



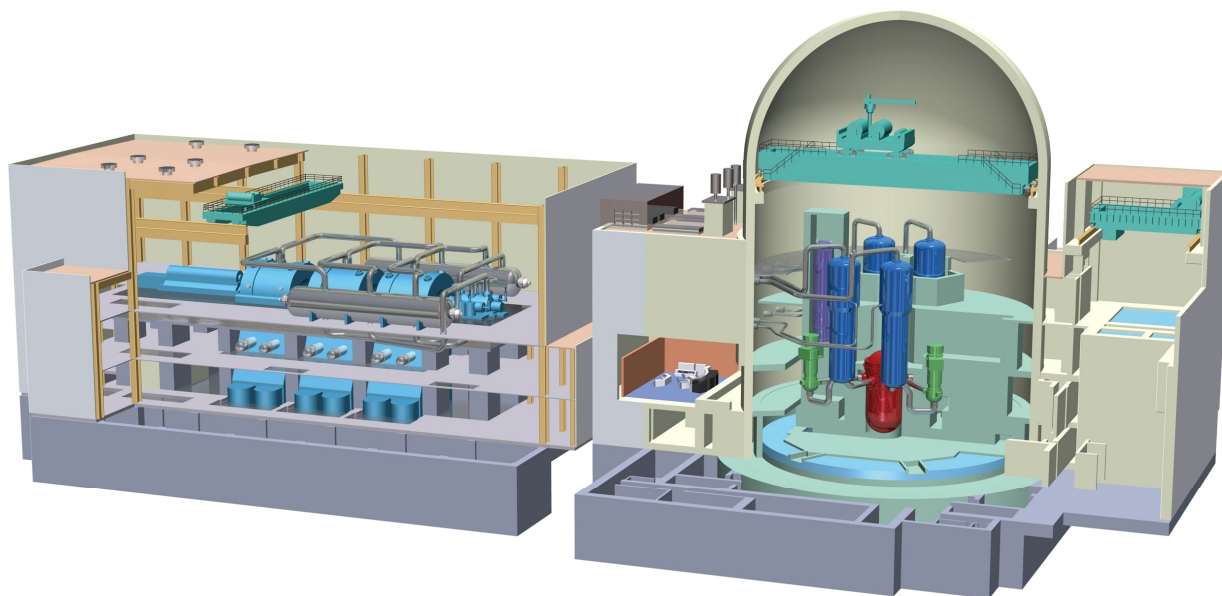
# DESIGN CONTROL DOCUMENT FOR THE US-APWR

## Chapter 7 Instrumentation and Controls

MUAP- DC007

REVISION 3

MARCH 2011



 **MITSUBISHI HEAVY INDUSTRIES, LTD.**

©2011  
Mitsubishi Heavy Industries, Ltd.  
All Rights Reserved

© 2011

**MITSUBISHI HEAVY INDUSTRIES, LTD.**

All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. ("MHI") in connection with the U.S. Nuclear Regulatory Commission's ("NRC") licensing review of MHI's US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of the licensing review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.

16-5, Konan 2-chome, Minato-ku

Tokyo 108-8215 Japan

---

---

**CONTENTS**

---

	<u>Page</u>
<b>7.0 INSTRUMENTATION AND CONTROLS .....</b>	<b>7.1-1</b>
7.1 Introduction .....	7.1-1
7.1.1 Identification of Safety-Related Systems and Non Safety-Related Systems.....	7.1-3
7.1.1.1 Overview .....	7.1-3
7.1.1.2 Reactor Trip System.....	7.1-3
7.1.1.3 Engineered Safety Feature Systems.....	7.1-3
7.1.1.4 Systems Required for Safe Shutdown .....	7.1-4
7.1.1.5 Information Systems Important to Safety .....	7.1-5
7.1.1.6 Interlock Systems Important to Safety.....	7.1-6
7.1.1.7 Control Systems not Required for Safety .....	7.1-6
7.1.1.8 Diverse Instrumentation and Control Systems .....	7.1-6
7.1.1.9 Data Communication Systems .....	7.1-6
7.1.1.10 Auxiliary Support Features and Emergency Power.....	7.1-6
7.1.2 Identification of Safety Criteria .....	7.1-7
7.1.3 Design Bases of Instrumentation and Control System.....	7.1-7
7.1.3.1 Defense in Depth and Diversity Concept .....	7.1-7
7.1.3.2 Single Failure Criterion .....	7.1-8
7.1.3.3 Redundancy Between Safety Divisions.....	7.1-8
7.1.3.4 Independence.....	7.1-8
7.1.3.5 Isolation .....	7.1-9
7.1.3.6 Integrity of Software .....	7.1-9
7.1.3.7 Qualification and Equipment Protection .....	7.1-10

---

7.1.3.8	Unified Architecture .....	7.1-11
7.1.3.9	Redundancy Within Divisions and Systems .....	7.1-11
7.1.3.10	Self-Diagnosis Function .....	7.1-11
7.1.3.11	Manual Testing, Bypasses, Overrides and Resets .....	7.1-12
7.1.3.12	Human-System Interface.....	7.1-13
7.1.3.13	Quality of Components and Modules .....	7.1-14
7.1.3.14	System Calibration, Testing and Surveillance .....	7.1-14
7.1.3.15	Information Displays .....	7.1-15
7.1.3.16	Consideration of Control System Induced Transients .....	7.1-15
7.1.3.17	Life Cycle Process.....	7.1-16
7.1.3.18	Quality Assurance Program .....	7.1-16
7.1.3.19	Identification .....	7.1-17
7.1.4	Combined License Information.....	7.1-17
7.1.5	References .....	7.1-17
7.2	Reactor Trip System .....	7.2-1
7.2.1	System Description .....	7.2-1
7.2.1.1	Functional Performance .....	7.2-2
7.2.1.2	Reactor Trip Logic .....	7.2-2
7.2.1.3	Reactor Trip Variables.....	7.2-3
7.2.1.4	Reactor Trip Initiating Signals .....	7.2-4
7.2.1.5	Manual Control and Actuated Devices .....	7.2-11
7.2.1.6	Bypasses .....	7.2-11
7.2.1.7	Interlocks .....	7.2-13
7.2.1.8	Redundancy .....	7.2-13
7.2.1.9	Diversity.....	7.2-13

---



---

7.2.1.10	Defense-In-Depth and Design Features.....	7.2-14
7.2.2	Design Basis Information .....	7.2-14
7.2.2.1	Single Failure Criterion .....	7.2-14
7.2.2.2	Quality of Components and Modules .....	7.2-14
7.2.2.3	Independence.....	7.2-14
7.2.2.4	Defense-in-Depth and Diversity .....	7.2-14
7.2.2.5	System Testing and Inoperable Surveillance .....	7.2-14
7.2.2.6	Use of Digital Systems .....	7.2-15
7.2.2.7	Setpoint Determination .....	7.2-15
7.2.2.8	Equipment Qualification .....	7.2-16
7.2.3	Analysis .....	7.2-16
7.2.3.1	FMEA Method and Results .....	7.2-16
7.2.3.2	Safety Analysis .....	7.2-17
7.2.3.3	Test and Inspection .....	7.2-17
7.2.3.4	Restrictive Setpoints.....	7.2-17
7.2.3.5	Reliability Analysis.....	7.2-18
7.2.4	Combined License Information.....	7.2-18
7.2.5	References .....	7.2-18
7.3	Engineered Safety Feature Systems .....	7.3-1
7.3.1	System Description .....	7.3-1
7.3.1.1	ESF System Level Logic .....	7.3-2
7.3.1.2	ESF Component Level Logic.....	7.3-3
7.3.1.3	Engineered Safety Features.....	7.3-5
7.3.1.4	Process Variables Monitored for ESF .....	7.3-5

---

7.3.1.5	ESF Initiating Signals, Logic, Actuation Devices and Manual Controls.....	7.3-6
7.3.1.6	Bypasses and Overrides .....	7.3-13
7.3.1.7	Interlocks .....	7.3-15
7.3.1.8	Redundancy .....	7.3-15
7.3.1.9	Diversity.....	7.3-15
7.3.1.10	Defense-In-Depth/Design Features.....	7.3-15
7.3.1.11	Turbine Trip to Prevent Unnecessary Emergency Core Cooling System Actuation.....	7.3-15
7.3.1.12	Block Turbine Bypass and Cooldown Valves .....	7.3-16
7.3.2	Design Basis Information .....	7.3-17
7.3.2.1	Single Failure Criterion .....	7.3-17
7.3.2.2	Quality of Components and Modules .....	7.3-17
7.3.2.3	Independence.....	7.3-17
7.3.2.4	Defense-In-Depth and Diversity .....	7.3-17
7.3.2.5	System Testing and Inoperable Surveillance .....	7.3-17
7.3.2.6	Use of Digital Systems .....	7.3-18
7.3.2.7	Setpoint Determination.....	7.3-18
7.3.2.8	Equipment Qualification .....	7.3-18
7.3.3	Analysis.....	7.3-18
7.3.3.1	FMEA .....	7.3-18
7.3.3.2	Safety Analysis .....	7.3-18
7.3.3.3	Test and Inspection .....	7.3-19
7.3.4	Combined License Information.....	7.3-19
7.3.5	References .....	7.3-19
7.4	Systems Required for Safe Shutdown .....	7.4-1

---

---

7.4.1	System Description .....	7.4-1
7.4.1.1	Normal and Safe Shutdown .....	7.4-1
7.4.1.2	Normal and Safe Shutdown Plant Systems .....	7.4-1
7.4.1.3	Instrumentation and Control Systems .....	7.4-2
7.4.1.4	HSIS .....	7.4-3
7.4.1.5	Normal and Safe Shutdown from Outside the MCR.....	7.4-3
7.4.1.6	Normal and Safe Shutdown Functions .....	7.4-4
7.4.2	Design Basis Information .....	7.4-7
7.4.2.1	I&C Systems Required for Safe Shutdown .....	7.4-8
7.4.2.2	Single Failure Criterion .....	7.4-8
7.4.2.3	Quality of Components and Modules .....	7.4-8
7.4.2.4	Independence.....	7.4-8
7.4.2.5	Periodic Testing.....	7.4-9
7.4.2.6	Use of Digital Systems .....	7.4-9
7.4.3	Analysis.....	7.4-9
7.4.3.1	Safety Analysis.....	7.4-9
7.4.3.2	Restrictive Setpoints.....	7.4-10
7.4.4	Combined License Information.....	7.4-10
7.4.5	References .....	7.4-10
7.5	Information Systems Important to Safety .....	7.5-1
7.5.1	System Description .....	7.5-1
7.5.1.1	Post-Accident Monitoring .....	7.5-1
7.5.1.2	Bypassed and Inoperable Status Indication .....	7.5-7
7.5.1.3	Plant Annunciator (Alarm) System .....	7.5-9
7.5.1.4	Safety Parameter Display System.....	7.5-10

---

---

7.5.1.5	Credited Manual Operator Actions .....	7.5-11
7.5.1.6	Facilities .....	7.5-13
7.5.2	Design Basis Information .....	7.5-14
7.5.2.1	Post Accident Monitoring.....	7.5-14
7.5.2.2	Bypassed and Inoperable Status Indication .....	7.5-15
7.5.2.3	Plant Annunciators .....	7.5-15
7.5.2.4	Safety Parameter Displays System.....	7.5-15
7.5.2.5	Facilities .....	7.5-16
7.5.3	Analysis.....	7.5-16
7.5.4	Combined License Information.....	7.5-17
7.5.5	References .....	7.5-17
7.6	Interlock Systems Important to Safety .....	7.6-1
7.6.1	System Description .....	7.6-1
7.6.1.1	CS/RHR Pump Hot Leg Isolation Valve Open Permissive Interlock.....	7.6-1
7.6.1.2	CS/RHR Valve Open Block Interlock .....	7.6-2
7.6.1.3	Primary Makeup Water Line Isolation Interlock .....	7.6-3
7.6.1.4	Accumulator Discharge Valve Open Interlock.....	7.6-4
7.6.1.5	CCW Supply and Return Header Tie Line Isolation Interlock .....	7.6-4
7.6.1.6	RCP Thermal Barrier HX CCW Return Line Isolation Interlock .....	7.6-5
7.6.1.7	Low-pressure Letdown Line Isolation Interlock .....	7.6-5
7.6.2	Design Basis Information .....	7.6-6
7.6.2.1	Single Failure Criterion .....	7.6-7
7.6.2.2	Quality of Components and Modules .....	7.6-7

---

---

7.6.2.3	Independence.....	7.6-7
7.6.2.4	System Testing and Inoperable Surveillance .....	7.6-7
7.6.2.5	Use of Digital Systems .....	7.6-7
7.6.3	Analysis.....	7.6-7
7.6.4	Combined License Information.....	7.6-8
7.6.5	References .....	7.6-8
7.7	Control Systems Not Required for Safety .....	7.7-1
7.7.1	Description .....	7.7-1
7.7.1.1	Reactor Control System .....	7.7-1
7.7.1.2	Nuclear Instrumentation System .....	7.7-13
7.7.1.3	Control Rod Drive Mechanism Control System.....	7.7-13
7.7.1.4	Rod Position Indication System.....	7.7-15
7.7.1.5	Incore Instrumentation System.....	7.7-15
7.7.1.6	Balance of Plant Control.....	7.7-16
7.7.1.7	Turbine Electro Hydraulic Governor Control System.....	7.7-17
7.7.1.8	Turbine Supervisory Instrumentation System .....	7.7-17
7.7.1.9	Turbine Protection Control .....	7.7-17
7.7.1.10	Electrical System Control .....	7.7-17
7.7.1.11	Radiation Monitoring System .....	7.7-17
7.7.1.12	Auxiliary Equipment Control System .....	7.7-18
7.7.2	Design Basis Information .....	7.7-18
7.7.2.1	Safety Classification .....	7.7-18
7.7.2.2	Effects of Control System Operation on Accidents .....	7.7-18
7.7.2.3	Effects of Control System Failures .....	7.7-18
7.7.2.4	Effects of Control System Failures Caused by Accidents .....	7.7-19

---

---

7.7.2.5	Environmental Control System .....	7.7-19
7.7.2.6	Use of Digital Systems .....	7.7-20
7.7.2.7	Independence .....	7.7-20
7.7.2.8	Defense-In-Depth and Diversity .....	7.7-20
7.7.2.9	Potential for Inadvertent Actuation .....	7.7-20
7.7.2.10	Control of Access .....	7.7-21
7.7.3	Analysis .....	7.7-21
7.7.4	Combined License Information.....	7.7-22
7.7.5	References .....	7.7-22
7.8	Diverse Instrumentation and Control Systems .....	7.8-1
7.8.1	System Description .....	7.8-1
7.8.1.1	Diverse HSI Panel .....	7.8-2
7.8.1.2	Diverse Automatic Actuation Cabinet.....	7.8-3
7.8.2	Design Basis Information .....	7.8-6
7.8.2.1	Single Failure .....	7.8-6
7.8.2.2	Diversity to Digital Safety and Non-Safety Systems.....	7.8-6
7.8.2.3	Separation and Independence .....	7.8-6
7.8.2.4	Testability .....	7.8-6
7.8.2.5	Maintenance Bypass .....	7.8-7
7.8.2.6	Operating Bypass .....	7.8-7
7.8.2.7	Quality .....	7.8-7
7.8.2.8	Defense-In-Depth and Diversity .....	7.8-7
7.8.2.9	Fire Protection .....	7.8-8
7.8.3	Analysis .....	7.8-8
7.8.3.1	Anticipated Transient without Scram.....	7.8-8

---

---

7.8.3.2	Adequacy of Manual Controls and Displays.....	7.8-8
7.8.3.3	Conformance to BTP 7-19.....	7.8-8
7.8.4	Combined License Information.....	7.8-9
7.8.5	References .....	7.8-9
7.9	Data Communication Systems.....	7.9-1
7.9.1	System Description .....	7.9-1
7.9.1.1	Control Network (Safety Bus and Unit Bus) .....	7.9-1
7.9.1.2	Safety VDU Communication.....	7.9-2
7.9.1.3	Data Links .....	7.9-3
7.9.1.4	I/O Bus .....	7.9-4
7.9.1.5	Maintenance Network.....	7.9-4
7.9.1.6	Station Bus .....	7.9-5
7.9.1.7	External Network Interface .....	7.9-5
7.9.2	Design Basis Information .....	7.9-5
7.9.2.1	Quality of Components and Modules .....	7.9-5
7.9.2.2	Software Quality .....	7.9-6
7.9.2.3	Performance Requirements .....	7.9-6
7.9.2.4	Potential Hazards and Single Failures .....	7.9-8
7.9.2.5	Control of Access .....	7.9-8
7.9.2.6	Cyber Security .....	7.9-8
7.9.2.7	Independence.....	7.9-8
7.9.2.8	Fail Safe Failure Modes .....	7.9-9
7.9.2.9	System Testing and Surveillances .....	7.9-9
7.9.2.10	Bypass and Inoperable Status Indications .....	7.9-9
7.9.2.11	EMI/RFI Susceptibility .....	7.9-9

---

---

7.9.2.12	Defense-In-Depth and Diversity .....	7.9-10
7.9.2.13	Seismic Hazards .....	7.9-10
7.9.3	Analysis .....	7.9-10
7.9.4	Combined License Information.....	7.9-10
7.9.5	References .....	7.9-10

---

---



---

**TABLES**


---

	<u>Page</u>
Table 7.1-1	List of Conventional Switches on the Operator Console ..... 7.1-20
Table 7.1-2	Regulatory Requirements Applicability Matrix (per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) ..... 7.1-21
Table 7.1-3	Deleted ..... 7.1-29
Table 7.2-1	Interface between RPS and Other Systems (for Figure 7.2-3) ..... 7.2-19
Table 7.2-2	Reactor Trip Signals ..... 7.2-20
Table 7.2-3	Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) ..... 7.2-21
Table 7.2-4	RT and ESF Permissives, Bypasses and Interlocks ..... 7.2-24
Table 7.2-5	Diverse Parameters in Two Separate Controller Groups ..... 7.2-27
Table 7.2-6	Reactor Protection System - Train Level Manual Controls (Conventional and Software Switches) ..... 7.2-27
Table 7.2-7	Reactor Protection System - Train Level Manual Controls (Software Switches) ..... 7.2-28
Table 7.2-8	FMEA for Reactor Trip in PSMS (for Figure 7.2-8) ..... 7.2-29
Table 7.3-1	Interface between ESFAS and Other Systems (for Figure 7.3-2) ..... 7.3-21
Table 7.3-2	Interface between SLS and Other Systems (for Figure 7.3-3) ..... 7.3-22
Table 7.3-3	Engineered Safety Features Actuation Signals ..... 7.3-23
Table 7.3-4	Engineered Safety Features Actuation Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) ..... 7.3-26
Table 7.3-5	ESF Actuation System - Train Level Manual Control (Conventional and Software Switches) ..... 7.3-28
Table 7.3-6	ESF Actuation System - Manual Reset and Bypass (Software Switches) ..... 7.3-30
Table 7.3-7	FMEA for ESF Actuation in PSMS (for Figure 7.3-6) ..... 7.3-32
Table 7.4-1	Component Controls for Shutdown ..... 7.4-11
Table 7.4-2	Indication for Shutdown ..... 7.4-16
Table 7.5-1	Summary of PAM Variable Types and Source Documents ..... 7.5-19
Table 7.5-2	PAM Main Design Criteria for Each Variable Type ..... 7.5-20

---

---

Table 7.5-3	PAM Variables .....	7.5-21
Table 7.5-4	Display Concept for Type A, B PAM Variables.....	7.5-24
Table 7.5-5	List of Accidents and Credited Manual Actions .....	7.5-25
Table 7.5-6	Function of Type A PAM Variables.....	7.5-26
Table 7.5-7	Function of Type B PAM Variables.....	7.5-27
Table 7.5-8	Function of Type C PAM Variables .....	7.5-28
Table 7.5-9	Function of Type D PAM Variables .....	7.5-29
Table 7.5-10	Function of Type E PAM Variables.....	7.5-30
Table 7.7-1	AOOs Due to the Control System Failures .....	7.7-23
Table 7.7-2	Controller Group Control System Distribution in the Reactor Control System .....	7.7-24
Table 7.7-3	Rod Control System Interlocks .....	7.7-25
Table 7.7-4	Process Control Parameters and Control Method Description.....	7.7-26
Table 7.8-1	Critical Safety Functions and Related Systems.....	7.8-10
Table 7.8-2	Variables Monitored by DAS .....	7.8-10
Table 7.8-3	System Actuation Times for Each Event .....	7.8-11
Table 7.8-4	Diverse Actuation Signals.....	7.8-12
Table 7.8-5	Components Actuated by DAS.....	7.8-13
Table 7.8-6	Diverse Actuation Variables, Ranges, Accuracies, and Setpoints (Nominal) .....	7.8-14
Table 7.8-7	Supplemental Information to MUAP-07006-P-A.....	7.8-15
Table 7.9-1	Interface between HSIS and Other Systems (For Figure 7.9-1) .....	7.9-12

---

---

---

**FIGURES**


---

	<u>Page</u>
Figure 7.1-1	US-APWR I&C Overall Architecture ..... 7.1-30
Figure 7.1-2	Typical HSI System Architecture in Main Control Room ..... 7.1-31
Figure 7.1-3	Layout of Main Control Room ..... 7.1-32
Figure 7.1-4	Class 1E UPS for PSMS ..... 7.1-33
Figure 7.1-5	Electrical Power Source for PSMS ..... 7.1-34
Figure 7.1-6	Non-Class 1E UPS for PCMS ..... 7.1-35
Figure 7.1-7	Electrical Power Source for PCMS ..... 7.1-36
Figure 7.2-1	Configuration of the Reactor Protection System ..... 7.2-32
Figure 7.2-2	Functional Logic Diagram for Reactor Protection and Control System ..... 7.2-33
Figure 7.2-3	Interface between RPS and Other Systems (for Table 7.2-1) ..... 7.2-54
Figure 7.2-4	Configurations of the Reactor Trip Breakers ..... 7.2-55
Figure 7.2-5	Summary of Fire Protection for Reactor Trip Breaker ..... 7.2-56
Figure 7.2-6	Signal Flow for High Source and Intermediate Range Neutron Flux Trips ..... 7.2-57
Figure 7.2-7	Signal Flow for Reactor Trip on Turbine Trip ..... 7.2-58
Figure 7.2-8	RPS Configuration for Use in FMEA (for Table 7.2-8) ..... 7.2-59
Figure 7.3-1	Configuration of Engineered Safety Features Actuation System and Safety Logic System ..... 7.3-36
Figure 7.3-2	Interface between ESFAS and Other Systems (for Table 7.3-1) ..... 7.3-37
Figure 7.3-3	Interface between SLS and Other Systems (for Table 7.3-2) ..... 7.3-38
Figure 7.3-4	Summary of Design Concept for Turbine Trip on Reactor Trip ..... 7.3-39
Figure 7.3-5	Summary of Design Concept for Block Turbine Bypass and Cooldown Valves ..... 7.3-40
Figure 7.3-6	Configuration of ESF System for Use in FMEA (for Table 7.3-7) ..... 7.3-41
Figure 7.4-1	Equipment Arrangement of Remote Shutdown Console ..... 7.4-18

---

Figure 7.4-2	The Cable Route of the Remote Shutdown Room .....	7.4-19
Figure 7.5-1	Configuration of Signal Processing for Safety PAM Variables ....	7.5-31
Figure 7.5-2	Configuration of Signal Processing for Non-Safety PAM Variable .....	7.5-32
Figure 7.5-3	Layout of TSC.....	7.5-33
Figure 7.5-4	Alarm System Configuration .....	7.5-34
Figure 7.6-1	Interlocks for CS/RHR Pump Hot Leg Isolation Valves .....	7.6-10
Figure 7.6-2	Interlocks for RHR Discharge Line Containment Isolation Valve.....	7.6-11
Figure 7.6-3	Interlocks for Containment Spray Header Containment Isolation Valve.....	7.6-12
Figure 7.6-4	Interlocks for Primary Makeup Water Stop Valve .....	7.6-13
Figure 7.6-5	Interlocks for Accumulator Discharge Valve .....	7.6-14
Figure 7.6-6	Interlocks for CCW Header Tie Line Isolation Valves.....	7.6-15
Figure 7.6-7	Interlocks for RCP Thermal Barrier Hx CCW Return Line Isolation Valve.....	7.6-16
Figure 7.6-8	Interlocks for Low Pressure Letdown Line Isolation Valve .....	7.6-17
Figure 7.7-1	Basic System for Insertion of Movable Neutron Detectors .....	7.7-27
Figure 7.8-1	The Signal Flow of the Status Signal to DAS .....	7.8-21
Figure 7.8-2	The Prevention Diagram of Reactor Trip, Turbine Trip and MFW Isolation in DAS .....	7.8-22
Figure 7.8-3	The Prevention Diagram of Emergency Feedwater Actuation in DAS .....	7.8-23
Figure 7.9-1	Interface between HSIS and Other Systems (for Table 7.9-1) ....	7.9-13

---

---

---

**ACRONYMS AND ABBREVIATIONS**

---

ac	alternating current
ACC	accumulator
ALR	automatic load regulator
AOO	anticipated operational occurrence
AOP	abnormal operating procedure
APWR	advanced pressurized water reactor
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
AVR	auto voltage regulator
BAT	boric acid tank
BISI	bypassed and inoperable status indication
BOP	balance of plant
BTP	branch technical position
CCF	common cause failure
CCW	component cooling water
CCWS	component cooling water system
CFR	Code of Federal Regulations
CFS	condensate and feedwater system
CHP	charging pump
COL	Combined License
COM	communication system
CPU	central processing unit
CRDM	control rod drive mechanism
CSA	channel statistical accuracy
CS	containment spray
CS/RHR	containment spray/residual heat removal
CSS	containment spray system
C/V	containment vessel
CVCS	chemical and volume control system
DAAC	diverse automatic actuation cabinet
DAS	diverse actuation system
dc	direct current
DCD	Design Control Document
DCS	data communication system
DHP	diverse HSI panel
DNB	departure from nucleate boiling

---

**ACRONYMS AND ABBREVIATIONS (CONTINUED)**

E/O	electrical to optical (or optical to electrical)
ECCS	emergency core cooling system
EFW	emergency feedwater
EFWS	emergency feedwater system
EHGS	turbine electro-hydraulic governor control system
EMI	electromagnetic interference
EOF	emergency operations facility
EOP	emergency operating procedure
EPG	emergency procedure guideline
ERDS	emergency response data system
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESW	essential service water
ESWS	essential service water system
FLB	feedwater line break
FMEA	failure modes and effects analysis
GDC	General Design Criteria
GTG	gas turbine generator
HEPA	high-efficiency particulate air
HFE	human factors engineering
HJTC	heated junction thermocouple
HSI	human-system interface
HSIS	human-system interface system
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
I/O	input/output
IAS	instrument air system
ICC	inadequate core cooling
IEEE	Institute of Electrical and Electronics Engineers
ITAAC	inspections, tests, analyses, and acceptance criteria
ITV	industrial television
LBLOCA	large break loss-of-coolant accident
LDP	large display panel
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
MCR	main control room
MELCO	Mitsubishi Electric Corporation
MELTAC	Mitsubishi Electric Total Advanced Controller

---

**ACRONYMS AND ABBREVIATIONS (CONTINUED)**

MFW	main feedwater
M/G	motor generator
MHI	Mitsubishi Heavy Industries, Ltd.
MOV	motor operated valve
MSLB	main steam line break
MSS	main steam supply system
NEI	Nuclear Energy Institute
NIS	nuclear instrumentation system
NRC	U.S. Nuclear Regulatory Commission
NUREG	NRC Technical Report Designation ( <u>N</u> uclear <u>R</u> egulatory Commission)
OC	operator console
OEM	original equipment manufacturer
OS	operating system
PA	postulated accident
PAM	post accident monitoring
PCMS	plant control and monitoring system
POL	problem oriented language
PRA	probabilistic risk assessment
PSMS	protection and safety monitoring system
PSS	process and post-accident sampling system
QA	quality assurance
QAP	quality assurance program
RCP	reactor coolant pump
RCS	reactor coolant system
RFI	radio frequency interference
RG	Regulatory Guide
RHR	residual heat removal
RHRS	residual heat removal system
RMS	radiation monitoring system
RPI	rod position indication
RPS	reactor protection system
RSC	remote shutdown console
RSR	remote shutdown room
RT	reactor trip
RTB	reactor trip breaker
RTD	resistance temperature detector
RTP	rated thermal power
RV	reactor vessel

---

**ACRONYMS AND ABBREVIATIONS (CONTINUED)**

RVWL	reactor vessel water level
RWSP	refueling water storage pit
SBLOCA	small break loss-of-coolant accident
SDCV	spatially dedicated continuously visible
SG	steam generator
SGTR	steam generator tube rupture
SIP	safety injection pump
SIS	safety injection system
SLS	safety logic system
SPDS	safety parameter display system
SRM	staff requirements memorandum
SRP	Standard Review Plan
SRSS	square root sum of the squares
SSA	signal selection algorithm
T <sub>avg</sub>	average temperature
TSC	technical support center
UHS	ultimate heat sink
UPS	uninterruptible power supply
VCT	volume control tank
V&V	verification and validation
VDU	visual display unit

---



## 7.0 INSTRUMENTATION AND CONTROLS

### 7.1 Introduction

The instrumentation and control (I&C) systems provide the capability to control and regulate the plant systems manually and automatically during normal plant operation, and provide reactor protection against unsafe plant operation. The primary purpose of the I&C systems is to provide automatic protection and exercise proper control against unsafe and improper reactor operation during steady state and transient power operations. The system also provides initiating signals to actuate safety functions, which are assigned to mitigate the consequences of faulted conditions and ensure safe shutdown. Safety functions are those actions required to achieve the system responses assumed in the safety analyses and those credited to achieve safe shutdown of the plant. The I&C system is primarily a digital system with the exception of the analog diverse actuation system (DAS). The overall I&C architecture for the US-APWR is shown in Figure 7.1-1.

The general specifications of the overall I&C system are summarized as follows:

- A. Main control board (refer to Figures 7.1-2 and 7.1-3)
  - Fully computerized
  - Safety visual display units (VDUs) and non-safety operational VDUs
  - Large display panel (LDP)
  - Minimal conventional switches, only for regulatory compliance (e.g., Regulatory Guide [RG] 1.62 [Reference 7.1-1]), refer to Table 7.1-1
- B. Safety-related I&C
  - Fully digital Mitsubishi Electric Corporation (MELCO) Mitsubishi Electric Total Advanced Controller (MELTAC) platform
  - Four train redundant reactor protection system (RPS)
  - Four train redundant engineered safety features actuation system (ESFAS)
  - Four train redundant safety logic system (SLS) for component control
  - Four train redundant safety grade human-system interface system (HSIS)
  - Conventional switches (for train level manual actuation)
- C. Non safety-related I&C
  - Fully digital, except analog DAS
  - Consists of MELTAC platform

- Duplex redundant digital architecture for each control and process monitoring subsystem
- Analog DAS

D. Data communication

- Fully multiplexed, including Class 1E signals.
- Multi-drop data bus and serial data link.
- Fiber optics communication networks.

The overall I&C system consists of the safety-related protection and safety monitoring system (PSMS) with the safety-related portion of the HSIS, the non safety-related plant control and monitoring system (PCMS), the non safety-related DAS, and the non safety-related portion of the HSIS. The HSIS consists of safety-related safety VDUs, post accident monitoring (PAM), non safety-related operational VDUs, and non safety-related LDP for normal plant operation. The safety VDUs and operational VDUs are located on both the operator console (OC) in the main control room (MCR) and the remote shutdown console (RSC) in the remote shutdown room (RSR). Operational VDUs are also provided for information only (i.e., no control capability) at the technical support center (TSC). Information to support emergency response operations (the same as provided on operational VDUs) is provided at the emergency operations facility (EOF).

The description and/or details described in this section are based on the following Mitsubishi Heavy Industries, Ltd. (MHI) topical and technical reports. If there are any inconsistencies between the topical reports and this chapter, the Design Control Document (DCD) has precedence.

- Safety I&C System Description and Design Process, MUAP-07004 (Reference 7.1-2)
- Safety System Digital Platform -MELTAC-, MUAP-07005 (Reference 7.1-3)
- Defense-in-Depth and Diversity, MUAP-07006 (Reference 7.1-4)
- HSI System Description and HFE Process, MUAP-07007 (Reference 7.1-5)

All nuclear steam supply systems and other I&C systems are designed and manufactured by MHI.

The I&C systems for the US-APWR are essentially the same as the I&C systems for new plants in Japan, including the Japanese advanced pressurized water reactor (APWR), and systems currently installed and being implemented for plant modernization in Japan. The I&C systems for the US-APWR are the same as the systems described in the topical reports, referenced above.

### **7.1.1 Identification of Safety-Related Systems and Non Safety-Related Systems**

#### **7.1.1.1 Overview**

Safety-related PSMS with safety-related portion of the HSIS consists of:

- RPS
- ESFAS and SLS
- Conventional switches (train level)
- Safety VDUs - Part of safety-related HSIS for manual operation and monitoring of critical safety functions, including PAM

A brief summary of all the safety-related systems is presented in this section, while more detailed descriptions are given in Section 7.2 for reactor trip system, Section 7.3 for engineered safety feature systems, Section 7.4 for systems required for safe shutdown, Section 7.5 for information systems important to safety, and Section 7.6 for interlock systems important to safety. Detailed descriptions of non safety-related systems are described in Section 7.7 for control systems not required for safety, Section 7.8 for diverse instrumentation and control systems, and Section 7.9 for data communication systems.

Safety functions are those actions required to achieve the system responses assumed in the safety analyses, and those credited to achieve safe shutdown of the plant. Some safety functions are automatically initiated by the PSMS. These same safety functions may also be manually initiated and monitored by operators using the HSIS. The HSIS is also used to manually initiate other safety functions that do not require time critical actuation and safety functions credited for safe shutdown. After manual initiation from the HSIS, all safety functions are executed by the PSMS. The HSIS also provides all plant information to operators, including critical parameters required for post accident conditions. The HSIS includes both safety and non-safety sections.

#### **7.1.1.2 Reactor Trip System**

The safety systems automatically trip the reactor and initiate engineered safety features (ESF) (if required) whenever predetermined limits are approached. The RPS maintains surveillance on nuclear and process variables, which are related to equipment mechanical limitations, such as pressure, and on variables that directly affect the heat transfer capability of the reactor, such as the reactor coolant flow and temperature. When a limit is approached, the RPS initiates the signal to open the reactor trip breakers (RTBs). This action removes power from the control rod drive mechanism (CRDM) coils, permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown.

#### **7.1.1.3 Engineered Safety Feature Systems**

The occurrence of a postulated accident (PA), such as a loss-of-coolant accident (LOCA) or a steam line break, requires a reactor trip plus actuation of one or more ESFs in order

to prevent or mitigate damage to the core and reactor coolant system (RCS) and to ensure containment integrity.

#### **7.1.1.3.1 Reactor Protection System**

The RPS will determine if setpoints are being approached for selected plant parameters. If setpoints are approached, the RPS will process signals through logic functions, to respond properly to the various conditions.

#### **7.1.1.3.2 Engineered Safety Features Actuation System**

Once the required logic is generated, the RPS will send signals to the ESFAS, which combines signals from all four RPS trains in 2-out-of-4 voting logic. Once the ESFAS receives the appropriate voting logic combination, it sends signals to the SLS to actuate appropriate ESF components for protective action.

The ESFAS also receives signals from conventional switches on the OC for train level manual actuation of ESF systems.

In the event of loss of offsite power (LOOP) and/or PA, ESF loads are connected to the emergency power bus in a pre-determined sequence by the load sequencing function, provided by the ESFAS and SLS. There are two types of load sequencing: one for LOOP and the other for emergency core cooling system (ECCS) actuation concurrent with LOOP.

The ESFAS also receives interlock signals from the RPS, such as the P-4 interlock, which indicates the reactor trip. Interlocks are developed redundantly within each RPS train. The RPS will send interlock signals to the ESFAS, which combines signals from all four RPS trains in 2-out-of-4 voting logic.

#### **7.1.1.3.3 Safety Logic System**

The SLS receives ESF system level actuation demand signals and LOOP load-sequencing signals for the safety components from the ESFAS. The SLS also receives manual component level control signals from the OC (safety VDUs and operational VDUs). This system performs the component level control logic for safety actuators (e.g., motor operated valves [MOVs], solenoid operated valves, switchgears).

#### **7.1.1.4 Systems Required for Safe Shutdown**

##### **7.1.1.4.1 Safety Logic System**

The SLS receives manual component level control signals from the OC (safety VDUs and operational VDUs) to control plant components to achieve safe shutdown.

##### **7.1.1.4.2 Safety Grade HSI**

The safety VDU processors manage the displays on the safety VDUs located on the OC and the RSC. They receive process parameter information from the RPS, actuation status information from the RPS and ESFAS, and component status information from the SLS. The safety VDU processors also receive operator commands such as screen navigation and soft control from the safety VDUs.

---

The safety VDUs are located on the OC and RSC and provide access to information and controls for safety systems.

Command signals from safety VDUs and operational VDUs are transmitted to the RPS, ESFAS and SLS via the PSMS communication system (COM). COM is the interface system between the safety-related PSMS and non-safety related PCMS. It provides command priority logic between the safety VDUs and operational VDUs. Command signal path and command priority logic is described in Technical Report MUAP-07004 Figure E-1 and Section 5.1.13, respectively.

#### **7.1.1.5 Information Systems Important to Safety**

##### **7.1.1.5.1 Post Accident Monitoring**

The purpose of displaying PAM parameters is to assist MCR personnel in evaluating the safety status of the plant. In accordance with RG 1.97 (Reference 7.1-6), PAM Type A, B, and C variables have redundant instrumentation and can be displayed on at least two redundant safety VDUs. Type A and B parameters are continuously displayed on the LDP and are continuously available on a safety VDU, or can be retrieved immediately.

##### **7.1.1.5.2 Bypassed and Inoperable Status Indication**

If any safety function is bypassed or inoperable at the train level, this is continuously indicated on the LDP. Other bypassed or inoperable conditions that do not result in inoperability of safety functions, at the train level, are displayed on operational VDUs but not on the LDP.

##### **7.1.1.5.3 Plant Alarms**

The alarm system provides all information necessary for detecting abnormal plant conditions. The alarm system enhances the operators ability to recognize fault conditions even when the number of faults, or their severity, are increasing. Information for all alarms is displayed on the alarm VDU, LDP, and the operational VDU. LDP alarms are located in the fixed area of the LDP.

##### **7.1.1.5.4 Safety Parameter Display System**

The safety parameter display system (SPDS) provides a display of plant parameters from which the status of plant safety system operation may be assessed. The SPDS is displayed on operational VDUs located in the MCR, TSC, and EOF. The primary function of the SPDS is to aid MCR operating personnel to make quick assessments of plant safety status. Duplication of the SPDS displays in the TSC and EOF improves the exchange of information between these facilities and the control room and assists plant management in the decision-making process. The SPDS operates during normal operations and during all classes of emergencies. The SPDS displayed information in the MCR, TSC, and EOF is identical. The functions and design of SPDS in the MCR are integrated into the overall human-system interface (HSI) design.

**7.1.1.6 Interlock Systems Important to Safety**

Interlocks important to safety are those that operate to reduce the probability of occurrence of specific events. Interlocks important to safety also ensure availability of ESFs. These interlock logics are implemented within the SLS, which receives process signals from the RPS.

**7.1.1.7 Control Systems not Required for Safety**

The function of the non-safety PCMS is to establish and maintain the plant operating conditions within prescribed limits. The PCMS includes the reactor control system, the balance of plant (BOP) control system, the incore instrumentation system, the non-safety part of the HSIS, and other I&C systems.

**7.1.1.8 Diverse Instrumentation and Control Systems**

The non safety-related DAS monitors and controls safety and non-safety systems, required to cope with anticipated operational occurrences (AOOs) and PAs concurrent with a common cause failure (CCF) that disables all functions of the PSMS and PCMS. The DAS includes automated actuations and manual controls.

**7.1.1.9 Data Communication Systems**

The data communication system (DCS) consists of the plant-wide unit bus, safety bus for each PSMS train, and maintenance network for each PSMS train and the PCMS (five maintenance networks total). The DCS also contains data links for point-to-point communication and an input/output (I/O) bus for each controller. This includes information and controls for the MCR, RSR, and TSC (monitoring only at the TSC). The DCS interfaces with the station bus, which is an information technology network (i.e., not I&C). The station bus provides information to plant personnel and to the EOF. Figure 7.1-1 shows the major components of the DCS within the overall I&C architecture.

**7.1.1.10 Auxiliary Support Features and Emergency Power**

Auxiliary support systems required for the safety-related I&C systems include Class 1E alternating current (ac) normal and emergency power, Class 1E direct current (dc) normal and emergency power, component cooling water (CCW) system, essential service water (ESW) system, and area heating, ventilation, and air conditioning (HVAC) systems. Electrical systems are described in Chapter 8. CCW/ESW/HVAC systems are described in Chapter 9. The interface between the auxiliary support systems and the safety-related I&C systems is described within this chapter.

The auxiliary support systems for non safety-related I&C systems include non-Class 1E ac normal power, non-Class 1E dc normal power, HVAC systems, instrument air system, component cooling water system (CCWS), and essential service water system (ESWS). Interface between the auxiliary support systems and the non safety-related I&C systems is described within this chapter.

The PSMS is powered from two Class 1E Power Sources. These sources are uninterruptible power supplies (UPSs) backed-up by Class 1E station batteries and by the Class 1E gas turbine generators (GTGs). Power sources for the PSMS are shown in

Figures 7.1-4 and 7.1-5. A description of the power distribution to PSMS equipment is described in Subsection 8.3.1. The Class 1E ac/dc power system is designed as safety-related equipment, fully conformed to the requirements of IEEE Std 308-2001 (Reference 7.1-21) with an exception that pertains to sharing of power systems at multi-unit nuclear power plants since the US-APWR is a single unit plant. More detail descriptions for this conformance are described in Section 8.3.

The PCMS is powered from two non-Class 1E UPSs. These UPSs are backed-up by station batteries and by the alternate ac power source, as shown on Figures 7.1-6 and 7.1-7. A description of the power distribution from the UPS to PCMS equipment is provided in Subsection 8.3.1.

### 7.1.2 Identification of Safety Criteria

Table 7.1-2 “Regulatory Requirements Applicability Matrix” describes the compliance of the US-APWR I&C system to regulatory requirements and guidance. The related sections of the DCD are also described.

Section 3 of each MHI Topical and Technical Report describes applicable code, regulatory, and industry standard compliance. The code, regulatory, and industry standards in the Section 3 of each Topical and Technical Report are also applicable to the US-APWR I&C design.

Compliance to the corresponding sections of Appendix C.I.7.1-A in RG 1.206 (Reference 7.1-7), “Digital Instrumentation and Control Systems Application Guidance”, are discussed in Subsection 7.1.3. Additionally, compliance with Appendices C.I.7.1-B, “Conformance with Institute of Electrical and Electronics Engineers (IEEE) Std 603”, and C.I.7.1-C, “Conformance with IEEE Std 7-4.3.2”, are discussed in MUAP-07004 Appendices A and B respectively. For some sections of IEEE Std 603-1991, complete compliance requires plant specific descriptions. For the US-APWR these plant specific items are addressed in the DCD.

### 7.1.3 Design Bases of Instrumentation and Control System

The design of the I&C system meets all code, regulatory, and industry standards, as shown in Table 7.1-2, including the specific safety requirements described in the subsections below. Since the RPS, ESFAS, SLS, and other subsystems of the PSMS use a common platform, the design bases for PSMS are listed in this subsection. design bases that are specific to the RPS, ESFAS, SLS, or other I&C subsystems are discussed in Sections 7.2 through 7.9.

#### 7.1.3.1 Defense in Depth and Diversity Concept

The architecture of the overall I&C system is based on the defense in depth and diversity concept. This concept defines four echelons of defense. These echelons are the control system, reactor trip system, engineered safety features actuation system, and monitoring and indicators.

Separation of functions and diversity of functions between these echelons minimize the potential for CCFs. In addition, the software applied for the PSMS has high integrity due

---

to design simplicity and a comprehensive software quality program including independent verification and validation (V&V).

The conventional, analog, and hardwired DAS is provided per guidance of branch technical position (BTP) 7-19 (Reference 7.1-8), to accommodate beyond design basis CCFs that could adversely affect all safety and non-safety control systems within all echelons. The DAS provides automated actuation of time critical safety functions. In addition, the DAS allows the operator to monitor critical safety functions and to manually actuate safety process systems, using equipment that is diverse from the PSMS and PCMS. For more detailed discussion on diversity and defense-in-depth features, refer to Topical Report MUAP-07006.

#### **7.1.3.2 Single Failure Criterion**

A single failure within the PSMS does not prevent the initiation or accomplishment of a protective function at the system level, even when a channel is intentionally bypassed for test or maintenance.

For more detailed discussion on this topic refer to MUAP-07004 Appendix A.5.1. |

#### **7.1.3.3 Redundancy Between Safety Divisions**

The redundancy between the safety divisions (i.e., trains A, B, C, and D) satisfies the single failure criterion during normal operation and during all planned on-line test/maintenance configurations. This redundancy ensures the safety function can always be performed despite any single failure. Spurious actuation at the train level is discussed in Subsection 7.1.3.9, and for specific ESF functions in Section 7.3.

