card on each ALU in the corresponding division. The manual input to the ALU is combined with the automatic RT logic so that either an automatic function or the manual command sets the RT outputs of the ALU. In both of these configurations, the manual RT from the MCR acts on the same RT devices as the PS automatic RT functions.

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)

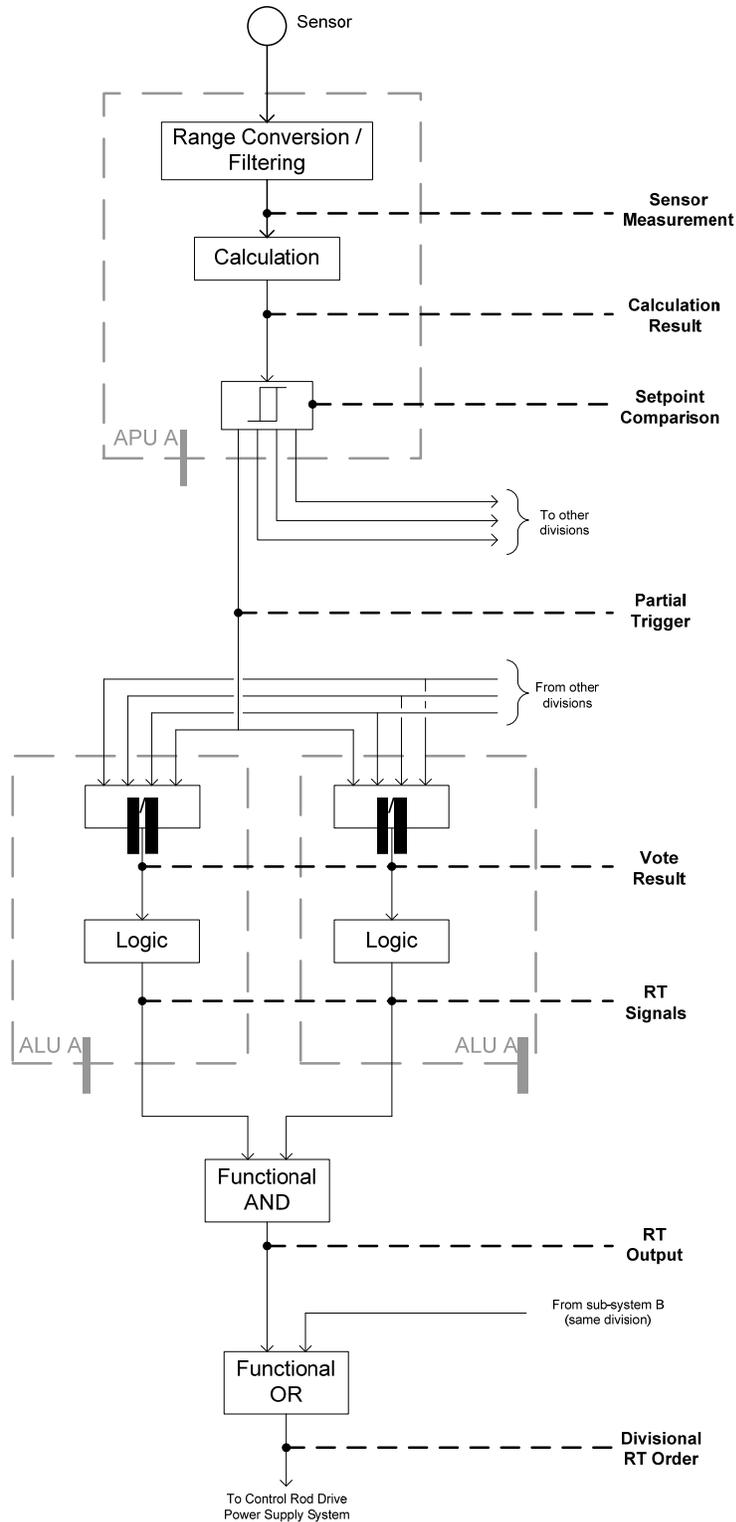


Figure 7-2—SPND-Based Reactor Trip Sequence (One Division)