#### **7.1.3.4 Independence**

Each train of the PSMS is independent from each other and from non-safety systems, including the PCMS. The physical independence is designed based on the RG 1.75 (Reference 7.1-22) which endorses IEEE Std 384-1992 (Reference 7.1-23). Electrical independence is maintained through qualified isolation devices, including fiber optic data communications cables. Functional independence between controllers is maintained through communication processors that are separate from function processors, and through logic that (1) ensures prioritization of safety functions over non-safety functions and (2) does not rely on signals from outside its own train to perform the safety function within the train.

For more detailed discussion on the methods used to ensure independence between I&C systems in different safety trains and between I&C systems in safety and non-safety systems refer to described in MUAP-07004 Appendix A.5.6 and Appendix B.5.6. |

Cabinets for each train of the PSMS are located in a separate plant equipment room fire area. These fire areas are separate from the fire areas where non-safety systems are located and separate from the fire areas of the MCR and the RSR. To ensure electrical independence, fiber optic cables or qualified isolators are used to interface all signals between plant equipment room fire areas. Electrical independence is also maintained between PSMS divisions and between the PSMS and non-safety systems within the MCR and the RSR.



In addition to these plant equipment room fire areas, electrical independence and physical separation are also maintained between divisions for instrumentation inputs and plant component control outputs interfaced with PSMS cabinets. The independence between the PSMS and PCMS for shared sensors is discussed in Subsection 7.1.3.16.

#### **7.1.3.5 Isolation**

Physical separation and electrical isolation are provided between the PSMS redundant trains and between the PSMS and non-safety systems, including the PCMS. Isolation devices are incorporated into conventional interfaces, data links, and communication networks that connect redundant trains, or carry signals to or from non-safety systems. The isolation devices ensure that credible faults, such as short circuits, open circuits, or the application of credible fault voltage do not propagate between systems. Chapter 8, Subsection 8.3.1.1.11 describes conformance to RG 1.204(Reference 7.1-24). This conformance bounds the credible electrical surges and faults that are considered for electrical isolation.

In addition, for digital interfaces communications isolation is provided to ensure functional independence between systems. Communication isolation includes communication buffers, which provide separation between communication processing, functional processing, and functional logic, which ensures prioritization of all safety functions. The conformance of the interdivisional communication design in the US-APWR PSMS to the Staff Positions of DI&C-ISG-04 (Reference 7.1-30) is described in MUAP-07004, Appendix E.

The isolation devices provide assurance that single failures in non-safety systems will not degrade the performance of safety systems, specifically in instances where protection signals are used by non-safety systems and non-safety signals are used by safety systems. For signals interfaced between redundant trains, the isolation devices provide assurance that failures in one train will not degrade the performance of other trains. The electrical, physical and functional isolation is also discussed in Subsection 7.1.3.4. The isolation from a design basis event of safety system based on the equipment qualification is discussed in Subsection 7.1.3.7. The PSMS digital components are located in a mild environment that is not impacted by any design basis event.

#### **7.1.3.6 Integrity of Software**

The design principles listed below are used for the software design of all digital safety and non-safety systems using the MELTAC platform. These principles assure simplicity and enable high efficiency in the design.

- A structured and modular architecture is applied.
- Basic software and application software are separated.
- Early detection of failures is facilitated by the self-diagnosis functions of the digital system.
- Basic software is implemented in a high level programming language. All functions execute with cyclical single task processing and no interrupts.

- Basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, error handling, etc.
- Application software is described in a graphically symbolized manner, using the problem oriented language (POL), so that functions can be easily understood.

For the non-safety I&C systems, efficiency and reliability of design, production, testing, and maintenance are achieved by using the same basic software and the design tools for the application software as is used for the safety systems.

The V&V program executed for safety systems conforms to all regulatory requirements for high integrity software.

#### 7.1.3.7 Qualification and Equipment Protection

The PSMS is qualified for worst-case environmental and seismic requirements for the place of its installation. The PSMS qualification envelopes the seismic and environmental boundary conditions for these locations are described in Sections 3.10 and 3.11. MUAP-07005 describes equipment qualification testing for the MELTAC platform. The environmental condition of the US-APWR is described in "US-APWR Equipment Environmental Qualification Program" MUAP-08015 (Reference 7.1-25).

Conducted and/or radiated electromagnetic interference (EMI) and radio frequency interference (RFI) induced by actuation of large equipment, lightning, or radio frequency emission could degrade performance of I&C systems and compromise safety. Therefore, adequate EMI/RFI protection is designed into I&C systems components, including controllers, I/O devices, and power supply circuits. In addition, optical fiber is used for data communication, which provides electrical independence and protection against EMI/RFI.

The PSMS is qualified for EMI/RFI compatibility, as demonstrated through type testing. The EMI/RFI test levels for the PSMS are intended to envelope the possible field strength necessary for expected locations. The US-APWR is designed and operated consistent with any restrictions identified in the EMI/RFI qualification report, such as wireless communication exclusion zones, and open cabinet door conditions. This feature is described in MUAP-07005 Section 5.3. The susceptibility envelope defined in RG 1.180(7.1-26) is applicable to the US-APWR and therefore applicable to the PSMS, because the US-APWR does not include any extraordinary conducted or radiated emissions sources that are not included in operating nuclear power plants today.

Safety-related I&C components, such as sensors, detectors, cables, and connectors are designed to be qualified for operation in both normal and abnormal environments, and to meet seismic requirements of the site in which they are located. Qualification is assured per applicable industry standards (IEEE Std 323-2003 [Reference 7.1-9]) and regulatory requirements (RG 1.89 [Reference 7.1-10]), as described in Section 3.11.

Instrument sensing lines are specified to be protected in compliance with RG 1.151 (Reference 7.1-11) which endorses ISA-S67-02, including freeze protection.

---

For details regarding PSMS qualification testing, refer to MUAP-07004 Sections 5.2.1 through 5.2.5. Refer to Chapter 3 for identification of the US-APWR qualification conditions.

The inspections, tests, analyses, and acceptance criteria (ITAAC) encompass the qualification of plant instrumentation, such as transmitters and nuclear instrumentation.

#### **7.1.3.8 Unified Architecture**

A unified architecture is applied to the design of integrated digital I&C systems of the US-APWR. The unified architecture provides a high quality and reliable platform for both the safety systems and non-safety systems, which simplifies communication between these systems. Maintenance resources are standardized for every system thereby reducing human error. An integrated digital technology is also used for VDU based operation.

Specification of the hardware modules, such as central processing units (CPUs) and I/O modules, used for each subsystem is basically the same throughout the I&C architecture, except for some specific application modules (e.g., rod position interface). This approach allows the total number of required spare parts to be minimized. The configuration of the basic software, POL, and engineering tools for specification of the application software, is the same in all digital I&C subsystems using the MELTAC platform. Maintenance procedures and tools (i.e., the engineering tool) are standardized for all subsystems; therefore, the training effort for the maintenance staff and potential for human error are minimized.

MELTAC is the only digital platform used for the safety systems of the US-APWR. All other safety I&C components are conventional analog.

#### **7.1.3.9 Redundancy Within Divisions and Systems**

To prevent disturbance of the plant caused by a failure of the safety or non-safety I&C systems, a redundant configuration is applied. Failed components, including CPU, I/O modules, and communication modules, are detected by self-diagnostic features. Redundant components are arranged in configurations for continuous parallel operation or standby operation, as described in MUAP-07005 Section 4.1.1.1. For standby operation, self-diagnostic features automatically switch to redundant stand-by components in case of failure. The redundant fail-over components continue uninterrupted control without causing any disturbance to the plant.

Ac power for the I&C system is supplied from two different sources. The configuration of the power supplies within each I&C subsystem ensures no loss of function due to a single failure of the electric power source.

#### **7.1.3.10 Self-Diagnosis Function**

The integrity of digital I&C components is continuously checked by their self-diagnosis features. These self-diagnostic features result in early detection of failures, and allow on-line repair that improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. In addition, the self-diagnostic features control redundant controller configuration, to maintain all system functions, even in the presence of failures. The self-

diagnosis is always working in the digital control system but does not affect system operation. Therefore, there is no impact to channel independence, system integrity and compliance to the single failure criterion during self-testing.

Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are specifically provided for functions with no self-diagnostics. The integrity of the self-diagnosis is confirmed by a periodic manually initiated software memory check, which includes the software memory which is used for self-diagnosis. For PSMS, this software memory check requires temporarily connecting each PSMS controller to the Maintenance Network. When a PSMS controller is connected to the Maintenance Network, it is considered inoperable. The functions affected by an inoperable controller are managed by plant technical specifications. PCMS controllers are permanently connected to the Maintenance Network.

Also, when I/O is checked by manual sensor calibration and output actuation of plant components, the digital components which are self-tested are also re-checked. This provides manual confirmation for the integrity of all digital functions. The coverage of self-diagnosis and manual test is described in MUAP-07004 Sections 4.3 and 4.4. MUAP-07005 Section 4.1.5.1 describes self-diagnosis. The self-testing is provided for MELTAC components of PSMS, with the exception of the conventional circuits within the I/O and PIF modules, and the touch screens of the safety VDU.

#### **7.1.3.11 Manual Testing, Bypasses, Overrides and Resets**

Manual test features are specifically provided to allow periodic testing of all functions that are not automatically tested through self-diagnostics. This includes primarily sensor calibration, manual initiation functions and final actuation of plant components. These manual tests also recheck the portions of the system that are self-tested, and thereby manually confirm the integrity of self-tested components and the integrity of the self diagnostic functions. All manual tests may be conducted on-line without full system actuation and without plant disturbance. The test of output modules for plant components is conducted along with the test of plant components. Since the reliability of the digital I&C equipment is significantly higher than the reliability of the plant components, the periodic test frequency is determined by the reliability of the plant components, not the reliability of the digital I&C equipment.

Safety systems may be placed in a bypass operation mode to allow manual testing and maintenance while the plant is on-line. For the RPS measurement channels, automatic bypass management logic prevents multiple bypassed conditions to ensure the minimum redundancy required by the technical specifications is always maintained. For other RPS functions and the ESFAS, train level maintenance bypasses are administratively controlled. Maintenance Bypasses may be manually initiated from the safety VDU for each respective PSMS train. To manually initiate a Maintenance Bypass from the operational VDU, the Bypass Permissive for the train must be enabled. The Bypass Permissive is part of the PSMS. There is one Bypass Permissive for each train. Administrative controls ensure the Bypass Permissive for only one train is enabled at any time. The manual Bypass Permissive is available from soft switches on the safety VDU.

Indication is provided for bypassed or inoperable conditions in accordance with RG 1.47 (Reference 7.1-12). Maintenance bypasses can be manually initiated within the PSMS, via safety VDUs. To manually initiate a Maintenance Bypass from the operational VDU, the Bypass Permissive for the train must be enabled. During this bypass mode, a single failure in the safety system will not result in a spurious plant trip or spurious system level ESF actuation.

In addition to maintenance bypasses, automatic and manual operating bypasses are provided to bypass certain protective actions that would otherwise prevent modes of operation, such as startup and shutdown. Interlocks are provided within the PSMS to automatically remove operating bypasses. This feature allows operating bypasses to be manually initiated from safety VDUs. To manually initiate an Operating Bypass from the operational VDU, the Bypass Permissive for each train must be enabled, one train at a time.

All manual and automatic demand signals for components, which are controlled by motor control centers and switchgear, may be bypassed at the component level for testing or maintenance by two deliberate manual operator actions from safety VDUs. This is referred to as the Lock function in MUAP-07004 Appendix D. The Lock function can also be used to block or override safety functions at the component level. To Lock safety-related components from operational VDUs, the Bypass Permissive for the train must be enabled. This Bypass Permissive is administratively controlled so that it is enabled for only one train at a time. When the permissive is enabled for a train from the safety VDU, Lock may be activated from the operational VDU individually for any components within that train. All bypasses are administratively managed by plant operators in accordance with plant technical specifications. The effect of bypasses is alarmed at the system level for each train via the bypassed and inoperable status indication (BISI).

After safety function actuation and after initiating conditions return to normal, safety functions are manually reset at the system level. These resets are available from safety VDUs. Reset signals from the operational VDU cannot be received by the PSMS without a manual Bypass Permissive signal from the safety system. If undetected reset signals exist at the time the Bypass Permissive is manually actuated, the reset errors will be indicated to operators by ESFAS reset demand status indication for the specific functions affected. The Bypass Permissive ensures additional spurious reset signals cannot be received by the PSMS at the time an AOO or PA occurs. Maintenance bypasses, operating bypasses, overrides, resets and Bypass Permissives are initiated separately for each safety division.

#### **7.1.3.12 Human-System Interface**

The MCR is designed to perform centralized monitoring and control of the I&C systems that are necessary for use during normal operation, AOOs, and PAs. Furthermore, the HSIS are also designed to reduce the potential for human error and to allow easy operation. In addition to the MCR, the HSI also includes the RSC, TSC, EOF, and local control stations, such as auxiliary equipment control console. Refer to Chapter 18 for a full discussion of all HSI issues.

---

**7.1.3.13 Quality of Components and Modules**

The quality of PSMS components and modules and the quality of the PSMS design process are controlled by a program that meets the requirements of American Society of Mechanical Engineers (ASME) NQA-1-1994 (Reference 7.1-13). Conformance to ASME NQA-1-1994 is described further in Section 17.5.

**7.1.3.14 System Calibration, Testing and Surveillance**

Testing from and including the sensors of the PSMS through to and including the actuated equipment and HSI is accomplished in a series of overlapping sequential tests and calibrations. The majority of the tests are conducted automatically, through self-diagnostics. Most remaining manual tests may be performed with the plant at full power. There are no exceptions for testing at power in PSMS.

The test frequency for manual tests is based on an uncertainty and reliability analysis, reference Subsection 7.2.2.7 and 7.2.3.5, respectively, for additional information. This analysis demonstrates the need to conduct most manual tests for PSMS equipment no more frequently than once per 30 months, which allows for fuel cycles up to 24 months plus 6 months to accommodate 25% margin for consistency with technical specification surveillance interval compliance. Therefore conducting manual tests for PSMS equipment on-line or off-line, during refueling shutdown, is at the discretion of the plant owner.

Periodic routine calibration will be performed for the field located transmitters of each safety-related instrument loop. Due to the digital design of the control platform in the US-APWR, a traditional calibration method will be performed from the sensor to the analog to digital converter. During this calibration, the digital display will provide the instrument output. As in a traditional calibration, the measured value on the display will be compared to an expected range. Calibration points encompass the trip setpoint to confirm required accuracy at the trip setpoint value(s).

The method of testing for indicating and non-indicating sensors is the same. Any operational or maintenance VDU, that obtains its digital value from the PSMS, can be used for calibration. If a sensor has no operational indications its digital value will be read using a maintenance VDU, such as the MELTAC Engineering Tool, which will be temporarily connected during CHANNEL CALIBRATION.

The PSMS meets the periodic testing requirements of IEEE Std 338-1987(Reference 7.1-27) which is endorsed by RG 1.22(Reference 7.1-28). The test intervals are specified in the technical specifications, Chapter 16. All periodic testing is conducted to written procedures. For more detailed discussion on this topic, refer to MUAP-07004 Sections 4.3 through 4.5, Appendix A.5.7, A.5.9, A.5.10, A.6.5 through A.6.7, and A.7.5.

Installed RTDs will be calibrated using the method defined in BTP 7-13(Reference 7.1-29). The following accuracy calibration is applicable to all safety related RTDs:

- A reference RTD is checked for acceptable accuracy and response time in controlled laboratory conditions.

- The reference RTD is installed. Loop current step response (LCRS) is checked to confirm applicability of laboratory test data.
- Measurements from installed RTDs are cross correlated to the reference RTD under known and sufficiently similar temperature and flow conditions (i.e., isothermal conditions of all RCS hot and cold legs to the extent practical).
- Calibration readout will be on digital displays, as discussed above, to ensure correct signal propagation and accuracy through the digital systems.

In addition, the LCRS is checked for installed RTDs used in the RPS or ESFAS, where response times are credited in the safety analysis. To detect response time degradation, the LCRS data is compared to the installed RTD's own historical data and to the LCRS for the reference RTD.

The accuracy and response time acceptance criteria account for expected instrument uncertainties and expected temperature and flow deviations. "As found" and "as-left" data is recorded and maintained.

#### **7.1.3.15 Information Displays**

Details on information displays are presented in Topical Report MUAP-07007, Chapter 18, and Section 7.5.

#### **7.1.3.16 Consideration of Control System Induced Transients**

Failures of the PCMS are bounded by the AOOs analyzed in the safety analysis, described in Chapter 15. These PCMS failures are described in Subsection 7.7.2.3. Chapter 8, Subsection 8.3.1.1.11 describes conformance to RG 1.204. This conformance bounds the envelope considered for PCMS EMI susceptibility. The PCMS uses the same hardware as the PSMS, which is qualified to RG 1.180. Therefore, additional lightning induced failures of the PCMS are precluded.

In some cases, it is advantageous to employ signals derived from instrumentation that are also used in the protection trains. This practice reduces the need for separate non-safety instrumentation, which would require additional penetrations into reactor pressure boundaries and introduce the need to additional maintenance in hazardous areas. For each parameter where instrumentation is shared, the PCMS receives four redundant signals from each train of the RPS. The signal selection algorithm (SSA), within the PCMS, receives input from all safety process trains but passes only the second highest operable process signal value to the control system's automation algorithms. The reactor control systems also have a modified signal selector using an average calculation process. (This average calculation for select signals in the reactor control system is different from the description in MUAP-07004 Section 4.2.5.) The SSA excludes process inputs that are failed or taken out of service for maintenance or testing.

The SSA of the PCMS ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or a single RPS train failure. As such, a single failure will not cause the PCMS to take erroneous control actions that challenge the PSMS, while the PSMS is in a degraded operability state due to a failed instrument

channel or failed RPS train. The SSA is designed with an augmented quality program, including software V&V.

The SSA is continuously tested as follows:

- The PCMS employs the same self-test features as the PSMS. These features are described in Section 4.1.5 of MUAP-07005.
- The basic software configuration and application software configuration, within the PCMS controller, is periodically confirmed by the same manually initiated method described in Section 4.1.4.1.c of MUAP-07005.

Since the SSA uses only digital values obtained from the PSMS via the unit bus, all functions of the SSA are completely covered by self-testing; no additional manual tests are required. The digital values obtained from the PSMS are confirmed during channel calibration for the safety sensors.

This SSA within the PCMS allows the RPS to have one instrument channel inoperable or bypassed at all times while still complying with General Design Criteria (GDC) 24 (Reference 7.1-14) and IEEE Std 603-1991 (Reference 7.1-15). As described in the probabilistic risk assessment (PRA) the RPS meets the plant reliability goals with only three channels in operation. Refer to US-APWR Probabilistic Risk Assessment, Technical Report MUAP-07030 (Reference 7.1-16).

The shared instrumentation signals are interfaced through fiber optic data networks. As such, an electrical fault in the PCMS cannot propagate to the protection channel. Refer to MUAP-07004 Section 4.2.5 for additional details.

#### **7.1.3.17 Life Cycle Process**

MHI applies its MELCO's safety system digital platform, MELTAC, to the PSMS and PCMS systems of the US-APWR. Full details of the life cycle process for the MELTAC basic software, including quality assurance (QA), management, development, installation, maintenance, training, operation, and the software safety plan are discussed in MUAP-07005 Section 6.0. A summary of the life cycle process for the system application software, including QA, management, development, installation, maintenance, training, operation, and the software safety plan are discussed in MUAP-07004 Section 6.0. A detailed description of the application software life cycle process, including BTP 7-14 (Reference 7.1-17) compliance, is provided in the Software Program Manual for the US-APWR Technical Report MUAP-07017 (Reference 7.1-18).

#### **7.1.3.18 Quality Assurance Program**

The overall quality assurance program (QAP) for the US-APWR I&C systems is described in Chapter 17. The specific QAP for the MELTAC platform is described in MUAP-07005 Section 6.0. These QAPs address all requirements of Title 10, Code of Federal Regulations (CFR), Part 50, Appendix B (Reference 7.1-19), and IEEE Std 7-4.3.2-2003 (Reference 7.1-20).



---

**7.1.3.19 Identification**

I&C equipments identification follows the guidance of RG 1.75, which endorses IEEE Std 384. The following color coding is provided on tags used for the identification of I&C system cabinets and for stand alone components, such as field instruments.

Identification shall not require frequent use of reference material.

- Train A: Red with white lettering
- Train B: Green with white lettering
- Train C: Blue with white lettering
- Train D: Yellow with Black lettering
- Non-safety train: White with Black lettering

This color coding is consistent with the color coding defined in Subsection 8.3.1.1.8 identification of class 1E electrical equipment and cables.

For computer-based systems, the configuration management plan describes the identification process for software. To ensure that the required computer system hardware and software are installed in the appropriate system configuration, the system meets the following identification criteria specific to software systems:

- Firmware and software identification ensures that the correct software is installed in the correct hardware component.
- The software has a means to retrieve identification from the firmware by using software maintenance tools.
- Physical identification requirements of the digital computer system hardware are in accordance with the identification requirements in IEEE Std 603-1991.

The configuration identification management is addressed in Technical Report MUAP-07017.

**7.1.4 Combined License Information**

No additional information is required to be provided by a Combined License (COL) applicant in connection with this section.

**7.1.5 References**

- 7.1-1 Manual Initiation of Protective Actions, Regulatory Guide 1.62 Revision 0, October 1973.
- 7.1-2 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.

- 
- 7.1-3     Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.
- 7.1-4     Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.
- 7.1-5     HSI System Description and HFE Process, MUAP-07007-P Rev.3 (Proprietary) and MUAP-07007-NP Rev.3 (Non-Proprietary), October 2009.
- 7.1-6     Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, Regulatory Guide 1.97 Revision 4, June 2006.
- 7.1-7     Combined License Applications for Nuclear Power Plants (LWR Edition), Regulatory Guide 1.206 Revision 0, June 2007.
- 7.1-8     Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.
- 7.1-9     IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations -Description, IEEE Std 323-2003.
- 7.1-10    Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, Regulatory Guide 1.89 Revision 1, June 1984.
- 7.1-11    Instrument Sensing Lines, Regulatory Guide 1.151 Revision 0, July 1983.
- 7.1-12    Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, Regulatory Guide 1.47 Revision 0, May 1973.
- 7.1-13    Quality Assurance Program Requirements for Nuclear Facilities, ASME NQA-1-1994.
- 7.1-14    Separation of Protection and Control Systems, General Design Criteria for Nuclear Power Plant 24, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.
- 7.1-15    IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.
- 7.1-16    US-APWR Probabilistic Risk Assessment, MUAP-07030 Rev.2 (Proprietary), December 2009.
- 7.1-17    Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems, BTP 7-14 Revision 5, March 2007.
- 7.1-18    Software Program Manual, MUAP-07017 Rev.3, January 2011.
- 7.1-19    Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix B.
-

- 
- 7.1-20 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.
- 7.1-21 IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, IEEE Std 308-2001.
- 7.1-22 Criteria for Independence of Electrical Safety Systems, Regulatory Guide 1.75 Revision 3, February 2005.
- 7.1-23 IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384-1992.
- 7.1-24 Guideline for Lightning Protection of Nuclear Power Plants, Regulatory Guide 1.204 Revision 0, November 2005.
- 7.1-25 US-APWR Equipment Environmental Qualification Program, MUAP-08015 Rev.0, February 2009.
- 7.1-26 Guideline for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Regulatory Guide 1.180 Revision 1, October 2003.
- 7.1-27 Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338-1987.
- 7.1-28 Periodic Testing of Protection System Actuation Functions, Regulatory Guide 1.22 Revision 0, February 1972.
- 7.1-29 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors, BTP 7-13 Revision 5, March 2007.
- 7.1-30 Highly Integrated Control Rooms – Digital Communication Systems, DI&C-ISG-04 Revision 1, March 2009.
-

**Table 7.1-1 List of Conventional Switches on the Operator Console**

Name	Quantity
Reactor Trip	4
ECCS Actuation	4
Containment Isolation Phase A	4
Containment Spray	8
MCR Isolation	4
Main Steam Line Isolation	2
Main Feedwater Isolation	2
Emergency Feedwater Isolation	2 per Loop
Emergency Feedwater Actuation	4
CVCS* Isolation	2
Turbine Trip	1
DAS Defeat (DAS Bypass)	1

Note: Chemical and volume control system

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 1 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
	<b>1. 10 CFR 50 and 52</b>									
a. 50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	X	X	X	X			7.2 to 7.6, 7.9	
b. 50.55a(h)(2)	Protection Systems (IEEE Std 603-1991 or IEEE Std 279-1971)	X	X	X	X	X			7.2 to 7.6, 7.9	
c. 50.55a(h)(3)	Safety Systems (IEEE Std 603-1991)	X	X	X	X	X			7.2 to 7.6, 7.9	
d. 50.34(f)(2)(v) [II.D.3]	Bypass and Inoperable Status Indication	X	X	X	X	X	X		7.2, 7.3, 7.5, 7.6, 7.9	
e. 50.34(f)(2)(xi) [II.D.3]	Direct Indication of Relief and Safety Valve Position			X		X	X		7.5	
f. 50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication	X	X	X	X	X			7.3, 7.5	
g. 50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation	X		X	X	X	X		7.5	
h. 50.34(f)(2)(xviii) [II.F.2]	Instrumentation for the Detection of Inadequate Core Cooling	X			X	X			7.5	
i. 50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems	X	X	X	X	X			7.3	
j. 50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage	X			X	X			7.5	
k. 50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves	X		X	X	X			7.4, 7.5	
l. 50.34(f)(2)(xxii) [II.K.2.9]	Failure Mode and Effect Analysis of Integrated Control System								N/A to US-APWR	

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 2 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
m. 50.34(f)(2)(xxiii) [II.K.2.10]	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip								N/A to US-APWR	
n. 50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording								N/A to US-APWR	
o. 50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram							X	7.8	
p. 52.47(b)(1)	ITAAC for Standard Design Certification	X	X	X	X	X	X	X	Refer to Tier 1	
q. 52.80(a)	ITAAC for Combined Licensee Applications	X	X	X	X	X	X	X	Refer to Tier 1	
	<b>2. GDC 10 CFR 50 Appendix A</b>									
a. GDC 1	Quality Standards and Records	X	X	X	X	X	X	X	7.2 to 7.9	
b. GDC 2	Design Bases for Protection Against Natural Phenomena	X	X	X	X	X	X	X	7.2 to 7.9	
c. GDC 4	Environmental and Dynamic Effects Design Bases	X	X	X	X	X	X	X	7.2 to 7.9	
d. GDC 10	Reactor Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 4	
e. GDC 13	Instrumentation and Control	X	X	X	X	X	X	X	7.2 to 7.9	
f. GDC 15	Reactor Coolant System Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 5	
g. GDC 16	Containment Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 6	
h. GDC 19	Control Room	X	X	X	X	X	X	X	7.2 to 7.9	

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 3 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS	
i. GDC 20	Protection System Functions	X	X	X	X	X			7.2 to 7.6, 7.9
j. GDC 21	Protection Systems Reliability and Testability	X	X	X	X	X			7.2 to 7.6, 7.9
k. GDC 22	Protection System Independence	X	X	X	X	X			7.2 to 7.6, 7.9
l. GDC 23	Protection System Failure Modes	X	X	X	X	X			7.2 to 7.6, 7.9
m. GDC 24	Separation of Protection and Control Systems	X	X	X	X	X	X	X	7.2 to 7.9
n. GDC 25	Protection System Requirements for Reactivity Control Malfunctions	X	X	X	X	X			7.2 to 7.6, 7.9
o. GDC 28	Reactivity Limits	X	X	X	X	X	X		7.6, Refer to Chapter 15
p. GDC 29	Protection Against AOOs	X	X	X	X	X	X		7.2 to 7.7, 7.9
q. GDC 33	Reactor Coolant Makeup	X	X	X	X	X	X		7.3, Refer to Chapter 9
r. GDC 34	Residual Heat Removal	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 5
s. GDC 35	Emergency Core Cooling	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 6
t. GDC 38	Containment Heat Removal	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 6
u. GDC 41	Containment Atmosphere Cleanup	X	X	X	X	X	X		7.3, 7.6, Refer to Chapter 6
v. GDC 44	Cooling Water	X	X	X	X	X	X		7.3, 7.6, Refer to Chapter 9

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 4 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
	<b>3. Staff Requirements Memoranda</b>									
a.	SRM to SECY 93087 II.Q	X	X	X	X	X	X	X	7.8	
b.	SRM to SECY 93087 II.T						X		7.5, 7.9	
	<b>4. RGs</b>									
a.	RG 1.22	X	X	X	X	X			7.2 to 7.6, 7.9	
b.	RG 1.47	X	X	X	X	X	X		7.2, 7.3, 7.5, 7.6, 7.9	
c.	RG 1.53	X	X	X	X	X			7.2 to 7.6, 7.9	
d.	RG 1.62	X	X	X	X	X			7.2, 7.3	
e.	RG 1.75	X	X	X	X	X	X	X	7.2 to 7.9	
f.	RG 1.97	X	X	X	X	X	X		7.5	
g.	RG 1.105	X	X	X		X			7.2 to 7.6, 7.9	



**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 5 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
h. RG 1.118	Periodic Testing of Electric Power and Protection Systems	X	X	X	X	X			7.2 to 7.6, 7.9	
i. RG 1.151	Instrument Sensing Lines	X					X		7.2 to 7.6	
j. RG 1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
k. RG 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
l. RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
m. RG 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
n. RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
o. RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	
p. RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9	

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 6 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS	
q. RG 1.174	An Approach for Using PRA in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis								N/A
r. RG 1.177	An Approach for Plant-Specific Risk-Informed Decision Making: technical specifications								N/A
s. RG 1.180	Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related I&C Systems	X	X	X	X	X			7.2 to 7.6, 7.9
t. RG 1.189	Fire Protection for Operating Nuclear Power Plants	X	X	X	X	X	X	X	7.2 to 7.9
u. RG 1.200	An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities								Refer to Chapter 19
v. RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants								Refer to Chapter 8 (Subsection 8.3.1.1.11)
w. RG 1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9
	<b>5. BTPs</b>								
a. BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS	X		X		X			7.6

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 7 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
b. BTP 7-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System (ECCS) Accumulator Lines	X		X		X			7.6	
c. BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service								N/A (US-APWR does not have a situation for restrictive setpoints)	
d. BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems	X	X	X	X	X			7.3	
e. BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors						X		7.7	
f. BTP 7-6	Guidance on Design of I&Cs Provided to Accomplish Changeover from Injection to Recirculation Mode								N/A (US-APWR does not have the Recirculation Mode.)	
g. BTP 7-7	Not used								N/A	
h. BTP 7-8	Guidance on Application of RG 1.22	X	X	X	X	X			7.2 to 7.6, 7.9	
i. BTP 7-9	Guidance on Requirements for RPS Anticipatory Trips	X				X			7.2	
j. BTP 7-10	Guidance on Application of RG 1.97	X		X	X	X	X		7.5	
k. BTP 7-11	Guidance on Application and Qualification of Isolation Devices	X	X	X	X	X			7.2 to 7.6, 7.9	
l. BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	X	X	X		X			7.2 to 7.6, 7.9	

**Table 7.1-2 Regulatory Requirements Applicability Matrix  
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5) (Sheet 8 of 8)**

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
m. BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	X							7.2, 7.3	
n. BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems	X	X	X	X	X			7.2 to 7.6, 7.9	
o. BTP 7-15	Not used								N/A	
p. BTP 7-16	Not used								N/A	
q. BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	X	X	X	X	X			7.2 to 7.6, 7.9	
r. BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems								N/A (No Programmable Logic Controllers are used in safety I&C system)	
s. BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems	X	X	X	X	X	X	X	7.8	
t. BTP 7-20	Not used								N/A	
u. BTP 7-21	Guidance on Digital Computer Real-Time Performance	X	X	X	X	X			7.2 to 7.6, 7.9	

**Table 7.1-3 Deleted**

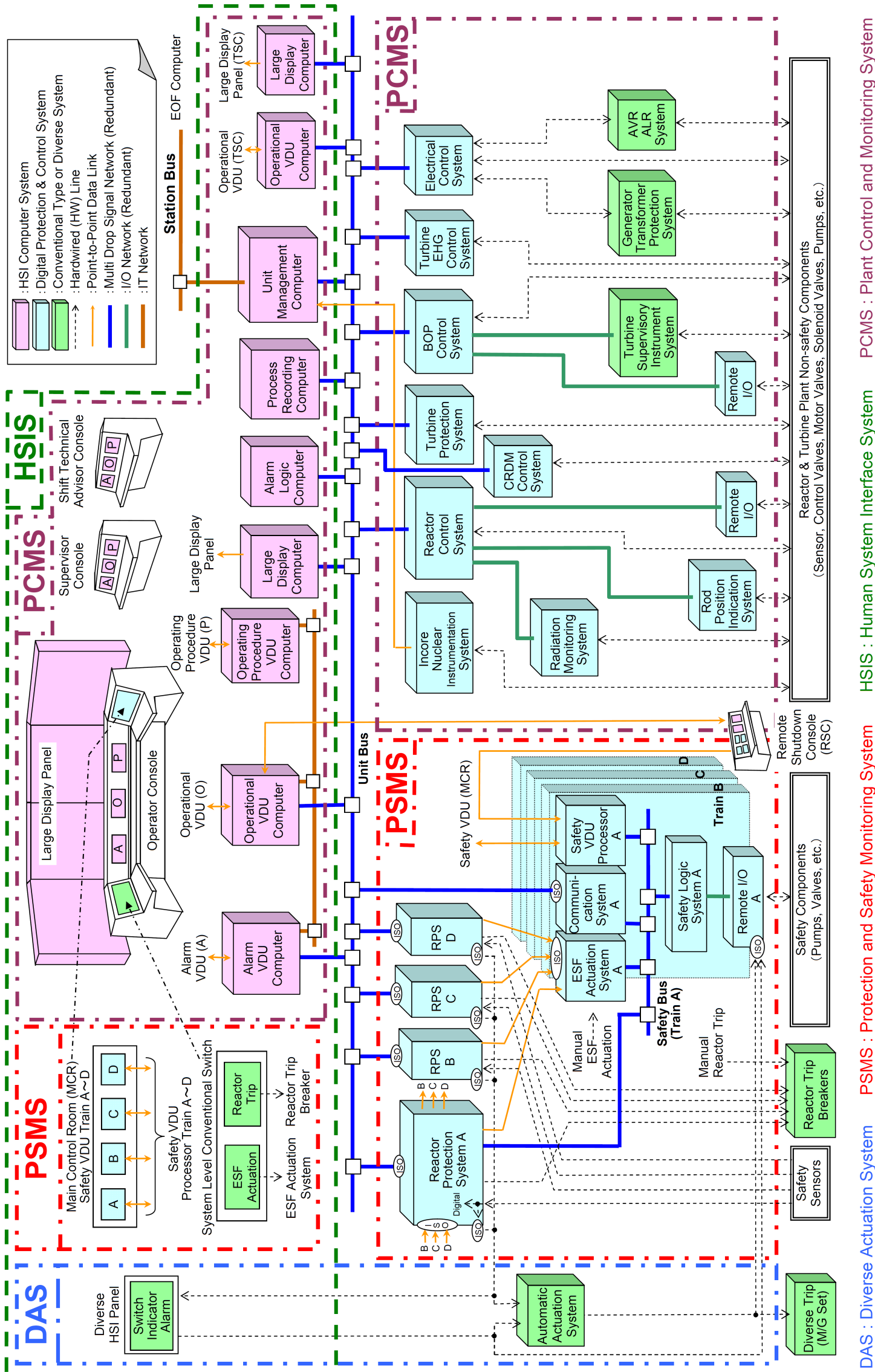


Figure 7.1-1 US-APWR I&C Overall Architecture

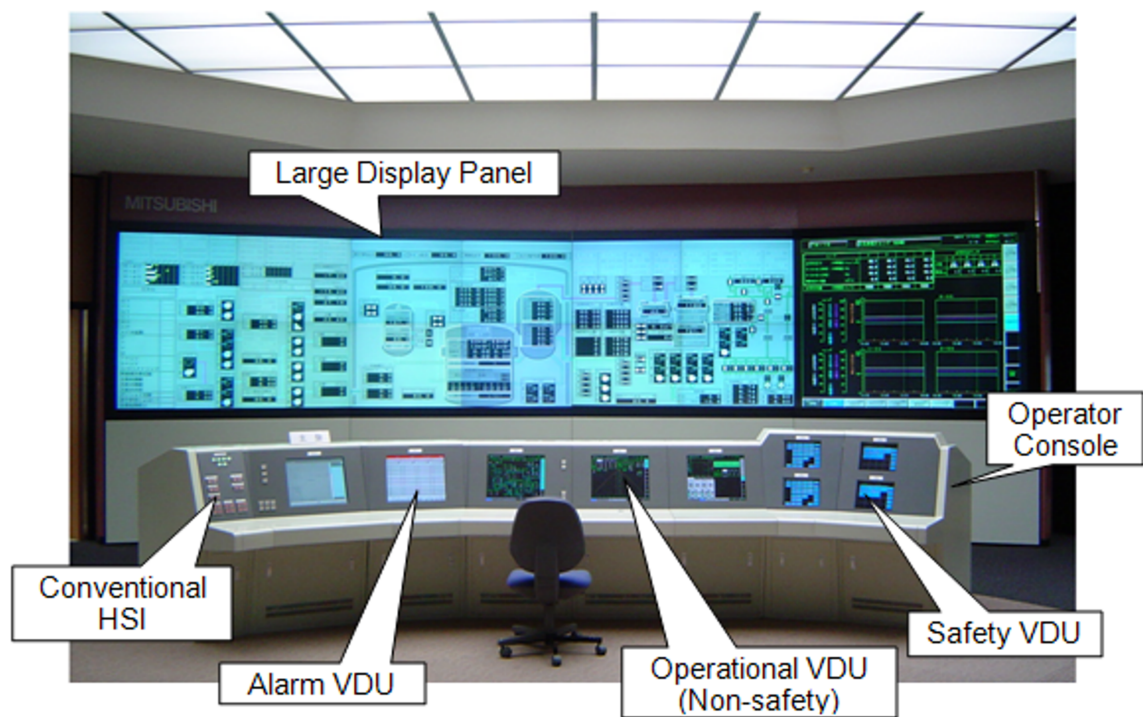
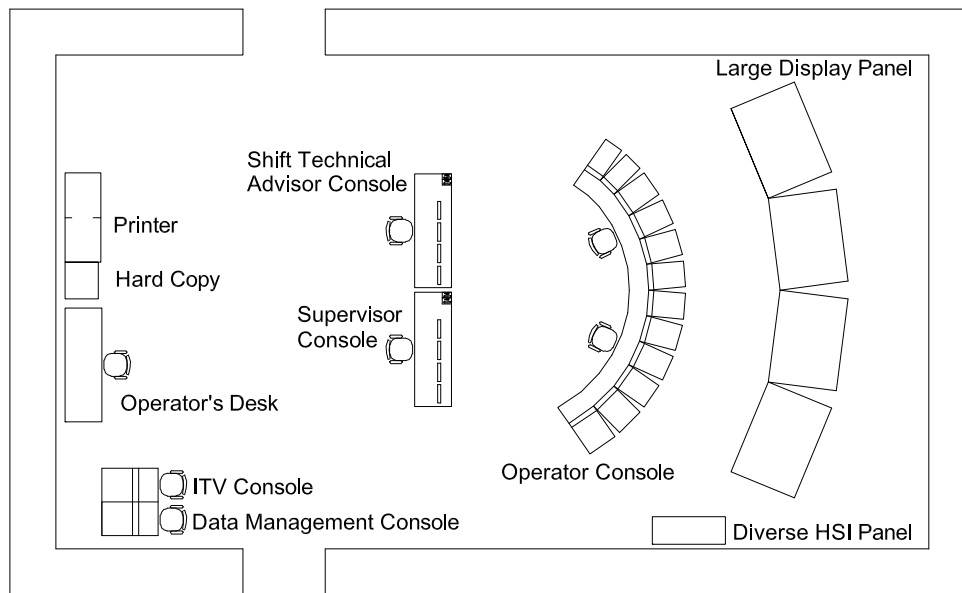
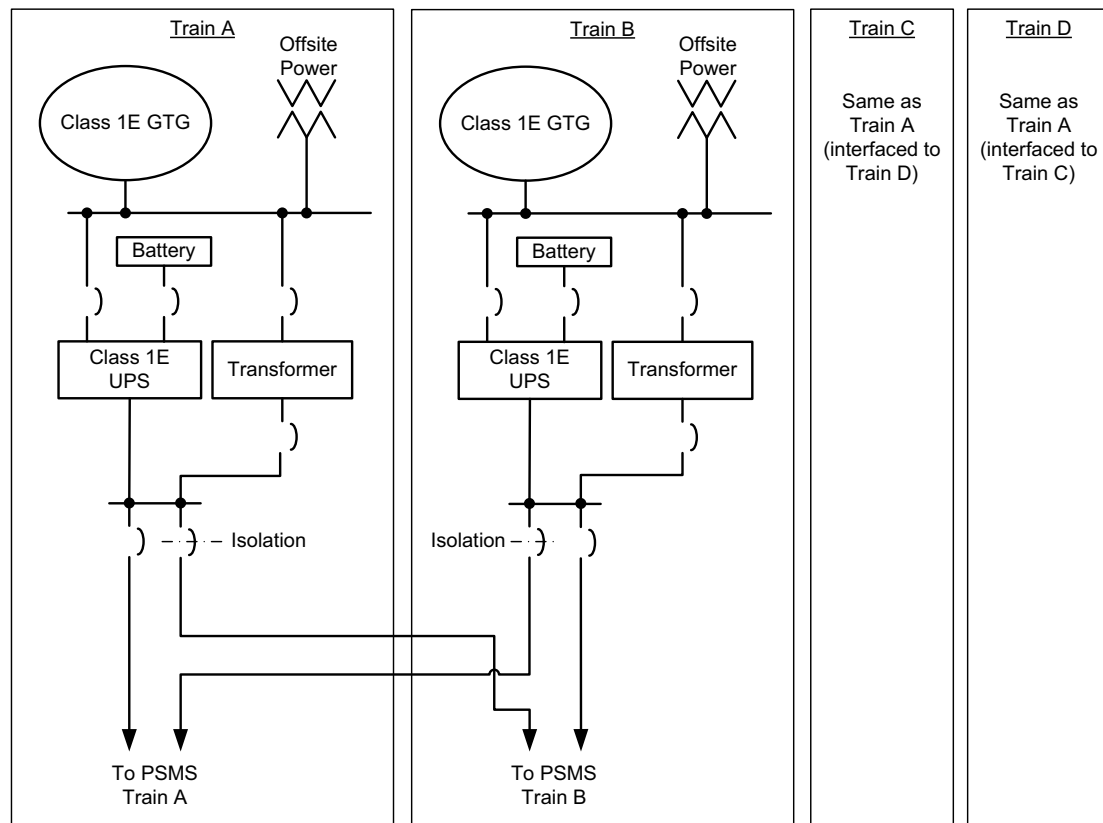


Figure 7.1-2 Typical HSI System Architecture in Main Control Room



**Figure 7.1-3 Layout of Main Control Room**



**Figure 7.1-4 Class 1E UPS for PSMS**

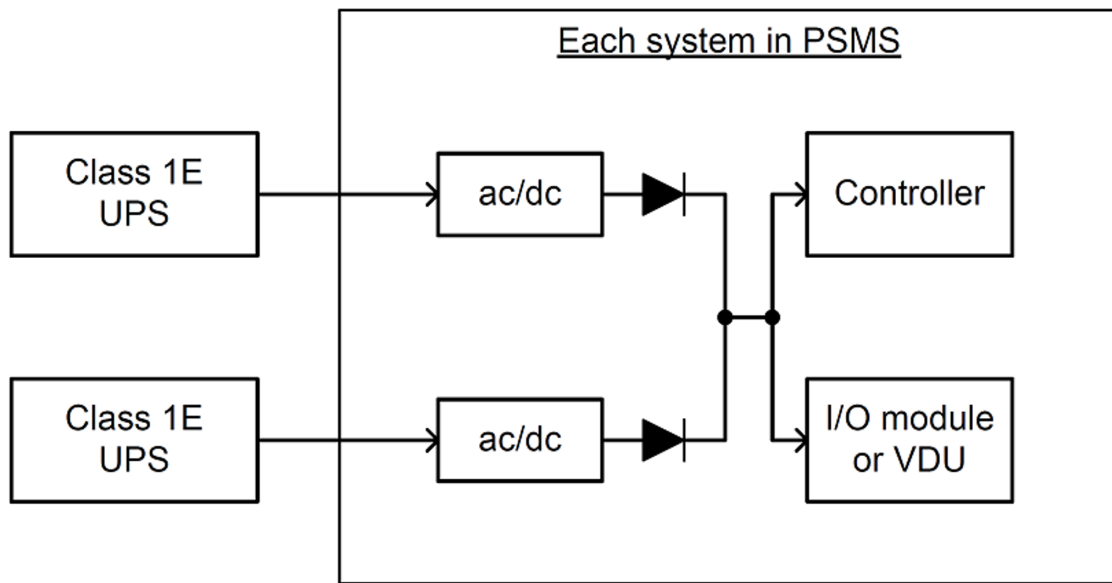


Figure 7.1-5 Electrical Power Source for PSMS

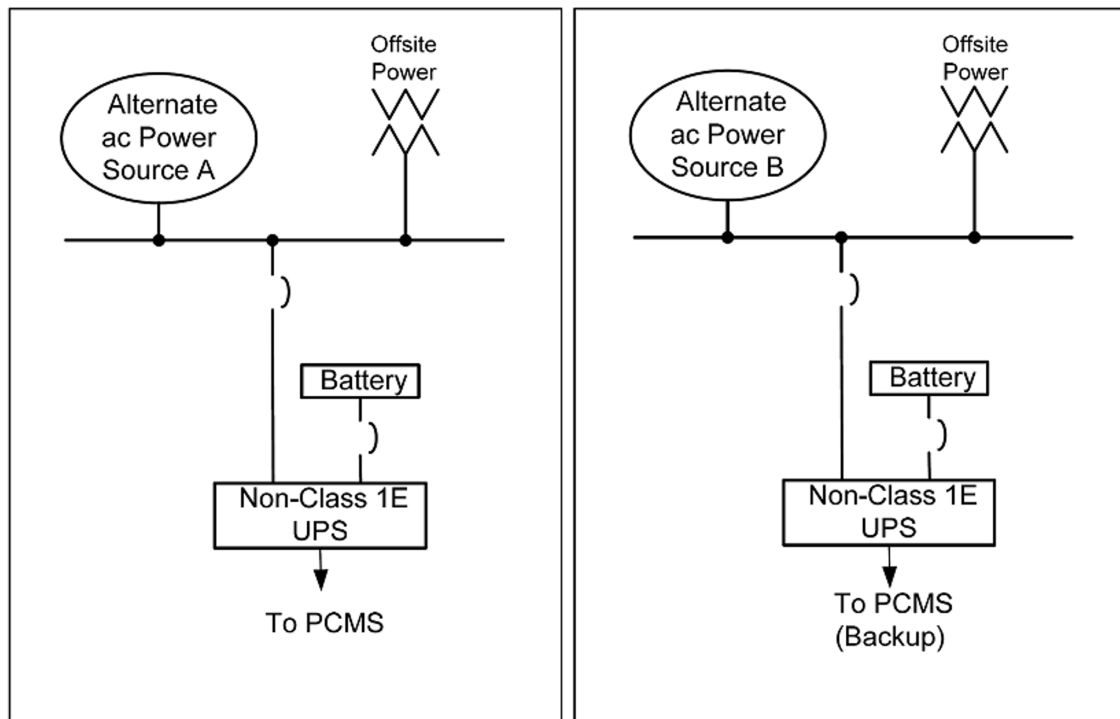


Figure 7.1-6 Non-Class 1E UPS for PCMS

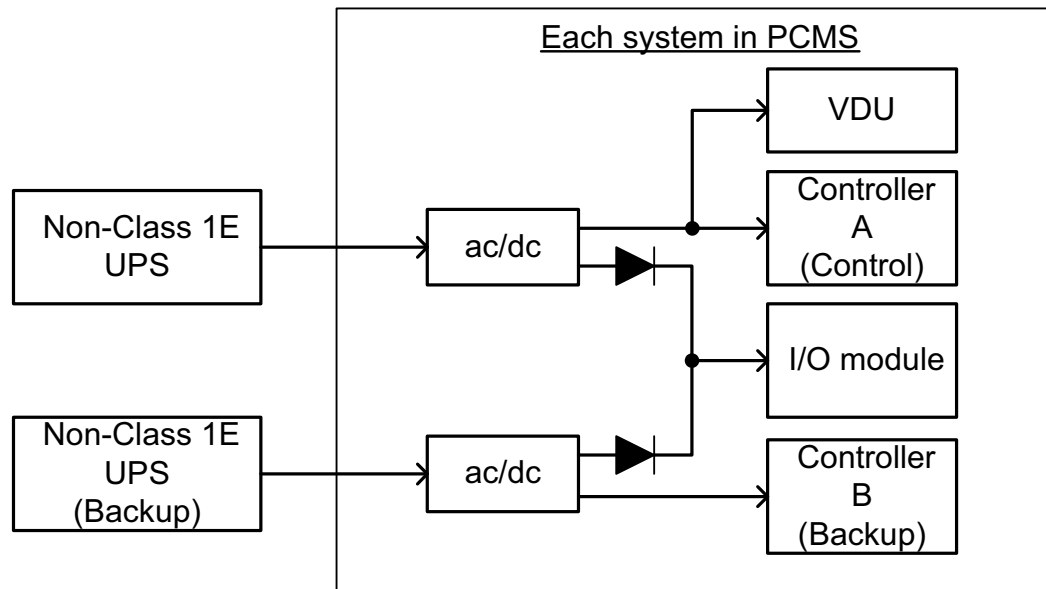


Figure 7.1-7 Electrical Power Source for PCMS

## 7.2 Reactor Trip System

### 7.2.1 System Description

The reactor trip (RT) system, which achieves the all RT functions, consists of the following Class 1E systems:

- Safety sensors
- RPS
- RTB
- Safety grade HSIS

Figure 7.2-1 shows the RPS configuration. Figure 7.2-2 sheet 2 shows the overall reactor trip functional logic.

The RPS automatically trips the reactor to ensure that specified acceptable fuel design limits are not exceeded. Fuel design limits are defined by several considerations, such as mechanical/hydraulic limitations on equipment, and heat transfer phenomena. The RPS maintains surveillance of process variables, which are direct measurements of equipment mechanical limitations, such as pressure and also on variables that are direct measurements of the heat transfer capability of the reactor (e.g., reactor coolant flow and reactor coolant temperature). Other parameters utilized in the RPS are calculated indirectly from a combination of process variables, such as delta T (i.e., reactor coolant hot leg temperature  $[T_{hot}]$  – reactor coolant cold leg temperature  $[T_{cold}]$ ). Whenever a direct process measurement or calculated variable exceeds a setpoint, the reactor will be shutdown in order to protect against either gross damage to the fuel cladding or a loss of system integrity, which could lead to the release of radioactive fission products into the containment vessel (C/V).

To initiate a reactor trip, the RPS interfaces with the following equipment:

- Sensors and manual inputs
- RTBs

The RPS consists of four redundant and independent trains. Four redundant measurements using sensors from the four separate trains are made for each variable used for reactor trip. This applies to all measurements with the exception of source range and intermediate range nuclear instrumentation sensors and main turbine stop valve position, which only have two trains. Selected analog measurements are converted to digital form by analog-to-digital converters within the four trains of the RPS. When the monitored signal requires signal conditioning, it is applied prior to its conversion to digital form. Following necessary calculations and processing, the measurements are compared against the applicable setpoint for that variable. A partial trip signal for a given parameter is generated if one train's measurement exceeds its limit. Each train sends its own partial trip signal to each of the other three trains over isolated serial data links. The

RPS will generate a RT signal if two or more trains of the same variable are in the partial trip state.

The RPS sends system status and process data to the non safety-related part of the HSIS and PCMS, via the unit bus. The RPS also receives operator bypass and reset signals from the HSIS, which are not required for safety, via the unit bus. The interfaces between RPS trains and other systems are shown in Figure 7.2-3 and described in Table 7.2-1.

#### **7.2.1.1 Functional Performance**

The RT system automatically initiates appropriate reactor trip:

- To protect fuel design limits for AOOs.
- To limit core damage for PAs.
- So that the energy generated in the core is compatible with the design provisions to protect the reactor coolant pressure boundary for limiting fault conditions.

The RT system initiates a turbine trip signal whenever a reactor trip is initiated. This function prevents the reactivity insertion that would otherwise result from excessive reactor system cooldown to avoid unnecessary actuation of the ESF system. The RT system provides for manual initiation of reactor trip by operator action.

#### **7.2.1.2 Reactor Trip Logic**

Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Two different parameters are monitored by the separate sensors that interface to two separate digital controllers within the RPS. Each of controllers process these inputs to generate reactor trip and/or ESF actuation signals. This two-fold diversity is duplicated in each redundant RPS train. The processing of diverse parameters results in functional redundancy within each RPS train. Functional diversity provides two separate methods of detecting the same abnormal plant condition, as described in Chapter 15 for specific AOOs and specific PAs, which helps to minimize the potential for CCF concurrent with these specific events. Each functionally diverse digital controller within a train can initiate a reactor trip. The RT signal from each of the four RPS trains is sent to a corresponding RT actuation train. Each of the four RT actuation trains consists of two RTBs. The reactor is tripped when two or more RT actuation trains receive a RT signal. When a limit is approached, the RPS initiates signals to open the RTBs. This action removes power to the CRDM coils permitting the rods to fall by gravity into the core. This rapid negative reactivity insertion will cause the reactor to shutdown (a description of the CRDM is provided in Section 3.9 and Chapter 4).

Figure 7.2-4 illustrates the configuration of the RTBs. The breakers are located in two fire-protected areas. Breakers with a "1" designation are located in one room. Breakers with a "2" designation are located in the second room. This configuration ensures a fire in one room does not prevent a reactor trip. Figure 7.2-5 shows the fire protection providing for RTBs that ensure that a reactor trip can be initiated with two trains if one fire area

completely fails by fire. The cables of each train are isolated for fire. The isolation between train A and B and between train C and D is based on IEEE Std 384-1992 (Reference 7.2-1) including minimum distance and barriers. Isolation between train A/B and train C/D is by separate fire areas. The logic functions within the RPS are limited to bistable calculations and voting for RT actuation. Each train performs 2-out-of-4 voting logic for like sensor coincidence to actuate trip signals to the four trains of the RTBs. Each train also includes a hardwired manual switch on the OC that directly actuates the RTBs. This switch bypasses the RPS digital controller. The trip demand, whether generated manually or automatically, initiates the following actions: 1) it de-energizes the under-voltage trip attachments on the RTBs, and 2) it energizes the shunt trip devices on the RTBs. Either action causes the breakers to trip.

The RPS is a microprocessor-based digital system that achieves high reliability through segmentation of primary and back-up trip/actuation functions, use of four redundant trains, failed equipment bypass functions, and microprocessor self-diagnostics, including data communications. The system also includes features to allow for manual periodic testing of functions that are not automatically tested by the self-diagnostics, such as the actuation of RTBs. Manual periodic tests can be conducted with the plant on-line and without jeopardy of spurious trips due to single failure(s) during testing.

#### **7.2.1.3 Reactor Trip Variables**

The following variables and signals are monitored to generate a reactor trip signal. The complete list of RT initiating signals is provided in Table 7.2-2. Table 7.2-3 provides range, accuracy, response time, and setpoint for each RT variables. Response time described in this table is within the delay time assumed in the safety analyses of Chapter 15. Setpoint described in this table is within the analytical limit assumed in the safety analysis of Chapter 15. The delay time and the analytical limit is shown in Table 15.0-4 of Subsection 15.0.0.3. Permissives and variables associated with RPS are described in Tables 7.2-4. Table 7.2-5 shows diverse parameters in two separate controller groups.

Some of the following variables are used by multiple safety functions and non-safety control functions;

- Neutron flux (source range, intermediate range and power range, neutron flux rate for power range)
- Reactor coolant cold leg and hot leg temperature ( $T_{\text{cold}}$  and  $T_{\text{hot}}$ )
- Pressurizer pressure
- Pressurizer water level
- Reactor coolant flow
- Reactor Coolant Pump (RCP) speed
- Steam Generator (SG) water level
- ECCS actuation signal

- Manual RT actuation signal
- Turbine trip signal

#### **7.2.1.4 Reactor Trip Initiating Signals**

The following subsection describes the RT initiating signals that are grouped according to their protection function. Train level manual controls are identified in Table 7.2-6 for conventional switches and in Table 7.2-7 for software switches.

Pre-trip alarms and non-safety interlocks are initiated below the RT setpoints to provide audible and visible indication of the approach to a trip condition.

##### **7.2.1.4.1 Nuclear Startup Protection Trips**

###### **7.2.1.4.1.1 High Source Range Neutron Flux**

A high source range neutron flux trip provides protection during reactor startup and plant shutdown. An operating bypass may be manually initiated when the neutron flux is above the P-6 setpoint value (intermediate range), which will also de-energize the high voltage power supply to the source range neutron flux detector. This trip is automatically bypassed by the power range neutron flux interlock P-10. The bypass automatically resets to reactivate the trip function when the intermediate range neutron flux decreases below the P-6 reset point.

Due to the limited duration of reactor startup and shutdown, there are only two source range instrument channels, trains A and D. The train A source range neutron flux detector interfaces to RPS trains A and B. The train D source range neutron flux detector interfaces to RPS trains C and D. Interfaces to RPS trains B and C are via isolated digital data links described in MUAP-07005 (Reference 7.2-2) Section 4.3.3. Signal flow for this trip signal is shown in Figure 7.2-6.

Source range and intermediate range neutron flux signals from the train A detectors are sent to the RPS controllers of train A and B through analog circuits installed in train A nuclear instrumentation system (NIS) cabinet and compared with trip setpoints in each train controller. The signals from the train A NIS cabinet to the train B RPS cabinet are isolated in the train B RPS cabinet. In the case of train D detectors, neutron flux signals are sent to train C and D controllers. The results of the comparison with trip setpoints in train D are sent to train A and trip signals of train A (train A partial trip) are generated as a result of 1-out-of-2 logic. Train D trip signals are generated by the same logic. Results of the 1-out-of-2 logic may be bypassed by the following operating bypass signals: (1) P-6 allows source range neutron flux trip manual operating bypass, (2) P-10 allows source range neutron flux trip automatic operating bypass, and (3) P-10 allows intermediate range trip manual operating bypass.

Similar trip logic functions are processed in each train. Partial trip signal from each train is sent to each trip breaker of the corresponding train and a 2-out-of-4 voting logic is implemented.

The source range channels can be individually bypassed in each RPS train to permit channel testing. Since there are only two source range channels, the duration of this



---

bypass is limited by the technical specifications. This operating bypass action is indicated in the MCR. Figure 7.2-2 sheet 3 shows the logic for this trip function.

#### **7.2.1.4.1.2 High Intermediate Range Neutron Flux**

This trip provides protection during reactor startup and shutdown. It can be manually bypassed if the power range channels are above 10 percent power (P-10). This operating bypass is automatically reset to reactivate the trip function when the power range channels indicate less than the reset point for P-10.

Due to the limited duration of reactor startup and shutdown, there are only two intermediate range instrument channels, trains A and D. Train A intermediate range neutron flux detector interfaces to RPS trains A and B. Train D intermediate range neutron flux detector interfaces to RPS trains C and D. Interfaces to RPS trains B and C are by isolated digital data links.

As described in Subsection 7.2.1.4.1.1, the results of the comparison with trip setpoints in train D are sent to train A and trip signals of train A (train A partial trip) are generated as a result of 1-out-of-2 logic. Train D trip signals are generated by the same logic. The intermediate range channels can be individually bypassed in each RPS train to permit channel testing. Since there are only two intermediate range channels, the duration of this maintenance bypass is limited by the technical specifications. This maintenance bypass action is indicated in the MCR. Figure 7.2-2 sheet 3 shows the logic for this trip function.

#### **7.2.1.4.1.3 High Power Range Neutron Flux (Low Setpoint)**

This parameter trips the reactor when two of the four power range channels exceed the trip setpoint. This trip provides protection during startup. It can be manually bypassed when the power range channels are above 10 percent power (P-10). This operating bypass automatically resets to reactivate the trip function when power range channels indicate less than the reset point for P-10. This operating bypass action is indicated in the MCR. Figure 7.2-2 sheet 3 shows the logic for this trip function.

#### **7.2.1.4.2 Nuclear Overpower Protection Trips**

Four power range nuclear instrumentation detectors are installed vertically at the four corners of the core. Each power range neutron flux detector assembly consists of an upper half detector and a lower half detector. Each detector has a total active length that covers almost the full active fuel length. They are used to measure power level, axial flux difference, and radial quadrant power tilt.

Basic power range signals are:

- Signals from the upper half of each power range neutron flux detector, which corresponds to the neutron flux in the upper section (four signals).
- Signals from the lower half of each power range neutron flux detector, which corresponds to the neutron flux in the lower section (four signals).

The following variables are derived from these basic signals:

- Nuclear power, this is derived from an average of the upper signal and lower signal.
- Axial flux difference, derived from the upper half flux minus lower half flux.

The RT signals derived from the nuclear instrumentation are described in the subsections below.

#### **7.2.1.4.2.1 High Power Range Neutron Flux (High Setpoint)**

This parameter trips the reactor when two of the four power range channels exceed the trip setpoint. This trip provides protection against excessive core power generation during normal plant operation, and is always active. Figure 7.2-2 sheet 4 shows the logic for this trip function.

#### **7.2.1.4.2.2 High Power Range Neutron Flux Positive Rate**

This trip protects the reactor when a sudden abnormal increase in power occurs in two out of the four power range channels. It is always active. A channel is tripped when rate sensitive circuits in the channel detects rate of change in nuclear power above the trip setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power goes below the trip setpoint value. Once latched, the channel can only be reset from the MCR by manual action. This manual action can only be completed after the rate of change in power goes below the trip setpoint value. Figure 7.2-2 sheet 4 shows the logic for this trip function.

#### **7.2.1.4.2.3 High Power Range Neutron Flux Negative Rate**

This trip protects the reactor when a sudden abnormal radial power distribution occurs with two or more dropped control rods. RT is initiated when two out of the four power range channels high negative flux rate exceed its setpoint. It is always active. A channel is tripped when rate sensitive circuits in the channel detect a rate of change in nuclear power below the setpoint value. The channel trip is latched such that the partial trip signal does not disappear when the rate of change in power goes above the setpoint value. Once latched, the channel can only be reset from the MCR by manual action. This manual action can only be completed after the negative flux rate goes below the trip setpoint value. Figure 7.2-2 sheet 4 shows the logic for this trip function.

### **7.2.1.4.3 Core Heat Removal Protection Trips**

#### **7.2.1.4.3.1 Over Temperature Delta T**

This trip provides protection to prevent a departure from nucleate boiling (DNB) or an exit boiling (hot-leg boiling). Setpoints for the DNB limit and the exit boiling limit are continuously and individually calculated by the RPS using a specific algorithm. Lower value of these two setpoints is used as the over temperature delta T trip setpoint.

RT is initiated when two out of four loops exceed its setpoint. Figure 7.2-2 sheet 5 shows the logic for this trip function.

1. Delta T compensation

$$\Delta T \frac{(1+T_7s)}{(1+T_8s)} \left( \frac{1}{1+T_9s} \right)$$

Where:  $\Delta T$  is the measured RCS  $\Delta T$ .

$s$  is the Laplace transform operator.

2. DNB protection setpoint

$$\Delta T_{SP1} = \Delta T_0 \left( K_1 - K_2 \frac{(1+T_2s)}{(1+T_3s)} (T_{avg} - T_{avg0}) + K_3 (P - P_0) - f_1(\Delta I) \right)$$

Where:  $\Delta T_{SP1}$  is the DNB protection setpoint.

$\Delta T_0$  is the indicated RCS  $\Delta T$  at RTP.

$s$  is the Laplace transform operator.

$T_{avg}$  is the measured RCS average temperature.

$T_{avg0}$  is the nominal  $T_{avg}$  at rated thermal power.

$P$  is the measured pressurizer pressure.

$P_0$  is the nominal RCS operating pressure.

$f_1(\Delta I)$  is the penalty function of the neutron flux difference between upper and lower part of the power range neutron flux detector. Increase in  $\Delta I$  beyond a predefined deadband decreases the reactor trip setpoint.

$K_1$ ,  $K_2$  and  $K_3$  are coefficient constants.

3. Core exit boiling protection setpoint

$$\Delta T_{SP2} = \Delta T_0 \left( K_4 - K_5 \frac{(1+T_4s)}{(1+T_5s)} (T_{avg} - T_{avg0}) + K_6 (P - P_0) \right)$$

Where:  $\Delta T_{SP2}$  is the core exit boiling protection setpoint.

$\Delta T_0$  is the indicated RCS  $\Delta T$  at RTP.

s is the Laplace transform operator.

$T_{avg}$  is the measured RCS average temperature.

$T_{avg0}$  is the nominal  $T_{avg}$  at rated thermal power.

P is the measured pressurizer pressure.

$P_0$  is the nominal RCS operating pressure.

K4, K5 and K6 are coefficient constants.

#### 7.2.1.4.3.2 Over Power Delta T

This trip provides primarily Overpower Protection and Core Heat Removal Protection in conjunction with the Overtemperature  $\Delta T$  trip. The setpoint for this trip is continuously calculated by the RPS using a specific algorithm.

RT is initiated when two out of four loops exceed its setpoint. Figure 7.2-2 sheet 5 shows the logic for this trip function.

##### 1. Delta T compensation

$$\Delta T \frac{(1+T_{13}s)}{(1+T_{14}s)} \left( \frac{1}{1+T_{15}s} \right)$$

Where:  $\Delta T$  is the measured RCS  $\Delta T$ .

s is the Laplace transform operator.

##### 2. Over power protection setpoint

$$\Delta T_{SP3} = \Delta T_0 \left( K_7 - K_8 \frac{T_6 s}{1+T_6 s} T_{avg} - K_9 (T_{avg} - T_{avg0}) - f_2(\Delta I) \right)$$

Where:  $\Delta T_{SP3}$  is the over power protection setpoint.

$\Delta T_0$  is the indicated RCS  $\Delta T$  at RTP.

s is the Laplace transform operator.

$T_{avg}$  is the measured RCS average temperature.

$T_{avg0}$  is the nominal  $T_{avg}$  at rated thermal power.

$f_2(\Delta I)$  is the penalty function of the neutron flux difference between upper and lower part of the power range neutron flux detector.

---

Increase in  $\Delta I$  beyond a predefined deadband decreases the reactor trip setpoint.

K7, K8 and K9 are coefficient constants.

#### **7.2.1.4.3.3 Low Reactor Coolant Flow**

This trip protects the reactor in the event of low reactor coolant flow in one or more loops. RT is initiated when two out of four flow sensors indicate low reactor coolant flow in any loop.

This trip is automatically bypassed when reactor power is below the P-7 permissive setpoint, as indicated by power range neutron flux and turbine inlet pressure. The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint. Figure 7.2-2 sheet 5 shows the logic for this trip function.

#### **7.2.1.4.3.4 Low Reactor Coolant Pump Speed**

This trip protects the reactor core in the event of loss of flow in all loops by tripping the reactor when the speed of two out of four RCPs falls below the setpoint. RCP speed is measured by an electro-magnetic speed detector. This trip is automatically bypassed by permissive P-7. The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint. Figure 7.2-2 sheet 5 shows the logic for this trip function.

#### **7.2.1.4.3.5 Low Pressurizer Pressure**

This trip protects the reactor against low pressure, which could lead to DNB. RT is initiated when two out of four pressurizer pressure channels exceed the low setpoint.

This trip is automatically bypassed when reactor power is below P-7 permissive setpoint (turbine inlet pressure or power range neutron flux). The operating bypass is automatically removed when reactor power is above the P-7 permissive setpoint. Figure 7.2-2 sheet 5 shows the logic for this trip function.

#### **7.2.1.4.4 Primary Over Pressure Protection Trips**

##### **7.2.1.4.4.1 High Pressurizer Pressure**

This trip protects the RCS against system over pressure. The trip signal is generated when two out of four pressurizer pressure channels exceed the trip setpoint. There are no operating bypasses associated with this trip. Figure 7.2-2 sheet 6 shows the logic for this trip function.

##### **7.2.1.4.4.2 High Pressurizer Water Level**

This trip prevents water relief through the pressurizer relief valves for system over pressurization. The trip signal is generated when two out of four pressurizer water level channels exceed the trip setpoint. This trip is automatically bypassed when reactor power is below P-7 permissive. This operating bypass is automatically removed when

---

reactor power is above the P-7 setpoint. Figure 7.2-2 sheet 6 shows the logic for this trip function.

#### **7.2.1.4.5 Loss of Heat Sink Protection**

The low SG water level trip protects the reactor from loss of its heat sink in the event of a loss of feedwater to the SGs. The trip signal is generated when two out of four water level sensors, in any SG, monitor water level at or below its trip setpoint. There are no operating bypasses associated with this RT. Figure 7.2-2 sheet 7 shows the logic for this trip function.

#### **7.2.1.4.6 Excessive Cooldown Protection**

The high-high SG water level trip protects the reactor from excessive cooldown in the event of excessive feedwater addition to the SGs, and prevents damage to the main turbine by water induction. The trip signal is generated when two out of four water level sensors in any SG exceed the setpoint. This trip is automatically bypassed when reactor power is below the P-7 permissive. This operating bypass is automatically removed when reactor power is above the P-7 setpoint. Figure 7.2-2 sheet 9 shows the logic for this trip function.

#### **7.2.1.4.7 Emergency Core Cooling System Actuation**

A trip signal is initiated from each RPS train with actuation of its respective ECCS train, manually or automatically. This trip protects the core against loss-of-coolant or a steam line break. Figure 7.2-2 sheet 11 shows the logic for this trip function.

#### **7.2.1.4.8 Turbine Trip**

RT on turbine trip(TT) is an anticipatory trip that is not credited in the safety analysis. Therefore, this is not a safety function but it is designed to be highly reliable. The high reliable design meets the guidance of BTP 7-9(Reference 7.2-12). The RPS and RTB which meet Class 1E criteria with Seismic Category I are applied as the signal processor and final actuation devices for RT on TT. The sensors for RT on TT also meet the requirements of IEEE Std 603-1991. The sensors are located in non-seismic areas (Turbine Building). The installation (including circuit routing) and design of the sensors is such that the effects of credible faults (i.e., grounding, shorting, application of high voltage, or electromagnetic interference) or failures in these areas could not be propagated back to the reactor protection system and degrade the reactor protection system performance or reliability. Thus the sensors in non-seismic areas are qualified to operate in a seismic event. (i.e., not fail to initiate a trip for conditions which would require a trip.)

RT is initiated by either of following two diverse turbine trip signals:

1. Main Turbine Stop Valve Position

The RT signal is generated within each RPS train when that train receives signals indicating that all four main turbine stop valves are closed. As for all other trips, a RT is generated when two out of four RPS trains have detected this condition.

There are only two limit switches on each main turbine stop valve interfaced to RPS trains A and D, as associated circuits. RPS train A routes the limit switch signals to train B, C, and D. RPS train D retransmits the limit switch signals to train A, B, and C. Interfaces to each RPS train are by isolated digital data links described in MUAP-07005 Section 4.3.3 and refer to Figure 7.2-7.

The main turbine stop valve limit switch inputs can be individually bypassed in each RPS train to permit channel testing. Since there are only two limit switch channels, the duration of this maintenance bypass is limited by the technical specifications. This maintenance bypass condition is displayed in the MCR.

This trip is automatically bypassed by permissive P-7 for power level lower than the P-7 setpoint. The operating bypass is automatically removed above P-7 power level. Figure 7.2-2 sheet 13 shows the logic for this trip function.

## 2. Turbine Emergency Trip Oil Pressure

The turbine emergency trip oil pressure trip signal is generated when two out of four oil pressure channels exceed the trip setpoint. Four oil pressure signals are independently interfaced to each train of the RPS as associated circuits.

This trip is automatically bypassed by permissive P-7 for power level lower than the P-7 setpoint. The operating bypass is automatically removed above the P-7 power level. Figure 7.2-2 sheet 13 shows the logic for this trip function.

### 7.2.1.5 Manual Control and Actuated Devices

In addition to automatic trip, operators can trip the RTBs using conventional, fixed position, hardwired switches on the OC. There is one switch for each RT actuation train. Actions by under-voltage trip and shunt trip attachments to trip reactor have been discussed in Subsection 7.2.1.2. There are no operating bypasses associated with the manual RT. Maintenance bypasses that allow manual RT testing are described in MUAP-07004 (Reference 7.2-3) Section 4.4.1. Figure 7.2-2 sheet 4 shows the logic for this trip function.

### 7.2.1.6 Bypasses

Portions of the safety system can be placed in a bypass mode to allow testing and maintenance while the plant is on-line. Such bypasses are known as maintenance bypasses. Maintenance bypasses are discussed in MUAP-07004.

In addition to maintenance bypasses, automatic and manual operating bypasses are provided to bypass certain protective actions that would otherwise prevent modes of operation such as startup. Automatic and manual operating bypasses are described in Subsections below. Maintenance and operating bypasses may be initiated from safety VDUs. To initiate a maintenance or operating bypass from an Operational VDU, the Bypass Permissive for the train must be enabled.

**7.2.1.6.1 Automatic Operating Bypasses**

Some operating bypasses are automatically initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). Automatically initiated operating bypasses for the RPS are as follows:

- High source range neutron flux trip is bypassed automatically by power range neutron flux (P-10).
- Low reactor coolant flow 1-out-of-4 trip is bypassed automatically during low power conditions (P-7).
- Low RCP speed trip is bypassed automatically by during low power conditions (P-7).
- Low pressurizer pressure trip is bypassed automatically by during low power conditions (P-7).
- High pressurizer water level trip is bypassed automatically by during low power conditions (P-7).
- High-high SG water level trip is bypassed automatically by during low power conditions (P-7).
- Reactor trip on turbine trip is bypassed automatically by during low power conditions (P-7).

All automatically initiated operating bypasses are automatically removed when the plant moves to an operating condition where the protective action would be required if an accident occurred. Refer to Table 7.2-4.

**7.2.1.6.2 Manual Operating Bypasses**

Some operating bypasses must be manually initiated. These operating bypasses can be manually initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). Manually initiated operating bypasses for the RPS are as follows:

- High source range neutron flux trip is bypassed manually with high intermediate range neutron flux (P-6)
- High intermediate range neutron flux trip is bypassed manually with high power range neutron flux (P-10)
- High power range neutron flux (low setpoint) trip is bypassed manually with high power range neutron flux (P-10)

All operating bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating regime where the protective action would



be required if an accident occurred. Status indication is provided in the MCR for all operating bypasses.

#### **7.2.1.7 Interlocks**

Interlocks ensure that operator actions cannot defeat an automatic safety function during any plant condition where that safety function may be required. These interlocks include permissives for manually initiated operating bypasses and interlocks to ensure manually initiated operating bypasses are automatically removed when plant conditions would require the trip functions. Interlocks are also provided to ensure that manually initiated maintenance bypasses can only defeat a single train or channel of the RPS but not multiple channels or trains that would impair the system's ability to function and meet the single failure criteria.

In addition, when safety functions are automatically initiated interlocks, such as reset functions of bistables within the RPS ensure completion of protective actions and ensure that opposing manual actions cannot be taken until acceptable plant conditions are achieved. For example, for most RT functions, when a trip parameter reaches the trip setpoint the partial trip signal will not automatically reset until the plant conditions return to pre-trip conditions. For other trip functions, the partial trip signal must also be manually reset; manual reset cannot occur until after the plant conditions return to pre-trip conditions. Manual reset may be initiated from safety VDUs. To initiate a manual reset from an Operational VDU, the Bypass Permissive for the train must be enabled.

Manual actions that oppose the protective action cannot be taken until three out of four partial trip signals are reset.

#### **7.2.1.8 Redundancy**

Redundancy within the RPS is consistent with conformance to the single failure criterion, the unavailability target value and the total safety goal of the plant.

The configuration of four trains with 2-out-of-4 voting logic is provided from sensors to RTBs in the RPS for most RT functions.

Where only two channels of instrumentation are provided, the configuration of 1-out-of-2 voting logic is provided to meet the single failure criterion. For source and intermediate range nuclear instrumentation, this 1-out-of-2 configuration has minimal adverse impact on plant availability due to susceptibility to spurious actuation, because these functions are only active during startup and shutdown. For main turbine stop valve position, the 1-out-of-2 configuration does not adversely affect plant availability, due to susceptibility to spurious actuation, because position signals must be received from all four main turbine stop valves to initiate protective actions.

#### **7.2.1.9 Diversity**

Each train of the RPS consists of two separate digital controllers to achieve defense-in-depth through functional diversity. Two or more initiating signals are identified for each postulated event in Chapter 15 and shown in Table 7.2-5. Functional diversity is provided as these initiating signals which are separated into two groups for each event and

assigned to the two digital controllers. Each functionally diverse digital controller within a train can initiate a partial RT signal.

Diversity is provided within the RTBs through the under voltage trip mechanism and through the shunt trip mechanism.

In addition, the non-safety DAS, which is completely diverse to the RPS, provides monitoring and control of safety-related and non safety-related plant systems. Section 7.8 provides a discussion of DAS.

#### **7.2.1.10 Defense-In-Depth and Design Features**

The RPS provides the reactor trip echelon of defense, as described in Subsection 7.1.3.1.

### **7.2.2 Design Basis Information**

#### **7.2.2.1 Single Failure Criterion**

The RPS meets the single failure criteria through four redundant and independent trains. One input channel may be out of service (or bypassed) continuously. Out-of-service times for additional input channels and complete RPS trains are limited by the technical specifications.

The potential for spurious actuation due to single failures is minimized using 2-out-of-4 logic at the system level for automatic and manual actuation functions.

#### **7.2.2.2 Quality of Components and Modules**

All safety functions of the RPS are implemented using Class 1E components. Non-safety functions are isolated from the RPS with the exception of the turbine trip inputs, which are treated as associated circuits as discussed in Subsection 7.2.1.4.8.

#### **7.2.2.3 Independence**

The independence and separation within the RPS are as described in Subsections 7.1.3.4 and 7.1.3.5, with the exception of the RTBs. Manual RT switches are hardwired from the MCR fire area to the RTBs without isolation. This isolation is not necessary since the reactor will be manually tripped if the MCR must be evacuated due to a fire. Separation and independence of the RTBs are shown in Figure 7.2-5.

#### **7.2.2.4 Defense-in-Depth and Diversity**

The diversity features within the RPS are described in Subsection 7.2.1.9. The defense in depth features within the RPS are described in Subsection 7.1.3.1.

#### **7.2.2.5 System Testing and Inoperable Surveillance**

Refer to Subsection 7.1.3.14 for details.

---

### 7.2.2.6 Use of Digital Systems

All RPS functions rely on digital systems, with the exception of manual RT from the MCR, refer to Subsections 7.1.3.8 and 7.1.3.17. This function uses conventional switches, which are hardwired directly to electro-mechanical RTBs.

### 7.2.2.7 Setpoint Determination

The setpoint determination method for the US-APWR is based on the following regulatory guidance, and industry standards:

ANSI/ISA-67.04.01-2000, "Setpoint for Nuclear Safety-Related Instrumentation," February 2000 (Reference 7.2-4).

ISA-RP67.04.02-2000, "Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation," January, 2000 (Reference 7.2-5).

RG 1.105, Revision 3, "Setpoint for Safety-Related Instrumentation," 1999 (Reference 7.2-6).

Instrument channel statistical accuracy (CSA) and instrument channel response time are integral parts of safety functions setpoint evaluation. The total response time of the instrument channel for the safety function is used in the plant safety analysis. The total response time for safety system actuation signals, and the response time for the actuated devices (which are required to be started to mitigate an AOO or PA), are the basis for calculating acceptable limits for degraded values of the monitored process variables. The CSA provides the margin that must be maintained between the setpoint and the acceptable degraded value of the variable.

CSA is the total uncertainty of an instrument channel from the sensor to the output of the device, which produces an actuation signal, or final indication. The response time of instrumentation channel is a signal propagation time from process monitoring sensor to output of the final device in the channel. The following paragraphs describe the methodology for instrument CSA calculation and instrument response time calculation. The instrument accuracy, setpoint, and response time described in Table 7.2-3 are determined by applying the methodology.

#### 7.2.2.7.1 Methodology for Instrument Channel Statistical Accuracy Calculation

The methodology applied to combine the uncertainty components for a channel is provided in Technical Report MUAP-07004 Section 6.5.4. Reconciliation of the final setpoint study for each plant cannot be performed until the design of the plant is finalized.

Technical Report MUAP-09022 (Reference 7.2-13) provides more detail description for instrument setpoint methodology. The setpoint methodology includes the relationship between analytical limit, setpoint and channel uncertainty. Technical Report MUAP-09022 also provides the channel uncertainty calculations associated with the safety related setpoints used for the RT and ESF actuation functions. The instrumentation channel uncertainty of a safety function channel is analyzed to determine the channel setpoint. The channel uncertainty value is calculated by combining instrumentation factors that affect the accuracy of each component in the channel/loop, using statistical methods. A

square root sum of the squares (SRSS) method is applied. The accuracy of each component consists of the nominal accuracy plus uncertainty due to temperature effects, time dependent drift, and other factors. The method is based on the guidance provided by ANSI/ISA-67.04.01-2000 and ISA-RP67.04.02-2000 that is equivalent to ANSI/ISA-S67.04 (Reference 7.2-7), Part I -1994, endorsed by RG 1.105.

#### **7.2.2.7.2 Methodology for System Response Time Calculation**

The methodology for calculating system response time is provided in MUAP-07004 Section 6.5.3.

#### **7.2.2.8 Equipment Qualification**

Refer to Subsection 7.1.3.7 for details.

#### **7.2.3 Analysis**

Detailed compliance to the GDC, IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 are described in MUAP-07004 Section 3.0, Appendix A and B.

This section provides the failure modes and effects analysis (FMEA) for PSMS and specifically, RT.

##### **7.2.3.1 FMEA Method and Results**

The methodology for the FMEA is provided in MUAP-07004 Section 6.5.1. The FMEA follows the guidance of IEEE Std 352-1987 which is referred from IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003, and IEEE Std 379-2000 (Reference 7.2-8) which is endorsed by RG 1.53 (Reference 7.2-9).

Safety functions are designed with multiple divisions. Each safety division is independent from the other safety divisions and from the non-safety division. Independence ensures that single failures cannot propagate between divisions within the safety system or between non-safety and safety divisions. Therefore, single failures cannot prevent proper protective action at the system level. The single failures considered in the non-safety division and safety divisions are described in the FMEA for each system.

The FMEA for reactor trip in PSMS is described in Table 7.2-8 and Figure 7.2-8. The FMEA demonstrates that:

- All PSMS failures are detectable (through self-diagnosis or manual surveillance tests).
- No single failure will prevent PSMS actuation.
- No single failure will result in spurious PSMS actuation, which results in a RT.
- The PSMS will fail to the safe state for all credible failures. The safe state for the RPS is trip. The safe state for the ESFAS/SLS is as-is.

The FMEA is conducted on the basis that one safety channel is continuously bypassed.

**7.2.3.2 Safety Analysis**

The RT system design requirements such as response time and setpoint determination, are considered and reflected in the safety analysis provided in Chapter 15. The response time, instrument accuracy, and setpoint as shown in Table 7.2-3, meet the safety analysis assumptions.

The Chapter 15 analysis addresses AOOs including spurious control rod withdrawals, plant load rejection, and turbine trip.

Control functions to mitigate the consequences of a plant load rejection and turbine trip are discussed in Section 7.7.

The rod control system interlocks that are provided to prevent abnormal power conditions, which could result from spurious control rod withdrawal, are discussed in Subsection 7.7.1.1.2.

The analysis for additional postulated failures is described as follows:

- **Loss of Cooling Water to Vital Equipment:** The US-APWR has four divisions of safety-related cooling water, corresponding to the four divisions of safety-related ESF equipment. These four divisions are controlled by the PSMS. Therefore, loss of a single division of cooling water does not prevent accomplishing the safety function.
- **Loss of Plant Instrument Air:** There is no reliance on plant instrument air for any safety functions. The loss of plant instrument air will result in the loss of main feedwater (MFW). This condition is considered in the safety analysis described in Chapter 15.
- **Loss of Power Source:** Any one division of subsystems in the PSMS is supplied power from redundant power sources. Therefore, loss of a single power source does not prevent accomplishing the safety function. The loss of a power source may result in a transient condition. This condition is considered in the safety analysis described in Chapter 15.

**7.2.3.3 Test and Inspection**

The RT system meets the testing requirements of IEEE Std 338-1987 (Reference 7.2-10), as discussed in Subsection 7.1.3.14. The initial and subsequent test intervals are specified in the technical specifications. Periodic testing conforms to RG 1.22 (Reference 7.2-11), as discussed in Subsection 7.1.3.14.

**7.2.3.4 Restrictive Setpoints**

For the US-APWR, the reactor will not be permitted to operate when one RCS loop is unavailable, as evidenced by the generation of a RT signal as a result of low reactor coolant flow conditions. Logic diagram Figure 7.2-2 sheet 5 shows that the RT signal is generated when low reactor coolant flow condition occurs in any one of the four RCS loops A, B, C or D. Therefore, the requirement for restrictive setpoints is not applicable.

---

**7.2.3.5 Reliability Analysis**

The methodology for calculating system and component reliability is provided in MUAP-07004 Section 6.5.2.

**7.2.4 Combined License Information**

No additional information is required to be provided by a COL Applicant in connection with this section.

**7.2.5 References**

- 7.2-1 Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384-1992.
- 7.2-2 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.
- 7.2-3 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.2-4 Setpoint for Nuclear Safety-Related Instrumentation, ANSI/ISA-67.04.01-2000.
- 7.2-5 Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation, ISA-RP67.04.02-2000.
- 7.2-6 Setpoint for Safety-Related Instrumentation, Regulatory Guide 1.105 Revision 3, December 1999.
- 7.2-7 Setpoint for Nuclear Safety-Related Instrumentation, ANSI/ISA-S67.04 Part1-1994.
- 7.2-8 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems, IEEE Std 379-2000.
- 7.2-9 Application of the Single-Failure Criterion to Safety Systems, Regulatory Guide 1.53 Revision 2, November 2003.
- 7.2-10 Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338-1987.
- 7.2-11 Periodic Testing of Protection System Actuation Functions, Regulatory Guide 1.22 Revision 0, February 1972.
- 7.2-12 Guidance on Requirements for Reactor Protection System Anticipatory Trips, BTP 7-9 Revision 5, March 2007.
- 7.2-13 US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.1 (Proprietary) and MUAP-09022-NP Rev.1 (Non-Proprietary), April 2010.

**Table 7.2-1 Interface between RPS and Other Systems (for Figure 7.2-3)**

<b>Interface Signals</b>	<b>Example of Signals</b>
(a) Signals to other RPS trains	RT signals, bypass signals
(b) Signals from other RPS trains	RT signals, bypass signals
(c) Operation signals from safety VDU	Manual trip signals, operating and maintenance bypass
(d) Information signals to safety VDU	PAM signals, process status signals
(e) Operation signals from operational VDU	Manual block, operating and maintenance bypass
(f) Information signals to non-safety HSIS	Non-safety indication, record and alarm signals
(g) Sensor signals	SG water level, NIS, RMS signals, turbine trip status signals
(h) ESF actuation signals to ESFAS	ESF actuation signals
(i) ESF actuation signals from ESFAS	ECCS actuation signal
(j) Interlock signals to SLS	Reactor coolant pressure signal, CCW surge tank water level for interlocks
(k) Process signals to reactor control system	Pressurizer water level signal, pressurizer water level bypass signals, Interlock signals
(l) RT signals to RTB	RT signals
(m) Status signals from RTB	RT status signals
(n) Process signals to DAS	Actuation signals, Indication signals
(o) Non-safety signals to RSC	Signals for non safety-related indication, record and operation for RSC
(p) Safety signals to RSC	Signals for safe shutdown to RSC
(q) Safety signals from RSC	Signals for safe shutdown from RSC
(r) Non-safety signals to various purpose	Various uses as control, test and monitoring by hardwired or optical signals
(s) Hardwired signals from RPS (other train)	Source range neutron flux detector power off
(t) Control signals to the sampling package at local	Start/stop demand to the sampling pump

Table 7.2-2 Reactor Trip Signals

Actuation Signal	Number of Sensors, Switches, or Signals	Division Trip Actuation Logic	Permissives and Bypasses (See Table 7.2-4)	Logic Diagram Figure 7.2-2
High Source Range Neutron Flux	2 Neutron Detectors	1/2	P-6, P-10	Sheet 3
High Intermediate Range Neutron Flux	2 Neutron Detectors	1/2	P-10	Sheet 3
High Power Range Neutron Flux (low setpoint)	4 Neutron Detectors	2/4	P-10	Sheet 3
High Power Range Neutron Flux (high setpoint)		2/4	None	Sheet 4
High Power Range Neutron Flux Positive Rate		2/4	None	Sheet 4
High Power Range Neutron Flux Negative Rate		2/4	None	Sheet 4
Over Temperature $\Delta T$	1 Composite Signal per RCS Loop	2/4	None	Sheet 5
Over Power $\Delta T$	1 Composite Signal per RCS Loop	2/4	None	Sheet 5
Low Reactor Coolant Flow	4 Flow Sensors per RCS Loop	2/4 per RCS Loop	P-7	Sheet 5
Low RCP Speed	1 Speed Sensor per RCP	2/4	P-7	Sheet 5
Low Pressurizer Pressure	4 Pressure Sensors	2/4	P-7	Sheet 5
High Pressurizer Pressure		2/4	None	Sheet 6
High Pressurizer Water Level	4 Level Sensors	2/4	P-7	Sheet 6
Low SG Water Level	4 Level Sensors per SG	2/4 per SG	None	Sheet 7
High-High SG Water Level		2/4 per SG	P-7	Sheet 9
Manual Reactor Trip	1 Switch per Train	1/1	None	Sheet 2
ECCS Actuation	Valid Signal	N/A	None	Sheet 11
Turbine Trip	Valid Signal	N/A	P-7	Sheet 13



**Table 7.2-3 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 1 of 3)**

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy* <sup>1,2</sup>	Response Time* <sup>1,2</sup>	Setpoint* <sup>3</sup>
High Source Range Neutron Flux	Neutron Flux	6 decades of neutron flux	5% of span	0.6 sec	1E+5 cps
High Intermediate Range Neutron Flux	Neutron Flux	Approximately 8 decades of neutron flux overlapping source range by approximately 2 decades and including 100% RTP	10% RTP* <sup>4</sup>	0.6 sec	25% RTP
High Power Range Neutron Flux (low setpoint)	Neutron Flux	1 to 120% RTP	4% RTP	0.6 sec	25% RTP
High Power Range Neutron Flux (high setpoint)	Neutron Flux	1 to 120% RTP	4% RTP	0.6 sec	109% RTP
High Power Range Neutron Flux Positive Rate	Neutron Flux	1 to 120% RTP	2% RTP	0.6 sec	10% RTP
High Power Range Neutron Flux Negative Rate	Neutron Flux	1 to 120% RTP	2% RTP	0.6 sec	7% RTP
Over Temperature $\Delta T$ (DNB Protection)  $\Delta T$ (Exit Boiling Limiting)	(a) $\Delta T$	0 to 150%	Total 5.6% RTP  Total 9.4% RTP	Total 6.0 sec  Total 6.0 sec	109.8% RTP  195.9* <sup>5</sup> % RTP
	(b) Reactor Coolant Cold Leg Temperature ( $T_{cold}$ )	510 to 630°F			
	(c) Reactor Coolant Hot Leg Temperature ( $T_{hot}$ )	530 to 650°F			
	(d) Pressurizer Pressure	1700 to 2500 psig			
	(e) Neutron Flux (difference between top and bottom power range neutron flux detectors)	-60 to +60% ( $\Delta I$ )			

**Table 7.2-3 Reactor Trip Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 2 of 3)**

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy* <sup>1,2</sup>	Response Time* <sup>1,2</sup>	Setpoint* <sup>3</sup>
Over Power $\Delta T$	(a) $\Delta T$	0 to 150%	Total 5.2% RTP	Total 6.0 sec	110.6* <sup>5</sup> % RTP
	(b) Reactor Coolant Cold Leg Temperature ( $T_{\text{cold}}$ )	510 to 630°F			
	(c) Reactor Coolant Hot Leg Temperature ( $T_{\text{hot}}$ )	530 to 650°F			
	(d) Neutron Flux (difference between top and bottom power range neutron flux detectors)	-60 to +60% ( $\Delta I$ )			
Low Reactor Coolant Flow	Reactor Coolant Flow	0 to 120% of rated flow	3% of rated flow	1.8 sec	90% of rated flow
Low RCP Speed	RCP Speed	0 to 120% of rated pump speed	0.5% of rated pump speed	0.6 sec	95.5% rated pump speed
Low Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	1.8 sec	1865 psig
High Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	1.8 sec	2385 psig
High Pressurizer Water Level	Pressurizer Water Level	0 to 100% of span	3% of span	1.8 sec	92% of span
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	1.8 sec	13% of span
High-High SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	1.8 sec	70% of span
Manual Reactor Trip Actuation	Switch Position	N/A	N/A	N/A	N/A
ECCS Actuation	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	3.3 sec	1765 psig
	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.3 sec	525 psig
	Containment Pressure	-7 to 80 psig	2.8% of span	3.3 sec	6.8 psig

**Table 7.2-3 Reactor Trip Variables, Ranges, Accuracies,  
Response Times, and Setpoints (Nominal) (Sheet 3 of 3)**

RT Function	Variables to be monitored	Range of Variables	Instrument Accuracy* <sup>1,2</sup>	Response Time* <sup>1,2</sup>	Setpoint* <sup>3</sup>
Turbine Trip	Turbine Emergency Trip Oil Pressure	0 to 3500psig	2% of span	1.0 sec	1000 psig
	Main Turbine Stop Valve Position	N/A	N/A	1.0 sec	5% open

Note:

1. Instrument accuracy and response time calculation methodology refer to Subsection 7.2.2.7.
2. Instrument accuracies and response times will be decided to take into account the specification of instruments.
3. Setpoints will be adjusted to compensate for loop accuracy.
4. Rated thermal power
5. This is nominal value. Calculation formulas are shown in Figure 7.2-2 sheet 5.