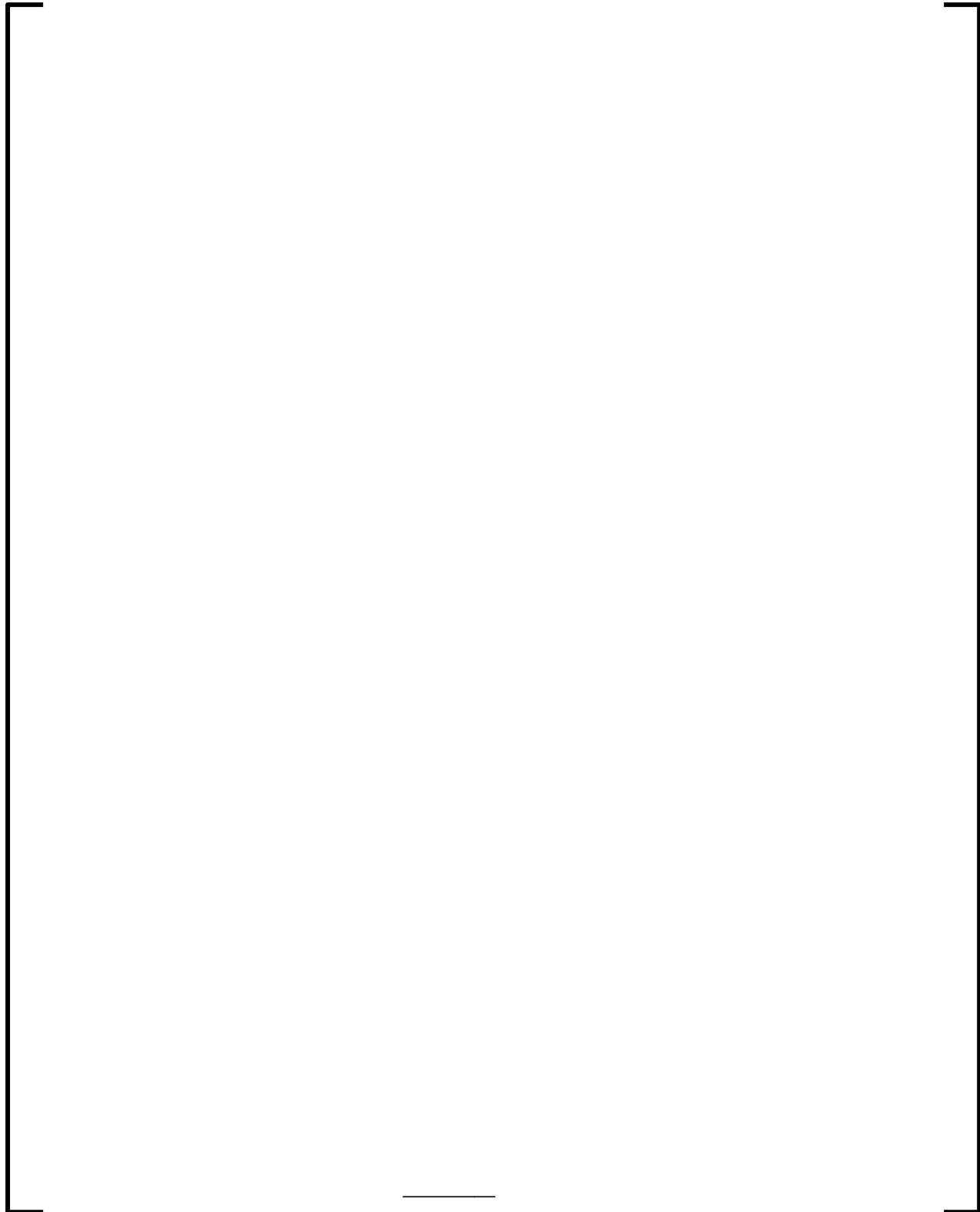


Figure 7-3—Reactor Trip Outputs in One Division

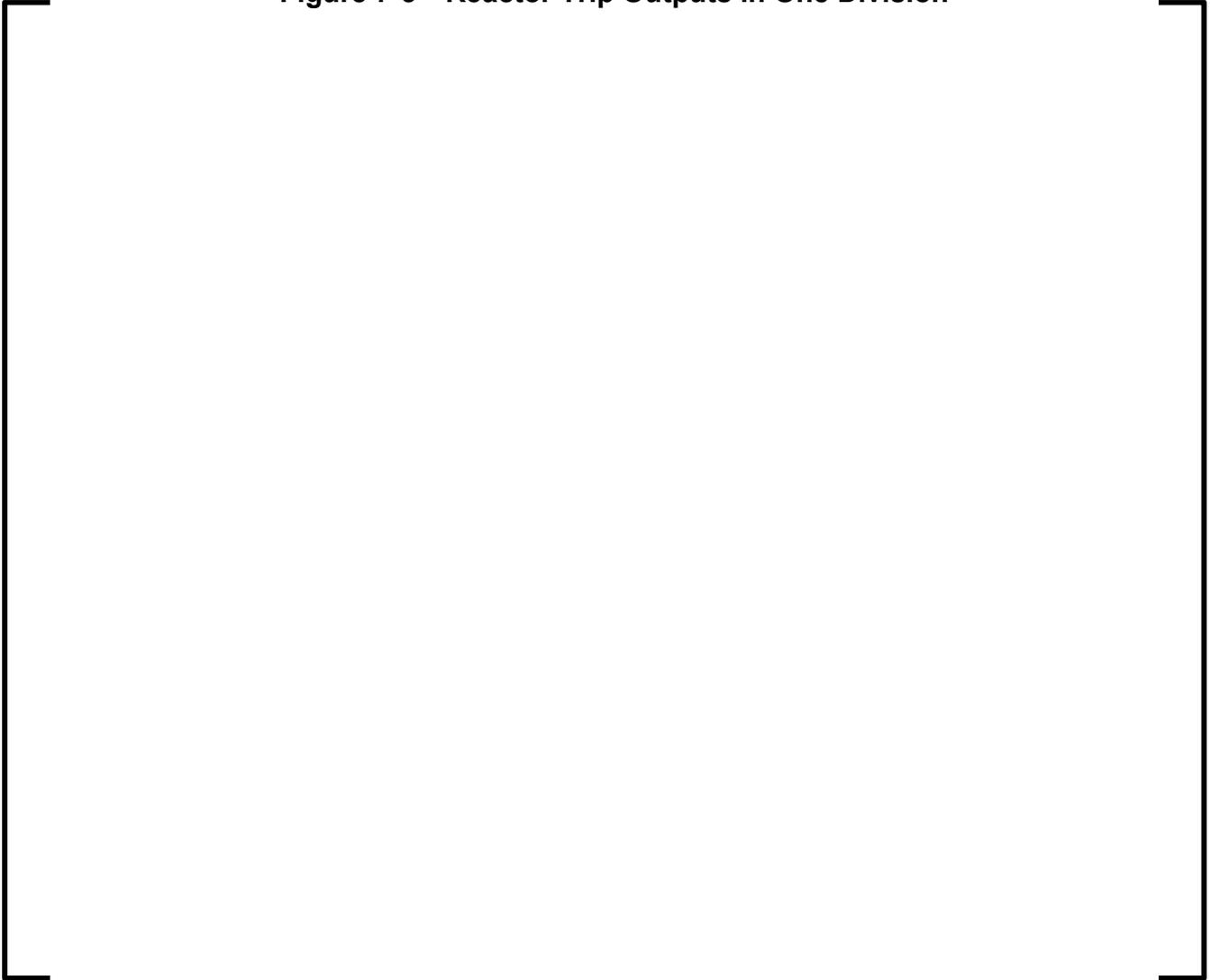


Figure 7-4—Concept for Manual Reactor Trip (One Division)