**Table 7.2-4 RT and ESF Permissives, Bypasses and Interlocks (Sheet 1 of 3)**

Designation		RT and/or ESF	Function	Activation or De-activation Setpoint* <sup>1</sup>
P-4	Reactor Trip (RTB open)	RT, ESF	(a) Permit manual rest of ECCS to block automatic actuation of ECCS while RTBs are open. (b) Permit low $T_{avg}$ MFW regulation valve closure. (c) Initiate turbine trip. (d) Permit high SG water level EFW isolation (e) Permit RCP trip by ECCS signal.	-
P-6	Intermediate Range Neutron Flux Above or Below Setpoint	RT	Above setpoint Permit manual operating bypass for high source range neutron flux reactor trip.  Below setpoint Remove manual operating bypass for high source range neutron flux reactor trip.	1E-10 A* <sup>2</sup>
P-7	Turbine Inlet Pressure (P-13) or Power Range Neutron Flux (P-10) Above Setpoint or Turbine Inlet Pressure (P-13) and Power Range Neutron Flux (P-10) Below Setpoint	RT	Above setpoint (a) Remove operating bypass for low pressurizer pressure reactor trip. (b) Remove operating bypass for low reactor coolant flow reactor trip. (c) Remove operating bypass for low RCP speed reactor trip. (d) Remove operating bypass for high pressurizer water level reactor trip. (e) Remove operating bypass for high-high SG water level reactor trip. (f) Remove operating bypass for reactor trip by turbine trip.  Below setpoint (a) Initiate operating bypass for low pressurizer pressure reactor trip. (b) Initiate operating bypass for low reactor coolant flow reactor trip. (c) Initiate operating bypass for low RCP speed reactor trip. (d) Initiate operating bypass for high pressurizer water level reactor trip. (e) Initiate operating bypass for high-high SG water level reactor trip. (f) Initiate operating bypass for reactor trip by turbine trip.	N/A

**Table 7.2-4 RT and ESF Permissives, Bypasses and Interlocks (Sheet 2 of 3)**

Designation		RT and/ or ESF	Function	Activation or De-activation Setpoint* <sup>1</sup>
P-10	Power Range Neutron Flux Above or Below Setpoint	RT	<p>Above setpoint</p> <p>(a) Initiate operating bypass for high source range neutron flux reactor trip.</p> <p>(b) Permit manual operating bypass for high intermediate range neutron flux reactor trip</p> <p>(c) Permit manual operating bypass for high power range neutron flux (low setpoint) reactor trip.</p> <p>Below setpoint</p> <p>(a) Permit to reset operating bypass for high source range neutron flux reactor trip.</p> <p>(b) Remove manual operating bypass for high intermediate range neutron flux reactor trip.</p> <p>(c) Remove manual operating bypass for high power range neutron flux (low setpoint) reactor trip.</p>	10% RTP* <sup>3</sup>
P-11	Pressurizer Pressure Above or Below Setpoint	ESF	<p>Below setpoint</p> <p>(a) Permit manual operating bypass for low pressurizer pressure ECCS actuation.</p> <p>(b) Permit manual operating bypass for high-high SG water level MFW isolation function for all MFW pumps, all MFW isolation valves, and all SG water filling control valves.</p> <p>(c) Permit manual operating bypass for high pressurizer water level CVCS isolation.</p> <p>(d) Permit manual operating bypass for EFW isolation.</p> <p>(e) Permit manual operating bypass for low main steam line pressure ECCS actuation.</p> <p>(f) Permit high main steam line pressure negative rate main steam line isolation function.</p> <p>(g) Permit manual operating bypass for low main steam line pressure main steam line isolation.</p> <p>Above setpoint</p> <p>(a) Remove manual operating bypass for low pressurizer pressure ECCS actuation.</p> <p>(b) Remove manual operating bypass for high-high SG water level MFW isolation function for all MFW pumps, all MFW isolation valves, and all SG water filling control valves.</p> <p>(c) Remove manual operating bypass for high pressurizer water level CVCS.</p> <p>(d) Remove manual operating bypass for EFW isolation.</p> <p>(e) Remove manual operating bypass for low main steam line pressure ECCS actuation.</p> <p>(f) Initiate operating bypass for high main steam line pressure negative rate main steam isolation.</p>	1915 psig

**Table 7.2-4 RT and ESF Permissives, Bypasses and Interlocks (Sheet 3 of 3)**

Designation		RT and/ or ESF	Function	Activation or De-activation Setpoint* <sup>1</sup>
P-11 (con- tinued)	Pressurizer Pressure Above or Below Setpoint (continued)	ESF (conti- nued)	(g) Remove manual operating bypass for low main steam line pressure main steam line isolation.	1915 psig
P-13	Turbine Inlet Pressure Below Setpoint	RT	Generate P-7 along with P-10	10% Turbine Power

Note:

1. Default lockup is 1.0% of rated value.
2. Default lockup of this value is 50% of setpoint value.
3. Default lockup of this value is 2.0% rated thermal power (RTP).

**Table 7.2-5 Diverse Parameters in Two Separate Controller Groups**

Group 1	Group 2	Remark
Over Power $\Delta T$ * <sup>6</sup> High Power Range Neutron Flux Rate	High Power Range Neutron Flux	Over Power Protection* <sup>1</sup>
Low RCP Speed Over Temperature $\Delta T$	Low Reactor Coolant Flow Low Pressurizer Pressure	Core Heat Removal Protection* <sup>2</sup>
Low SG Water Level High Pressurizer Water Level	High Pressurizer Pressure	Loss of Heat Sink Protection* <sup>3</sup>
High Source Range Neutron Flux High Intermediate Range Neutron Flux	High Power Range Neutron Flux (Low Setpoint)	Nuclear Startup Protection* <sup>4</sup>
High Pressurizer Water Level	High Pressurizer Pressure	Primary Over Pressure Protection* <sup>5</sup>

Note:

1. Example of design basis event in the safety analysis is "Uncontrolled Control Rod Assembly Withdrawal at Power."
2. Example of design basis event in the safety analysis is "Loss of Forced Reactor Coolant Flow Including Trip of Pump Motor."
3. Example of design basis event in the safety analysis is "Feedwater System Pipe Break Inside and Outside Containment."
4. Example of design basis event in the safety analysis is "Uncontrolled Control Rod assembly Withdrawal from a Subcritical or Low Power Startup Condition, or Spectrum of Rod Ejection Accident."
5. Example of design basis event in the safety analysis is "Loss of External Electrical Load or Turbine Trip."
6. Overpower  $\Delta T$  also has a function of Core Heat Removal Protection in conjunction with Overtemperature  $\Delta T$ , although the primary function of Overpower  $\Delta T$  is Overpower Protection.

**Table 7.2-6 Reactor Protection System - Train Level Manual Controls (Conventional and Software Switches)**

Manual Control	Trains				This is shown on Figure 7.2-2
Manual Reactor Trip Actuation #1	A				Sheet 2&4
Manual Reactor Trip Actuation #2		B			Sheet 2&4
Manual Reactor Trip Actuation #3			C		Sheet 2&4
Manual Reactor Trip Actuation #4				D	Sheet 2&4

**Table 7.2-7 Reactor Protection System - Train Level Manual Controls  
(Software Switches)**

Manual Control	Trains				This is shown on Figure 7.2-2
Reactor Trip Reset #1	A				Sheet 4
Reactor Trip Reset #2		B			Sheet 4
Reactor Trip Reset #3			C		Sheet 4
Reactor Trip Reset #4				D	Sheet 4
Manual Bypass Control for High Source Range Neutron Flux Reactor Trip Train A	A				Sheet 3
Manual Bypass Control for High Source Range Neutron Flux Reactor Trip Train B		B			Sheet 3
Manual Bypass Control for High Source Range Neutron Flux Reactor Trip Train C			C		Sheet 3
Manual Bypass Control for High Source Range Neutron Flux Reactor Trip Train D				D	Sheet 3
Manual Bypass Control for High Intermediate Range Neutron Flux Reactor Trip Train A	A				Sheet 3
Manual Bypass Control for High Intermediate Range Neutron Flux Reactor Trip Train B		B			Sheet 3
Manual Bypass Control for High Intermediate Range Neutron Flux Reactor Trip Train C			C		Sheet 3
Manual Bypass Control for High Intermediate Range Neutron Flux Reactor Trip Train D				D	Sheet 3
Manual Bypass Control for High Power Range Neutron Flux (low setpoint) Reactor Trip Train A	A				Sheet 3
Manual Bypass Control for High Power Range Neutron Flux (low setpoint) Reactor Trip Train B		B			Sheet 3
Manual Bypass Control for High Power Range Neutron Flux (low setpoint) Reactor Trip Train C			C		Sheet 3
Manual Bypass Control for High Power Range Neutron Flux (low setpoint) Reactor Trip Train D				D	Sheet 3
Manual Reset for High Power Range Neutron Flux Positive/ Negative Rate Reactor Trip Train A	A				Sheet 4
Manual Reset for High Power Range Neutron Flux Positive/ Negative Rate Reactor Trip Train B		B			Sheet 4
Manual Reset for High Power Range Neutron Flux Positive/ Negative Rate Reactor Trip Train C			C		Sheet 4
Manual Reset for High Power Range Neutron Flux Positive/ Negative Rate Reactor Trip Train D				D	Sheet 4



Table 7.2-8 FMEA for Reactor Trip in PSMS (for Figure 7.2-8) (Sheet 1 of 3)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
Sensor	Fail high	Self-diagnostic alarm from the affected RPS train. Annunciation of partial trip from the affected RPS train. Cross channel comparison.	Bistable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide reactor trip. If unrestricted bypass of one instrument channel has already been executed in another train, RT logic becomes 1-out-of-2 due to the sensor failure. Remaining two trains provide reactor trip.
	Fail low	Self-diagnostic alarm from the affected RPS train. Annunciation of partial trip from the affected RPS train. Cross channel comparison.	Bistable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide reactor trip. If unrestricted bypass of one instrument channel has already been executed in another train, RT logic becomes 1-out-of-2 due to the sensor failure. Remaining two trains provide reactor trip.
	Fail as is	Cross channel comparison.	Bistable does not change to trip state in the affected RPS train when process reaches trip level.	RT logic becomes 2-out-of-3 due to the sensor failure. Remaining three trains provide reactor trip. If unrestricted bypass of one instrument channel has already been executed in another train, RT logic becomes 2-out-of-2 due to the sensor failure. Remaining two trains provide reactor trip.
RPS Input part (from Sensor)	Fail high	Self-diagnostic alarm from the affected RPS train. Annunciation of partial trip from the affected RPS train. Cross channel comparison.	Bistable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the input failure. Remaining three trains provide reactor trip.
	Fail low	Self-diagnostic alarm from the affected RPS train. Annunciation of partial trip from the affected RPS train. Cross channel comparison.	Bistable changes to trip state and partial trip signal is generated in the affected RPS train.	RT logic becomes 1-out-of-3 due to the input failure. Remaining three trains provide reactor trip.
	Fail as is	Cross channel comparison.	Bistable does not change to trip state in the affected RPS train when process reaches trip level.	RT logic becomes 2-out-of-3 due to the input failure. Remaining three trains provide reactor trip.

Table 7.2-8 FMEA for Reactor Trip in PSMS (for Figure 7.2-8) (Sheet 2 of 3)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
<b>RPS</b> Processing part (in RPS)	No data output	Self-diagnostic alarm from the affected RPS train. Annunciation of communication error from the affected other RPS trains. Annunciation of breaker opened in the affected RTB train.	Partial trip signal does not reach to other RPS trains when process reaches trip level. If the processing part is failed, the trip signal from the failed RPS train is provided to the RTB, the breaker is opened in the affected RTB train.	RTB circuit becomes 1-out-of-3 due to the processing failure. Remaining three trains provide reactor trip.
	No data output	Annunciation of communication error from the affected other RPS trains.	Partial trip signal does not reach to other RPS trains when process reaches trip level. Trip signals from other RPS trains dose not reach to the affected train when process reaches trip level.	RT logic becomes 2-out-of-3 due to the communication failure. Remaining three trains provide reactor trip.
<b>RPS</b> Output part (to RTB)	Spurious trip	Annunciation of breaker opened in the affected RTB train.	Breaker is opened in the affected RTB train.	RTB circuit becomes 1-out-of-3 due to the output failure. Remaining three trains provide reactor trip. If another breaker is open due to periodic manual surveillance testing, reactor will be tripped spuriously, thus the periodic test is administrated to minimize the test duration and to prevent spurious trip.
	Fail as is	Manual periodic test.	Breaker does not open in the affected RTB train when process reaches trip level.	RTB circuit becomes 2-out-of-3 due to the output failure. Remaining three trains provide reactor trip.

Table 7.2-8 FMEA for Reactor Trip in PSMS (for Figure 7.2-8) (Sheet 3 of 3)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
RTB	Spurious trip	Annunciation of breaker opened in the affected RTB train. Manual periodic test.	Breaker is opened in the affected RTB train.	RTB circuit becomes 1-out-of-3 due to the breaker failure. Remaining three trains provide reactor trip. If another breaker is open due to periodic manual surveillance testing, reactor will be tripped spuriously, thus the periodic test is administered to minimize the test duration and to prevent spurious trip.
	Fail as is	Manual periodic test.	Breaker does not open in the affected RTB when process reaches trip level.	RTB circuit becomes 2-out-of-3 due to the breaker failure. Remaining three trains provide reactor trip.
<b>Safety Bus</b> Inside part of RPS	No data input or output	Annunciation of communication error.	Safety signals can not be sent and received.	No failure effect on RT function.
<b>Safety Bus</b> Outside part of RPS	Fail to dis-connection	Annunciation of communication error.	There is no impact for a single disconnection due to its ring configuration of the safety bus.	No failure effect on RT function.
<b>Unit bus</b> Inside part of RPS	No data output	Annunciation of communication error	Non-safety information signal can not be sent.	No failure effect on RT function.
<b>Unit bus</b> Outside part of RPS	Fail to dis-connection	Annunciation of communication error.	There is no impact for a single disconnection due to its ring configuration of the unit bus.	No failure effect on RT function.

Note:

- One train failure is considered for each component except for non-safety unit bus.

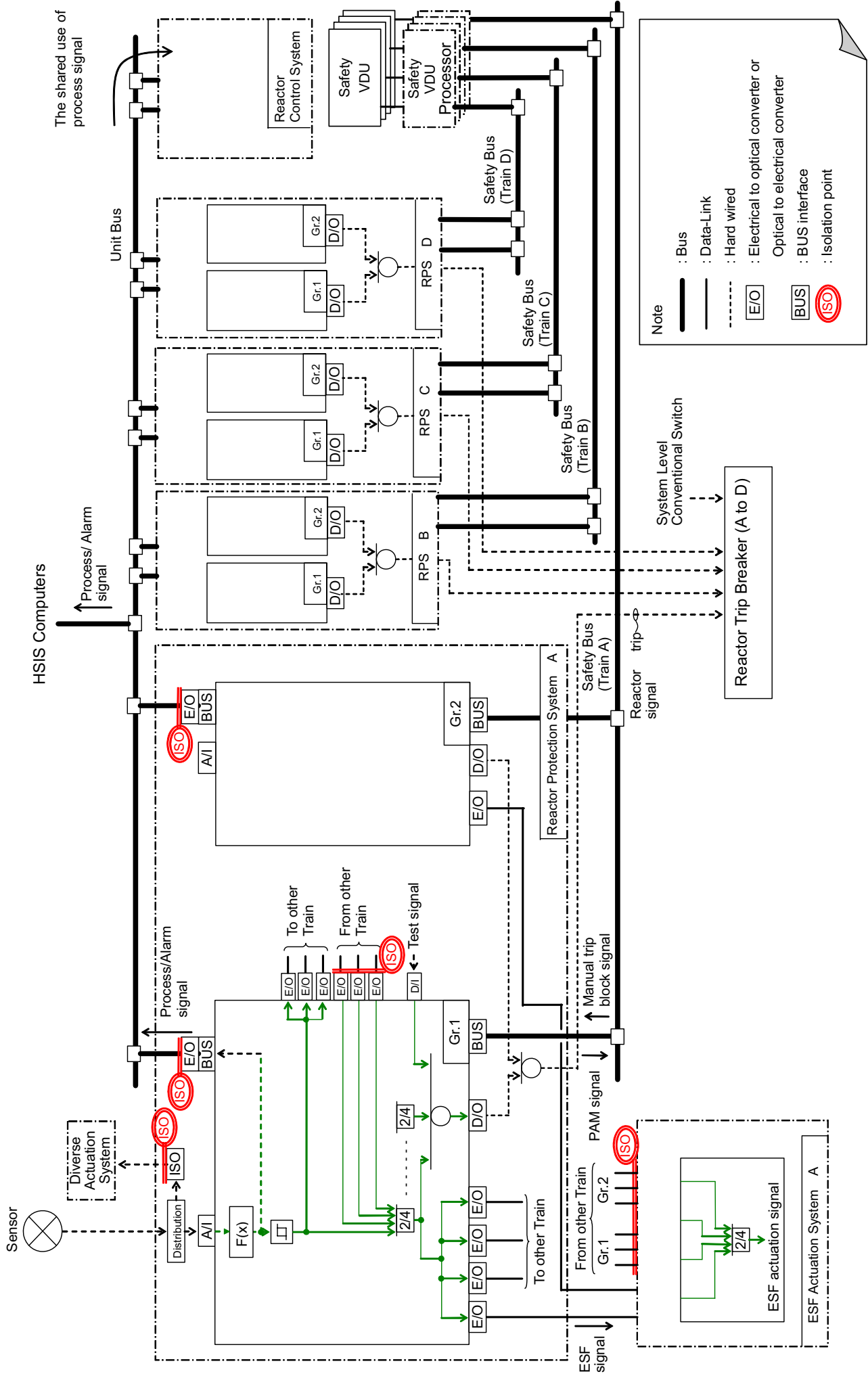


Figure 7.2-1 Configuration of the Reactor Protection System



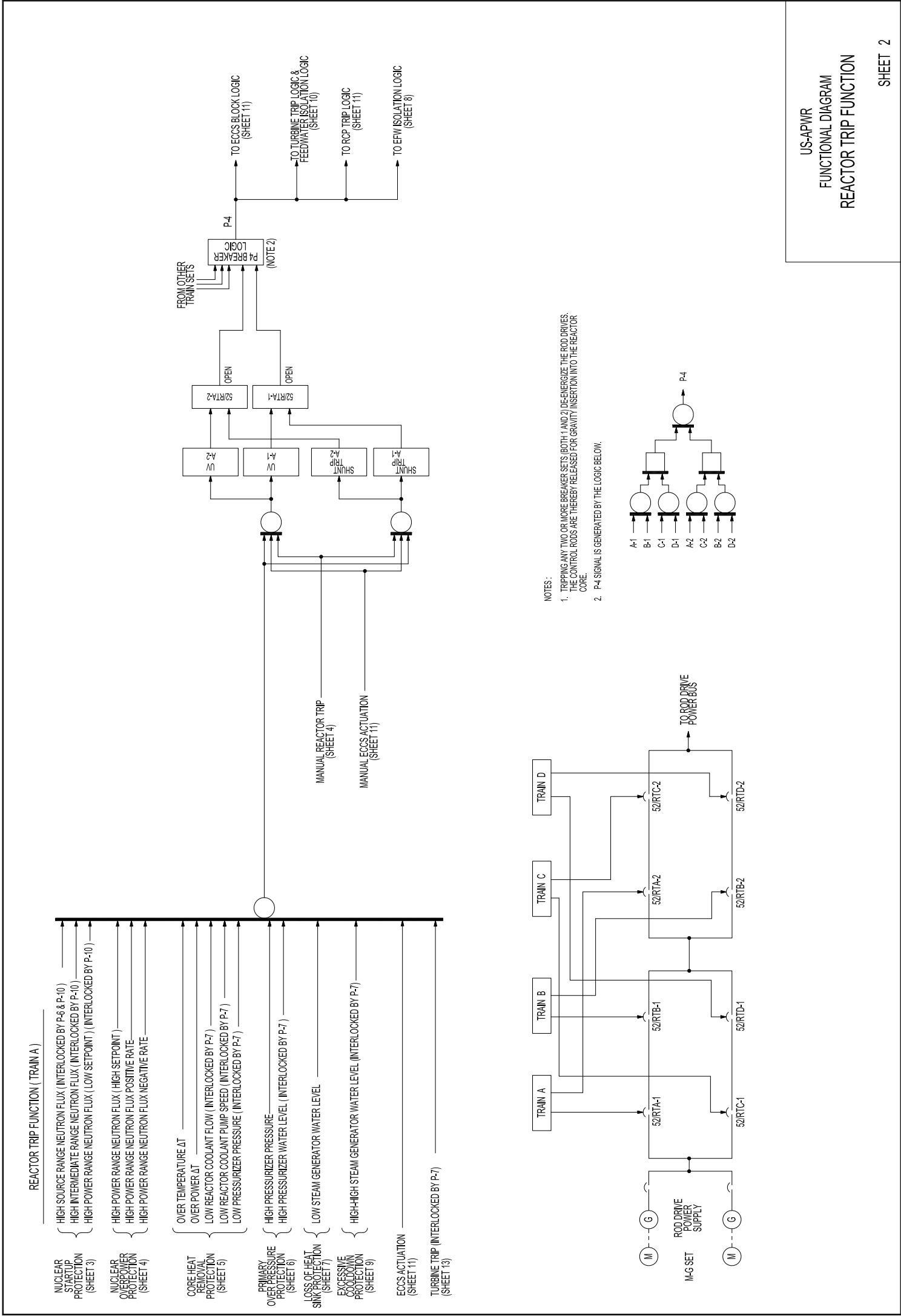


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 2 of 21)

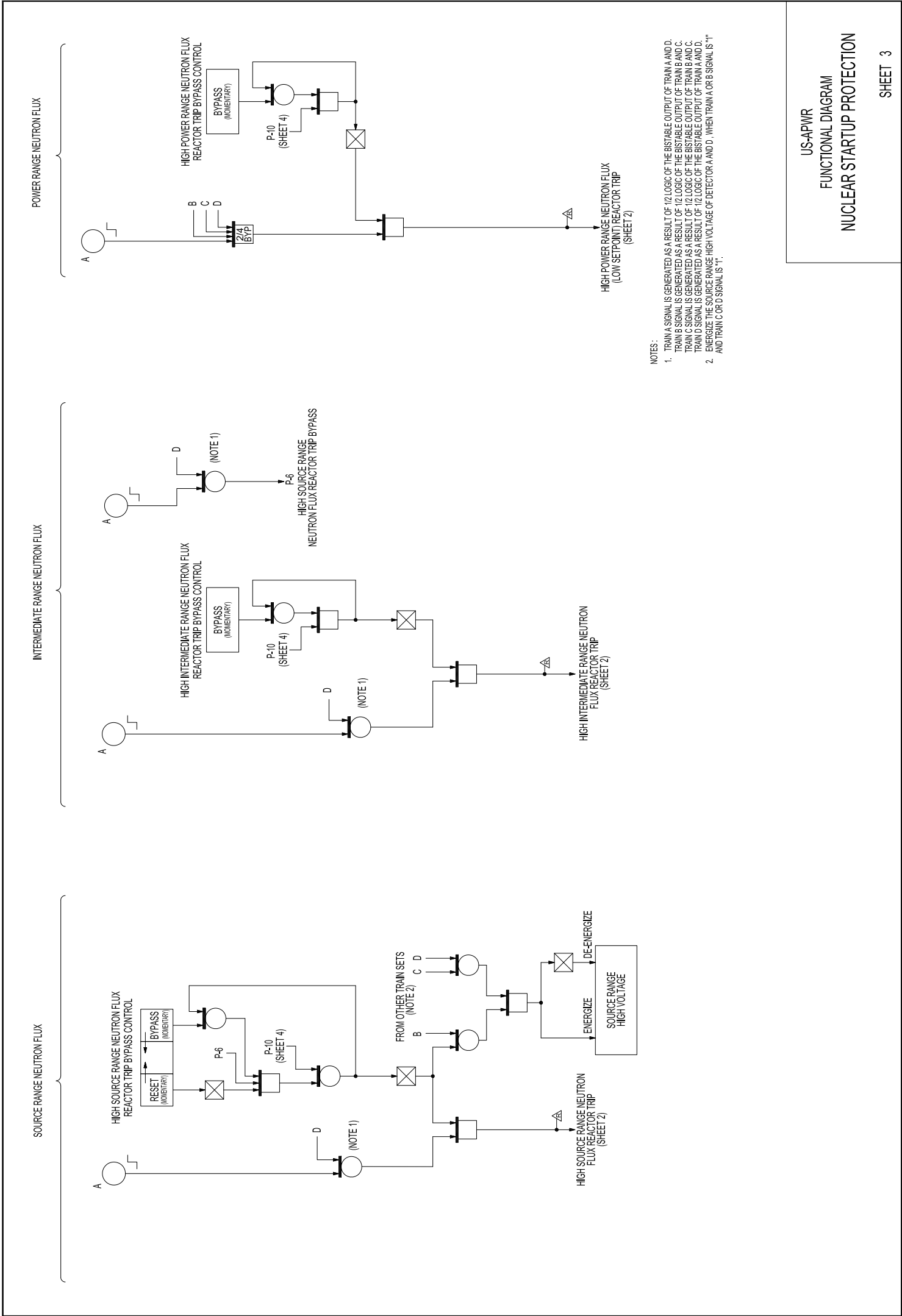


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 3 of 21)

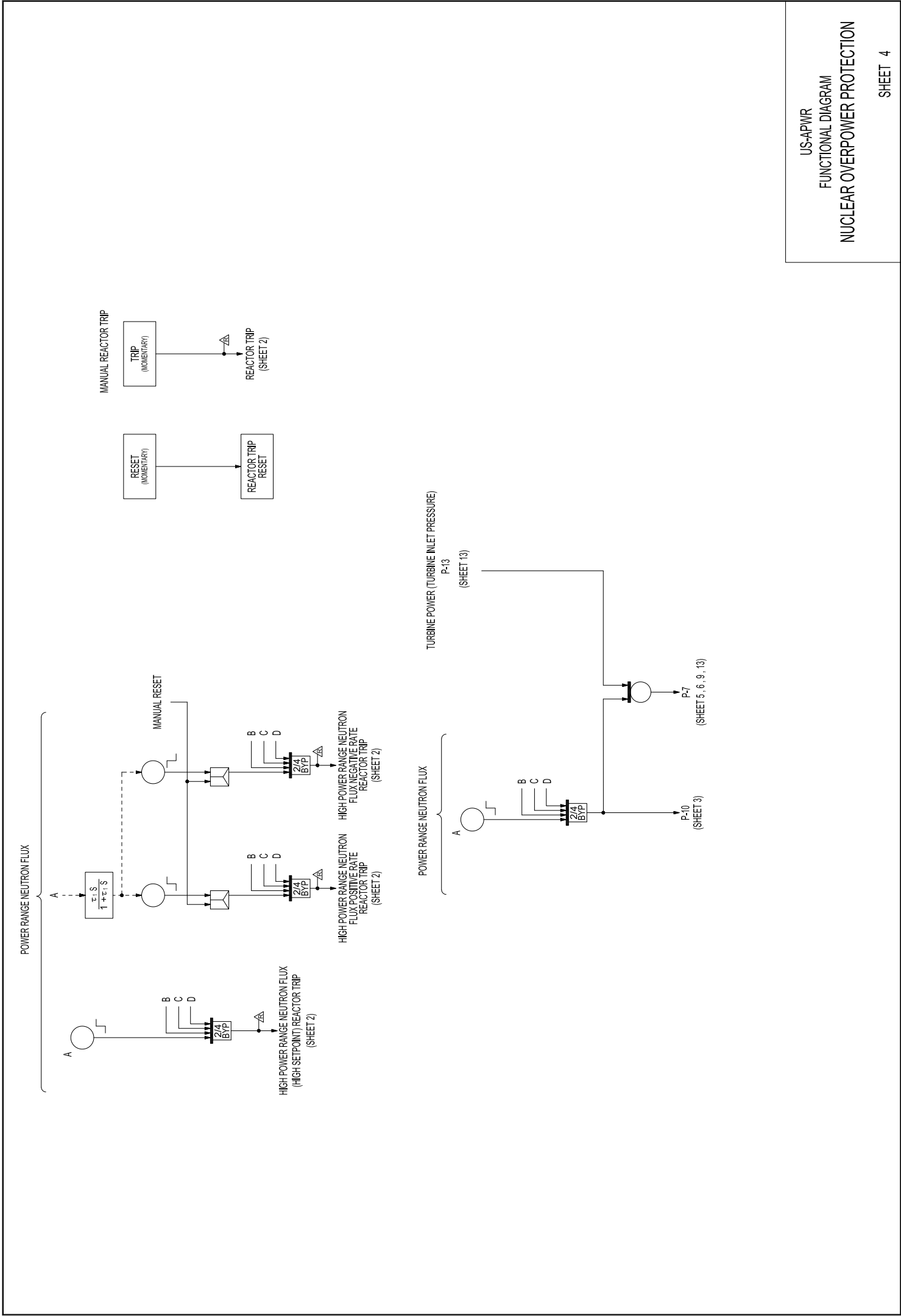
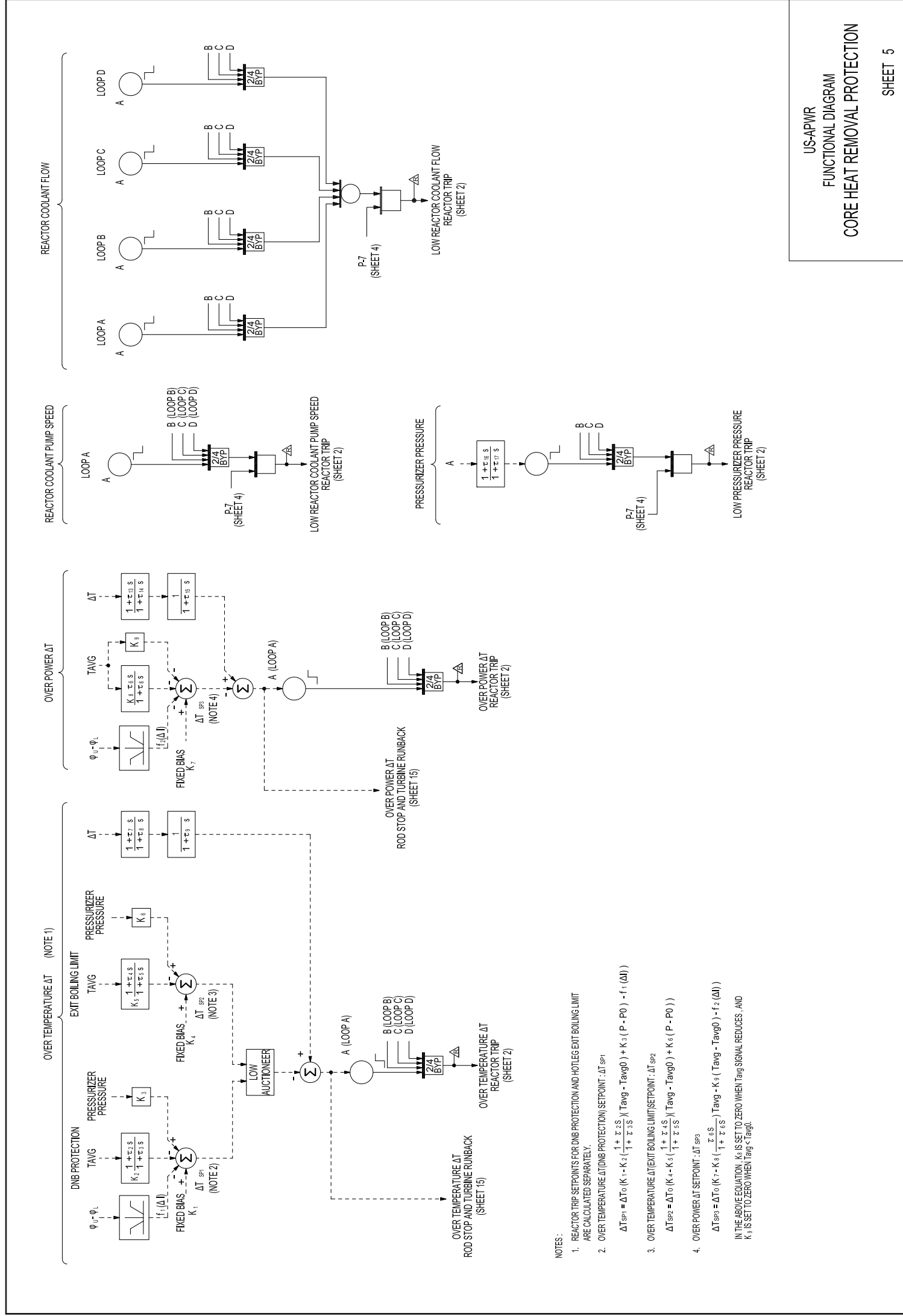


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 4 of 21)





**Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 5 of 21)**



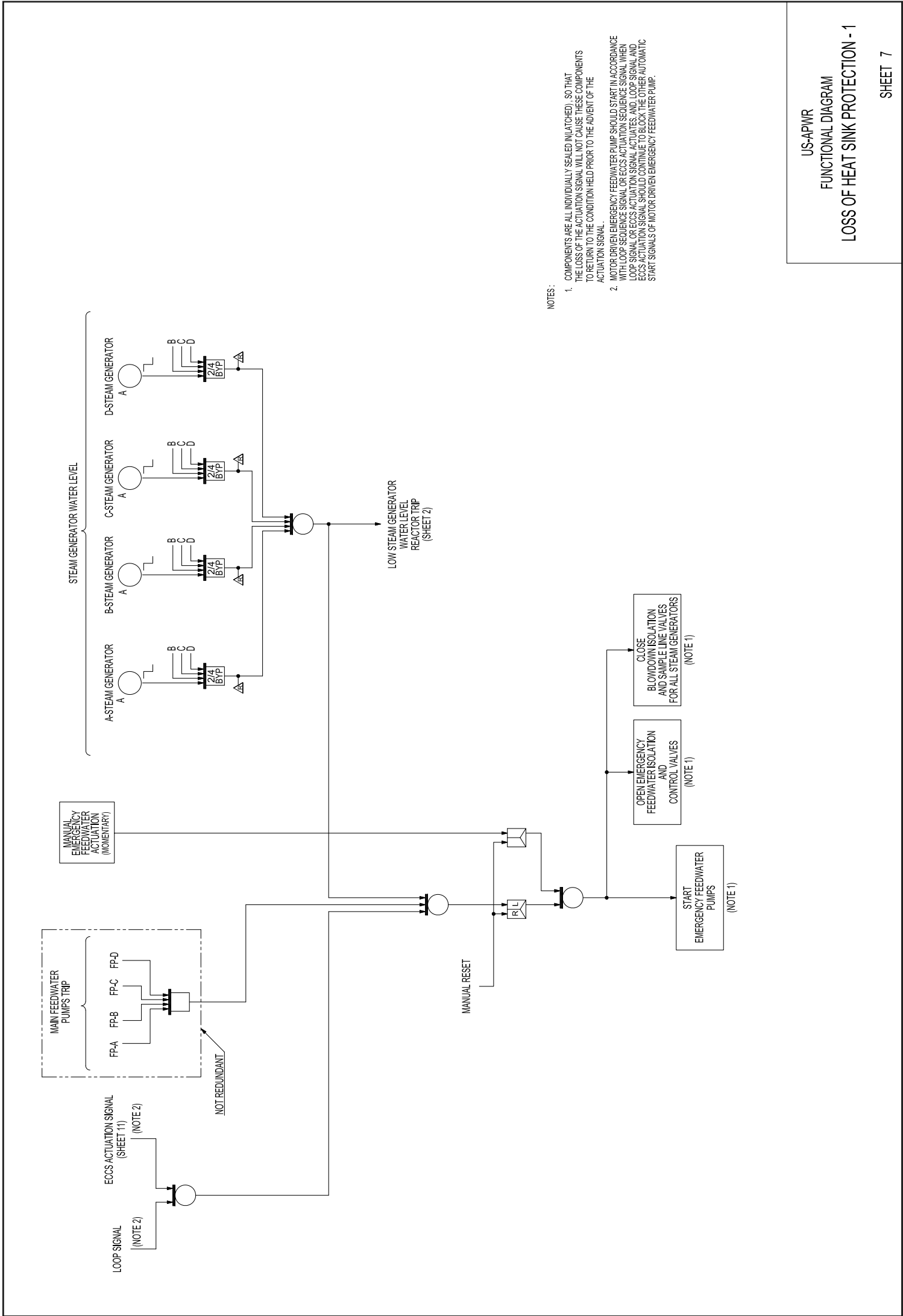


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 7 of 21)

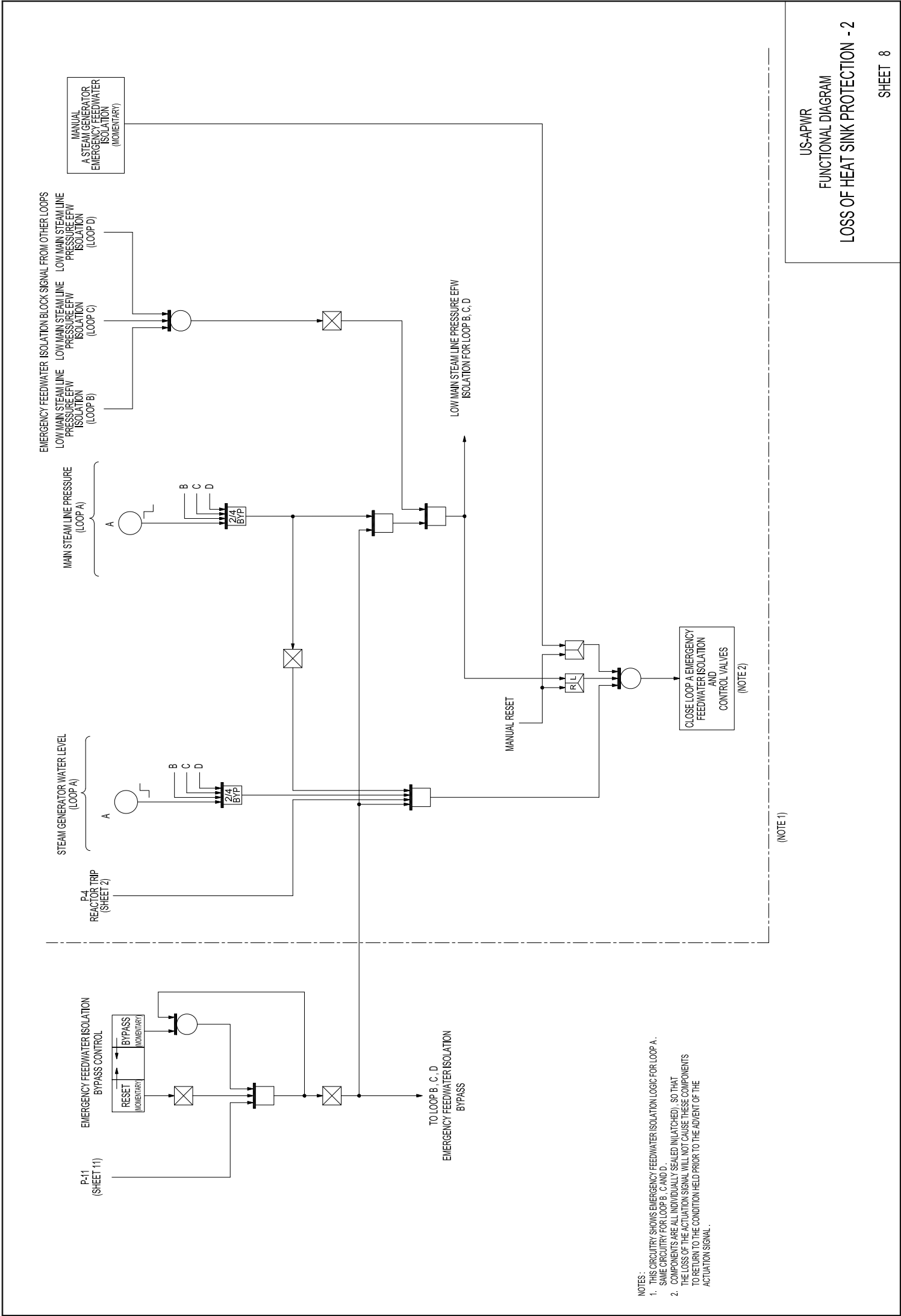


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 8 of 21)

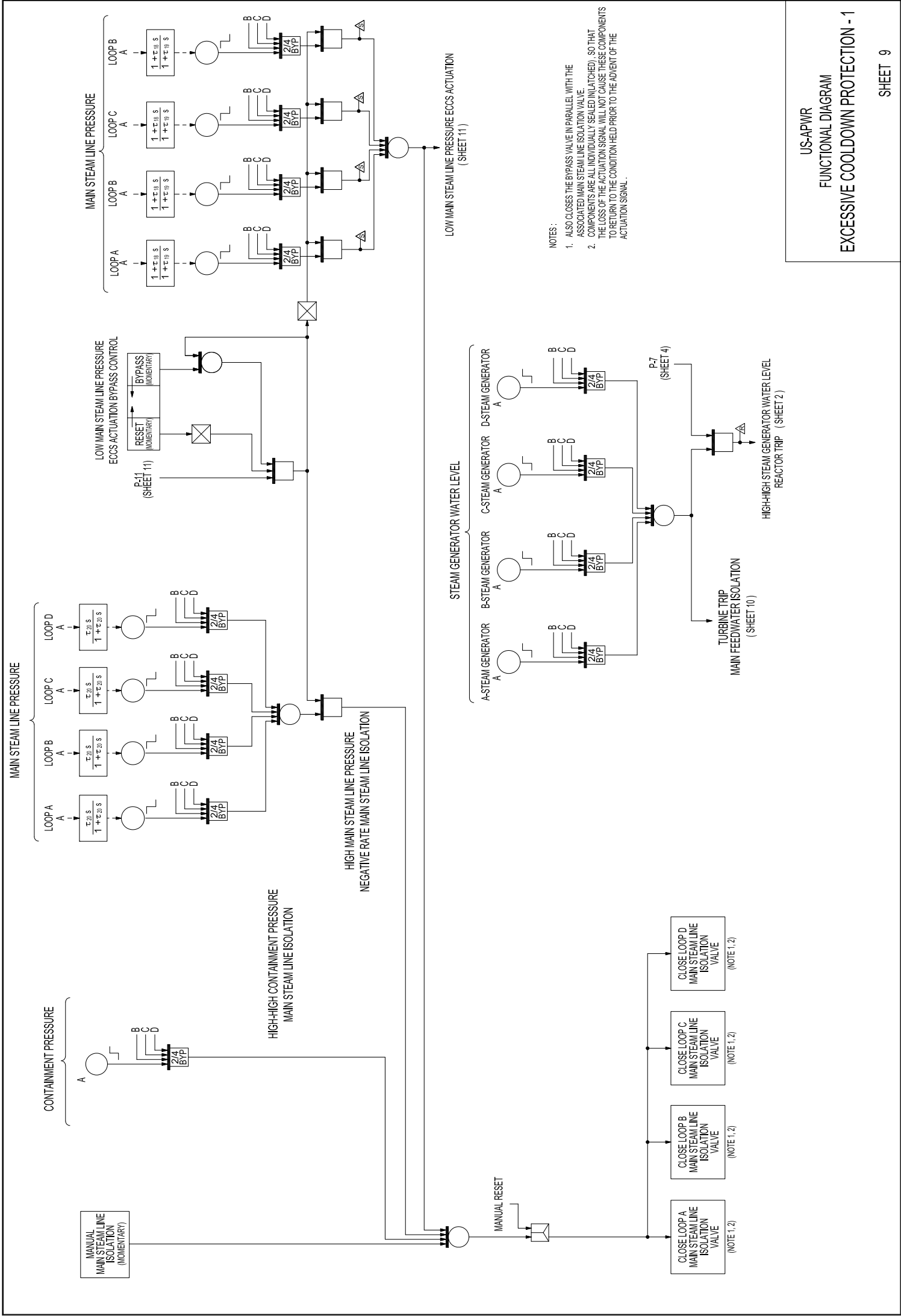


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 9 of 21)

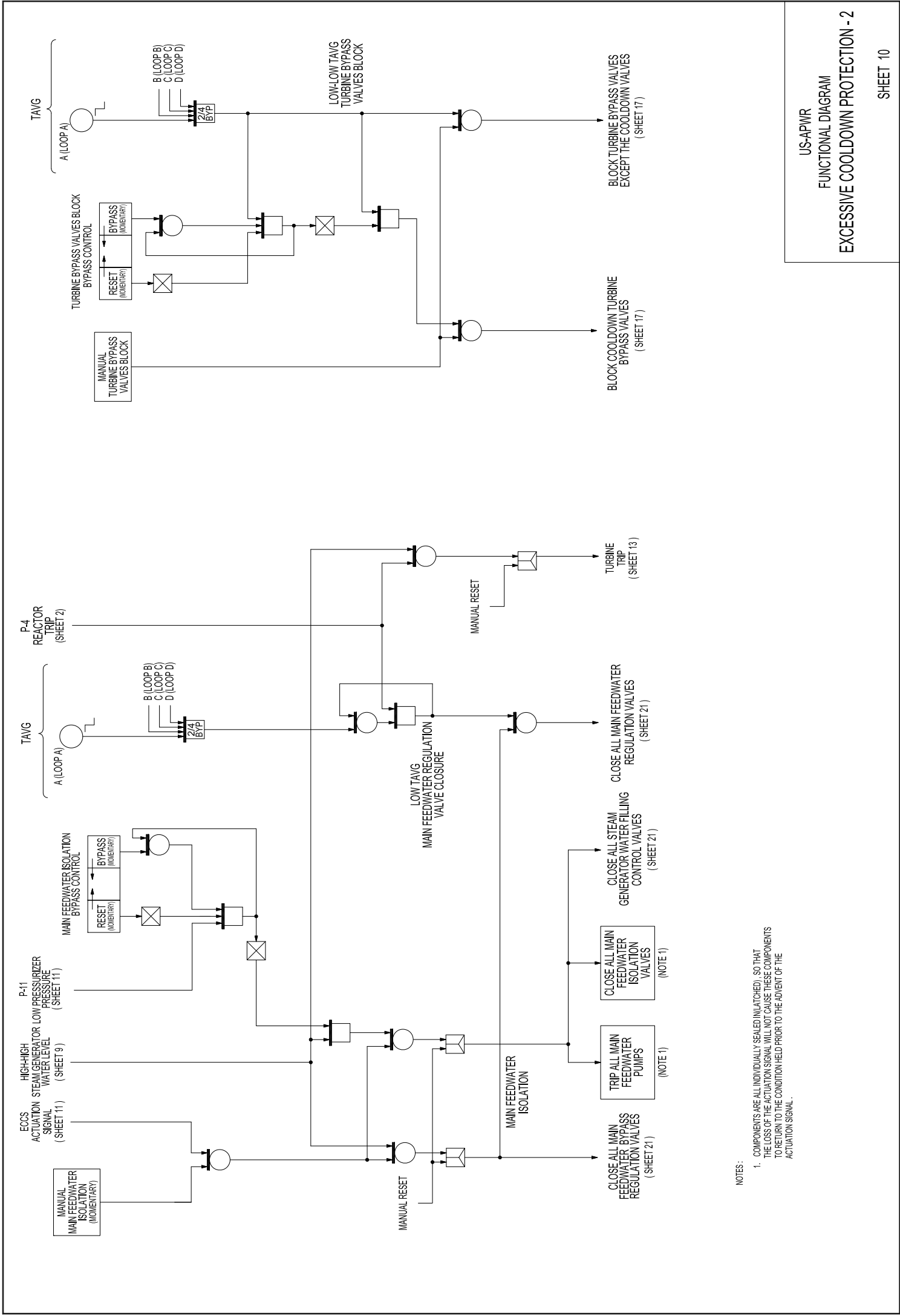


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 10 of 21)

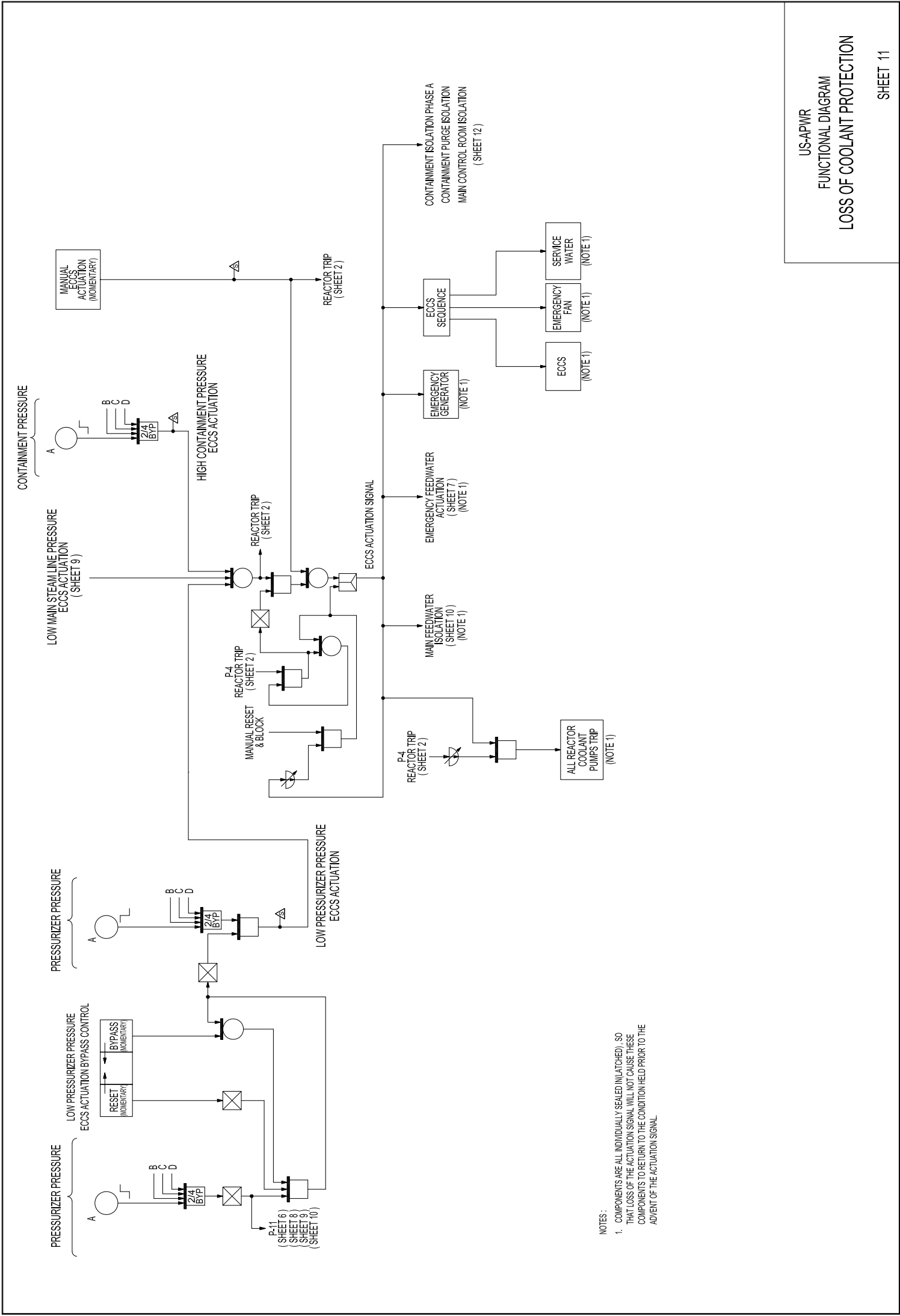


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 11 of 21)

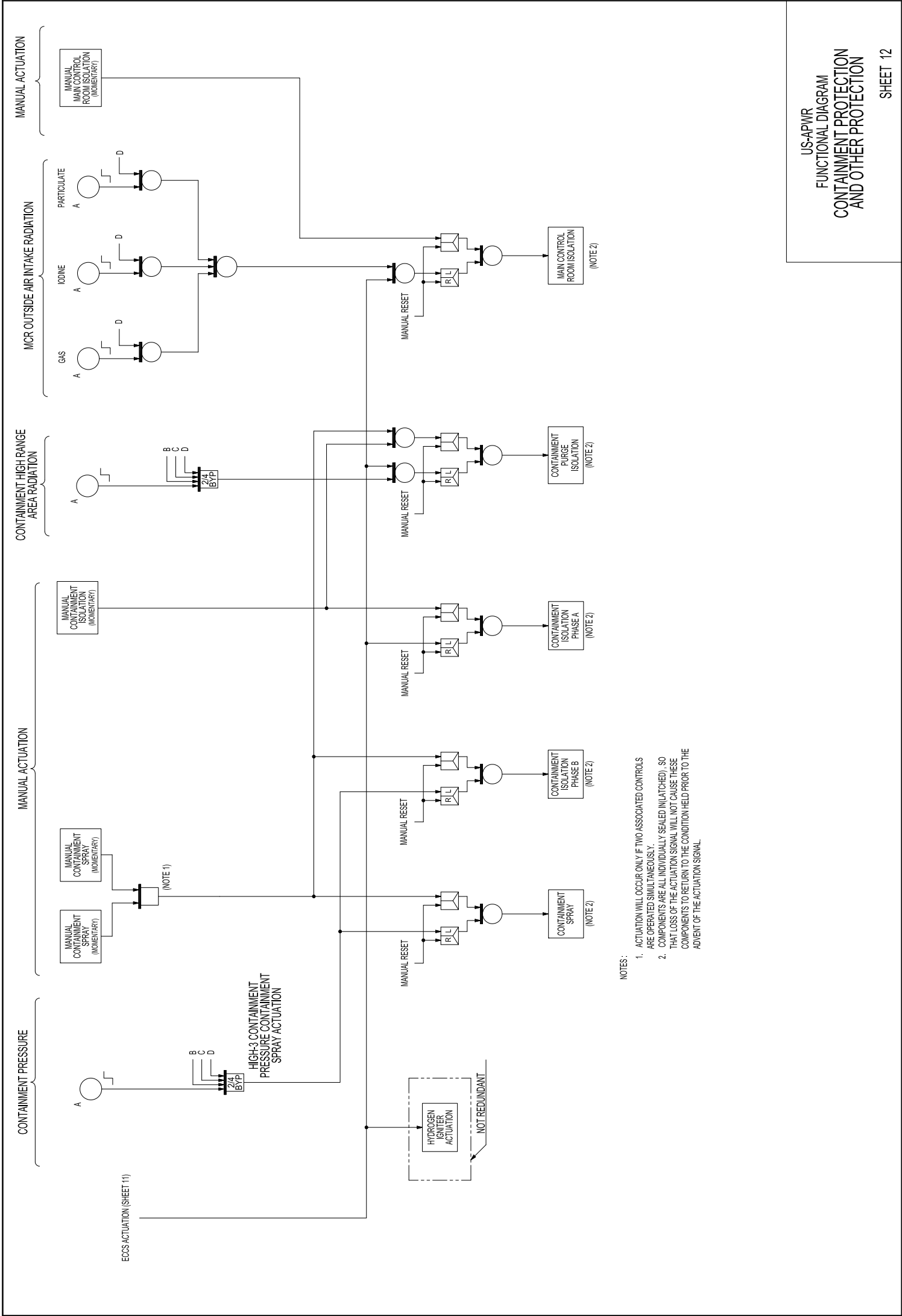


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 12 of 21)



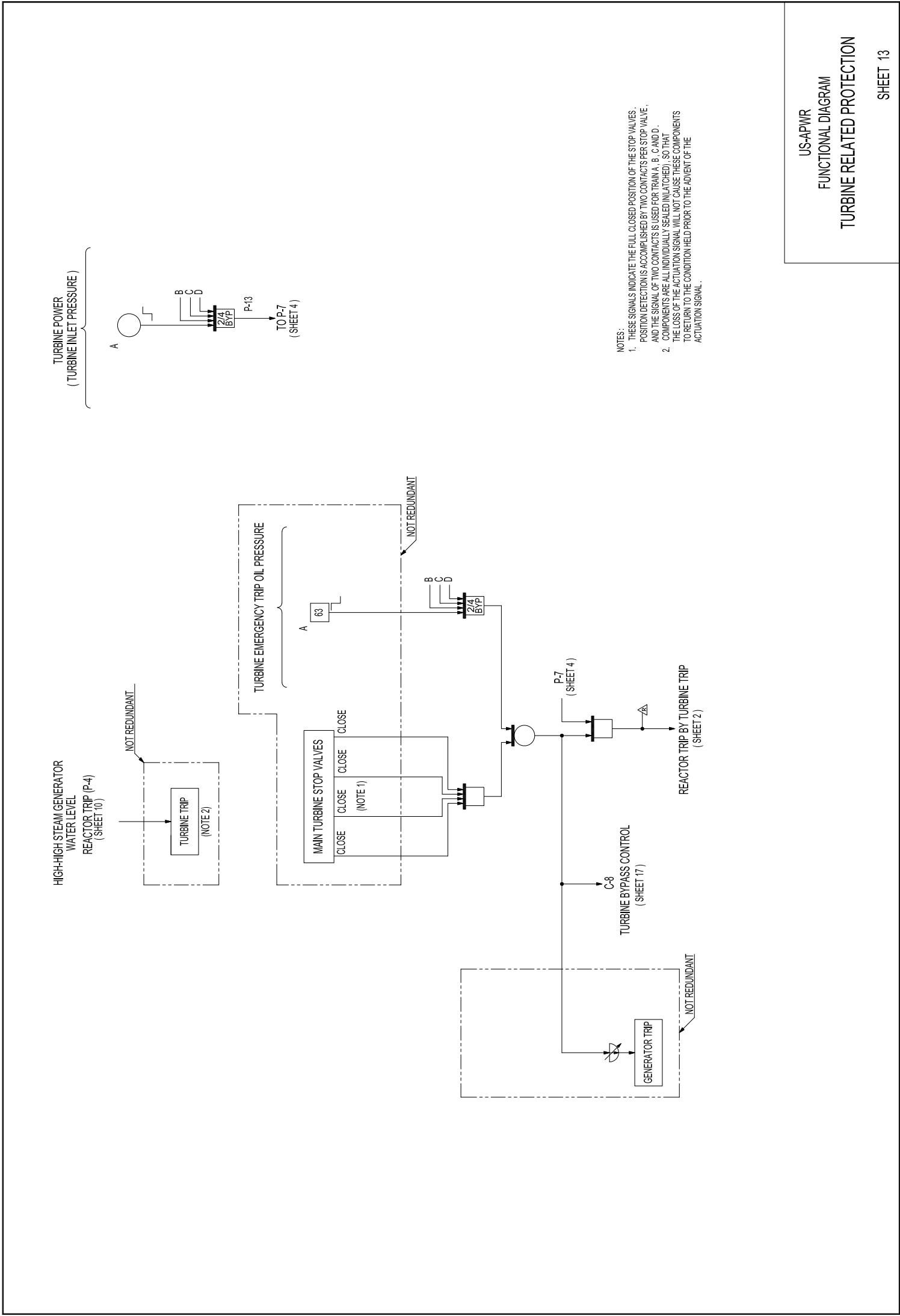


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 13 of 21)

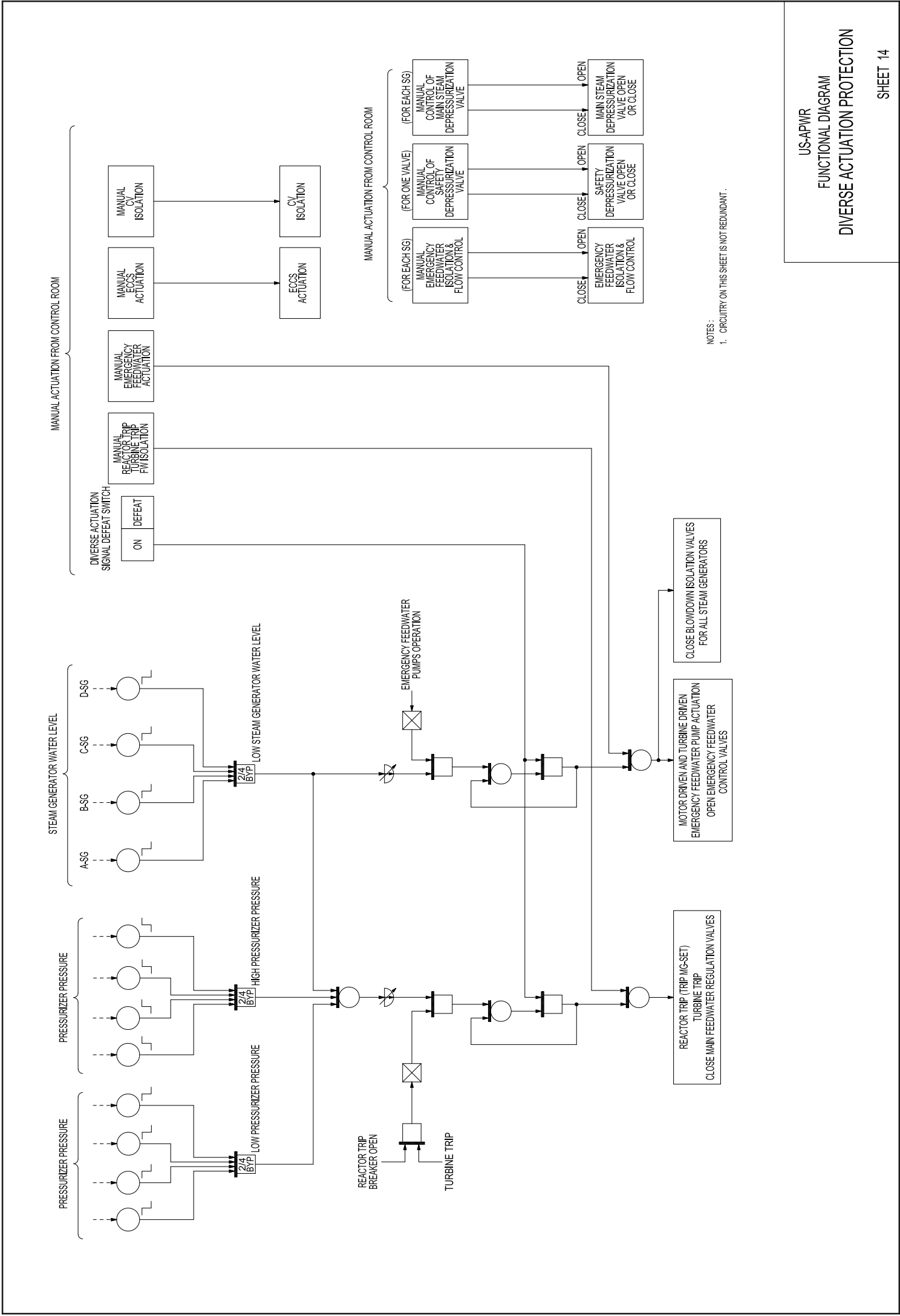


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 14 of 21)

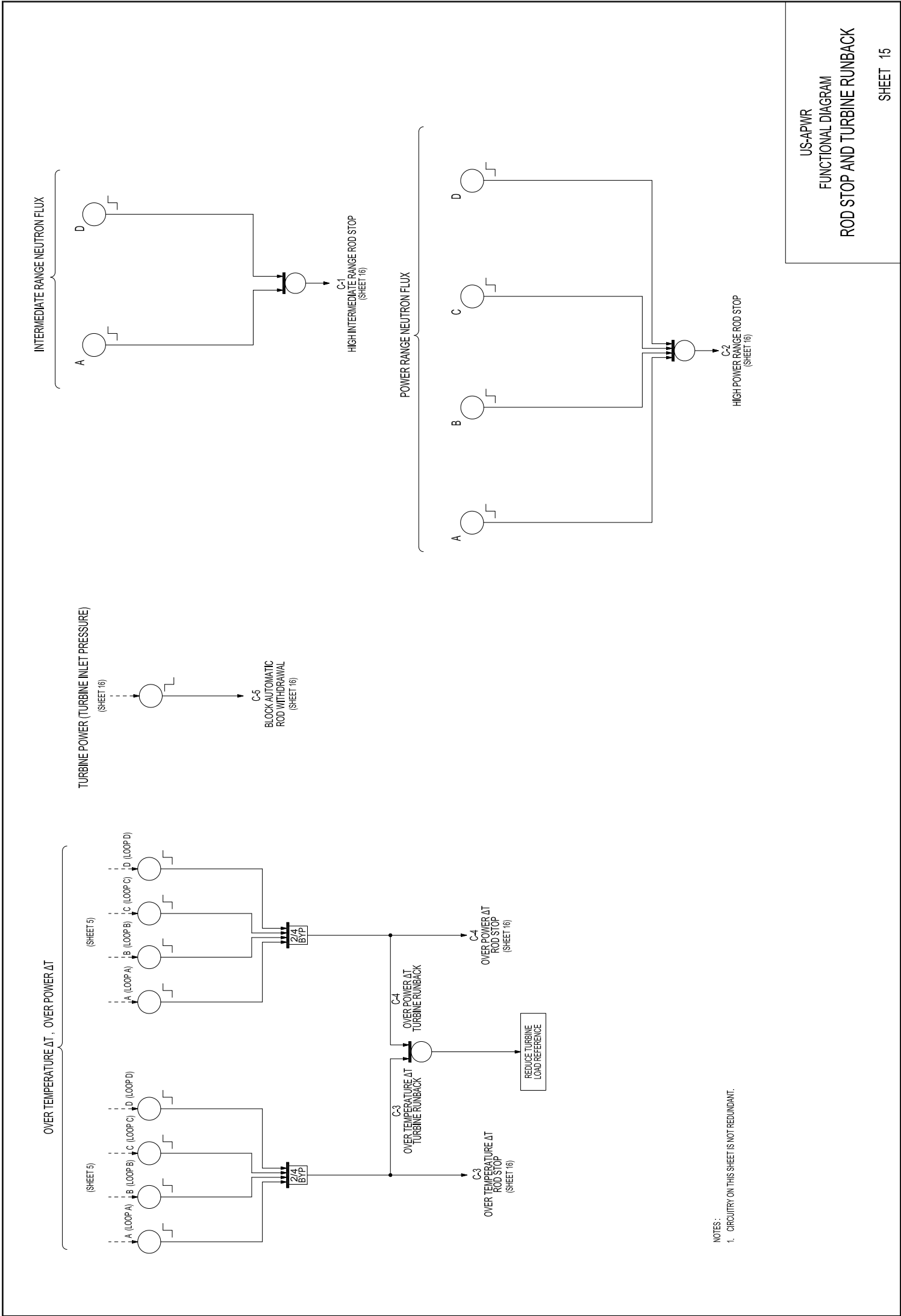


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 15 of 21)

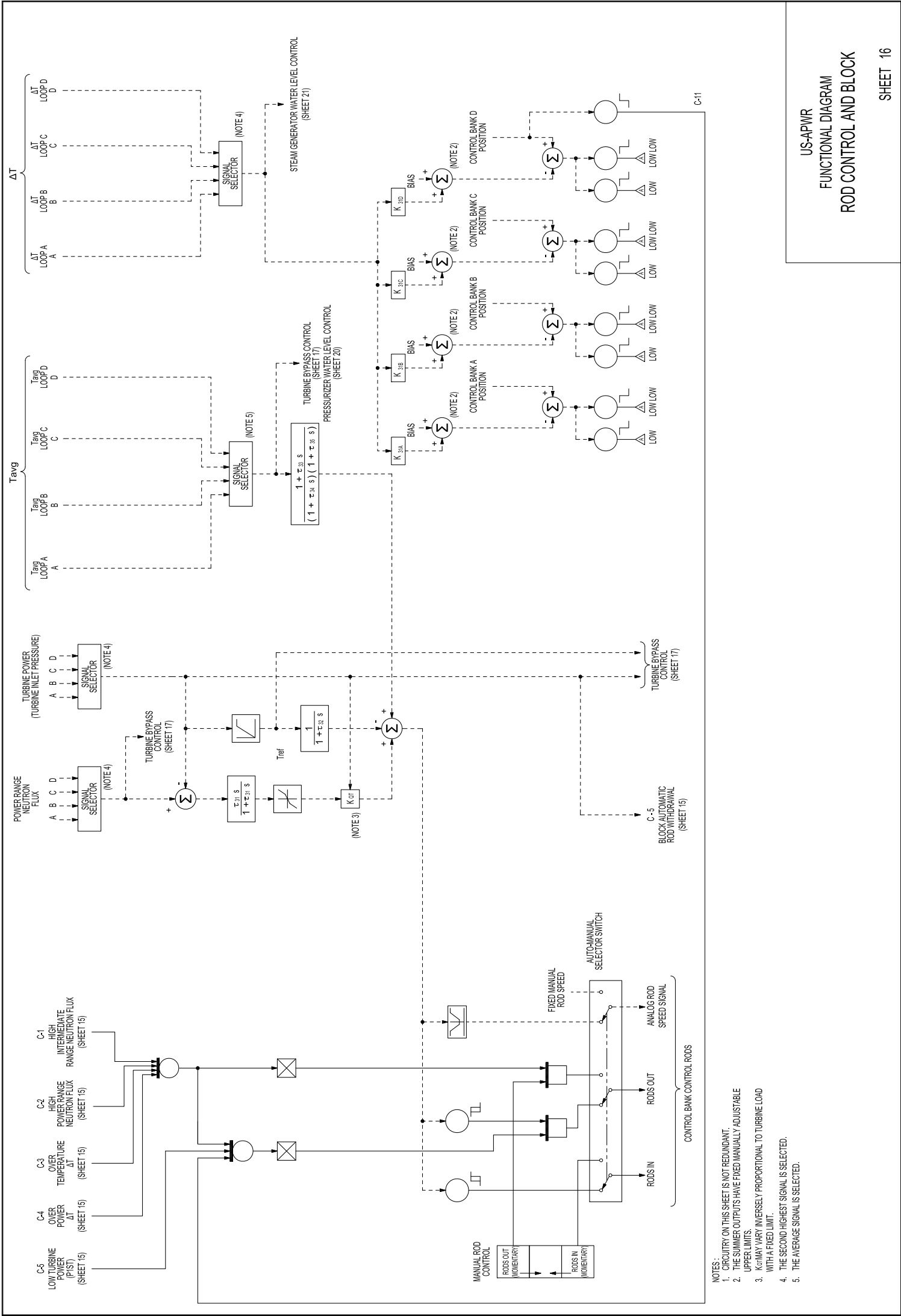


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 16 of 21)

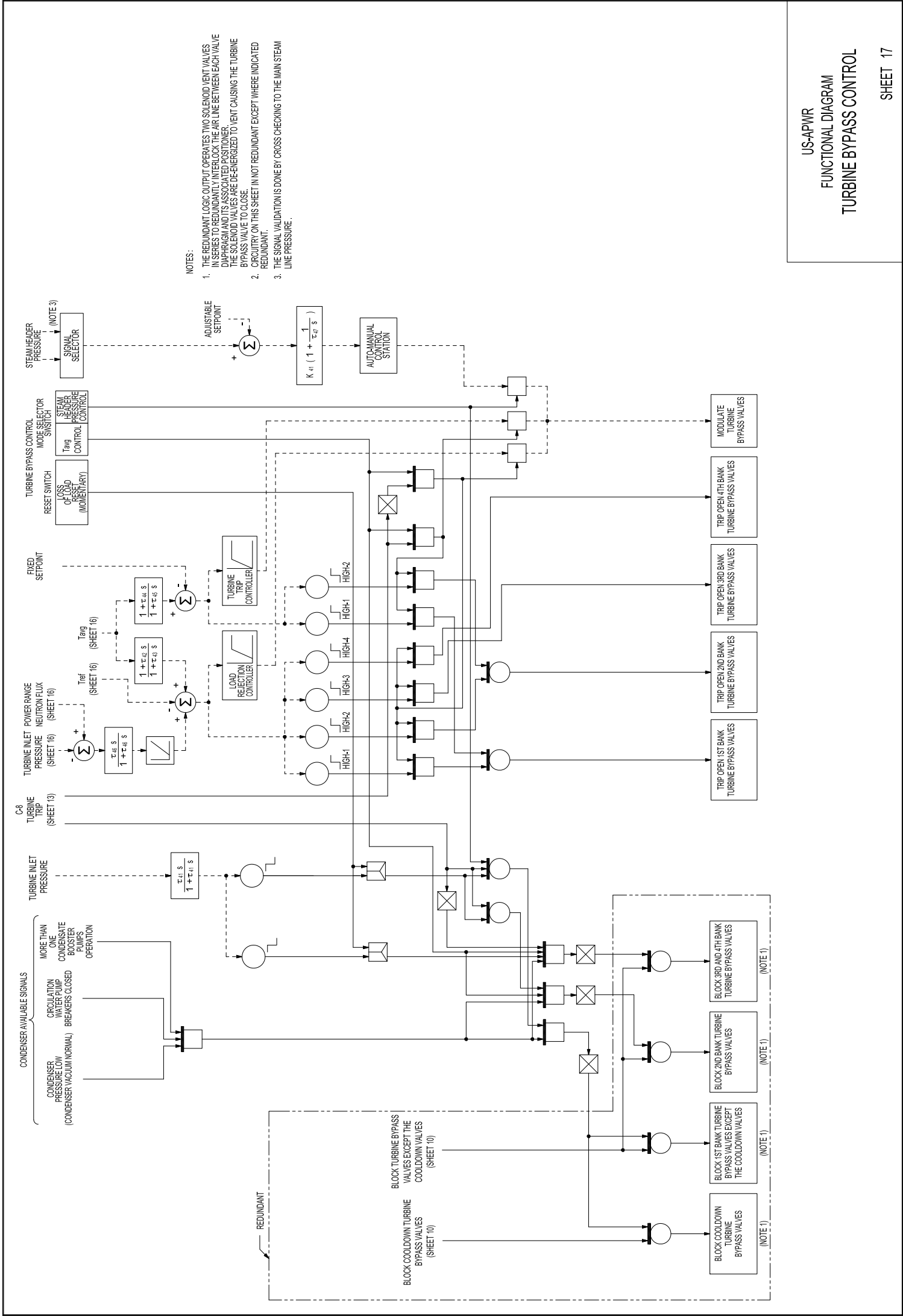


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 17 of 21)

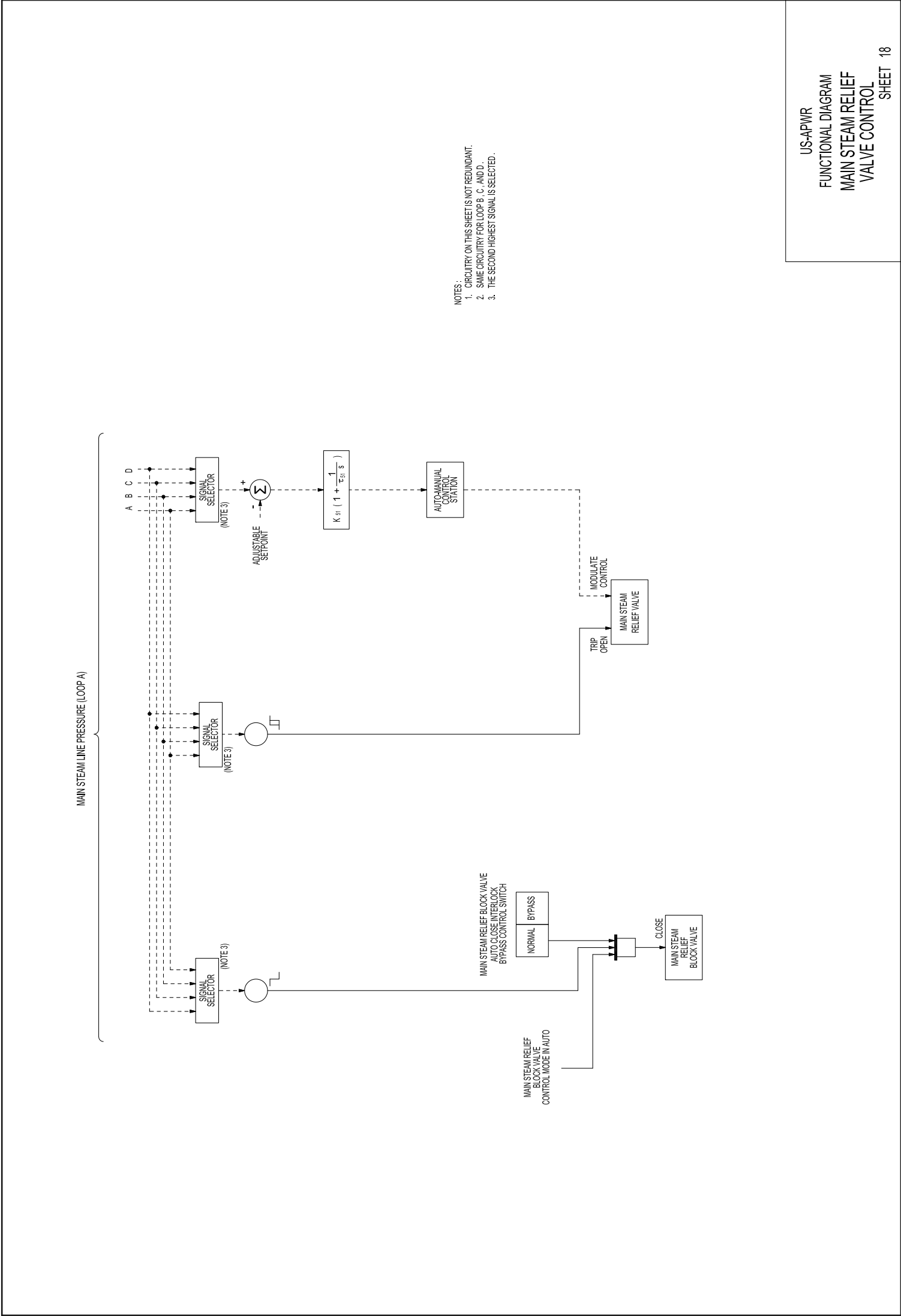


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 18 of 21)

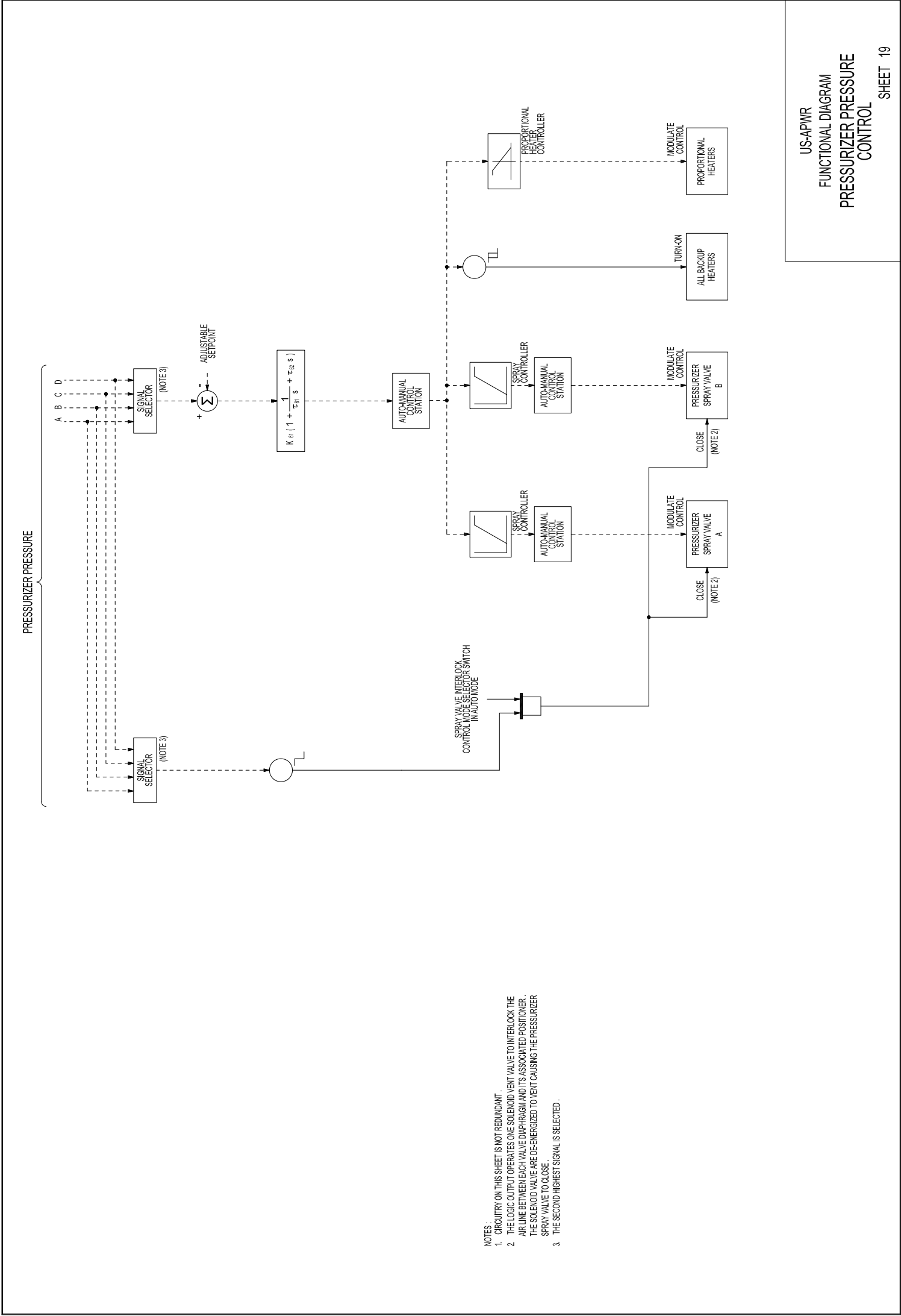
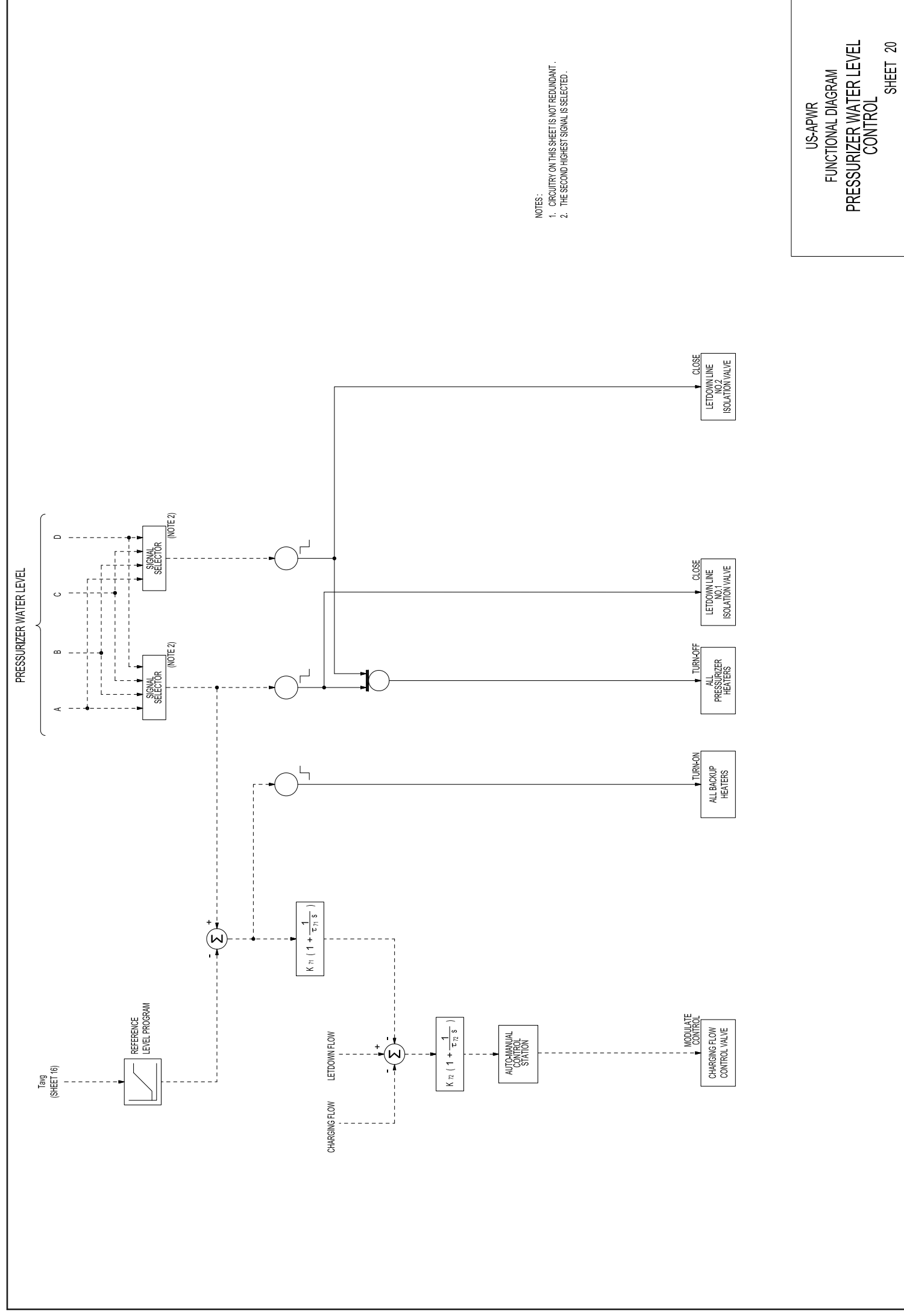


Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 19 of 21)



**Figure 7.2-2 Functional Logic Diagram for Reactor Protection and Control System (Sheet 20 of 21)**





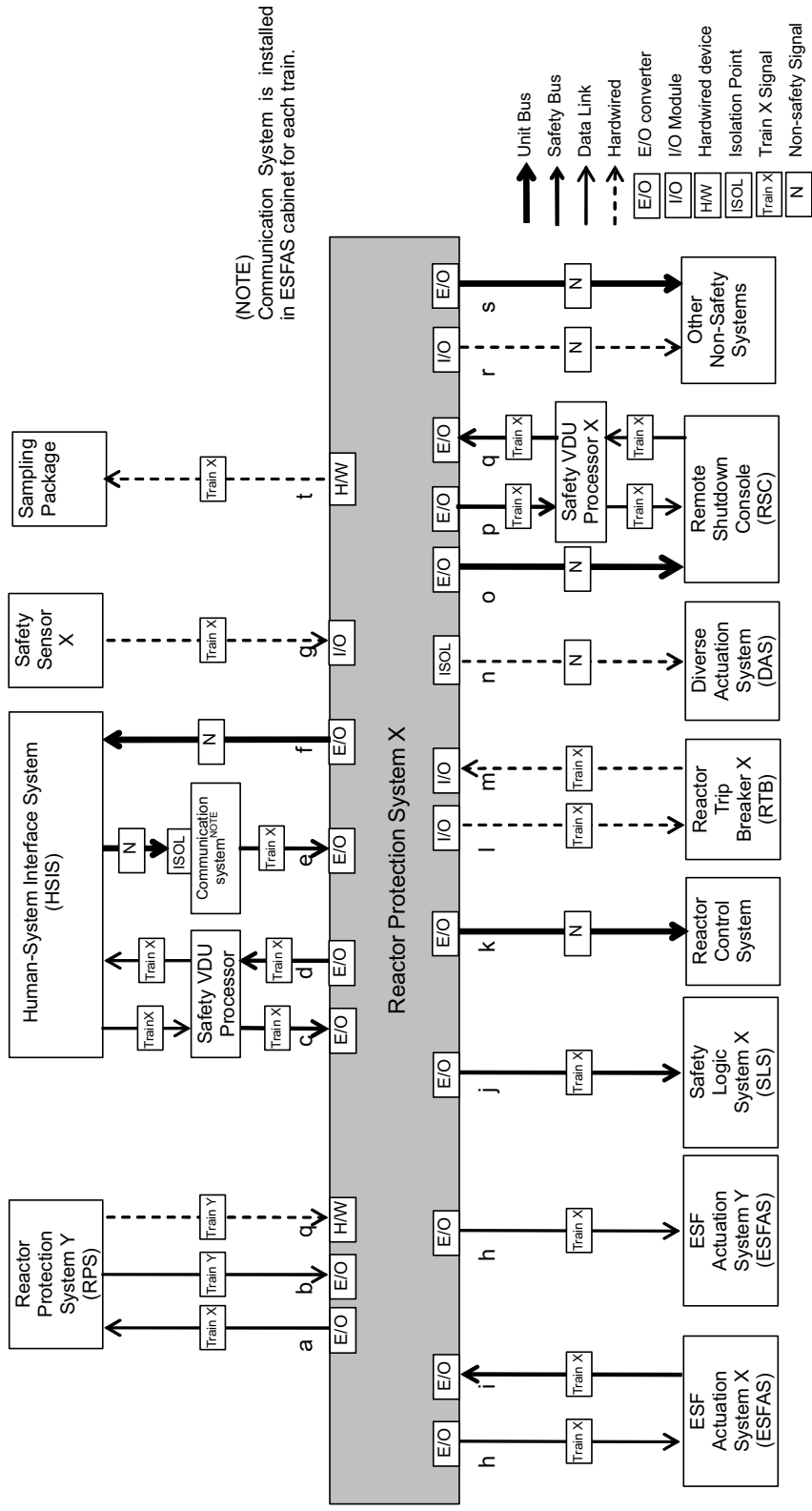


Figure 7.2-3 Interface between RPS and Other Systems (for Table 7.2-1)