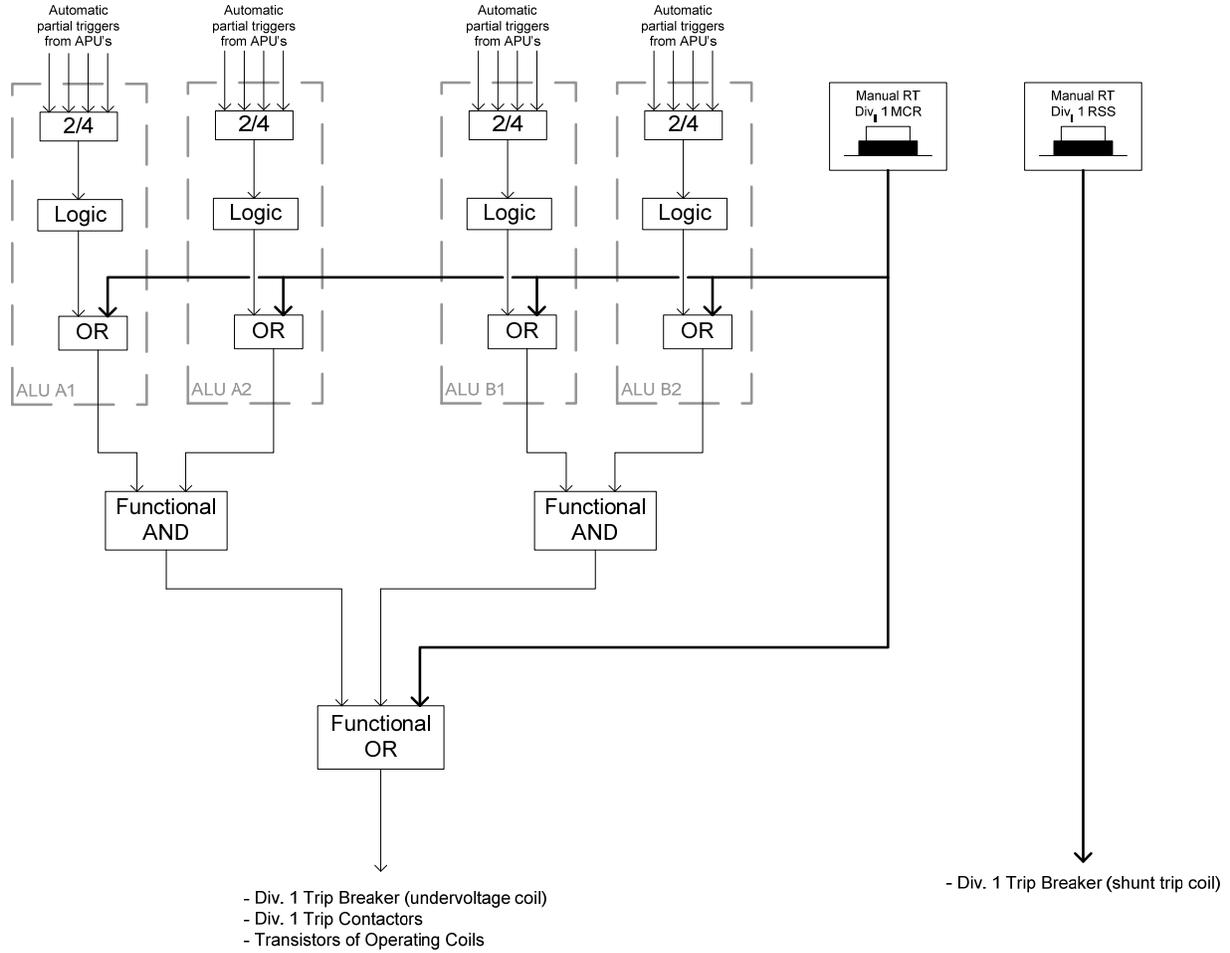


Figure 7-5—Reactor Trip Breakers and Reactor Trip Contactors

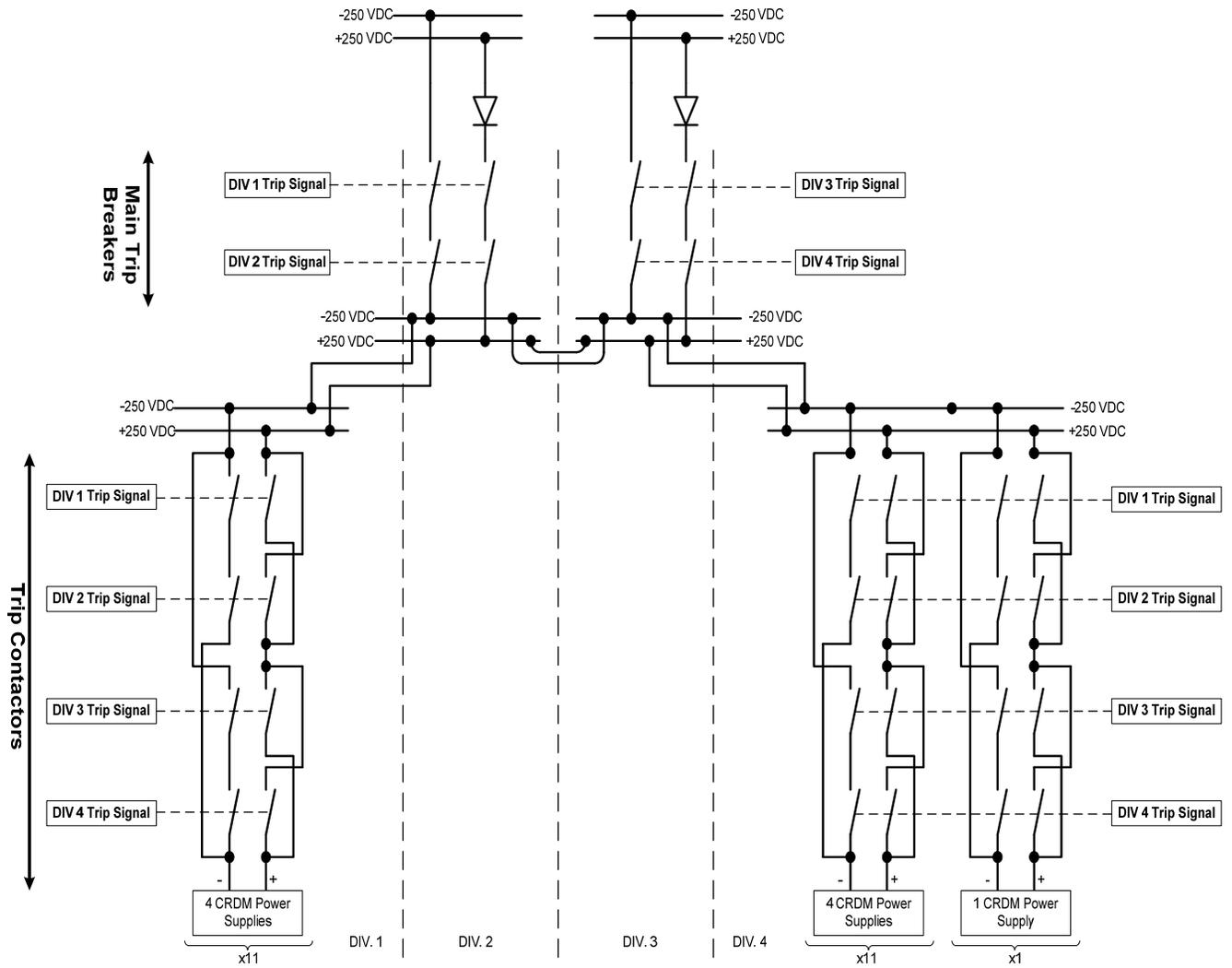
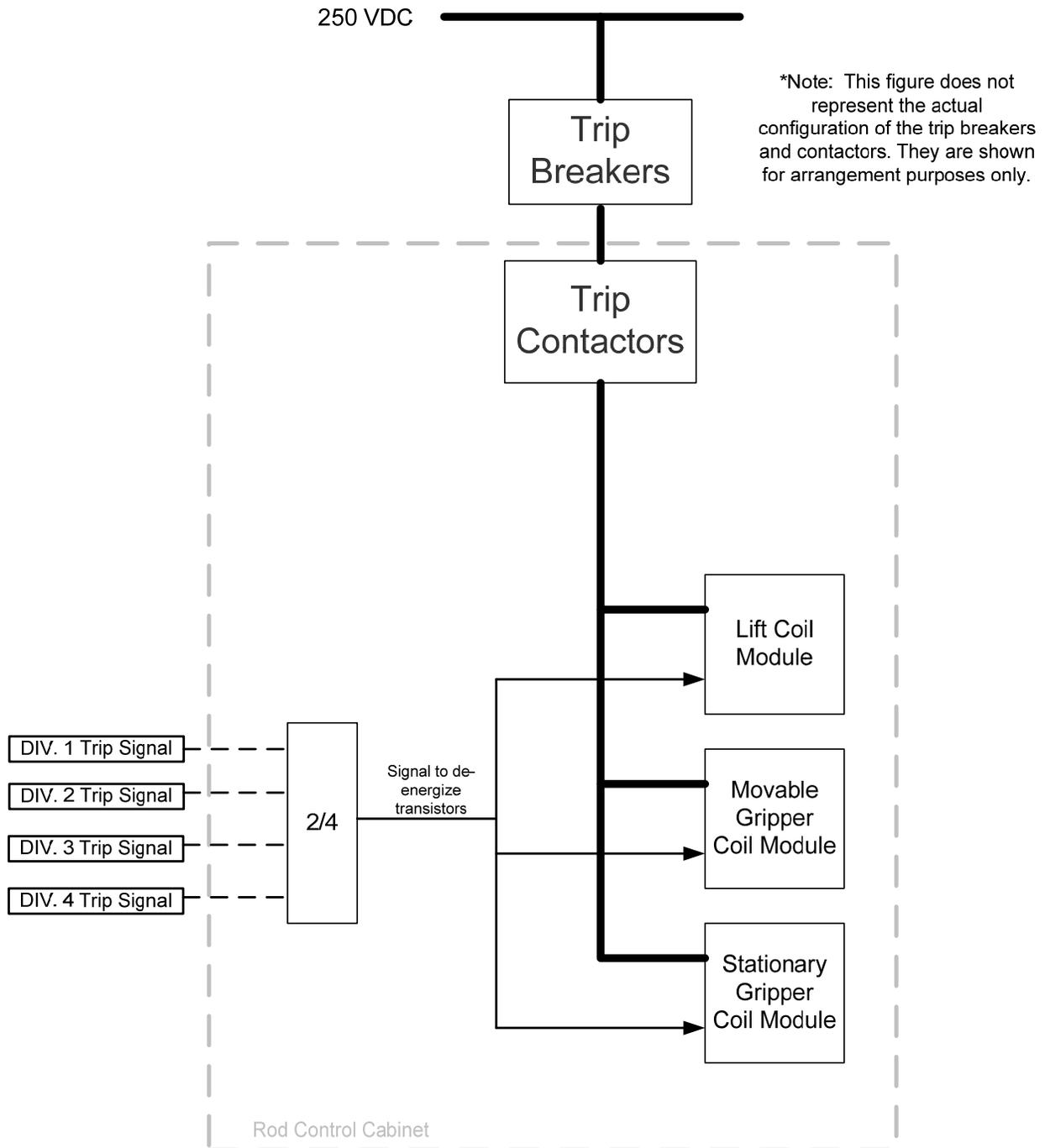


Figure 7-6—Reactor Trip Signals to Rod Control Transistors



8.0 ENGINEERED SAFETY FEATURES ACTUATION

8.1 *Typical Automatic ESF Actuation Sequence*

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

For the four divisions functioning together, the 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 transferred to redundant ALUs in the PS division responsible for the ESF system actuation.
- Two out of four voting is performed on the partial trigger signals in each ALU. If any additional logic is needed (e.g., comparison to permissive conditions), the ALU performs this logic.
- If the vote result is TRUE and the actuation logic, if any, is satisfied, the ALU generates an ESF actuation signal.
- The actuation signal is latched via a set-reset function block in the ALU to confirm completion of the function.

- The ESF actuation signals of the redundant ALUs in each subsystem are combined in a hardwired logical OR; therefore, either of the redundant ALUs 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. In cases where inappropriate actuation of an ESF function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The concept of modification toward actuation is described in Section 7.3. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows:

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

Section 7.4 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, the PAC system is used to prioritize the actuation orders. The PAC system collects the actuation signals from multiple I&C systems and transfers the proper actuation order to the actuator according to pre-defined priority assignments.