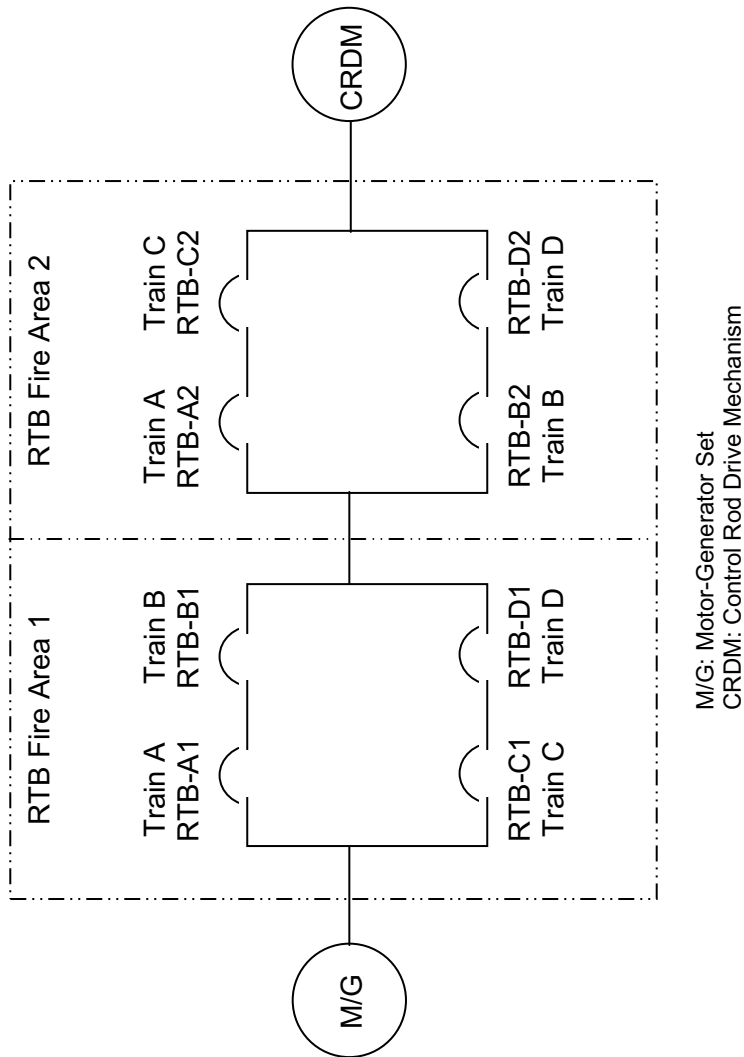


Figure 7.2-4 Configurations of the Reactor Trip Breakers

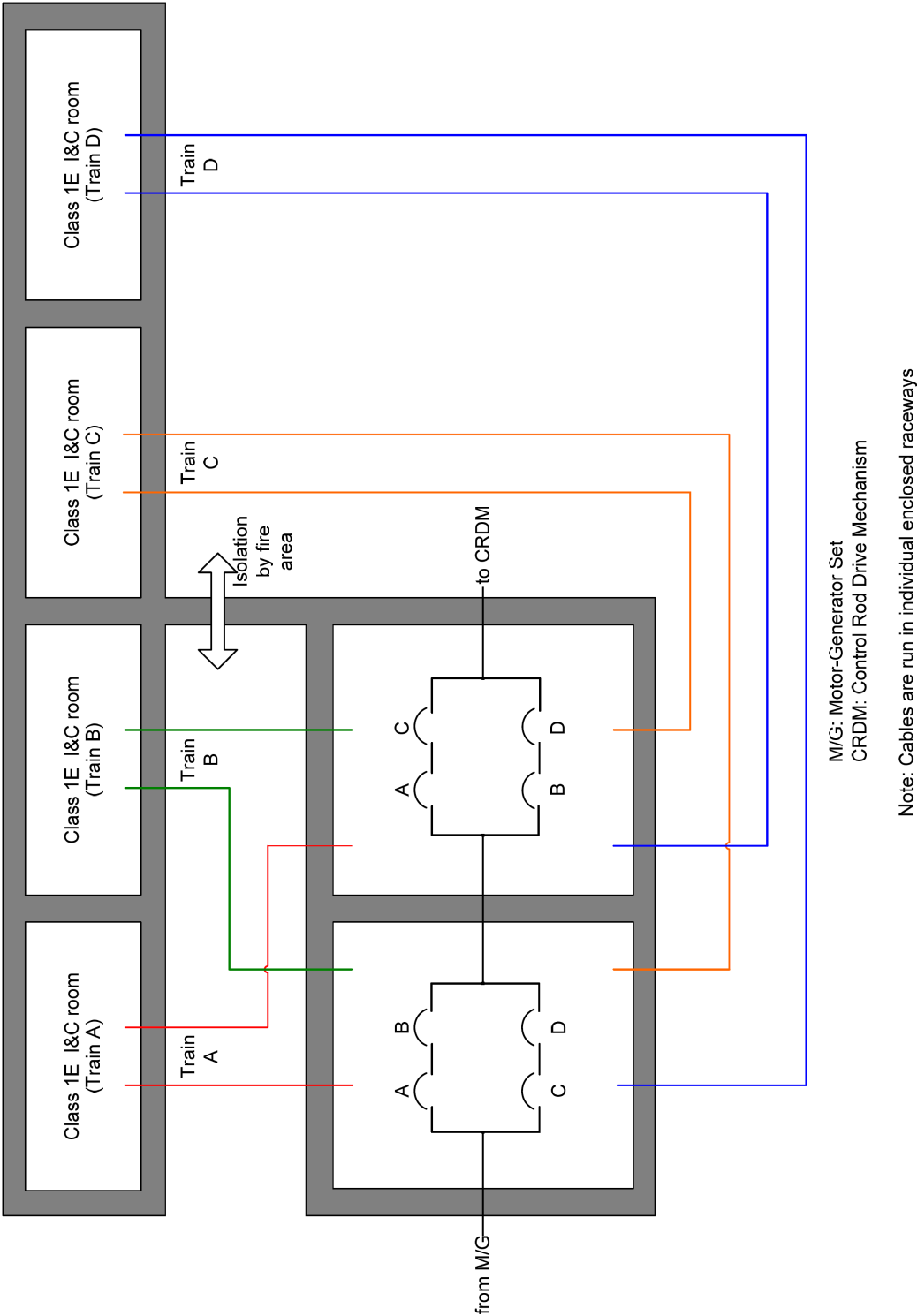


Figure 7.2-5 Summary of Fire Protection for Reactor Trip Breaker

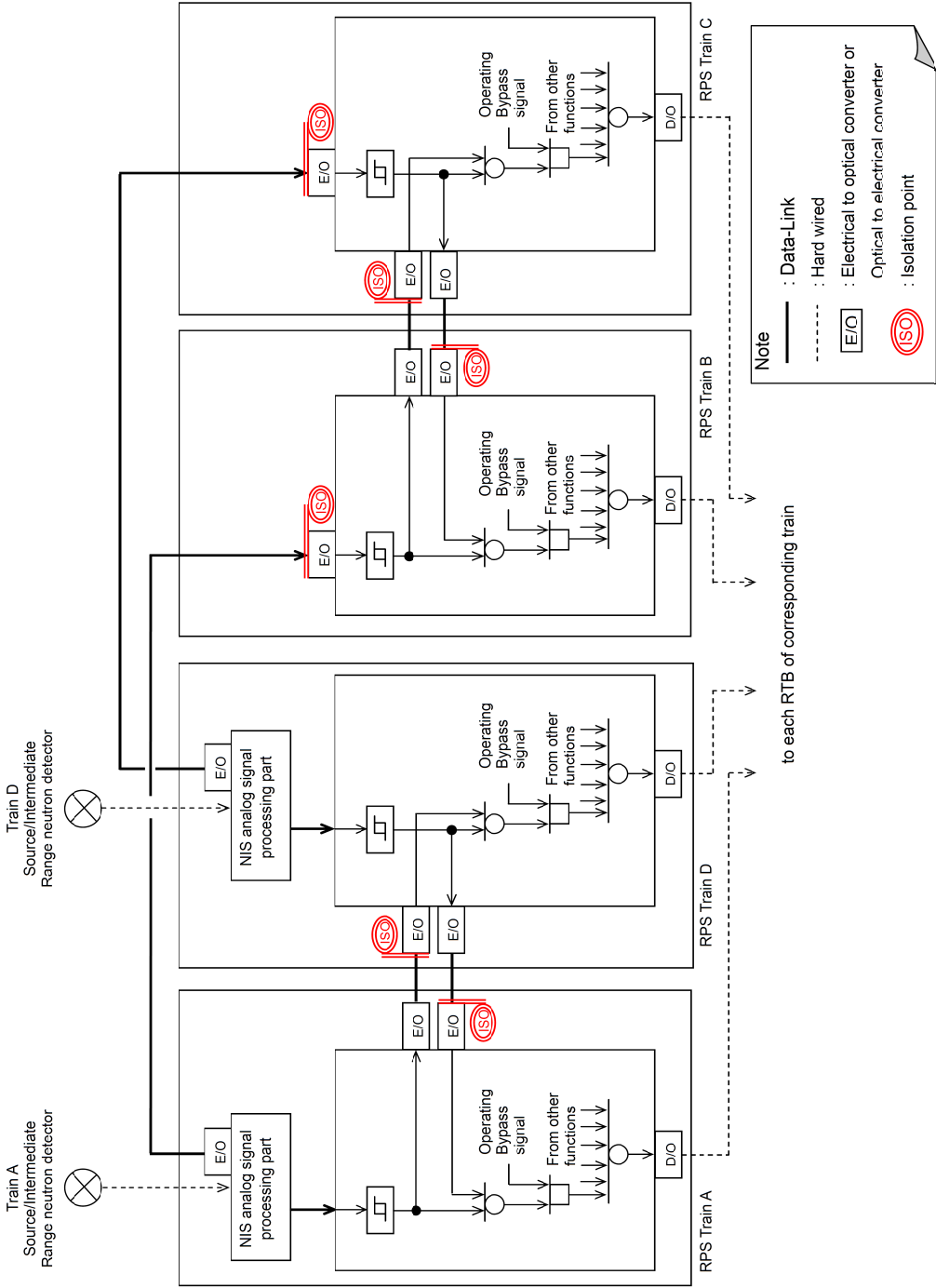


Figure 7.2-6 Signal Flow for High Source and Intermediate Range Neutron Flux Trips

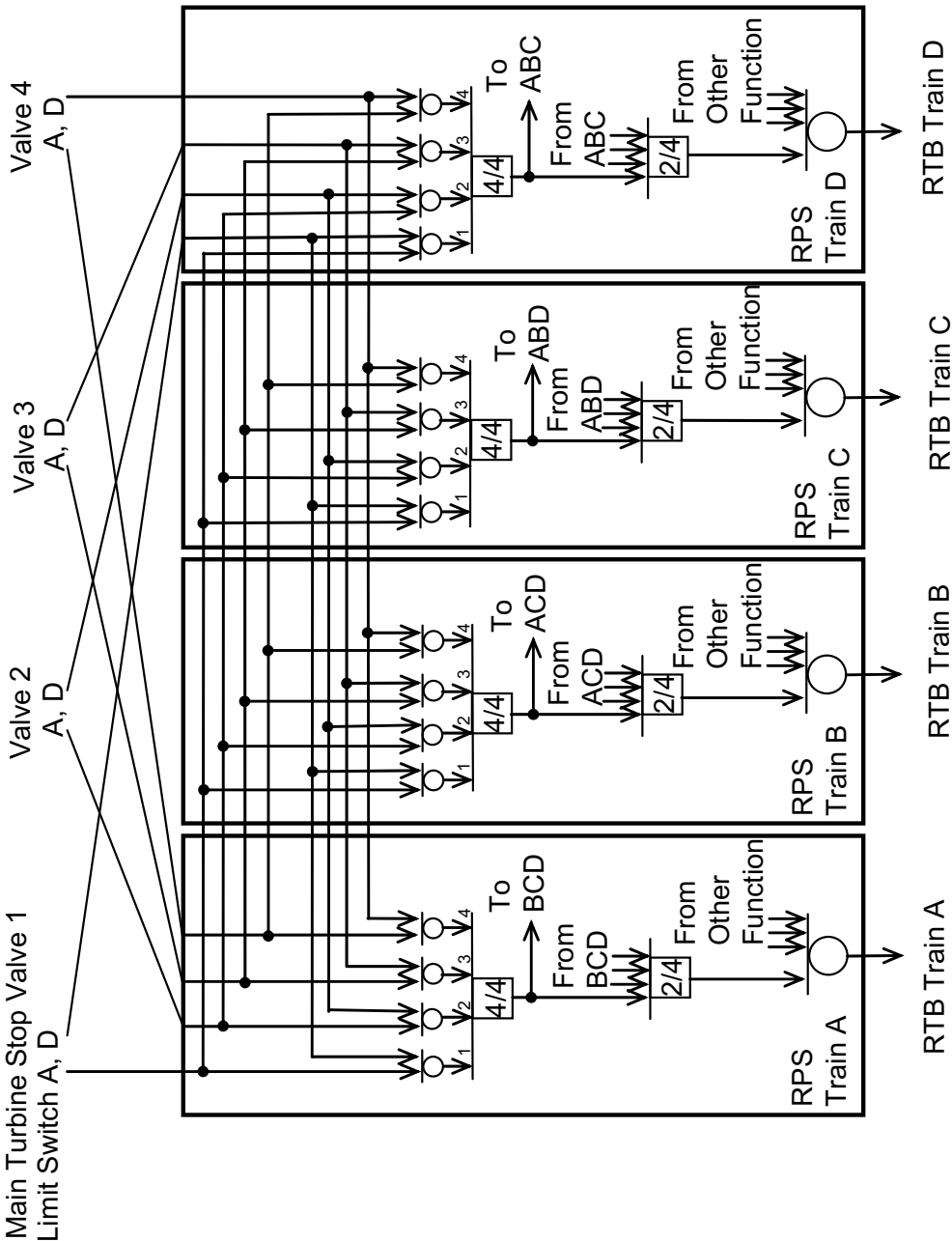
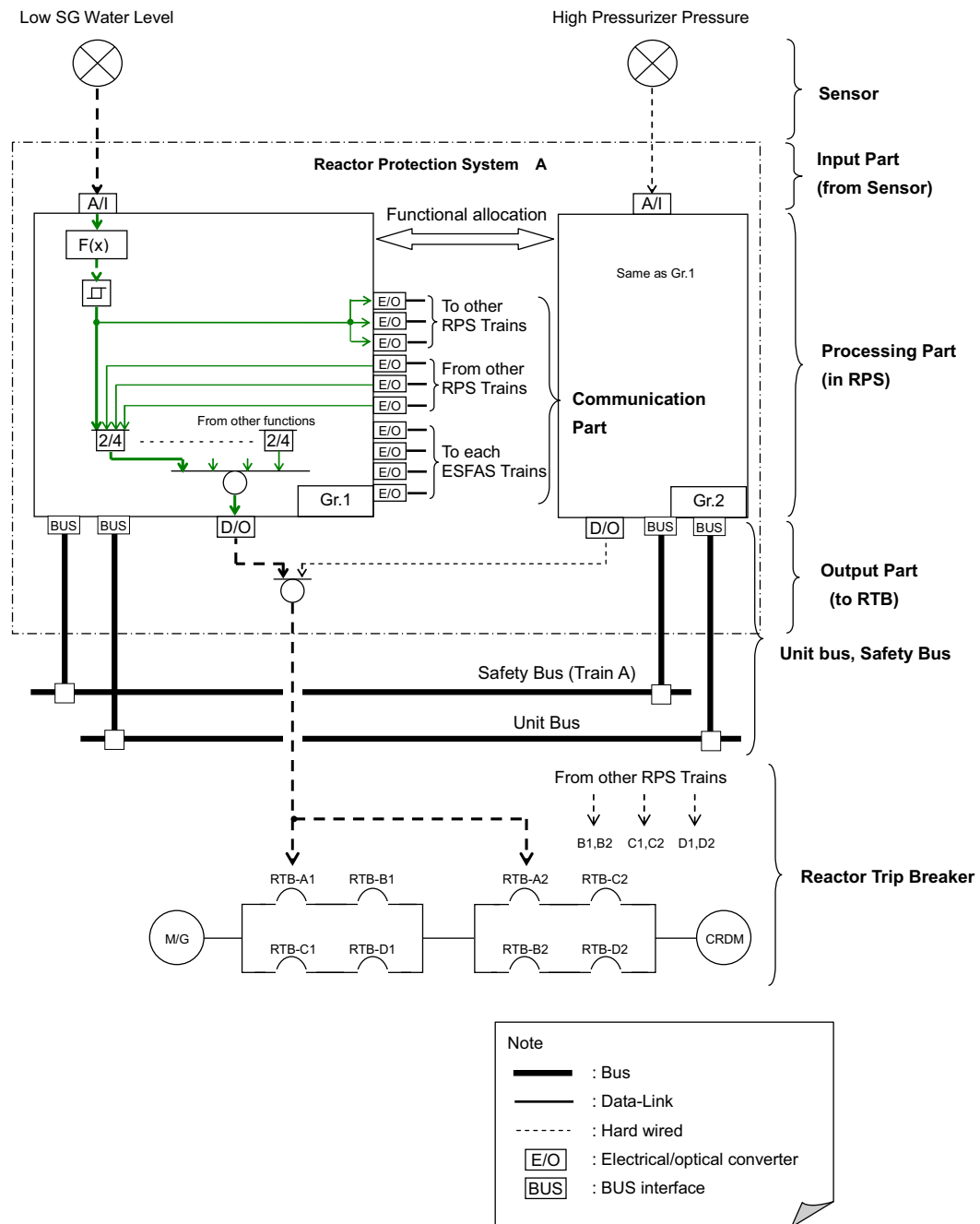


Figure 7.2-7 Signal Flow for Reactor Trip on Turbine Trip



(Train A is shown for representative train.)

Figure 7.2-8 RPS Configuration for Use in FMEA (for Table 7.2-8)

---

### 7.3 Engineered Safety Feature Systems

#### 7.3.1 System Description

The ESF system consists of

- Safety sensors
- RPS
- ESFAS
- SLS
- Safety grade HSIS which includes processors and VDUs common to above both RPS and ESFAS
- Conventional safety-related switches (for system related actuation.)

Figure 7.3-1 shows the overall ESF system configuration.

ESF systems provide I&C functions to sense accident conditions and initiate the operation of necessary ESF system components to mitigate accident conditions in a timely manner. The occurrence of a PA, such as a LOCA or a steam line break, requires a RT plus actuation of one or more ESF systems in order to mitigate the consequences. The RPS receives signals from various sensors and transmitters. The RPS then determines if the setpoints are being exceeded and, if they are, the RPS combines the signals into logic matrices indicative of primary or secondary system boundary ruptures. Once the required logic combination is completed, the RPS sends ESF actuation signals to each train of the ESFAS. Each train of the ESFAS combines the signals from all RPS trains using 2-out-of-4 voting logic to actuate its respective train of the SLS.

Control from the ESF system includes; the ECCS, containment systems, containment spray system (CSS), emergency feedwater system (EFWS), annulus emergency exhaust system, and MCR HVAC system. These systems, its subsystems and/or components are actuated by the ESFAS signal as necessary to mitigate specific accident/event condition(s). Examples of systems activated by the ESFAS include; ECCS, main steam line isolation, containment spray (CS), containment isolation, emergency feedwater (EFW), MCR isolation, emergency generator start up, ESWS, and RT (at the train level). Individual ESF systems can be manually actuated from the MCR.

The following items make up the ESF system:

- Process variable sensors
- RPS for processing process input signals and voting to determine the need for system level ESF actuation
- ESFAS for voting logic, which combines signals from all RPS trains and generates train level actuation signals to the SLS. The ESFAS also sequences the actuation



---

of plant components to avoid overloading plant electrical systems during LOOP conditions.

- SLS to distribute train level actuation signals from the ESFAS to the control logic for designated plant components
- Systems and components associated with ESF system
- Safety VDU processors and safety VDUs to provide manual component level control of plant components after initial automatic actuation by the ESFAS. Safety VDUs also provide reset for ESFAS actuation.
- Conventional switches for manual initiation at train level

The ESFAS and SLS send system status and process data to the HSIS and PCMS, which is not required for safety, via the unit bus. The ESFAS and SLS also receive manual component control and reset signals from the HSIS, which are not required for safety, via the unit bus. The interfaces for each ESFAS division are shown in Figures 7.3-2 and 7.3-3 and are described in Tables 7.3-1 and 7.3-2.

#### 7.3.1.1 ESF System Level Logic

There are four trains for the ESF system in the US-APWR. The system level ESF actuation signals from all four RPS trains are transmitted over isolated data links to an ESFAS controller in each train of the ESF system. Each ESFAS controller consists of a duplex architecture using dual CPUs to enhance reliability. The RPS provides bistable calculations and voting logic to the ESFAS for ESF actuation. 2-out-of-4 coincidence voting logic is performed within each train through the redundant subsystems within each ESFAS controller. Each ESFAS subsystem generates a train level ESF actuation signal when the required 2-out-of-4 coincidence is met from the four RPS actuation signals. System level ESF manual actuation signals are hardwired from conventional switches located on the OC. These signals are also processed by the logic in each redundant subsystem of each ESFAS train to generate the same train level ESF actuation signal. Train level manual actuation signals are generated for each ESFAS signal from separate switches for each ESFAS train. To avoid spurious actuation from a single contact or signal path failure, each switch contains two contacts that are interfaced to two separate digital inputs. Each ESFAS subsystem processes these signals through redundant train level manual actuation 2-out-of-2 logic.

Whether automatically or manually initiated, train level ESF actuation signals are transmitted from both subsystems of the ESFAS controller to the corresponding train of the SLS. The number of ESFAS trains that generate train level ESF actuation signals corresponds to the number of mechanical ESF trains being actuated.

The ESFAS also provides automatic load sequencing for the Class 1E GTG to accommodate the site LOOP accident. Each ESFAS train monitors three under voltage inputs, using 2-out-of-3 logic, to detect a loss of power condition for its respective train, and generates a LOOP signal. Upon detecting a loss of power, the ESFAS starts the Class 1E GTG for its train and disconnects the loads for its train from the electrical bus.

---

Once the Class 1E GTG is capable of accepting loads, the ESFAS sequences the loads for its train back onto the electrical bus in an order appropriate for the current train level ESF actuation signal(s). The ESFAS sequencing logic accommodates ESF actuation signals occurring prior to or during a loading sequence. The ESFAS load sequencing function is independent for each train. The ESFAS also provides automatic load sequencing when an ESFAS is actuated during normal power conditions (i.e., no LOOP). Logic for the ESFAS load sequencing function is described in Subsection 8.3.1.

Safety plant components are manually loaded on the non-safety alternate ac power source from the SLS during station blackout (which includes a loss of the Class 1E GTG Power Source).

#### 7.3.1.2 ESF Component Level Logic

The SLS controls safety-related plant components in all trains based on ESF actuation signals, process instrumentation and component level manual actions from the operational VDUs and safety VDUs.

There are four SLS trains in the US-APWR. The SLS consists of multiple controllers in each train. Plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures, and optimization of controller performance. In general, complete plant process systems are assigned to a single controller. Multiple process systems are assigned to the same controller or a single process system is assigned to multiple controllers only if the plant effects of controller failure and maintenance are demonstrated to be acceptable, based on MUAP-09020 "Function Assignment Analysis for Safety Logic System" (Reference 7.3-11).

Each train of the SLS receives ESF system level actuation demand signals and load sequencing signals from its respective train of the ESFAS. The SLS also receives manual component level control signals from the OC and RSC (safety VDUs and operational VDUs). The SLS also receives process signals from the RPS for interlocks and controls of plant process systems. The system performs the component level control logic for safety actuators (e.g., MOVs, solenoid operated valves, and switchgears).

The SLS controllers for each train are located in separate I&C rooms. The system has conventional I/O portions and I/O portions with priority logic to accommodate signals from the DAS. All SLS I/O will be located within the Class 1E I&C equipment rooms and Class 1E electrical rooms. These rooms are maintained in a mild environment condition by the safety ventilation system at all times.

SLS is a microprocessor based system that achieves high reliability through redundancy within each train and microprocessor self-diagnostics, including data communications. The system also includes features to allow periodic testing of functions that are not automatically tested by the self-diagnostics, such as final actuation of safety components. Manual periodic tests can be conducted with the plant on-line and without the risk of spurious system level actuation due to single failures during testing.

To enhance reliability, each SLS controller consists of a duplex architecture using redundant CPUs operating in a redundant parallel configuration. In MUAP-07005 (Reference 7.3-1), this is referred to as a redundant parallel controller configuration.

Each controller of the duplex architecture receives ESF actuation signals and load sequencing signals from the corresponding duplex controller of the ESFAS. The SLS also includes I/O modules mounted in I/O chassis. These I/O chassis can be located within the same cabinet as the controllers, or remotely in separate cabinets that are distributed throughout the plant to reduce the length of cable from the process component or instrument to the I/O chassis. Signals from each SLS controller in the duplex architecture are combined in the output modules using 1-out-of-2 logic for control of plant components to the desired safety state. The SLS I/O modules include contact input conversion devices and power interface devices. The power interface module receives input signals and controls the actuation device (such as motor starters, switchgear, etc.). The actuation devices, in turn, control motive power to the final ESF component. Each train of the SLS thus interfaces the PSMS to each train of the ESF equipment.

Each controller has multiple I/O chassis, each chassis has multiple I/O modules and each I/O module accommodates one or more process interfaces. The plant process interfaces are assigned to I/O modules/chassis with consideration of maintenance and potential SLS equipment failures. Based on the FMEA (refer to Table 7.3-7), acceptable plant level effects for failure or maintenance of any I/O module or any I/O chassis are demonstrated. I/O modules are duplicated within a single SLS train if a single failure of the I/O module will cause a spurious reactor trip.

The primary functions performed by the SLS are described below.

#### **7.3.1.2.1 Control of ESF Components**

The ESFAS provides all the system level ESF actuation logic, including the automatic load sequence, for the Class 1E GTG. Whether automatically or manually generated, train level ESF actuation signals are transmitted from each ESFAS train to the corresponding train of the SLS. Within the SLS, the train level ESF actuation signals are then broken down to component actuation signals to actuate each component associated with an ESF. The logic within each train of the SLS accomplishes this function and performs the necessary interlocking to ensure that components are properly aligned for safety.

The SLS also controls ESF components, such as the EFW control valve, based on manual component level controls from operational VDUs and safety VDUs, including all components required for credited manual operator actions, refer to Subsection 7.5.1.5. To ensure spurious command signals from Operational VDUs cannot adversely affect multiple safety divisions, all safety components controlled by the PSMS, regardless of their position under normal operating conditions, are commanded to the correct safety position by automatic safety interlocks or automatic ESFAS actuation signals.

#### **7.3.1.2.2 Control of Safe Shutdown Components**

The systems necessary for safe shutdown and associated controls are discussed in Section 7.4.

**7.3.1.2.3 Control of Interlocks Important to Safety**

The SLS provides interlocks, which operate to reduce the probability of specific events occurring or to verify the state of a safety system. These include interlocks to prevent over pressurization of low-pressure systems and interlocks to ensure availability of ESF systems. Interlocks important to safety are discussed in Section 7.6.

**7.3.1.2.4 Functional Allocation in SLS Controllers**

For Functional Allocation in SLS Controllers, refer to MUAP-09020 "Function Assignment Analysis for Safety Logic System" (Reference 7.3-11).

**7.3.1.3 Engineered Safety Features**

For the US-APWR, the ESF consists of the ECCS, containment isolation systems, CSS, EFWS, annulus emergency exhaust system, and MCR HVAC system. These systems are discussed in Chapters 6, 9, and 10.

ESF systems activate the required components to mitigate plant conditions relating to the occurrence of specific credible limiting fault(s). Examples of such limiting faults are; LOCA, large or small steam line break, LOOP, LOCA followed by LOOP, or LOOP followed by LOCA, or both occurring together, control rod ejection, SG tube rupture, and all credible accidents in which radioactive fission products could be released from the RCS.

**7.3.1.4 Process Variables Monitored for ESF**

A number of process variables, equipment status and plant parameters that are monitored to establish the degraded plant condition(s) and are used for generating ESF actuation signals to initiate various required ESF systems. Table 7.3-3 provides a list of process variables and signals. Table 7.3-4 provides range, accuracy, response time, and setpoint for each ESF actuation variables. Response time described in this table is within the delay time assumed in the safety analyses of Chapter 15. Setpoint described in this table is within the analytical limit assumed in the safety analysis of Chapter 15. The delay time and the analytical limit is shown in Table 15.0-4 of Subsection 15.0.0.3. Table 7.3-5 and 7.3-6 provides list of manual train level inputs for actuation.

Some of the following variables are shared instrument used by multiple safety functions and non-safety control functions;

- Pressurizer pressure
- Pressurizer water level
- Main steam line pressure
- SG water level
- Containment pressure

- 
- Containment high range area radiation
  - MCR outside air intake radiation
  - MFW pumps trip signal
  - RT signal (P-4 interlock)
  - LOOP signal
  - Reactor coolant cold leg and hot leg temperatures ( $T_{avg}$  signal)

#### **7.3.1.5 ESF Initiating Signals, Logic, Actuation Devices and Manual Controls**

The following subsections provide a functional description of ESF actuation signals, actuated systems/components and initiating logic for actuating each ESF function.

Except as noted in specific sections below, all actuation signals are latched at the train level, whether automatically or manually initiated, and require manual reset. Latching ensures the protective action goes to completion and ensures that components remain in their safety position after the process returns to its pre-trip condition. Manual reset can only be initiated after the process returns to its pre-trip condition.

Except as noted in specific sections below, the description is for one train and is applicable to all four trains. All manual actuations, bypasses, overrides, and resets are initiated separately for each train.

##### **7.3.1.5.1 Emergency Core Cooling System**

ESF actuation signal for ECCS function is generated when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheets 9 and 11.

- Manual actuation
- Low pressurizer pressure initiating signal is generated on a condition when 2-out-of-4 signals for low pressurizer pressure are present and pressurizer pressure ECCS actuation bypass is not activated. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 11.
- Low main steam line pressure initiating signal is generated when 2-out-of-4 signals for low pressure in any one of the four loops A, B, C, or D are present and main steam line pressure ECCS actuation bypass is not active. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 9.

The low pressurizer pressure ECCS actuation bypass and low main steam line pressure ECCS actuation bypass can be activated manually only when pressurizer pressure interlock P-11 is present (i.e., when the pressurizer pressure signal is lower than the P-11

---

setpoint). These manually initiated operating bypasses are automatically removed when the pressurizer pressure signal is higher than the P-11 setpoint.

- High containment pressure initiating signal is generated when 2-out-of-4 signals for high containment pressure are present. There is no operating bypass associated with this ECCS actuation signal. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 11.

An activated ECCS signal is latched separately for each train and cannot be manually overridden for 160 seconds. After ECCS is manually overridden the override is automatically removed when the P-4 RT interlock clears (i.e., RTB re-closed). An ECCS actuation signal cannot be manually reset for 160 seconds after actuation and until the initiating signals have cleared.

An ECCS actuation signal aligns the required ESF systems valves (e.g., containment isolation valves, EFW valves) and starts the ESF system pumps and fans, required to mitigate the specific accident and/or AOO conditions. An ECCS actuation signal results in the following actions:

- Trip RCPs: There are two Class 1E RCP breakers for each RCP. One breaker is located in the Class 1E electrical room and the other is located in the electrical room in the turbine building. All Class 1E RCP breakers are tripped in 15 seconds after both the ECCS actuation signal and the P-4 RT interlock signal are present. The P-4 interlock is generated when breaker open status signals are received from any combination of RTBs that would result in a RT. Logic for this actuation is included on Figure 7.2-2 sheet 11.
- Start emergency generator: Actuation of ECCS signal starts the emergency power source.
- Safety injection pumps
- RT: RT is initiated by the ECCS actuation signal, refer to Section 7.2.
- Main feedwater isolation
- Emergency feedwater actuation
- Containment isolation phase A
- Containment purge isolation
- Hydrogen igniter actuation: This is a non-safety function. Isolation is provided within the PSMS for this function.
- MCR isolation
- ESWS actuation

---

The ECCS actuation signal also initiates automatic load sequencing, reference Subsection 7.3.1.1.

The P-4 interlock is generated independently in each RPS division. The logic is shown in Figure 7.2-2 sheet 2. Each RPS train receives status signals from the RTBs in its own train. RTB status signals are interfaced between RPS trains through the same fiber optic data links used for all RPS partial trip signals. P-4 interlocks from each RPS train are interfaced to each ESFAS train through 2-out-of-4 logic.

#### **7.3.1.5.2 Main Steam Line Isolation**

The main steam line isolation signal closes the main steam isolation valves and associated bypass valves for all four loops. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 9 and sheet 11.

There are only two ESFAS trains for main steam line isolation, A and D.

An ESF actuation signal for the main steam Isolation function is generated when any of the following initiating signals are present:

- High-high containment pressure: This initiation signal is present when 2-out-of-4 signals for High-high containment pressure are present.
- Low main steam line pressure: This initiation signal is present when 2-out-of-4 signals for low main steam line pressure are present in any one of the four loops A, B, C, or D and the low main steam line pressure ECCS actuation bypass is not activated. The low main steam line pressure ECCS actuation bypass is described in Subsection 7.3.1.6.3.
- High main steam line pressure negative rate: This initiation signal is present when 2-out-of-4 signals for high main steam line pressure negative rate is present in any one of the four steam line loops A, B, C, or D. High main steam line pressure negative rate trip is only active when the low main steam line pressure trip is inactive. Logic for this actuation is included on Figure 7.2-2 sheet 9.
- Manual actuation

Once the main steam line isolation signal is generated, it is latched and can only be reset by manual action. Activation of this signal closes the main steam isolation valves and associated bypass valves for all four loops. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 9 and sheet 11.

#### **7.3.1.5.3 Containment Spray Actuation**

ESF actuation signal for CS function is generated when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 12.

- High-3 containment pressure signal: This signal is the result of 2-out-of-4 signals from High-3 containment pressure.

- 
- Manual actuation: Unlike other manual actuations, which are actuated by a single switch for each train, the manual actuation signal for each CS train is activated when 2-out-of-2 CS manual controls are operated concurrently.

#### **7.3.1.5.4 Containment Isolation Phase A**

ESF actuation signal for containment isolation phase A function is generated on a condition when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 12.

- ECCS actuation signal
- Manual actuation

For any single containment penetration, isolation can be accomplished by either of two redundant trains. There are only two ESFAS trains for containment isolation phase A, A and D.

#### **7.3.1.5.5 Containment Isolation Phase B**

ESF actuation signal for containment isolation phase B function is generated on a condition when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 12.

- High-3 containment pressure signal: This signal is the result of 2-out-of-4 signals from High-3 containment pressure.
- Manual CS actuation

For any single containment penetration, isolation can be accomplished by either of two redundant trains. All containment isolation functions are distributed among all four ESFAS trains.

#### **7.3.1.5.6 Containment Purge Isolation**

ESF actuation signal for containment purge isolation function is generated when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 12.

- ECCS actuation signal
- High containment high range area radiation: This signal is the result of 2-out-of-4 signals for high containment radiation.
- Manual containment isolation phase A actuation
- Manual CS actuation



---

For any single containment penetration, isolation can be accomplished by either of two redundant trains. There are only two ESFAS trains for containment purge isolation, A and D.

#### **7.3.1.5.7 MCR Isolation**

ESF actuation signal for this function is generated when any of the following initiating signals are present. Logic for this actuation circuit is shown on Figure 7.2-2 sheet 12.

- Manual actuation
- ECCS actuation signal
- High MCR outside air intake radiation: There are six MCR outside air intake radiation monitors interfaced separately to RPS trains A and D (two gas monitors, two iodine monitors, and two particulate monitors). RPS trains A and D provide separate bistable setpoint comparison functions for each monitor. These bistable output signals are distributed from RPS trains A and D to each of the four ESFAS trains. Within each of the four ESFAS trains the MCR Isolation signal is actuated on a signal from either the A or D train detectors using 1-out-of-2 logic for each type of monitor. The MCR Isolation actuation signal is distributed to the Main Control Room HVAC System (MCRVS) which consist of two 100% trains (A and D) of subsystems Main Control Room Emergency Filtration System (MCREFS) and four 50% trains of subsystems Main Control Room Air Temperature Control System (MCRATCS). For a detailed system explanation, refer to Section 9.4.

#### **7.3.1.5.8 Main Feedwater Isolation**

There are only two ESFAS trains for MFW isolation, A and D.

Logic for the main feedwater isolation circuit is shown on Figure 7.2-2 sheet 10.

##### **7.3.1.5.8.1 Main Feedwater Regulation Valve Closure**

ESF actuation signal for MFW regulation valve closure functions when any of the following signals are present:

- Low  $T_{avg}$  in any 2-out-of-4 loops A, B, C, or D and P-4 interlock is present.

Resulting signal from MFW regulation valve closure closes all MFW regulation valves.

##### **7.3.1.5.8.2 Main Feedwater Isolation**

ESF actuation signal for MFW isolation functions when any of the following signals are present:

- Manual actuation
- ECCS actuation signal

- 
- High-high SG water level: (high-high water level in any of the SGs A, B, C, or D) (see description above)
  - The bypass signal from the MFW isolation bypass control switch (operating bypass) can be activated only when pressurizer pressure P-11 interlock is present (i.e., when the pressurizer pressure signal is lower than the P-11 setpoint). This operating bypass is automatically removed on deactivation of P-11 interlock (i.e., when pressurizer pressure signal is above the P-11 setpoint). This bypass function bypasses the MFW isolation signal for all MFW pumps, all MFW isolation valves, and all SG water filling control valves.

A resulting signal for MFW isolation actuates the following:

- Trip all MFW pumps
- Close all MFW isolation valves
- Close all SG water filling control valves
- Close all MFW bypass regulation valves
- Close all MFW regulation valves

The actuation signals to trip non safety-related MFW pumps are electrically isolated in the SLS via power interface modules.

#### **7.3.1.5.9 Emergency Feedwater Actuation**

ESF actuation signal for EFW function is generated when any of the following initiating signals are present:

- Low SG water level: Low SG water level in any SGs A, B, C, or D, based on 2-out-of-4 signals.
- ECCS actuation signal.
- LOOP signal. Refer to Subsection 7.3.1.1.
- MFW pumps trip: EFW actuation on trip of all MFW pumps is an anticipatory function that is not credited in the safety analysis. Therefore, this is not a safety function but is designed to be highly reliable. Isolation is provided within the PSMS for this function. Redundant trip signals for each MFW pump are interfaced from the PCMS to the PSMS via the unit bus. Since these non-safety signals can only result in safety actuation, there is no potential for adverse interaction with the safety function. Since actuation requires signals from all four MFW pumps, there is minimal potential for spurious actuation.
- Manual actuation

Resulting signals actuate the following:

- Start EFW pumps: Train A actuating signal starts train A EFW pumps. Likewise, trains B through D start their corresponding EFW pumps.
- Close SG blowdown isolation valves and sample line valves of all SGs A, B, C, and D.
- Open EFW isolation valves.

Logic for the emergency feedwater actuation circuit is shown on Figure 7.2-2 sheet 7.

#### **7.3.1.5.10 Emergency Feedwater Isolation**

There are four emergency feedwater isolation signals, one for each loop A, B, C and D. The following description is for loop A. All loops are identical. Logic for this ESF function is included on Figure 7.2-2 sheet 8.

There are two separate ESFAS trains for the emergency feedwater isolation valves for each SG (there are two isolation valves per SG).

ESF actuation signal for emergency feedwater isolation loop A function is generated when any of the following initiating signals are present:

- Manual actuation
- Loop A low main steam line pressure: this signal is present when 2-out-of-4 main steam line pressure signals from SG A indicate low pressure, there is no low main steam line pressure EFW isolation block signal from any other SG loop (B, C, or D), and there is no EFW bypass control (operating bypass).
- Loop A high SG water level: this signal is present when there is 2-out-of-4 high SG water level signals from SG A (with time delay), there is no loop A low main steam line pressure signal, the reactor is tripped (P-4 interlock is active) and there is no EFW isolation bypass control (operating bypass).

The EFW isolation bypass control can be manually actuated when the low pressurizer pressure P-11 interlock is present. This operating bypass is automatically removed by the P-11 interlock when pressurizer pressure rises above P-11 setpoint. The EFW isolation bypass control is common to all SG loops A, B, C, and D, whereas there are separate EFW isolation bypass controls for each ESFAS train.

#### **7.3.1.5.11 CVCS Isolation**

There are two ESFAS trains for chemical and volume control system (CVCS) Isolation, train A and train D.

The ESF actuation signal for the CVCS isolation function is generated on a condition when any of the following initiating signals are present:

- 
- Manual actuation
  - High pressurizer water level: this signal is present when 2-out-of-4 signals are present for high pressurizer water level and high pressurizer water level CVCS isolation bypass control (operating bypass) is not present.

The CVCS isolation bypass control (operating bypass) can only be actuated when P-11 interlock is present. This operating bypass is automatically removed by the P-11 interlock when pressurizer pressure rises above the P-11 setpoint.

The resulting actuation signal is latched. Logic diagram for this function is included on Figure 7.2-2 sheet 6.

#### **7.3.1.5.12 Deleted**

### **7.3.1.6 Bypasses and Overrides**

The safety system can be placed in a bypass mode to allow testing and maintenance while the plant is on-line. Such bypasses are known as maintenance bypasses. Maintenance bypasses are discussed in MUAP-07004 (Reference 7.3-2). In addition to maintenance bypasses, automatic and manual operating bypasses are provided to block certain protective actions that would otherwise prevent modes of operations such as startup. Automatic and manual bypasses are described in the following subsections. Maintenance and operating bypasses may be initiated from safety VDUs. To initiate a maintenance or operating bypass from an Operational VDU, the Bypass Permissive for the train must be enabled.

#### **7.3.1.6.1 ESF System Maintenance Bypass**

Bypasses are provided in each ESF system train to block the actuation of one or more ESF signals (e.g., ECCS actuation, EFW, main steam isolation, etc.). The purpose of these bypasses is to allow maintenance on an ESF process system, or to accommodate an ESFAS/SLS controller failure. There are alarms for ESF systems out of service conditions that block functionality at the train level.

#### **7.3.1.6.2 Automatic Operating Bypasses**

These operating bypasses are automatically initiated separately within each PSMS division when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of automatically initiated operating bypasses:

- High main steam line pressure negative rate initiating signal for main steam line isolation is automatically bypassed when the P-11 interlock clears (when pressurizer pressure is above the setpoint). This operating bypass can be manually removed when the P-11 is present (when pressurizer pressure is below the setpoint).
- When the P-4 interlock clears (RTB closed) the low  $T_{avg}$  initiating signal for main feedwater isolation (for closing all main feedwater regulation valves) is

---

automatically bypassed. This operating bypass is automatically removed when the P-4 interlock is present (RTB open ).

#### 7.3.1.6.3 Manual Operating Bypasses

Some operating bypasses must be manually initiated. These operating bypasses can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of manually initiated operating bypasses:

- Low pressurizer pressure initiating signal for the ECCS actuation function can be manually bypassed only when the P-11 interlock is present (pressurizer pressure is below the setpoint). This operating bypass is automatically removed when the P-11 interlock clears (when pressurizer pressure is above the setpoint).
- Low main steam line pressure initiating signal for the ECCS actuation function and main steam line isolation function can be manually bypassed only when the P-11 interlock is present (pressurizer pressure is below the setpoint). This operating bypass is automatically removed when the P-11 interlock clears. When this operating bypass is active, the high main steam line pressure negative rate trip is enabled.
- MFW isolation function can be bypassed manually only when the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.
- The EFW isolation function actuated by low main steam line pressure can be manually bypassed if the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.
- The manual bypass for high pressurizer water level initiation signal for CVCS isolation can only be actuated when the P-11 interlock is present. This operating bypass is automatically removed when the P-11 interlock clears.

All operating bypasses, either manually or automatically initiated, are automatically removed when the plant moves to an operating condition for which the protective action would be required if an accident occurred. Status indication is provided in the MCR for all operating bypasses.

#### 7.3.1.6.4 Manual Overrides

Manual overrides must be manually initiated. These manual overrides can be manually initiated separately within each PSMS train when the plant process permissive condition is sensed by the PSMS input channel(s). The following is a list of train level manually initiated overrides:

- The ECCS actuation can be manually overridden at the train level when the P-4 interlock is present (RTB open). This manual override is automatically removed

---

when the P-4 interlock clears (RTB closed). In MUAP-07004 Appendix D (e), this override is referred to as a reset.

- The block cooldown turbine bypass valve actuation by low-low  $T_{avg}$  may be manually overridden at the train level. This manual override cannot be initiated until after automatic system level actuation. The manual override may be manually reset by the operator at any time, and is automatically reset when the low-low  $T_{avg}$  initiation signal returns to normal. This signal blocks the cooldown turbine bypass valves. In MUAP-07004 Appendix D (b), this override is referred to as an operating bypass.

#### 7.3.1.7 Interlocks

The interlocks for initiating and automatically removing operating bypasses are discussed above. The interlocks for manual overrides are discussed above. The interlocks for resetting system level actuation and channel level actuation are discussed in Subsection 7.3.1.6 for each specific safety function. The interlocks for maintenance bypasses are discussed in Subsection 7.1.3.11.

#### 7.3.1.8 Redundancy

There are four redundant ESF trains for all ESF systems, except as specifically identified in Subsection 7.3.1.5. In addition, within each train, ESFAS and SLS controllers are redundant. Therefore, a controller failure or a controller taken out of service for maintenance has no adverse effect on the protective function. The reliability of the ESFAS/SLS, as analyzed in the PRA, is based on having two controllers in service.

#### 7.3.1.9 Diversity

All ESF systems are automatically initiated from signals that originate in the RPS. Manual actuation of ESF systems is carried out through a diverse signal path that bypasses the RPS.

The SLS receives signals from the DAS to actuate ESF plant components. These signals are interfaced from DAS via qualified isolators within the SLS. The SLS provides priority logic to combine the DAS and SLS signals and to ensure the safety function always has priority. The DAS/SLS interface is described in MAUP-07006 (Reference 7.3-3) Sections 6.2.1.3 and 6.2.4, and shown in Figure 7.3-1.

#### 7.3.1.10 Defense-In-Depth/Design Features

The ESFAS and SLS implement the ESF system echelon of defense-in-depth scheme, as described in Subsection 7.1.3.1.

#### 7.3.1.11 Turbine Trip to Prevent Unnecessary Emergency Core Cooling System Actuation

The turbine is tripped on a reactor trip or high-high SG water level in any SG. Turbine trip on RT is an un-credited non-safety function in the safety analysis. However, turbine trip on RT is assumed in the safety analysis in order to prevent unnecessary ECCS actuation

and to shift to the safe shutdown state by appropriate actions after AOO and PA conditions. Turbine trip on RT cannot be completely designed as Class 1E because the equipment to execute the turbine trip is located in the turbine building, which is seismic category II. Therefore, turbine trip on RT is designed as reliably as possible by applying the following design concepts:

1. Turbine trip on reactor trip is designed as an "Associated Circuit" per IEEE Std 384-1992 (Reference 7.3-4) and RG 1.75 (Reference 7.3-5).
2. The cables outside electrical cabinets in the turbine building are routed in dedicated raceways.
3. Four turbine trip solenoid valves are arranged in a 1-out-of-2 configuration. A trip will be generated by train A or train D. The power for each turbine trip solenoid valve is supplied by a separate Class 1E power source (one per train).

The turbine trip signals are interfaced from the SLS, which receives RT signals from the RTBs. The design is shown in Figure 7.3-4.

#### 7.3.1.12 Block Turbine Bypass and Cooldown Valves

There are two ESFAS trains for block turbine bypass and cooldown valves, train A and train D.

The block turbine bypass valve signal is initiated on the following conditions:

- Low-low  $T_{avg}$  signal: This signal is present when 2-out-of-4 RCS loops indicate low-low  $T_{avg}$ .
- The manual turbine bypass block switch is selected to close (manual actuation).

The resulting block turbine bypass valve signal blocks the opening of the turbine bypass valves to the condenser. This block does not affect the turbine bypass valves to the condenser, which are referred to as the "turbine bypass cooldown valves." The block is automatically removed when the low-low  $T_{avg}$  signal goes above its setpoint.

Logic for this function is included on Figure 7.2-2 sheet 10.

The block cooldown turbine bypass signal initiates on the same low-low  $T_{avg}$  signal and manual actuation, as described above. The resulting block cooldown turbine bypass signal blocks the turbine bypass cooldown valves to the condenser. The block is automatically removed when the low-low  $T_{avg}$  signal goes above its setpoint.

The block cooldown turbine bypass signal may be manually overridden by the turbine bypass block bypass control switch (operating bypass). The override can only be actuated after the signal is actuated from low-low  $T_{avg}$ . The override is automatically reset when the low-low  $T_{avg}$  signal returns to normal. The override may be manually reset from the turbine bypass block bypass control switch. The block turbine bypass override has no effect on the block turbine bypass valve signal (i.e., it only affects the cooldown signal).

Logic for this function is included on Figure 7.2-2 sheet 10.

Block turbine bypass and cooldown valves is a non-safety function. However, block turbine bypass and cooldown valves is assumed in the safety analysis in order to prevent an excessive cooldown due to multiple valves being open. Block turbine bypass and cooldown valves cannot be completely designed as Class 1E because the equipment to execute the block turbine bypass and cooldown valves is located in the turbine building, which is seismic category II. Therefore, block turbine bypass and cooldown valves is designed as reliably as possible by applying the following design concepts:

1. Block turbine bypass and cooldown valves is designed as an "Associated Circuit" per IEEE Std 384-1992 (Reference 7.3-4) and RG 1.75 (Reference 7.3-5).
2. The cables outside electrical cabinets in the turbine building are routed in dedicated raceways.

Block turbine bypass and cooldown valves signal is interfaced from the SLS to the turbine bypass and cooldown valves. The design is shown in Figure 7.3-5.

### **7.3.2 Design Basis Information**

#### **7.3.2.1 Single Failure Criterion**

The ESF systems meet the single failure criterion through multiple redundant and independent trains for all safety functions. Out of service times for ESFAS/SLS trains are limited by the technical specifications.

The potential for spurious actuation due to single failures is minimized by the use of 2-out-of-4 logic at the system level for automatic initiation functions and 2-out-of-2 logic within each train for manual actuation functions.

#### **7.3.2.2 Quality of Components and Modules**

All safety functions of the ESF systems are implemented using Class 1E components. Non-safety functions are isolated from the ESF systems with the exception of the turbine trip outputs, which are treated as associated circuits as described in Subsection 7.3.1.11.

#### **7.3.2.3 Independence**

The independence and separation within the ESFAS and SLS is as described in Subsection 7.1.3.4.

#### **7.3.2.4 Defense-In-Depth and Diversity**

Refer to Subsections 7.3.1.9 and 7.1.3.1.

#### **7.3.2.5 System Testing and Inoperable Surveillance**

Refer to Subsection 7.1.3.14.



---

#### 7.3.2.6 Use of Digital Systems

All ESF systems rely on digital systems. Refer to Subsections 7.1.3.8 and 7.1.3.17.

#### 7.3.2.7 Setpoint Determination

The safety functions performed by the ESF systems rely primarily on sensor inputs and setpoints from the RPS. In addition, setpoints for ESF systems meet the requirements of RG 1.105 (Reference 7.3-6). Refer to Subsection 7.2.2.7. The instrument accuracy, setpoint, and response time described in Table 7.3-4 are determined by applying the methodology. Technical Report MUAP-09022 (Reference 7.3-11) provides more detail description for setpoint methodology and channel uncertainty calculations for ESF functions. Setpoints determination for inputs interfaced directly into the ESFAS, such as under voltage inputs for emergency load sequencing, utilize the same setpoint determination methodology or a setpoint methodology that is specific to the instrument, as recommend by the original equipment manufacturer (OEM).

#### 7.3.2.8 Equipment Qualification

Refer to Subsection 7.1.3.7 for details.

### 7.3.3 Analysis

Detailed compliance to the GDC, IEEE Std 603-1991 (Reference 7.3-7) and IEEE Std 7-4.3.2-2003 (Reference 7.3-8) is described in MUAP-07004 Section 3.0, Appendix A and B.

#### 7.3.3.1 FMEA

The FMEA method for ESF actuation in the PSMS is identical to that used in the RPS, as described in Subsection 7.2.3.1. The safe state for ESFAS/SLS is “as-is.”

The FMEA for ESF actuation in PSMS is provided in Table 7.3-7. Figure 7.3-6 shows the configuration of system diagram for ESFAS as used in the FMEA table. Train A is illustrated as the representative features in this figure, while the PSMS consists of four trains.

#### 7.3.3.2 Safety Analysis

The ESF system design requirements such as response time and setpoint determination, are considered and reflected in the safety analysis, contained in Chapter 15. The response time, instrument accuracy, and setpoint as shown in Table 7.3-4, meet the safety analysis assumptions.

Chapter 15 analysis for US-APWR addresses AOOs and PAs.

The analysis for additional postulate failures are described as follows:

- Loss of cooling water to vital equipment: The US-APWR has four divisions of safety-related cooling water, corresponding to the four divisions of safety-related ESF equipment. These four divisions are controlled by the PSMS. Therefore,

---

loss of a single division of cooling water does not prevent accomplishing the safety function.

- Loss of plant instrument air: There is no reliance on plant instrument air for any safety functions. The loss of plant instrument air will result in the loss of MFW. This condition is considered in the safety analysis described in Chapter 15.
- Loss of power source: Any one division of subsystems in the PSMS is supplied power from redundant power sources. Therefore, loss of a single power source does not prevent accomplishing the safety function. The loss of power source may result in a transient condition. This condition is considered in the safety analysis described in Chapter 15.

#### 7.3.3.3 Test and Inspection

The ESF systems meet the testing requirements of IEEE Std 338-1987 (Reference 7.3-9), as discussed in Subsection 7.1.3.14. The initial and subsequent test intervals are specified in the technical specifications. Periodic testing conforms to RG 1.22 (Reference 7.3-10), as discussed in Subsection 7.1.3.14.

#### 7.3.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 7.3(1) Deleted

#### 7.3.5 References

- 7.3-1 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.
- 7.3-2 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.3-3 Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.
- 7.3-4 Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std 384-1992.
- 7.3-5 Physical Independence of Electric Systems, Regulatory Guide 1.75 Revision 3, February 2005.
- 7.3-6 Setpoint for Safety-Related Instrumentation, Regulatory Guide 1.105 Revision 3, December 1999.
- 7.3-7 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.

- 
- 7.3-8      IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.
- 7.3-9      Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std 338-1987.
- 7.3-10     Periodic Testing of Protection System Actuation Functions, Regulatory Guide 1.22 Revision 0, February 1972.
- 7.3-11     Function Assignment Analysis for Safety Logic System, MUAP-09020-P Rev.1 (Proprietary) and MUAP-09020-NP Rev.1 (Non-Proprietary), March 2010.
- 7.3-12     US-APWR Instrument Setpoint Methodology, MUAP-09022-P Rev.1 (Proprietary) and MUAP-09022-NP Rev.1 (Non-Proprietary), April 2010.

**Table 7.3-1 Interface between ESFAS and Other Systems (for Figure 7.3-2)**

Interface Signals	Example of Signals
(a) Signals from RPS	ECCS actuation signals
(b) ESF actuation signals to RPS	ECCS actuation signals
(c) Operation signals from safety VDU	Manual ECCS actuation signal, ECCS reset signals
(d) Signals to safety VDU	Status signals
(e) Operation signals from operational VDU	Manual ECCS actuation signal, ECCS reset signals
(f) Signals to operational VDU	Status signals
(g) ESF manual actuation signals from OC	Manual ECCS actuation signals
(h) Signals to SLS	ECCS actuation signal, ECCS/LOOP sequence signals
(i) Component status signals from SLS	Safety component status signals
(j) Signals from Class 1E switchgear	Undervoltage signals
(k) Control signals to reactor control system	Control rod withdrawal block signals
(l) Control signals from reactor control system	Area monitor signals
(m) Signals to other non-safety systems	Generator trip signals
(n) Signals from other non-safety systems	MFW pump trip signals, undervoltage signals

**Table 7.3-2 Interface between SLS and Other Systems (for Figure 7.3-3)**

<b>Interface Signals</b>	<b>Example of Signals</b>
(a) Interlock signals from reactor control system	Non-safety interlock signals
(b) Signals to reactor control system	Safety component status signals
(c) Signals from ESFAS	ECCS actuation signal, ECCS/LOOP sequence signals
(d) Signals to ESFAS	Safety component status signals
(e) Interlock signals from RPS	Reactor coolant pressure signal, CCW surge tank water level for Interlocks
(f) Manual operation signals from safety VDU	Start/stop demand signals, open/close demand signals
(g) Information signals to safety VDU	Operation demand result signals, safety component status signals
(h) Operation signals from operational VDU	Start/stop demand signals, open/close demand signals
(i) Information signals to operational VDU	Component status signals
(j) Signals from safety local contact	MOV limit switch signals, charging pump bearing hydraulic low signals
(k) Interlock signals to BOP control system	Interlock signals
(l) Interlock signals from BOP control system	Turbine driven EFW pump reset completion signals
(m) Turbine trip signals from turbine protection system	Turbine trip signals
(n) Signals to safety control unit or solenoid valve	Start/Stop demand signals, open/close demand signals
(o) Status signals from safety control unit	Component status signals
(p) Signals to non-safety control unit or solenoid valve	Start/Stop demand signals, open/close demand signals
(q) Status signals to DAS	EFW pump start status signals
(r) Non-safety control signals from DAS	Operation signals

**Table 7.3-3 Engineered Safety Features Actuation Signals (Sheet 1 of 3)**

Actuation Signal	Number of Sensors, Switches, or Signals	Actuation Logic	Permissives and Bypasses
			For Permissives and Bypasses Refer Table 7.2-4
1. Emergency Core Cooling System - Logic diagram Figure 7.2-2 Sheet 11			
Low Pressurizer Pressure	4 Pressure Sensors (Shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line	2/4 per Steam Line	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
High Containment Pressure	4 Pressure Sensors	2/4	None
Manual Actuation	1 Switch per Train	1/1	Can be manually reset to block re-initiation of ECCS signal while P-4 is active. This block is automatically removed when P-4 becomes inactive.
2. Containment Spray - Logic diagram Figure 7.2-2 Sheet 12			
High-3 Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual Actuation	2 Switches per Train	2/2	None
3. Main Control Room Isolation - Logic diagram Figure 7.2-2 Sheet 12			
MCR Outside Air Intake Radiation	2 Gas Radiation Detectors	1/2	None
	2 Iodine Radiation Detectors	1/2	None
	2 Particulate Radiation Detectors	1/2	None
ECCS Actuation	Valid ECCS Signal	1/1	None
Manual Actuation	1 Switch per Train	1/1	None
4. Containment Purge Isolation - Logic diagram Figure 7.2-2 Sheet 12			
Containment High Range Area Radiation	4 Radiation Detectors	2/4	None
ECCS Actuation	Valid ECCS signal	1/1	None
Manual Containment Isolation	1 Switch per Train	1/1	None
Manual CS Actuation	2 Switches per Train	2/2	None
5. Containment Isolation Phase A - Logic diagram Figure 7.2-2 Sheet 12			
ECCS Actuation	Valid ECCS Signal	1/1	None
Manual Actuation	1 Switch per train	1/1	None

**Table 7.3-3 Engineered Safety Features Actuation Signals (Sheet 2 of 3)**

Actuation Signal	Number of Sensors, Switches, or Signals	Actuation Logic	Permissives and Bypasses
			For Permissives and Bypasses Refer Table 7.2-4
6. Containment Isolation Phase B - Logic diagram Figure 7.2-2 Sheet 12			
High-3 Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual CS Actuation	2 Switches per train	2/2	None
7A. Main Feedwater Regulation Valve Closure Figure 7.2-2 Sheet 10			
Low T <sub>avg</sub> coincident with RT (P-4)	4 Temperature Sensors (T <sub>avg</sub> ) (Shared with RT)	2/4	None
	1Signal per Train (P-4)	1/1	None
7B. Main Feedwater Isolation Figure 7.2-2 Sheet 10			
High-High SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	None
ECCS Actuation	Valid ECCS signal	1/1	None
Manual Actuation	2 Switches	1/2 per Valve	None
8. Main Steam Line Isolation - Logic diagram Figure 7.2-2 Sheet 9			
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line (Shared with ECCS)	2/4 per Steam Line	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
High Main Steam Line Pressure Negative Rate		2/4 per Steam Line	Operating bypass of unblock permitted while P-11 is active, automatically blocked by inactive P-11.
High-High Containment Pressure	4 Pressure Sensors (Shared with ECCS)	2/4	None
Manual Actuation	2 Switches	1/2 per Valve	None
9. Emergency Feedwater Actuation - Logic diagram Figure 7.2-2 Sheet 7			
Low SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	None
ECCS actuation	Valid ECCS signal	1/1	None
LOOP signal	Valid Blackout signal	1/1	None
MFW Pumps tripped	All pumps trip signal	1/1	None
Manual Actuation	1 Switch per train	1/1	None

**Table 7.3-3 Engineered Safety Features Actuation Signals (Sheet 3 of 3)**

Actuation Signal	Number of Sensors, Switches, or Signals	Actuation Logic	Permissives and Bypasses
			For Permissives and Bypasses Refer Table 7.2-4
10 Emergency Feedwater Isolation - Logic diagram Figure 7.2-2 Sheet 8			
High SG Water Level	4 Level Sensors per SG (Shared with RT)	2/4 per SG	Permitted while P-4 is active Automatically blocked while steam line pressure is low Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Low Main Steam Line Pressure	4 Pressure Sensors per Steam Line (Shared with ECCS)	2/4 per Steam Line	Automatically blocked while EFW Isolation signal from other SG is initiated.
Manual Actuation	2 Switches per SG	1/2 per SG	None
11. CVCS Isolation - Logic Diagram Figure 7.2-2 Sheet 6			
High Pressurizer Water Level	4 Level Sensors (Shared with RT)	2/4	Operating bypass permitted while P-11 is active, automatically unbypassed by inactive P-11.
Manual Actuation	1 Switch per train	1/1	None



**Table 7.3-4 Engineered Safety Features Actuation Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 1 of 2)**

ESF Function	Variables to be monitored	Range of Variables	Instrument Accuracy*1,2	Response Time*1,2,3	Setpoint*4
<b>Emergency Core Cooling System Actuation</b>					
(a) Low Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	3.0 sec	1765 psig
(b) Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
(c) High Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	6.8 psig
<b>Containment Spray</b>					
High-3 Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	34.0 psig
<b>Main Control Room Isolation</b>					
High MCR Outside Air Intake Radiation	MCR Gas Radiation	1E-7 to 1E-2 $\mu\text{Ci/cc}$	6% of span	60 sec	2E-6 $\mu\text{Ci/cc}$
	MCR Iodine Radiation	1E-11 to 1E-5 $\mu\text{Ci/cc}$	6% of span	60 sec	8E-10 $\mu\text{Ci/cc}$
	MCR Particulate Radiation	1E-12 to 1E-7 $\mu\text{Ci/cc}$	6% of span	60 sec	8E-10 $\mu\text{Ci/cc}$
<b>Containment Purge Isolation</b>					
High Containment High Range Area Radiation	Containment Area Radiation	1 to 1E+7 R/h	6% of span	15 sec	100 R/h
<b>Main Feedwater Isolation</b>					
(a) High-High SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	3.0 sec	70% of span
(b) Low $T_{\text{avg}}$ coincident with RT (P-4)	Reactor Coolant Temperature	530 to 630 °F	2.0 °F	8.0 sec	564 °F
<b>Main Steam Line Isolation</b>					
(a) Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
(b) High Main Steam Line Pressure Negative Rate	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	100 psi
(c) High-High Containment Pressure	Containment Pressure	-7 to 80 psig	2.8% of span	3.0 sec	22.7 psig

**Table 7.3-4 Engineered Safety Features Actuation Variables, Ranges, Accuracies, Response Times, and Setpoints (Nominal) (Sheet 2 of 2)**

ESF Function	Variables to be monitored	Range of Variables	Instrument Accuracy* <sup>1,2</sup>	Response Time* <sup>1,2,3</sup>	Setpoint* <sup>4</sup>
<b>Emergency Feedwater Actuation</b>					
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	3.0 sec	13% of span
LOOP Signal	LOOP Signal	0 to 8.25 kV	1.5% of span	3.0 sec	4727 V with ≤ 0.8 sec time delay
<b>Emergency Feedwater Isolation</b>					
(a)High SG Water Level	SG Water Level	0 to 100% of span (narrow Range taps)	3% of span	3.0 sec	50% of span
(b)Low Main Steam Line Pressure	Main Steam Line Pressure	0 to 1400 psig	3% of span	3.0 sec	525 psig
<b>CVCS Isolation</b>					
High Pressurizer Water Level	Pressurizer Water Level	0 to 100% of span	3% of span	3.0 sec	92% of span

Note:

1. Instrument accuracy and response time calculation methodology refer to Subsection 7.2.2.7.
2. Instrument accuracies and response times will be decided to take into account the specification of instruments.
3. Additional time during LOOP is referred to Chapter 8.
4. Setpoints will be adjusted to compensate for loop accuracy.

**Table 7.3-5 ESF Actuation System - Train Level Manual Control  
(Conventional and Software Switches) (Sheet 1 of 2)**

<b>Manual Control<sup>*1</sup></b>	<b>Trains</b>				<b>Fig 7.2-2</b>
Manual ECCS Actuation Train A	A				Sheet 11
Manual ECCS Actuation Train B		B			Sheet 11
Manual ECCS Actuation Train C			C		Sheet 11
Manual ECCS Actuation Train D				D	Sheet 11
Manual EFW Actuation Train A	A				Sheet 7
Manual EFW Actuation Train B		B			Sheet 7
Manual EFW Actuation Train C			C		Sheet 7
Manual EFW Actuation Train D				D	Sheet 7
Manual SG A EFW Isolation (A EFW Control Valve)	A				Sheet 8
Manual SG A EFW Isolation (A EFW Isolation Valve)		B			Sheet 8
Manual SG B EFW Isolation (B EFW Control Valve)		B			Sheet 8
Manual SG B EFW Isolation (B EFW Isolation Valve)	A				Sheet 8
Manual SG C EFW Isolation (C EFW Control Valve)			C		Sheet 8
Manual SG C EFW Isolation (C EFW Isolation Valve)				D	Sheet 8
Manual SG D EFW Isolation (D EFW Control Valve)				D	Sheet 8
Manual SG D EFW Isolation (D EFW Isolation Valve)			C		Sheet 8
Manual Main Steam Line Isolation #1 <sup>*2</sup>	A				Sheet 9
Manual Main Steam Line Isolation #2 <sup>*2</sup>				D	Sheet 9
Manual MFW Isolation #1	A				Sheet 10
Manual MFW Isolation #2				D	Sheet 10
Manual Containment Isolation Phase A #1	A				Sheet 12
Manual Containment Isolation Phase A #2				D	Sheet 12
Manual CS Actuation Train A # 1 <sup>*3</sup>	A				Sheet 12
Manual CS Actuation Train A # 2 <sup>*3</sup>	A				Sheet 12
Manual CS Actuation Train B # 1 <sup>*3</sup>		B			Sheet 12
Manual CS Actuation Train B # 2 <sup>*3</sup>		B			Sheet 12
Manual CS Actuation Train C # 1 <sup>*3</sup>			C		Sheet 12
Manual CS Actuation Train C # 2 <sup>*3</sup>			C		Sheet 12
Manual CS Actuation Train D # 1 <sup>*3</sup>				D	Sheet 12
Manual CS Actuation Train D # 2 <sup>*3</sup>				D	Sheet 12
Manual MCR Isolation Train A	A				Sheet 12
Manual MCR Isolation Train B		B			Sheet 12

**Table 7.3-5 ESF Actuation System - Train Level Manual Control  
(Conventional and Software Switches) (Sheet 2 of 2)**

Manual Control* <sup>1</sup>	Trains				Fig 7.2-2
Manual MCR Isolation Train C			C		Sheet 12
Manual MCR Isolation Train D				D	Sheet 12
Manual CVCS Isolation #1	A				Sheet 6
Manual CVCS Isolation #2				D	Sheet 6

Note:

1. Manual controls are located in the MCR unless otherwise noted.
2. Also closes the bypass valve in parallel with the associated main steam line isolation valve.
3. Actuation will occur only if the two associated control switches are operated simultaneously.

**Table 7.3-6 ESF Actuation System - Manual Reset and Bypass  
(Software Switches) (Sheet 1 of 2)**

<b>Manual Control*<sup>1</sup></b>	<b>Trains</b>				<b>Fig 7.2-2</b>
Manual Reset for EFW Actuation Train A	A				Sheet 7
Manual Reset for EFW Actuation Train B		B			Sheet 7
Manual Reset for EFW Actuation Train C			C		Sheet 7
Manual Reset for EFW Actuation Train D				D	Sheet 7
Manual Bypass Control for EFW Isolation Train A	A				Sheet 8
Manual Bypass Control for EFW Isolation Train B		B			Sheet 8
Manual Bypass Control for EFW Isolation Train C			C		Sheet 8
Manual Bypass Control for EFW Isolation Train D				D	Sheet 8
Manual Reset for Main Steam Line Isolation #1	A				Sheet 9
Manual Reset for Main Steam Line Isolation #2				D	Sheet 9
Manual Reset & Block ECCS Actuation Train A* <sup>2</sup>	A				Sheet 11
Manual Reset & Block ECCS Actuation Train B* <sup>2</sup>		B			Sheet 11
Manual Reset & Block ECCS Actuation Train C* <sup>2</sup>			C		Sheet 11
Manual Reset & Block ECCS Actuation Train D* <sup>2</sup>				D	Sheet 11
Manual Bypass Control for ECCS Train A on Low Pressurizer Pressure	A				Sheet 11
Manual Bypass Control for ECCS Train B on Low Pressurizer Pressure		B			Sheet 11
Manual Bypass Control for ECCS Train C on Low Pressurizer Pressure			C		Sheet 11
Manual Bypass Control for ECCS Train D on Low Pressurizer Pressure				D	Sheet 11
Manual Bypass Control for CVCS Isolation Train A	A				Sheet 6
Manual Bypass Control for CVCS Isolation Train B		B			Sheet 6
Manual Bypass Control for CVCS Isolation Train C			C		Sheet 6
Manual Bypass Control for CVCS Isolation Train D				D	Sheet 6
Manual Reset for CVCS Isolation #1	A				Sheet 6
Manual Reset for CVCS Isolation #2				D	Sheet 6
Manual Reset for EFW Isolation of Loop A (EFW Control Valve)	A				Sheet 8
Manual Reset for EFW Isolation of Loop B (EFW Control Valve)		B			Sheet 8
Manual Reset for EFW Isolation of Loop C (EFW Control Valve)			C		Sheet 8
Manual Reset for EFW Isolation of Loop D (EFW Control Valve)				D	Sheet 8
Manual Reset for EFW Isolation of Loop A (EFW Isolation Valve)		B			Sheet 8
Manual Reset for EFW Isolation of Loop B (EFW Isolation Valve)	A				Sheet 8
Manual Reset for EFW Isolation of Loop C (EFW Isolation Valve)				D	Sheet 8

**Table 7.3-6 ESF Actuation System - Manual Reset and Bypass  
(Software Switches) (Sheet 2 of 2)**

Manual Control* <sup>1</sup>	Trains				Fig 7.2-2
Manual Reset for EFW Isolation of Loop D (EFW Isolation Valve)			C		Sheet 8
Manual Bypass Control for ECCS Actuation Train A on Low Main Steam Line Pressure	A				Sheet 9
Manual Bypass Control for ECCS Actuation Train B on Low Main Steam Line Pressure		B			Sheet 9
Manual Bypass Control for ECCS Actuation Train C on Low Main Steam Line Pressure			C		Sheet 9
Manual Bypass Control for ECCS Actuation Train D on Low Main Steam Line Pressure				D	Sheet 9
Manual Bypass Control for MFW Isolation Train A	A				Sheet 10
Manual Bypass Control for MFW Isolation Train B		B			Sheet 10
Manual Bypass Control for MFW Isolation Train C			C		Sheet 10
Manual Bypass Control for MFW Isolation Train D				D	Sheet 10
Manual Reset for MFW Regulation Valve Closure #1	A				Sheet 10
Manual Reset for MFW Regulation Valve Closure #2				D	Sheet 10
Manual Reset for MFW Isolation #1	A				Sheet 10
Manual Reset for MFW Isolation #2				D	Sheet 10
Manual Reset for CS Actuation Train A	A				Sheet 12
Manual Reset for CS Actuation Train B		B			Sheet 12
Manual Reset for CS Actuation Train C			C		Sheet 12
Manual Reset for CS Actuation Train D				D	Sheet 12
Manual Reset for Containment Isolation Phase B Train A	A				Sheet 12
Manual Reset for Containment Isolation Phase B Train B		B			Sheet 12
Manual Reset for Containment Isolation Phase B Train C			C		Sheet 12
Manual Reset for Containment Isolation Phase B Train D				D	Sheet 12
Manual Reset for Containment Isolation Phase A #1	A				Sheet 12
Manual Reset for Containment Isolation Phase A #2				D	Sheet 12
Manual Reset for Containment Purge Isolation #1	A				Sheet 12
Manual Reset for Containment Purge Isolation #2				D	Sheet 12
Manual Reset for MCR Isolation Train A	A				Sheet 12
Manual Reset for MCR Isolation Train B		B			Sheet 12
Manual Reset for MCR Isolation Train C			C		Sheet 12
Manual Reset for MCR Isolation Train D				D	Sheet 12

Note:

1. Manual controls are located in the MCR unless otherwise noted.
2. Block permitted with active P-4
3. All bypass controls (operating bypasses) permitted with active P-11, and automatically unbypassed by inactive P-11.

Table 7.3-7 FMEA for ESF Actuation in PSMS (for Figure 7.3-6) (Sheet 1 of 4)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
Sensor	Fail high	Self-diagnostic alarm from the affected RPS train. Annunciation of partial actuation from the affected RPS train. Cross channel comparison.	Bistable changes to actuation state and partial actuation signal is generated in the affected RPS train.	ESF actuation logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation. If unrestricted bypass of one instrument channel has already been executed in another train, ESF actuation logic becomes 1-out-of-2 due to the sensor failure. Remaining two trains provide ESF actuation.
	Fail low	Self-diagnostic alarm from the affected RPS train. Annunciation of partial actuation from the affected RPS train. Cross channel comparison.	Bistable changes to actuation state and partial actuation signal is generated in the affected RPS train.	ESF actuation logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation. If unrestricted bypass of one instrument channel has already been executed in another train, ESF actuation logic becomes 1-out-of-2 due to the sensor failure. Remaining two trains provide ESF actuation.
	Fail as is	Cross channel comparison.	Bistable does not change to actuation state in the affected RPS train when process reaches actuation level.	ESF actuation logic becomes 2-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation.

Table 7.3-7 FMEA for ESF Actuation in PSMS (for Figure 7.3-6) (Sheet 2 of 4)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
<b>RPS</b> Input part (from Sensor)	Fail high	Self-diagnostic alarm from the affected RPS train. Annunciation of partial actuation from the affected RPS train. Cross channel comparison.	Bistable changes to actuation state and partial actuation signal is generated in the affected RPS train.	ESF actuation logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation. If unrestricted bypass of one instrument channel has already been executed in another train, ESF actuation logic becomes 1-out-of-2 due to the sensor failure. Remaining two trains provide ESF actuation.
	Fail low	Self-diagnostic alarm from the affected RPS train. Annunciation of partial actuation from the affected RPS train. Cross channel comparison.	Bistable changes to actuation state and partial actuation signal is generated in the affected RPS train.	ESF actuation logic becomes 1-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation.
	Fail as is	Cross channel comparison.	Bistable does not change to actuation state in the affected RPS train when process reaches actuation level.	ESF actuation logic becomes 2-out-of-3 due to the sensor failure. Remaining three trains provide ESF actuation.
<b>RPS</b> Processing part (in RPS)	No data output	Self-diagnostic alarm from the affected RPS train. Annunciation of communication error from other RPS trains.	Partial actuation signal does not reach to other RPS trains when process reaches actuation level.	ESF actuation logic becomes 2-out-of-3 due to the processing failure. Remaining three trains provide ESF actuation.
	Spurious Status Change	Ractor Trip Annunciation of the affected RPS train	The affected RPS train emits Reactor Trip Signal.	Ractor Trip logic becomes 1-out-of-3 due to the spurious signal. Remaining three trains provide ESF actuation.
<b>RPS</b> Communication part (between RPS trains)	No data output	Annunciation of communication error from the affected other RPS trains.	Partial actuation signal does not reach to other RPS trains when process reaches actuation level. Trip signals from other RPS trains dose not reach to the affected train when process reaches actuation level.	ESF actuation logic becomes 2-out-of-3 due to the communication failure. Remaining three trains provide ESF actuation.



Table 7.3-7 FMEA for ESF Actuation in PSMS (for Figure 7.3-6) (Sheet 3 of 4)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
<b>RPS</b> Communication part (to ESFAS)	No data output	Annunciation of communication error from the affected ESFAS trains.	Partial actuation signal does not reach to the ESFAS trains when process reaches actuation level.	ESF actuation logic becomes 2-out-of-3 due to the communication failure. Remaining three trains provide ESF actuation.
	No data output	Self-diagnostic alarm in the affected ESFAS train.	One parallel redundant part fails. Another parallel redundant part process the signal.	No failure effect to ESF function.
<b>ESFAS</b> Communication part (from RPS)	No data output	Self-diagnostic alarm in the affected ESFAS train.	One parallel redundant part fails. Another parallel redundant part process the signal.	No failure effect to ESF function.
	No data output	Self-diagnostic alarm in the affected ESFAS train.	One parallel redundant part fails. Another parallel redundant part process the signal.	No failure effect to ESF function.
<b>ESFAS</b> Processing part (in ESFAS)	Spurious Status Change	ESF Actuation Annunciation of the affected ESFAS train	The affected train actuates ESF function.	Remaining three trains provide appropriate ESF actuation.
	No data output	Self-diagnostic alarm in the affected SLS train.	One parallel redundant part fails. Change to another parallel redundant part.	No failure effect to ESF function.
<b>ESFAS</b> Communication part (to SLS)	No data output	Self-diagnostic alarm in the affected ESFAS and SLS train.	One train ESF does not actuate when process reaches actuation level.	Three trains of ESF can be actuated due to the communication failure. Remaining three trains provide ESF actuation.
	Fail to dis- connection	Self-diagnostic alarm in the affected ESFAS and SLS train.	There is no impact for a single disconnection due to its ring configuration of the safety bus.	No failure effect to ESF function.
<b>SLS</b> Communication part (from ESFAS)	No data output	Self-diagnostic alarm in the affected SLS train.	One parallel redundant part fails. Another parallel redundant part process the signal.	No failure effect to ESF function.

Table 7.3-7 FMEA for ESF Actuation in PSMS (for Figure 7.3-6) (Sheet 4 of 4)

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
<b>SLS</b> Processing part (in SLS)	No data output	Self-diagnostic alarm.	One parallel redundant part fails. Another parallel redundant part process the signal.	No failure effect to ESF function.
	Spurious Status Change	Refer to MUAP-09020 "Functional Assignment Analysis for Safety I&C System"	Refer to MUAP-09020 "Functional Assignment Analysis for Safety I&C System"	Refer to MUAP-09020 "Functional Assignment Analysis for Safety I&C System"
<b>SLS</b> Output part (to Component)	Spurious change status	Manual periodic test or plant system disturbance.	One train ESF changes their status.  (If the change of their status affects plant disturbances, appropriate design such as duplicated output module are adopted.)	One train of ESF can be actuated due to the output failure. All trains can still provide ESF actuation. The periodic test is administrated to detect the failure for components whose spurious actuation does not cause a plant disturbance.
	Fail as is	Manual periodic test.	One train ESF does not actuate when process reaches actuation level.	One train of ESF can fail due to the output failure. The remaining one or three trains provide ESF actuation, depending on the two or four train mechanical system configuration. For four train mechanical systems, if another train is being tested, two trains provide ESF actuation. The periodic test is administrated to detect the failure.
Unit Bus Inside part of PSMS	No data output	Annunciation of communication error	No failure effect to ESF function.	No failure effect to ESF function.
Unit Bus Outside part of PSMS	Fail to dis- connection	Annunciation of communication error	There is no impact for a single disconnection due to its ring configuration of the safety bus.	No failure effect to ESF function.

Note:

- One train failure is considered for each component except for non-safety unit bus.

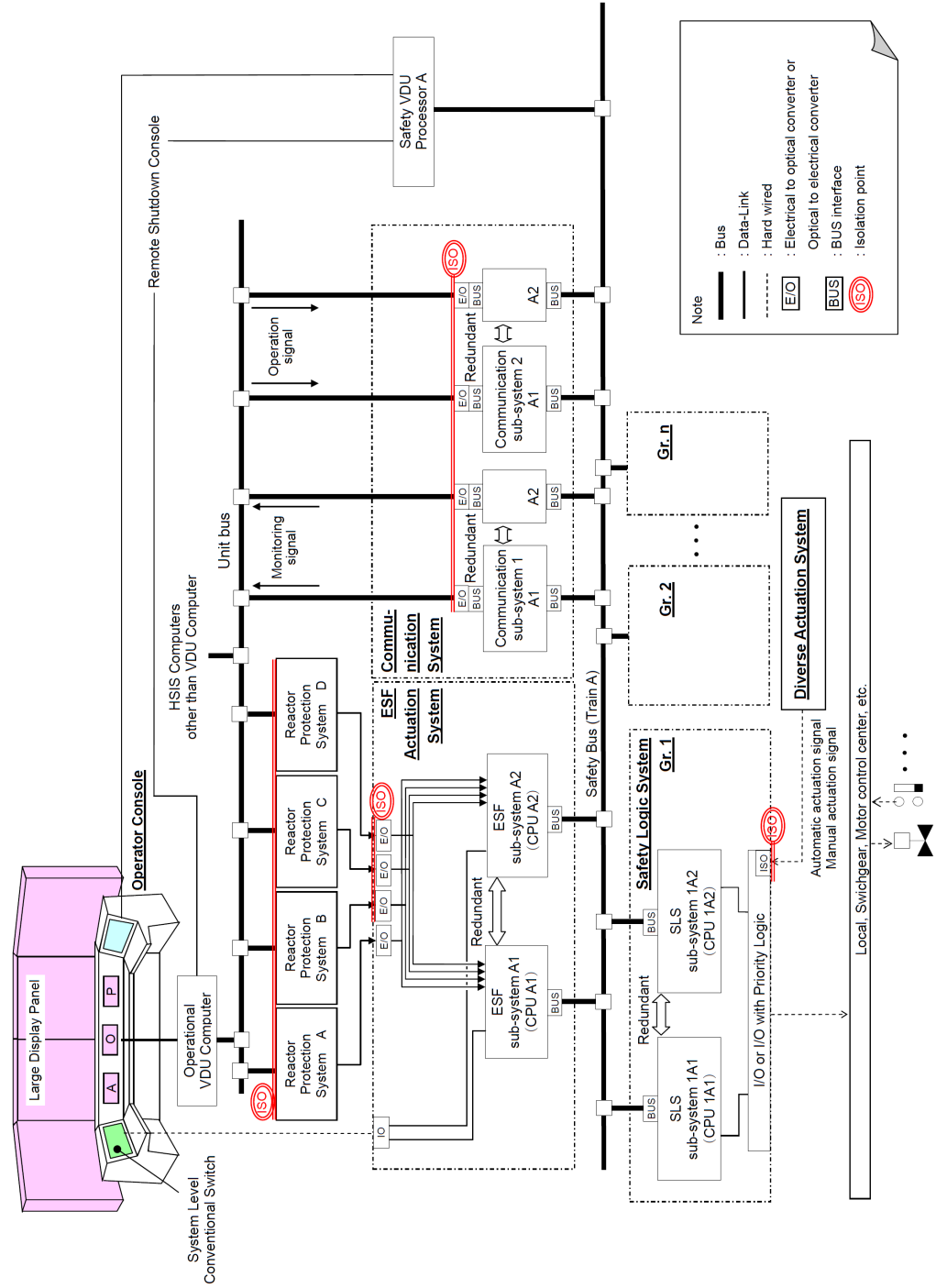


Figure 7.3-1 Configuration of Engineered Safety Features Actuation System and Safety Logic System

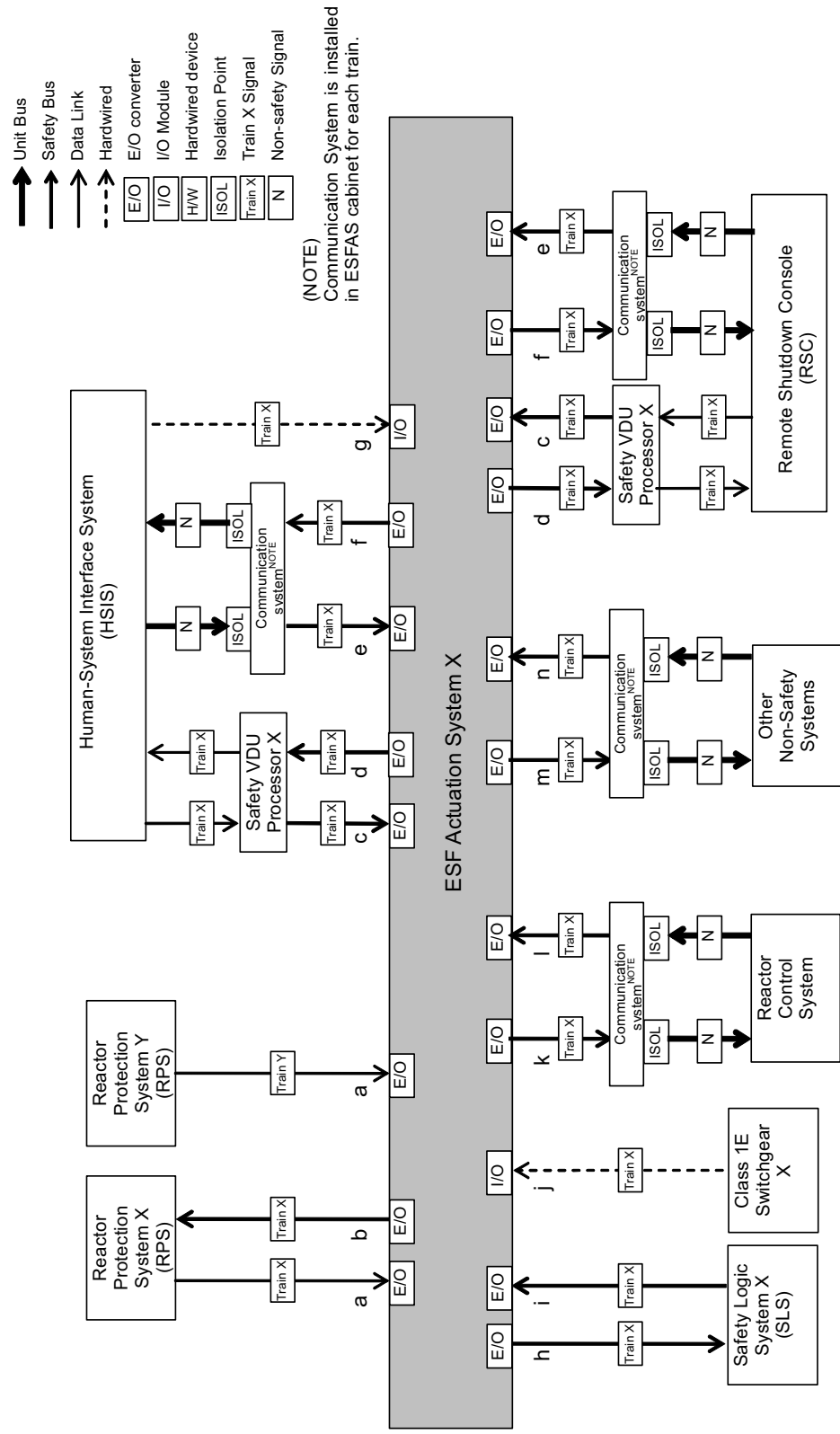


Figure 7.3-2 Interface between ESFAS and Other Systems (for Table 7.3-1)