8.4 Divisional Assignments – ESF Actuation Outputs

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

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

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

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

8.5 System Level Manual ESF Actuations

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

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

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

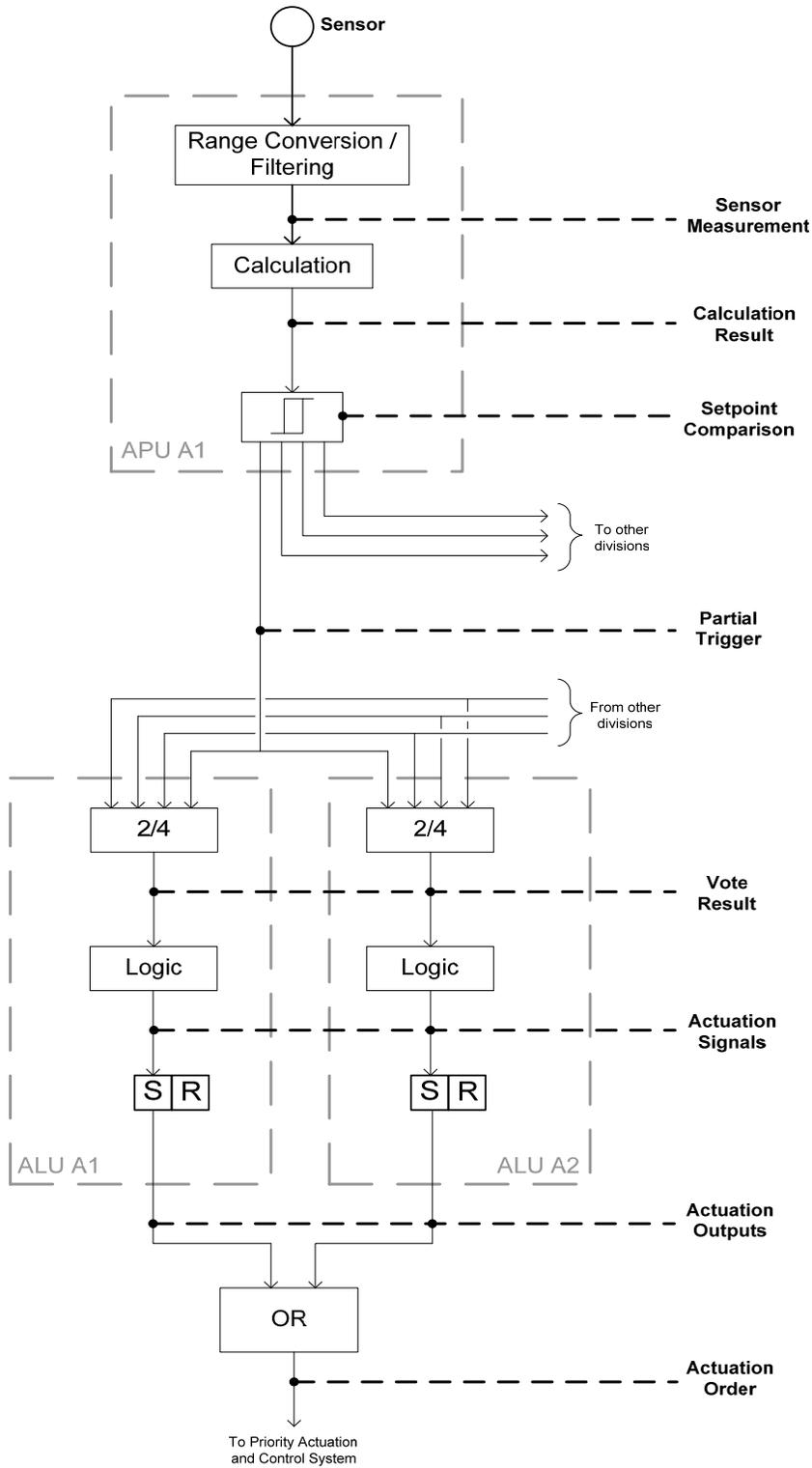
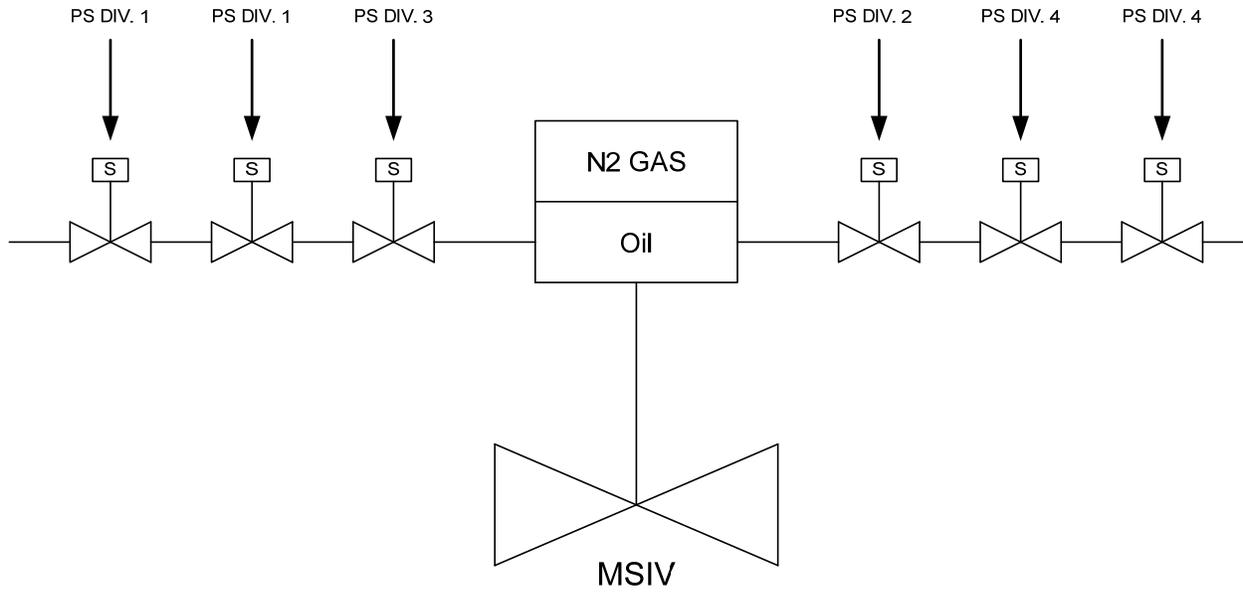


Figure 8-2—Example of PS Divisional Assignment to an ESF Actuation



9.0 PERMISSIVE SIGNALS

9.1 *Definition*

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

The state of a permissive signal is defined as follows:

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

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

The plant condition related to a permissive is automatically detected based on a given set of sensors. One-fourth of the redundant sensors are acquired by the 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*

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

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

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

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

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

10.0 SIGNAL DIVERSITY

10.1 *Definition*

Signal diversity, as applied to the PS, is the use of two diverse parameters to initiate RT to mitigate the effects of the same design basis event. The two independent PS subsystems are used to initiate RTs using diverse signals as inputs. A set of design rules facilitates:

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

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

10.2 *Design Rules*

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

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

This architecture is designed to provide two functionally independent subsystems. This independence is maintained from the point where inputs enter the cabinet associated with a subsystem through the actuation outputs of the ALU assigned to a subsystem. The cabinets of both subsystems within a division are supplied by the same divisional

power sources, and the actuation outputs of the two subsystems can be combined in hardwired logic.

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

1. A subsystem is assigned for the primary RT initiation function for each event requiring RT. The remaining functions are then assigned to subsystems based on rules 2 through 8 below.
2. A sensor used for a primary RT initiation signal in a given subsystem cannot be used by the second, diverse initiating signal (if one exists) in the other subsystem.
3. If signal conditioning modules rely on signals from an APU (e.g., source range detector conditioning), the related sensor must be acquired only by this APU.
4. The functions that have not yet been assigned and that use sensors already assigned to a subsystem (due to RT function assignment) are assigned to the same subsystem as the sensors.
5. The functions acting on the same actuators are grouped and assigned to the same subsystem.
6. The permissive functions are implemented in the subsystems where they are used. If a permissive is required in both subsystems, it is implemented twice, once in each subsystem.
7. If a signal is required in both subsystems, it is implemented twice, once in each subsystem.
8. Once the subsystem has been determined, the functions are assigned to the different APUs within the subsystem. Functions using the same sensors are assigned to the same APU.

11.0 INTERCHANNEL COMMUNICATION

11.1 *Communication Interfaces*

The use of interchannel communication in the PS is demonstrated by communication between two function computers located in two different divisions of the PS (Figure 11-1). 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.

11.2 *Communications Independence*

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

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

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

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

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

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

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

For communication between redundant divisions in the PS, the buffering circuit consists of the PROFIBUS controller and the DPRAM; both are contained in the communication module. The communication module provides buffering so the function 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 independently 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 sent messages and received messages.

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

Figure 11-1—TXS Communication Principle

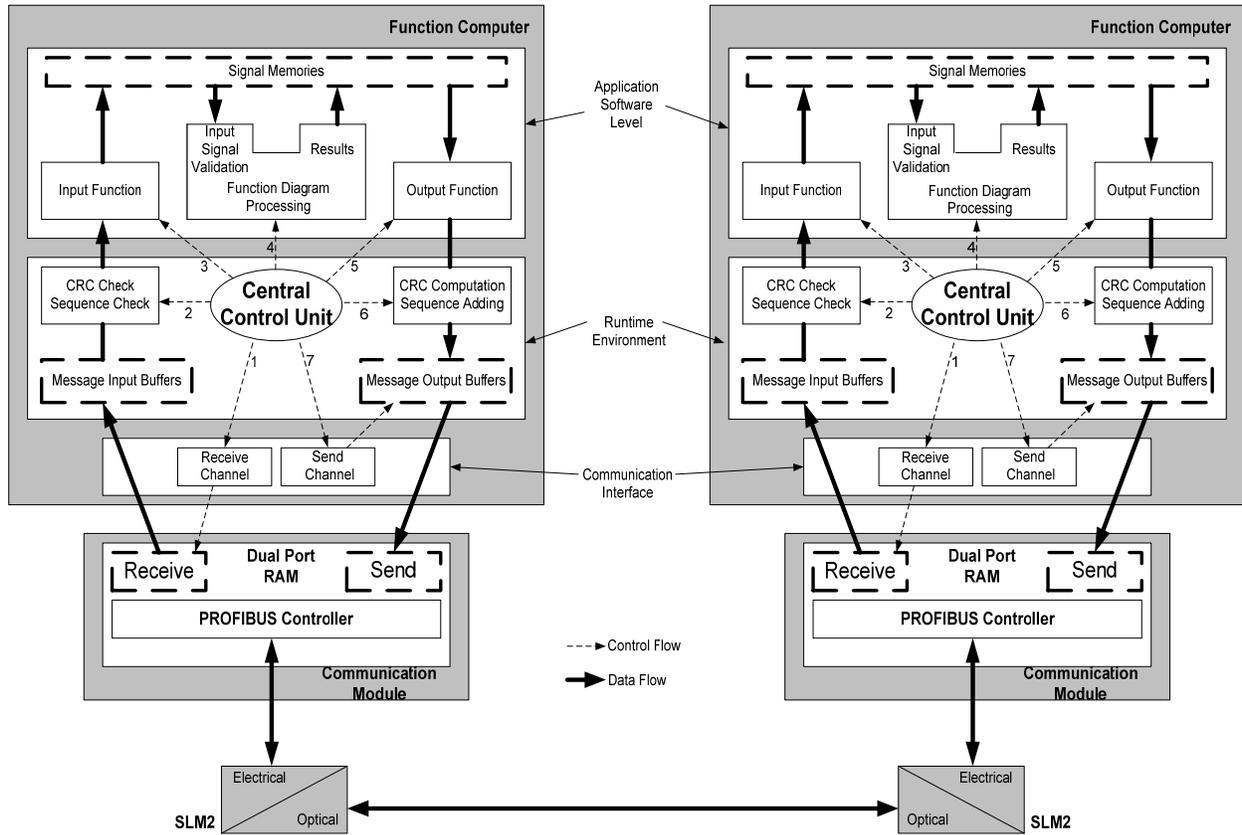


Figure 11-2—Communications Independence (IEEE Std 7-4.3.2)

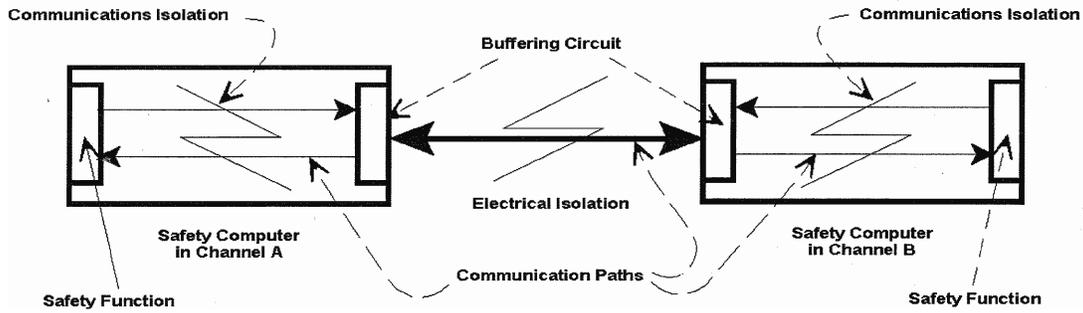
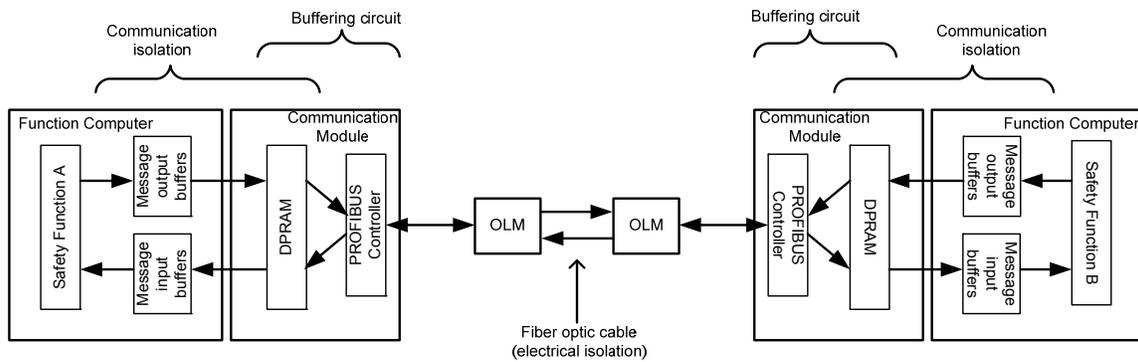


Figure 11-3—Communications Independence (U.S. EPR Implementation)



12.0 SAFETY TO NON-SAFETY-RELATED INTERFACE

12.1 *General Requirements for Interfaces*

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

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

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

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

12.2 *Protection System – Service Unit Interface*

The SU provides functions needed for monitoring, testing, diagnostics, and modifying application software. The SU does not influence the automatic protective functions performed by the PS during normal operation. The SU accesses the system through

the Class 1E MSI, which serves as the point of communication isolation between the SU and the PS units performing the safety-related protective functions. Electrical isolation is provided through optical connections between the SU and the MSI. This interface was reviewed and approved in Reference 23.

12.3 Protection System – PICS Interface

The PICS is the primary operator interface to the U.S. EPR I&C systems to be used in all plant conditions as long as it is verified as functioning correctly. Therefore, it is required that the operator is capable of performing 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 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 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.

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

GW supports the exchange of information between the TXS PS computers and the PICS. It acts as a protocol converter between the TXS communication protocol format and the specific protocol format required by the PICS. No direct physical network connection exists between GW and the PS computers performing the protective functions. This connection is through the Class 1E MSI computer.

Annex E of Reference 14 describes a method of implementing the safety to non-safety-related interface. The related figure from that annex is reproduced in Figure 12-1. Figure 12-2 is an equivalent figure depicting the PS implementation. The PS design conforms to the guidance of Reference 14, and incorporates additional layers of communication isolation between GW and the PS function computers that use data from 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 11.0.

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

12.4 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 accomplished primarily through electrically isolated, hardwired connections from the PS to the system that requires the information. In some cases, this interface may be accomplished by the PS sending information to the control system through the MSI and GW in the same manner as described in Section 12.3.

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-related 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-related system.

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

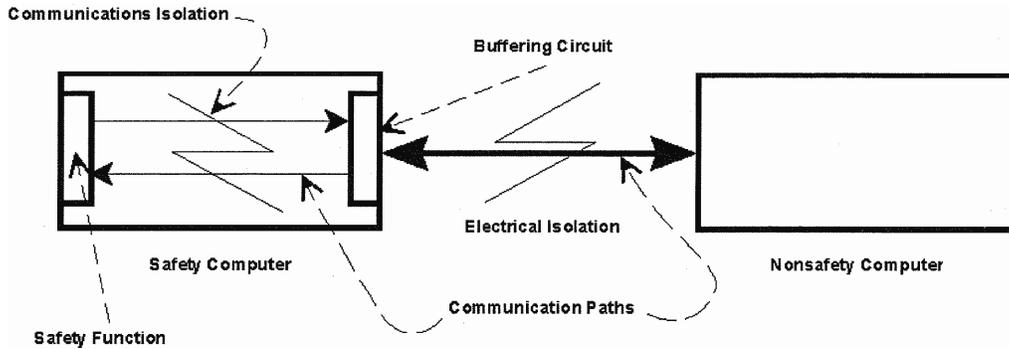
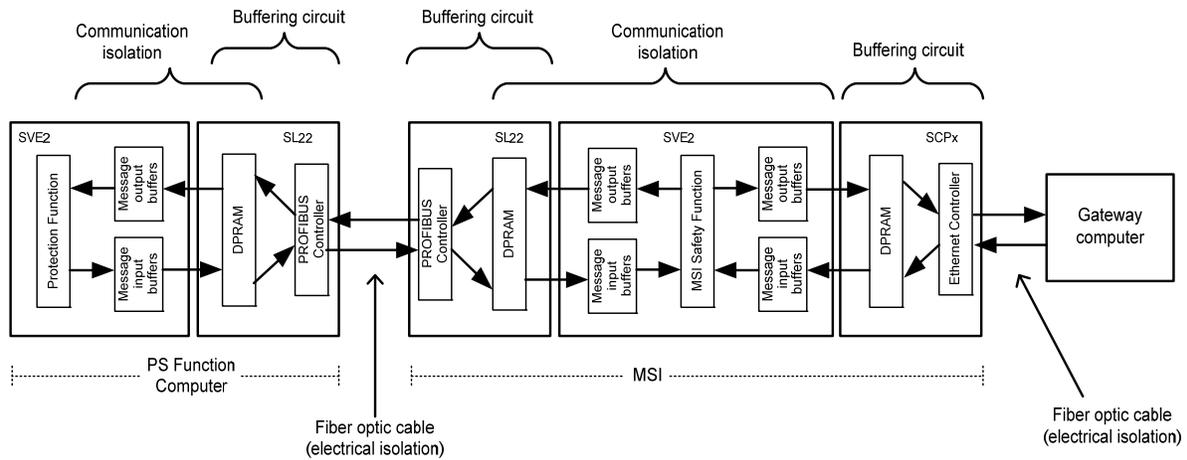


Figure 12-2—Safety to Non-Safety-Related Communication Interface (U.S. EPR Implementation)



13.0 COMPLIANCE WITH IEEE STD 603

13.1 *Use of IEEE Std 603-1998*

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 A of this report). As shown in appendix A, 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 PS 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). Compliance with each clause of IEEE Std 603-1998 is addressed in U.S. EPR FSAR Tier 2, Section 7.1.

14.0 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 manual RT and ESF actuation capability at the system level.

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

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

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

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

15.0 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 7-17, "Guidance on Self-Test and Surveillance Test Provisions," Revision 5, March 2007.
12. Regulatory Guide 1.62, "Manual Initiation of Protective Actions," Revision 0, October 1973.
13. NUREG-0800, Section 7.9, "Data Communication Systems," Revision 5, March 2007.

U.S. Industry Standards

14. IEEE Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
15. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
16. IEEE Standard 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
17. IEEE Standard 323-1974, "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. EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System," May 2000 Enclosure to letter, James F. Mallay (Siemens Power Corporation) to Document Control Desk (NRC), "Publication of EMF-2110(NP)(A) Revision 1, TELEPERM XS: A Digital Reactor Protection System," NRC:00:033, Siemens Power Corporation, July 12, 2000).

-
25. 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, AREVA NP Inc., November 28, 2006).
 26. 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, AREVA NP Inc., December 21, 2006).
 27. 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, AREVA NP Inc., January 29, 2007).
 28. 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, AREVA NP Inc., December 15, 2006).
 29. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology," AREVA NP Inc., March 2007

Appendix A

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
<p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>	<p>Only definitions with differences are listed.</p> <p>Regulatory Guide (RG) 1.53 Rev. 2 now endorses IEEE Std 379-2000.</p>
<p>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.</p>	<p>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.</p> <p>NOTE - A division can have one or more channels.</p>	<p>Makes allowance for interchannel communication, used in some digital applications.</p>
<p>NOTE: The electrical portion of the safety systems, that perform safety functions, is classified as Class 1E.</p>	<p>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.</p>	<p>Note 2 adds clarification on definition that has no impact on requirements.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>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:</p>	<p>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:</p>	No difference.
<p>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.</p>	<p>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.</p>	No difference.
<p>4.2 The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	<p>b) The safety functions and corresponding protective actions of the execute features for each design basis event.</p>	No difference.
<p>4.3 The permissive conditions for each operating bypass capability that is to be provided.</p>	<p>c) The permissive conditions for each operating bypass capability that is to be provided.</p>	No difference.
<p>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.</p>	<p>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.</p>	No difference.
<p>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.</p>	<p>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:</p>	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
<p>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.)</p>	<p>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.)</p>	No difference.
<p>5.1 Single-Failure Criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of:</p>	<p>5.1 Single-failure criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of</p>	No difference.
<p>(1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures;</p>	<p>a) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures.</p>	No difference.
<p>(2) all failures caused by the single failure; and</p>	<p>b) All failures caused by the single failure.</p>	No difference.
<p>(3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.</p>	<p>c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.</p>	No difference.
<p>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.</p>	<p>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.</p>	<p>The additional clarification on single failure does not affect requirements.</p> <p>RG 1.53 Rev. 2 now endorses IEEE Std 379-2000.</p> <p>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.</p>

IEEE 603-1991	IEEE 603-1998	Comment
<p>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.</p>	<p>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.</p>	<p>No difference.</p>
<p>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.</p>	<p>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.</p>	<p>No difference.</p>

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
<p>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.</p>	<p>5.6.3.2 Equipment in proximity a) <i>Separation</i>. 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.</p>	<p>RG 1.75 Rev. 3 now endorses IEEE Std 384-1992.</p>
<p>(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.</p>	<p>b) <i>Barrier</i>. 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.</p>	<p>No difference.</p>
<p>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.</p>	<p>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.</p>	<p>RG 1.53 Rev. 2 now endorses IEEE Std 379-2000.</p>
<p>5.6.4 Detailed Criteria. IEEE Std 384-1981 provides detailed criteria for the independence of Class 1E equipment and circuits.</p>	<p>5.6.4 Detailed criteria. IEEE Std 384-1992 provides detailed criteria for the independence of Class 1E equipment and circuits.</p>	<p>RG 1.75 Rev. 3 now endorses IEEE Std 384-1992.</p>

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.
<p>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:</p> <p>(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.</p>	<p>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:</p> <ul style="list-style-type: none"> - 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
<p>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.</p>	<p>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.</p>	No difference.
<p>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.</p>	<p>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.</p>	No difference.
<p>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.</p>	<p>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.</p>	No difference.
<p>5.8.3.1 This display instrumentation need not be part of the safety systems.</p>	<p>a) This display instrumentation need not be part of the safety systems.</p>	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
<p>6. Sense and Command Features - Functional and Design Requirements.</p> <p>In addition to the functional and design requirements in Section 5, the following requirements shall apply to the sense and command features:</p>	<p>6. Sense and command features-functional and design requirements.</p> <p>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.</p>	No difference.
<p>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.</p>	<p>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).</p>	No difference.
<p>6.2 Manual Control</p> <p>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.</p>	<p>6.2 Manual control. Means shall be provided in the control room to</p> <p>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.</p>	No difference.
<p>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.</p>	<p>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.</p>	No difference.

IEEE 603-1991	IEEE 603-1998	Comment
<p>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.</p>	<p>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.</p>	<p>No difference.</p>
<p>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:</p>	<p>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:</p>	<p>No difference.</p>
<p>(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:</p>	<p>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:</p>	<p>No difference.</p>

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
<p>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.</p>	<p>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.</p>	<p>RG 1.105 Rev. 3 now endorses ANSI/ISA S67.04-1994.</p>
<p>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.</p>	<p>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.</p>	<p>No difference.</p>
<p>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:</p>	<p>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.</p>	<p>No difference.</p>
<p>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.</p>	<p>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.</p>	<p>No difference.</p>

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.
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.

IEEE 603-1991	IEEE 603-1998	Comment
(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
<p>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.</p>	<p>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.</p>	<p>No difference.</p>
<p>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.</p>	<p>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.</p>	<p>No difference.</p>