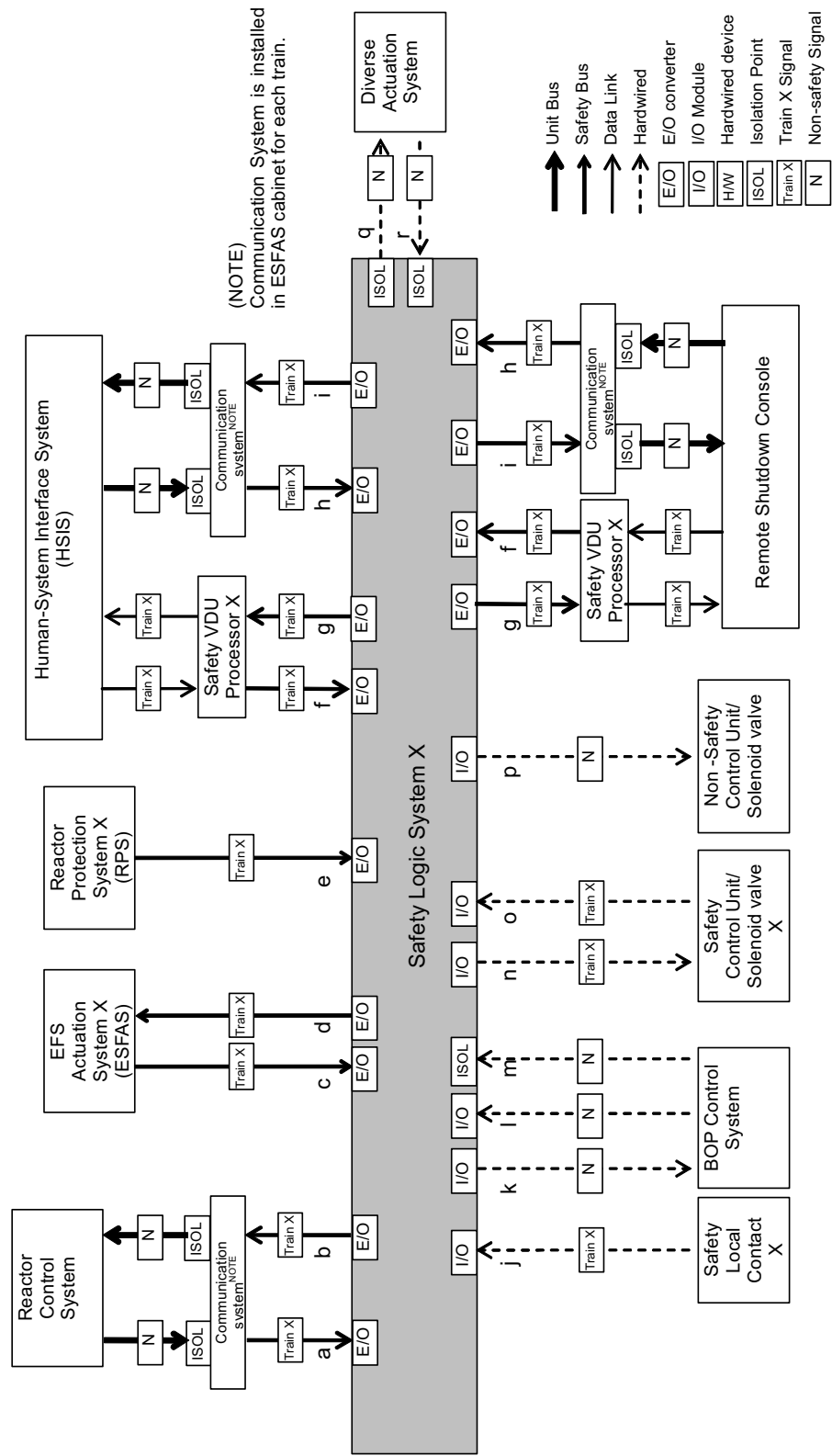


Figure 7.3-3 Interface between SLS and Other Systems (for Table 7.3-2)

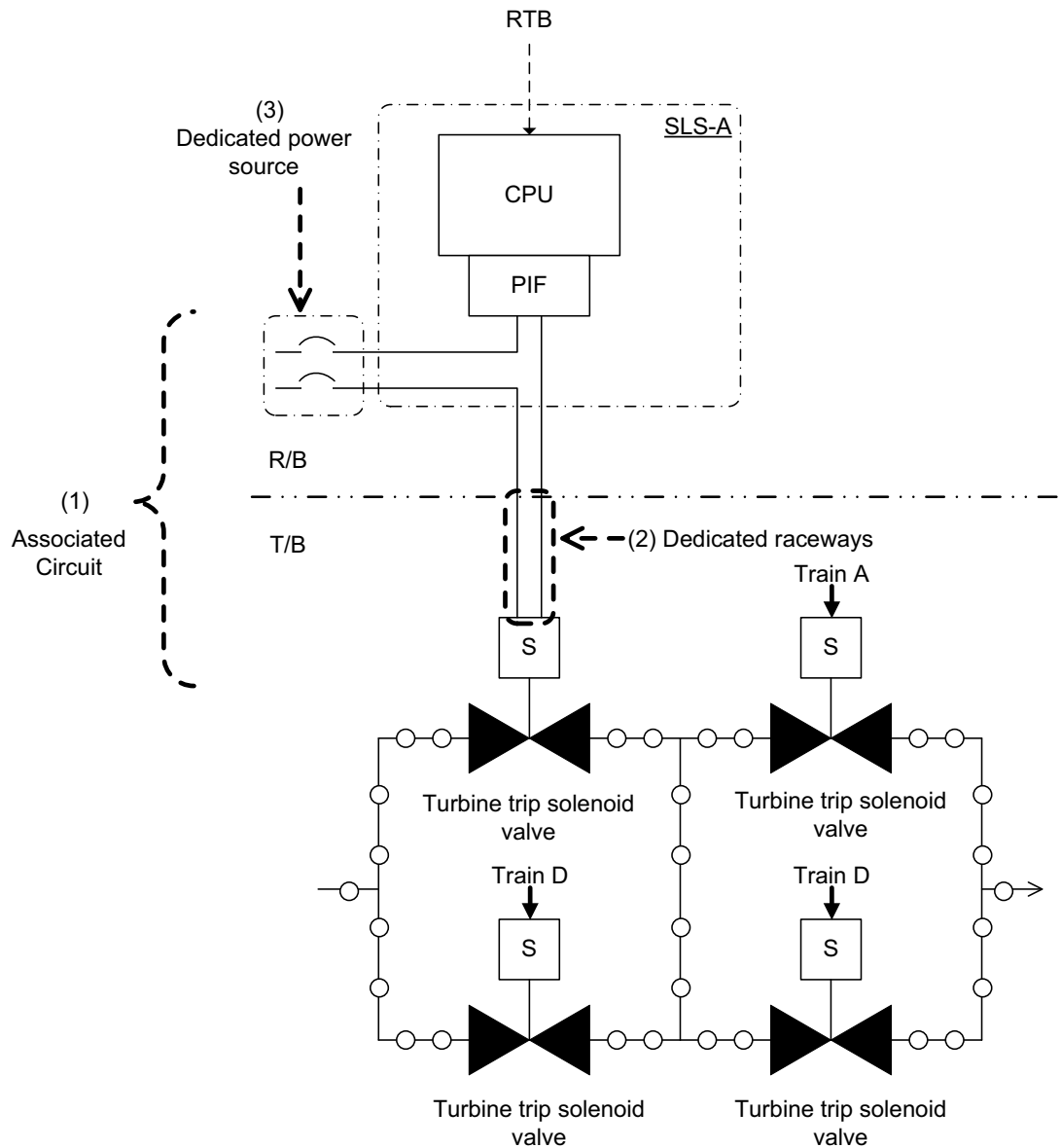


Figure 7.3-4 Summary of Design Concept for Turbine Trip on Reactor Trip



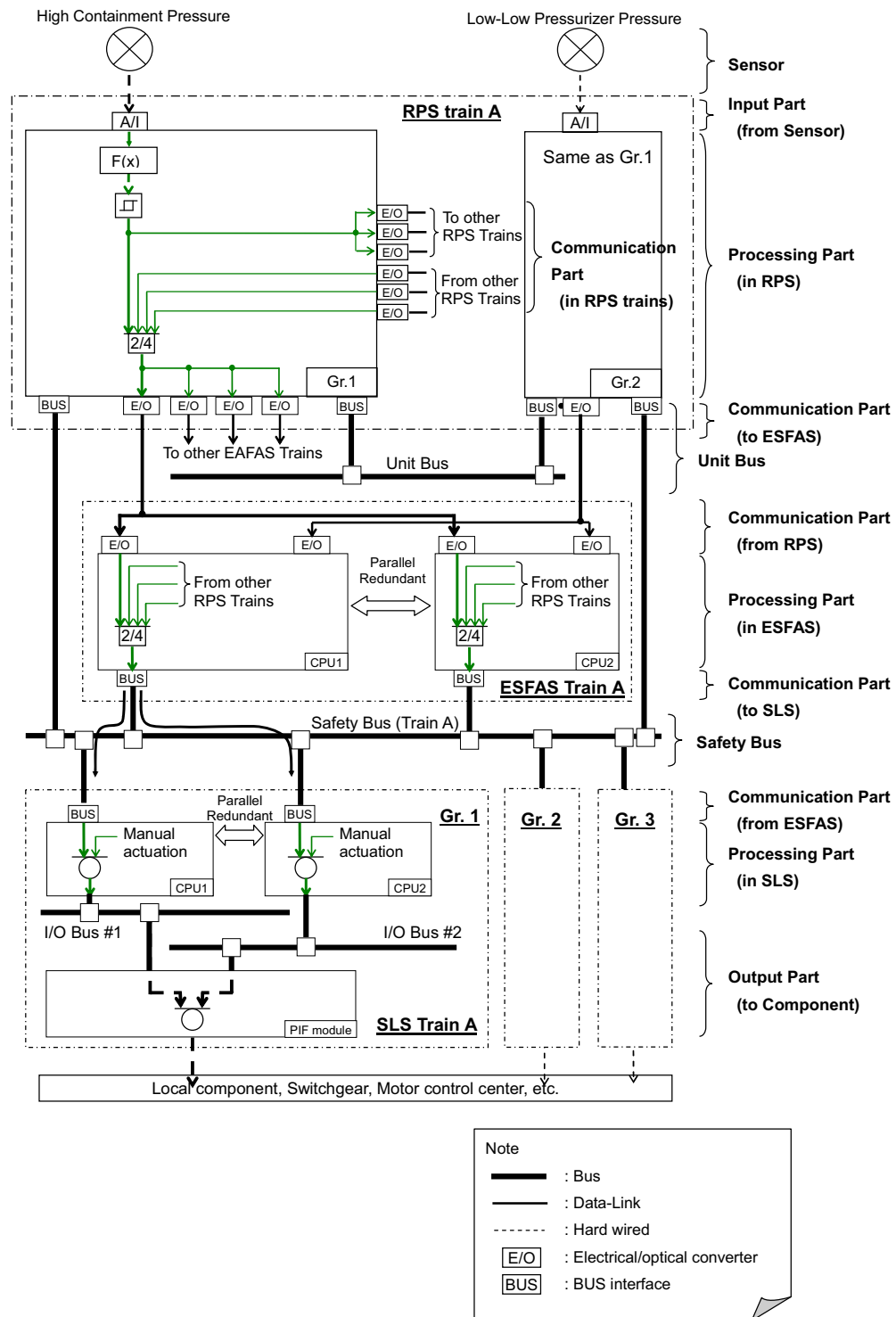


Figure 7.3-6 Configuration of ESF System for Use in FMEA (for Table 7.3-7)



## **7.4 Systems Required for Safe Shutdown**

### **7.4.1 System Description**

#### **7.4.1.1 Normal and Safe Shutdown**

Plant operators can achieve normal shutdown (using both safety-related and non safety-related systems) from the MCR or RSR. Safe shutdown is achieved using only safety-related I&C systems.

The systems necessary for both normal and safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Second, the systems provide residual heat removal (RHR) capability to maintain adequate core cooling. Boration capability is also provided to compensate for xenon decay and to maintain the required core shutdown margin.

Manual controls through the safety VDUs or operational VDUs on the OC in the MCR, or at the RSC in the RSR, allow operators to transition to and maintain hot standby, transition to cold shutdown, and maintain cold shutdown. If the MCR is uninhabitable, controls and monitoring of shutdown functions can be performed from the RSR, which is located outside the MCR fire area in the reactor building.

#### **7.4.1.2 Normal and Safe Shutdown Plant Systems**

There are no plant systems specifically dedicated to achieve normal and safe shutdown systems. However, there are number of plant systems that are available to establish and maintain normal and safe shutdown conditions. The PSMS is designed to mitigate accident conditions and automatically achieve stable hot standby conditions for the plant. The following functions support the cold shutdown objectives:

- Perform reactivity control to maintain the core in a sub-critical condition
- Maintain RCS inventory
- Provide boration capability to compensate for xenon decay and maintain the required core shutdown margin
- Provide pressure control
- Provide RHR capability to maintain adequate core cooling

The following systems can be used to support these objectives.

- RHR system - for decay heat removal and maintaining reactor coolant temperature within acceptable limits.
- CVCS - for reactivity control and RCS inventory control.
- Reactor pressure control - Initial reduction in reactor coolant pressure is achieved via passive systems.

**7.4.1.2.1 Residual Heat Removal System**

The residual heat removal system (RHRS) consists of four independent subsystems, each having one CS/RHR heat exchanger, one CS/RHR pump, and connecting piping and valves. Because the ECCS uses the advanced accumulator (ACC) design and an improved high head injection subsystem, the low head injection subsystem found in a conventional plant is not necessary and is not provided. The RHR function is transferred to the CSS and the CS/RHR heat exchangers, and the CS/RHR pumps are used for both RHRS and CSS.

The RHRS has the following functions;

- Removes reactor core decay heat and other residual heat from the reactor coolant.
- Transfers refueling water between the reactor cavity and the refueling water storage pit (RWSP) at the beginning and end of refueling operations.

A detailed description of the RHR system is described in Section 5.4.

**7.4.1.2.2 Chemical and Volume Control System**

The concentration of boron in the RCS is adjusted through the operation of the CVCS. For increasing the boron concentration, the necessary amount of concentrated boric acid solution is injected into the RCS. For decreasing the boron concentration, primary make-up water is added to the RCS to dilute the coolant water to the required boron concentration. The concentration of boric acid in the reactor coolant is measured by sampling and chemical titration, as appropriate. The CVCS includes; the boron recycle system, the regenerative heat exchanger, letdown heat exchanger, letdown orifices, purification filters, demineralizers, volume control tank (VCT), boric acid tanks (BATs), boric acid transfer pumps, charging pumps (CHPs), seal water injection filters, required piping, valves, and instrumentation.

A detailed description of the CVCS is described in Section 9.3.

**7.4.1.3 Instrumentation and Control Systems**

The I&C system equipment required for safe shutdown function(s) are safety-related and are common between this system and various other safety-related systems of the plant, including SLS, RPS, and ESFAS. Safety-related I&C equipment in these safety systems have been evaluated to demonstrate compliance with the provision of applicable GDC, RGs including the attributes of RG 1.206 Appendix C.I.7-B (Reference 7.4-1), SRP Chapter 7 (Reference 7.4-2) guidelines including Appendix 7.0A, BTPs and applicable industry standards including IEEE Std 603-1991 (Reference 7.4-3) and IEEE Std 7-4.3.2-2003 (Reference 7.4-4) for the design considerations and design attributes including initiating circuit, logic bypass, interlocks, redundancy, defense in depth and diversity features, single failure criterion, quality of components and modules, independence, periodic testing, and use of digital systems.

---

#### 7.4.1.4 HSIS

All functions needed to achieve and maintain both normal and safe shutdown can be manually initiated and monitored by operators using the operational VDUs or the safety grade HSIS. The operational VDUs provide HSI for all safety and non safety-related safe shutdown functions. The safety grade HSIS provides all safety-related controls and plant information, including critical parameters required for post accident conditions. The operational VDUs and safety grade HSIS are accessible in the MCR and the RSR.

Tables 7.4-1 and 7.4-2 provide a list of component controls and instrumentation used to achieve safe shutdown.

#### 7.4.1.5 Normal and Safe Shutdown from Outside the MCR

GDC 19 (Reference 7.4-5) requires, "Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot standby of the reactor, including necessary I&C systems to maintain the unit in a safe condition during hot standby, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures."

In the event the MCR is uninhabitable for any reasons including fire, the control and monitoring of normal and safe shutdown functions can be performed from the RSR, which is located outside the MCR fire area in the reactor building. This capability meets the requirements of GDC 19.

The requirements for designing the RSR are: (1) LOOP is possible following the evacuation from MCR, and (2) during normal operation, operators may have to evacuate the MCR immediately, without any action to plant, whenever they decide that evacuation from the MCR is necessary.

The RSR is designed in accordance with the following principles based on the above requirements.

1. The RSR is designed to shutdown the reactor, maintain the reactor in hot standby condition, and transition the reactor safely to cold shutdown. There are no unique required control actions outside the RSR to achieve or maintain hot standby or cold shutdown. Periodic RCS effluent sampling is a local operation for shutdown from the RSR, as it is for shutdown from the MCR.
2. The I&C equipment in the RSR is electrically isolated from any credible faults that may originate in the MCR. In addition, I&C equipment in the RSR is not affected by any spurious signals that may originate in the MCR. Prior to activation of HSI at the RSR, it is assumed that there are no prior failures that adversely affect the operability of I&C equipment in the RSR.
3. The safety-related I&C equipment in the RSR meets all Class 1E requirements including seismic category I qualification and conformance to the single failure criterion.

- 
4. When control is transferred from the MCR to the RSR, there is no disturbance to the state of plant components or to continuous control processes (i.e., phase seamless transition).
  5. The operator has the same functional control and monitoring capability at the RSR as in the MCR. The RSC provides equivalent functions of the operational VDUs and the safety VDUs in the MCR. The equipment arrangement of the RSC is displayed in Figure 7.4-1. The transfer of control to the RSR has no effect on any non-safety or safety-related control functions, including automatic load sequencing to accommodate LOOP. The operator has complete capability to control all manual and automatic modes.
  6. Adequate emergency lighting is provided on the pathways from the MCR to the RSR and to accommodate local effluent sampling.
  7. Communication is provided between the RSR and local effluent sampling areas and emergency response facilities. Refer to Subsection 9.5.2.
  8. During normal plant operation, the RSR is locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is under strict administrative control through secured areas with key access. Any access to these areas is indicated and alarmed in the MCR. All HSI at the RSR is electrically isolated from the safety and non-safety control systems. Controls at the RSR are disabled when controls are active in the MCR. Therefore, a fire or any other failure in the RSR, during normal operation, will have no effect on MCR controls.
  9. The RSR is located in the reactor building. The transfer switch panels are in two separate locations, one is in the RSR, and another one is located outside of the MCR on the escape route to the RSR. The transfer switch logic design is described in Topical Report MUAP-07004 (Reference 7.4-6) Section 4.2.4.d.

The cable routes for each transfer switch panels are separated into another fire area shown in Figure 7.4-2.

All safety functions are controlled by the PSMS. All PSMS controllers are located in Class 1E I&C rooms, which are electrically and physically isolated from both the MCR and RSR. Therefore, all functions of the PSMS, including safe shutdown functions, are independent from the MCR, and can be controlled from VDUs in the RSR. Therefore, if any PSMS function is required, including ESF, it can be manually actuated from the RSR. If any ESF function actuates inadvertently, it can be controlled or terminated from the RSR.

#### **7.4.1.6 Normal and Safe Shutdown Functions**

HSI is provided in the MCR and RSR for control of normal and safe shutdown plant components and for monitoring functions as shown in Tables 7.4-1 and 7.4-2, respectively. Shutdown functions consist of normal shutdown operation, and safe shutdown operation (i.e., safe shutdown using only safety-related plant equipment). These shutdown functions are described as follows.

---

The COL Applicant is to provide a description of component controls and indications required for safe shutdown related to the ultimate heat sink (UHS).

#### **7.4.1.6.1 Normal Shutdown**

##### **7.4.1.6.1.1 Hot Standby**

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain hot standby are as follows.

1. Shutdown the reactor using control rods.
2. Supply boric acid water to RCS for shutdown (CVCS).
3. Remove heat of RCS by the following measures:
  - i. Main steam release by turbine bypass system or to the atmosphere (main steam supply system [MSS]).
  - ii. Provide feedwater to SGs (condensate and feedwater system [CFS] and MSS).
4. Control pressure of the RCS (RCS and CVCS).
5. Supply instrument air (instrument air system [IAS]).
6. Assure CCW and ESW (CCWS and ESWS).
7. Provide HVAC function to the required areas including the containment, MCR (HVAC).
8. Utilize power systems, which support the above functions, for LOOP.

##### **7.4.1.6.1.2 Hot and Cold Shutdown**

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain cold shutdown are as follows. This describes functions to achieve and maintain cold shutdown from hot standby, therefore this includes functions to achieve and maintain hot shutdown. The capabilities and limitations of these systems are defined in the sections of this document that describe the respective process systems.

1. Remove heat from the RCS by the following measures:
  - i. Main steam release by turbine bypass system or to the atmosphere (MSS).
  - ii. Provide feedwater to SGs (CFS and MSS).
  - iii. Use RHRS (RHRS).
2. Control pressure and inventory of RCS (RCS and CVCS).

- 
3. Supply boric acid water to RCS (CVCS).
  4. Sample the boron concentration in RCS (process and post-accident sampling system [PSS]).
  5. Supply instrument air (IAS).
  6. Assure CCW and ESW (CCWS and ESWS).
  7. Provide HVAC function to the required areas including the containment, MCR (HVAC).
  8. Monitor neutron flux.
  9. Manually initiate appropriate ESF system shutdown operating bypasses.

#### **7.4.1.6.2 Safe Shutdown**

##### **7.4.1.6.2.1 Hot Standby**

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain hot standby using only safety-related equipment are as follows.

1. Trip the reactor, which accomplishes the reactor shutdown condition.
2. Remove heat from RCS by the following measures:
  - i. Main steam release to the atmosphere (MSS).
  - ii. Provide EFW to SGs (EFWS and MSS).
3. Control pressure of the RCS (RCS).
4. Provide HVAC functions to the required areas including the MCR (HVAC).
5. Utilize the emergency power system for the above functions in the event of LOOP.

##### **7.4.1.6.2.2 Hot and Cold Shutdown**

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain cold shutdown using only safety-related equipment are as follows. This describes functions to achieve and maintain cold shutdown from hot standby, therefore this includes functions to achieve and maintain hot shutdown. The capabilities and limitations of these systems are defined in the sections of this document that describe the respective process systems.

1. Remove heat of RCS by the following measures:
  - i. Main steam release to the atmosphere (MSS).
  - ii. Provide EFW to SGs (EFWS and MSS).

- 
- iii. Use RHRS (RHRS).
  - 2. Control pressure and inventory of RCS (RCS).
  - 3. Supply boric acid water to RCS (safety injection system [SIS]).
  - 4. Assure CCW and ESW (CCWS and ESWS).
  - 5. Provide HVAC function to the required areas including the MCR (HVAC).
  - 6. Monitor the neutron flux.
  - 7. Manually initiate appropriate ESF system shutdown operating bypasses.
  - 8. Utilize the emergency power system for the above functions in the event of LOOP.

#### 7.4.2 Design Basis Information

The US-APWR normal and safe shutdown design, including the design of the RSR, is based on the following codes and standards:

- 1. 10 CFR 50, Appendix A General Design Criteria 19 "Control Room."
- 2. RG 1.68.2 (Reference 7.4-7), Rev. 1, "Initial Startup Test Program to Demonstrate Remote Shutdown Capability for Water-cooled Nuclear Power Plants."
- 3. Standard Review Plan 7.4, Rev. 5, "Safe Shutdown System."
- 4. RG 1.189 (Reference 7.4-8), "Fire Protection for Operating Nuclear Power Plants."

In addition, the design of the safe shutdown systems including the design of the RSR is based on the following CFR;

- 1. 10 CFR 50.55a(a)(1), "Quality Standards."
- 2. 10 CFR 50.55a(h), "Protection Systems and Safety Systems"
- 3. 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves"
- 4. 10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records."
- 5. GDC 2, "Design Bases for Protection against Natural Phenomena."
- 6. GDC 4, "Environmental and Missile Design Bases."
- 7. GDC 13, "Instrumentation and Control."
- 8. GDC 24, "Separation of Protection and Control Systems."
- 9. GDC 34, "Residual Heat Removal."

---

10. GDC 35, "Emergency Core Cooling."

11. GDC 38, "Containment Heat Removal."

#### **7.4.2.1 I&C Systems Required for Safe Shutdown**

Safe shutdown, using only safety-related equipment, relies on monitoring instrumentation interfaced through the PSMS and safety grade HSI.

#### **7.4.2.2 Single Failure Criterion**

All functions of the RPS, ESFAS, SLS, and safety grade HSIS, including those used to achieve safe shutdown, meet the single failure criterion. Safety-related plant instrumentation and component controls, used to achieve safe shutdown, are redundant.

The PSMS is the I&C system credited for safe shutdown. The PSMS meets the single failure criteria through multiple redundant and independent trains, which control multiple redundant and independent mechanical trains, as described in MUAP-07004 Section 4.1(b). The PSMS is completely isolated from all non-safety I&C systems, such that there are no failures in non-safety I&C systems that can adversely affect the PSMS, as described in MUAP-07004 Section 3.3(6).

The test method for all I&C equipment within the PSMS, including equipment used for safe shutdown, is the same. Self-diagnosis with overlapping manual tests that encompass PSMS I/O and interfacing plant process components, such as sensors, pumps and valves, ensure there are no undetectable failures. There are at least two fully redundant and independent trains for all safe shutdown components to satisfy the single failure criterion. Table 7.4-1 shows that there is redundancy for each component credited for safe shutdown.

#### **7.4.2.3 Quality of Components and Modules**

All functions of the RPS, ESFAS, SLS, and safety grade HSIS, including those used to achieve safe shutdown, are Class 1E, and meet all appropriate quality requirements. Class 1E plant instrumentation and component controls are provided for all safe shutdown functions.

The operational VDUs and interfaces to the SLS, which may also be used to achieve normal and safe shutdown, are developed through an augmented quality program that includes software V&V, and seismic and environmental testing to levels consistent with the PSMS.

#### **7.4.2.4 Independence**

Redundant divisions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are independent from each other and from the non-safety division. This independence is also applicable to redundant divisions of safety-related plant instrumentation and component controls for all safe shutdown functions as described in Subsections 7.1.3.4 and 7.1.3.5.



---

Within the PSMS, which is the I&C system credited for safe shutdown, there are no components that are common to redundant trains, such as common switches for actuation, reset, mode, test, or any other features which could compromise the independence of the redundant trains.

Within the mechanical systems credited for safe shutdown, the main steam isolation valves and main feedwater isolation valves are common to both redundant safe shutdown trains. Each valve has two separate and redundant solenoid operators which are assigned to separate trains.

#### **7.4.2.5 Periodic Testing**

All functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are periodically tested, as described in Subsection 7.1.3.14. This testing encompasses safety-related plant instrumentation and component controls for all safe shutdown functions. It is noted that fast response RTDs are not used for the RTDs of wide range RCS temperature for safe shutdown and PAM, therefore, the response time testing in BTP 7-13(Reference 7.4-9) is not applicable to the RTDs in this section.

#### **7.4.2.6 Use of Digital Systems**

All functions of the PCMS, used to achieve normal shutdown, and all functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, rely on digital systems, as described in Subsections 7.1.3.8 and 7.1.3.17. Analog plant instrumentation and conventional electro-mechanical components (e.g., solenoids, motor starters and switchgears) are relied on for safe shutdown functions.

### **7.4.3 Analysis**

Detailed compliance to the GDC, IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 are described in MUAP-07004 Section 3.0, Appendix A and B.

#### **7.4.3.1 Safety Analysis**

Chapter 15 addresses AOOs including, plant load rejection and turbine trip. These analyses demonstrate that the PSMS has sufficient capability to achieve hot standby condition.

Control functions to mitigate the consequences of the plant load rejection and turbine trip are discussed in Section 7.7.

The analysis for additional postulated failures are described as follows:

- Loss of cooling water to vital equipment: The US-APWR has four divisions of safety-related cooling water, corresponding to the four divisions of safety-related ESF equipment. These four divisions are controlled by the PSMS. Therefore, loss of a single division of cooling water does not prevent accomplishing the safe shutdown function.
- Loss of plant instrument air: Instrument air is used for normal shutdown. There is no reliance on plant instrument air for safe shutdown. The loss of plant instrument

---

air will result in the loss of MFW. This condition is considered in the safety analysis, Chapter 15.

- Loss of power source: Any one division of subsystems for the safe shutdown is supplied power from redundant power sources. Therefore, loss of a single power source does not prevent accomplishing the safe shutdown function.

#### 7.4.3.2 Restrictive Setpoints

For the US-APWR, the reactor will not be permitted to operate at power, even when one RCS loop is unavailable as evidenced by; low reactor coolant flow conditions, therefore there are no restrictive setpoints.

#### 7.4.4 Combined License Information

COL 7.4(1) *The COL Applicant is to provide a description of component controls and indications required for safe shutdown related to the UHS.*

#### 7.4.5 References

- 7.4-1 Combined License Applications for Nuclear Power Plants (LWR Edition), Regulatory Guide 1.206 Revision 0, June 2007.
- 7.4-2 U.S. Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800, March 2007.
- 7.4-3 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.
- 7.4-4 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.
- 7.4-5 Control Room, General Design Criteria for Nuclear Power Plant 19, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.
- 7.4-6 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.4-7 Initial Startup Test Program to Demonstrate Remote Shutdown Capability for Water-cooled Nuclear Power Plants, Regulatory Guide 1.68.2 Revision 1, July 1978.
- 7.4-8 Fire Protection for Operating Nuclear Power Plants, Regulatory Guide 1.189 Revision 1, March 2007.
- 7.4-9 Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors, BTP 7-13 Revision 5, March 2007.

**Table 7.4-1 Component Controls for Shutdown (Sheet 1 of 5)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
RT System	RTB	No	Yes	2	4	
RCS	RCP	Yes	No	-	-	Available with off-site power.
	Safety Depressurization Valve	No	Yes	1	2	Note1
	Safety Depressurization Valve Block Valve	No	Yes	1	2	Note1
	Pressurizer Heater Backup Group	No	Yes	2	4	
	Pressurizer Spray Valve	Yes	No	-	-	
	Reactor Vessel (RV) Vent Valve	No	Yes	1	2	These valves could be used only if the venting becomes necessary.
CVCS	Charging Pump	Yes	No	-	-	Automatic start in LOOP.
	Charging Flow Control Valve	Yes	No	-	-	
	Letdown Line 1st (2nd) Stop Valve	Yes	No	-	-	
	Letdown Line inside C/V Isolation Valve	Yes	No	-	-	
	CHP Inlet Line VCT Side 1st, 2nd Isolation Valve	Yes	No	-	-	
	CHP Inlet Line BAT Side Isolation Valve	Yes	No	-	-	
	CHP Inlet Line RWSAT Side Isolation Valve	No	No	-	-	These valves are automatically opened on Low Volume Control Tank Water Level.

Note1: The configuration of the Safety Depressurization Valves and Safety Depressurization Valve – Block Valves meets the single failure criteria (for both electrical and mechanical failures), to ensure the capability for depressurization when required and to prevent spurious depressurization. There are two depressurization lines, each with one Safety Depressurization Valve (normally closed) and one Safety Depressurization Valve – Block Valve (normally open), each assigned to different trains. Four trains are used, such that the four valves in the two depressurization lines do not share any common train assignments. Should a Safety Depressurization valve fail to open when required, depressurization can be achieved through the other line. Should a Safety Depressurization valve spuriously open, the series block valve can be closed.

**Table 7.4-1 Component Controls for Shutdown (Sheet 2 of 5)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
CVCS (conti-nued)	Pressurizer Auxiliary Spray Valve	Yes	No	-	-	
	RHR Letdown Line Flow Control Valve	Yes	No	-	-	
	Seal Water Return Line 1st, 2nd Isolation Valve	Yes	Yes	1	2	These valves are used to holdup seal water inside containment in Safe Shutdown.
SIS	Safety Injection Pump (SIP)	No	Yes	2	4	Table 6.3-6
	SIPs Suction Isolation Valve	No	Yes	2	4	Table 6.3-6
	SIPs Discharge Containment Isolation Valve	No	Yes	2	4	Table 6.3-6
	Direct Vessel Safety Injection Line Valve	No	Yes	2	4	Table 6.3-6
	Emergency Letdown Line 1st, 2nd Isolation Valve	No	Yes	1	2	Table 6.3-6
	Accumulator Discharge Valve	Yes	Yes	4	4	Table 6.3-6
	ACC Nitrogen Supply Line Isolation Valve	No	Yes	4	4	These valves are used in case of ACC discharge valve failure to close. Table 6.3-6
	ACC Nitrogen Discharge Valve	No	Yes	1	2	
RHRS	CS/RHR Pump	Yes	Yes	2	4	Table 5.4.7-1
	1st/2nd CS/RHR Pump Hot Leg Isolation Valve	Yes	Yes	2	4	Table 5.4.7-1
	CS/RHR Hx Outlet Flow Control Valve	Yes	No	-	-	
	CS/RHR Hx Bypass Flow Control Valve	Yes	No	-	-	
	CS/RHR Pumps RWSP Suction Isolation Valve	Yes	Yes	2	4	CSS Valves Table 6.2.2-3
	RHR Discharge Line Containment Isolation Valve	Yes	Yes	2	4	Table 5.4.7-1

**Table 7.4-1 Component Controls for Shutdown (Sheet 3 of 5)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
RHRS (conti-nued)	RHR Flow Control Valve	Yes	Yes	2	4	Table 5.4.7-1
	CS/RHR Pump Full-Flow Test Line Stop Valve	No	Yes	2	4	Table 5.4.7-1
EFWS	EFW Pump (Motor-Driven or Turbine Driven)	No	Yes	2	4	Table 5.4.7-1
	EFW Control Valve	No	Yes	2	4	Table 10.4.9-3
	EFW Isolation Valve	No	Yes	2	4	Table 10.4.9-3
	T/D-EFW Pump MS Line Steam Isolation Valve	No	Yes	1	4	Table 10.4.9-3
	T/D-EFW Pump Actuation Valve	No	Yes	1	4	Table 10.4.9-3
MSS	Main Steam Depressurization Valve	No	Yes	2	4	Table 10.3.3-1
	Main Steam Relief Valve	Yes	No	-	-	
	Main Steam Relief Valve Block Valve	No	Yes	2	4	Table 10.3.3-1
	Main Steam Isolation Valve	Yes	Yes	4	4	Table 10.3.3-1
	Main Steam Bypass Isolation Valve	Yes	Yes	4	4	Table 10.3.3-1
	Turbine Bypass Valve	Yes	No	-	-	
CFS	MFW Bypass Regulation valve	Yes	No	-	-	
	SG Water Filling Control Valve	Yes	No	-	-	
CCWS	CCW Pump	Yes	Yes	2	4	Automatic start in LOOP. Table 9.2.2-3
	CS/RHR Hx CCW Outlet Valve	Yes	Yes	2	4	Table 9.2.2-3
ESWS	ESW Pump	Yes	Yes	2	4	Automatic start in LOOP. Table 9.2.2-3
	ESW Pump Discharge Valve	Yes	Yes	2	4	Table 9.2.2-3
IAS	Instrument Air Compressor	Yes	No	-	-	Automatic start in LOOP.

**Table 7.4-1 Component Controls for Shutdown (Sheet 4 of 5)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
PSS	Letdown Demineralizer Inlet Sampling Valve	Yes	No	-	-	Local Manual Valve
	RHR Loop Sampling Stop Valve	Yes	No	-	-	Installed inside sampling rack.
	Inside Sampling Hood Isolation Valve	Yes	No	-	-	Installed inside sampling rack.
	Loop Sampling Line In and out side C/V Isolation Valve	Yes	No	-	-	
SGBDS	SGBD Line Containment Isolation Valve	No	Yes	4	4	Close on EFW Pump Start Signal. Table 10.3.3-1
	SGBD Line Isolation Valve	No	Yes	4	4	Close on EFW Pump Start Signal. Table 10.3.3-1
	SGBD Sampling Line Containment Isolation Valve	No	Yes	4	4	Close on EFW Pump Start Signal. Table 10.3.3-1
Other	ECCS Actuation Signal Block	Yes	Yes	4	4	
	Main Steam Line Pressure Signal Block	Yes	Yes	4	4	
	Emergency Power Generator	No	Yes	2	4	Automatic start in LOOP.
HVAC	MCR Air Handling Unit & Damper	Yes	Yes	2	4	Automatic start in LOOP.
	Class 1E Electrical Room Air Handling Unit & Damper	Yes	Yes	2	4	Automatic start in LOOP.
	Class 1E Electrical Room Return Air Fan	Yes	Yes	2	4	Automatic start in LOOP
	Class 1E Battery Room Exhaust Fan & Damper	Yes	Yes	2	4	Automatic start in LOOP.
	Class 1E Electrical Room In-duct heater	Yes	Yes	2	4	Automatic start in LOOP
	CCW Pump Area Air Handling Unit	No	Yes	2	4	
	Essential Chiller Unit Area Air Handling Unit	No	Yes	2	4	
	EFW Pump Area Air Handling Unit	No	Yes	2	4	

**Table 7.4-1 Component Controls for Shutdown (Sheet 5 of 5)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
HVAC (continued)	Essential Chiller Unit	Yes	Yes	2	4	
	Essential Chilled Water Pump & Valves	Yes	Yes	2	4	
	Containment Fan Cooler Unit	Yes	No	-	-	Automatic start in LOOP.
	Reactor Cavity Cooling Fan	Yes	No	-	-	Automatic start in LOOP.
	CRDM Cooling Fans & Unit	Yes	No	-	-	Automatic start in LOOP.
	Non-Class 1E Electrical Room Air Handling Unit & Damper	Yes	No	-	-	Automatic start in LOOP.
	Non-Class 1E Electrical Room Return Air Fan	Yes	No	-	-	
	Non-Class 1E Battery Room Exhaust Fan & Damper	Yes	No	-	-	Automatic start in LOOP.
	Auxiliary Building Air Handling Unit & Damper	Yes	No	-	-	
	MS/FW Piping Area Air Handling Unit & Damper	Yes	No	-	-	
	Non- Essential Chiller Unit	Yes	No	-	-	Automatic start in LOOP.
	Non- Essential Chilled Water Pump & Valves	Yes	No	-	-	Automatic start in LOOP.
	Non-Essential Chiller Condenser Water Pump & Valves	Yes	No	-	-	Automatic start in LOOP.
	Non-Essential Chilled Water System Cooling Tower Fan	Yes	No	-	-	Automatic start in LOOP

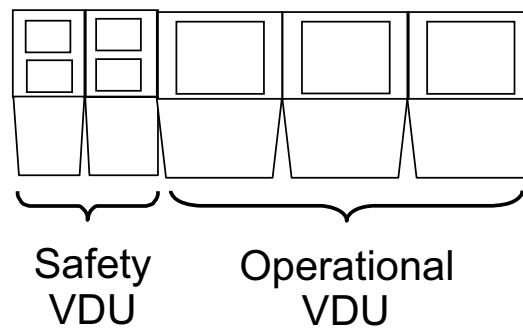
Table 7.4-2 Indication for Shutdown (Sheet 1 of 2)

Systems	Instruments	Number of Required Channels	Normal Shutdown	Safe Shutdown	Remarks
RCS	Pressurizer Water Level	2	Yes	Yes	
	Pressurizer Pressure	2	Yes	Yes	
	Reactor Coolant Hot Leg Temperature (Wide Range)	1per Loop	Yes	Yes	
	Reactor Coolant Cold Leg Temperature (Wide Range)	1per Loop	Yes	Yes	
	Reactor Coolant Pressure	1per Loop	Yes	Yes	
CVCS	Boric Acid Tank Water Level	1 per tank	Yes	No	
	RCP Seal Water Return Line Flow	1 per RCP	Yes	No	
	RCP Seal Water Outlet Temperature	1 per RCP	Yes	No	
	Charging Flow	1	Yes	No	
SIS	Safety Injection Pump Discharge Flow	1 per Line	No	Yes	Used to maintain RCS inventory during Safe Shutdown.
	Safety Injection Pump Minimum Flow	1 per Line	No	Yes	
	Safety Injection Pump Discharge Pressure	1 per Line	No	Yes	
	Safety Injection Pump Suction Pressure	1 per Line	No	Yes	
	Accumulator Pressure	1 per Tank	No	Yes	For ACC isolation during Safe Shutdown.
RHRS	CS/RHR Hx Outlet Temperature	1 per Line	Yes	Yes	
	CS/RHR Pump Discharge Flow	1 per Line	Yes	Yes	
	CS/RHR Pump Minimum Flow	1 per Line	Yes	Yes	
	CS/RHR Pump Discharge Pressure	1 per Line	Yes	Yes	
	CS/RHR Pump Suction Pressure	1 per Line	Yes	Yes	
EFWS	EFW Pit Water Level	2 per Pit	No	Yes	
	EFW Flow	1 per Line	No	Yes	
	EFW Pump Discharge Pressure	1 per Line	No	Yes	
CFS	SG Water Level (Wide Range)	1 per SG	Yes	Yes	
MSS	Main Steam Line Pressure	2 per Line	Yes	Yes	



**Table 7.4-2 Indication for Shutdown (Sheet 2 of 2)**

<b>Systems</b>	<b>Instruments</b>	<b>Number of Required Channels</b>	<b>Normal Shutdown</b>	<b>Safe Shutdown</b>	<b>Remarks</b>
CCWS	CCW Surge Tank Water Level	2 per Tank	Yes	Yes	
	CCW Header Pressure	1 per Line	Yes	Yes	
	CCW Header Flow	1 per Line	Yes	Yes	
	CCW Supply Temperature	1 per Line	Yes	Yes	
ESWS	CCW Hx ESW Flow	1 per Line	Yes	Yes	
	ESW Header Pressure	1 per Line	Yes	Yes	
RWS	RWSP Water Level (Wide Range)	2	No	Yes	
NIS	Source Range Neutron Flux	2	No	Yes	



**Figure 7.4-1**     **Equipment Arrangement of Remote Shutdown Console**

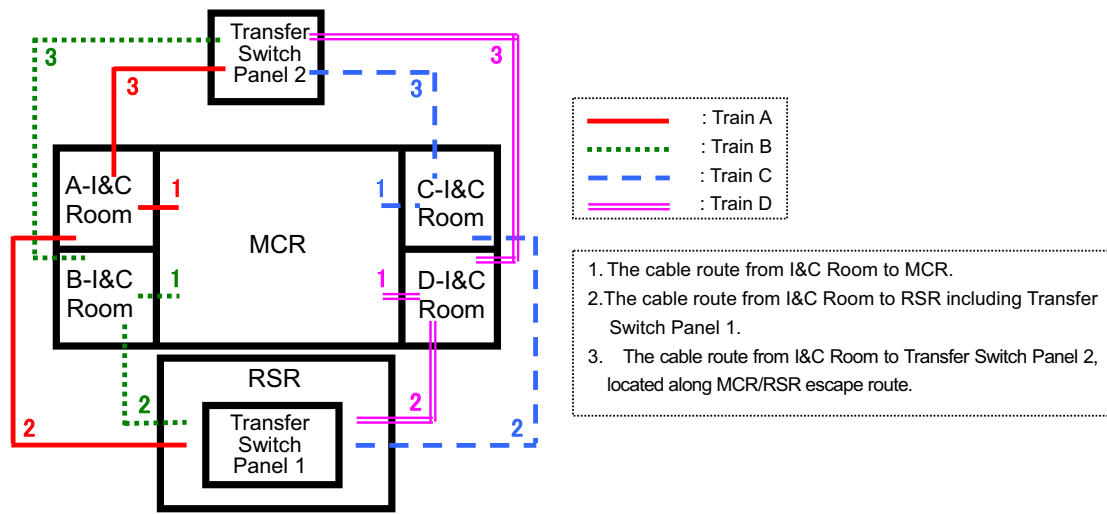


Figure 7.4-2 The Cable Route of the Remote Shutdown Room

---

## 7.5 Information Systems Important to Safety

### 7.5.1 System Description

This section describes the I&C systems PSMS and PCMS that provide information to the plant operators for: (1) assessing plant conditions and safety system performance, and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator actions related to accident mitigation. The information systems important to safety also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of AOOs.

This section describes the following information systems important to safety:

- Post accident monitoring (PAM)
- Bypassed and inoperable status indication (BISI)
- Plant annunciators (alarms)
- Safety parameter displays system (SPDS)

Information important to safety, which supports emergency response operations, is available via the emergency response data system (ERDS). Refer to Subsection 7.9.1.7.

The information important to safety is available for display at the following facilities:

- MCR
- RSR
- TSC
- EOF

Controls for credited manual operator actions are available in the MCR.

#### 7.5.1.1 Post-Accident Monitoring

The purpose of displaying PAM parameters is to assist MCR personnel in evaluating the safety status of the plant. PAM parameters are direct measurements or derived variables representative of the safety status of the plant. The primary function of the PAM parameters is to aid the operator in the rapid detection of abnormal operating conditions. As an operator aid, the PAM variables represent a minimum set of plant parameters from which the plant safety status can be assessed.

Safety-related PAM parameters are displayed on the safety VDUs, operational VDUs, and on the LDP. Non safety-related PAM parameters are displayed on operational VDUs. The parameters selected comply with the guidelines of RG 1.97 (Reference 7.5-1). Display of at least two trains of each safety-related parameter is available.

The safety VDUs for each train are isolated from each other and from non-safety systems.

---

IEEE Std 497-2002 (Reference 7.5-2) provides selecting and categorizing principles for PAM variables. Table 7.5-1 provides a summary of the selection criteria and source documents for each PAM variable type.

Table 7.5-2 provides the US-APWR design attributes for each variable type.

Table 7.5-3 provides a list of PAM variables, their ranges, monitored functions or systems, quality and variable type. To further clarify the US-APWR PAM variable selection basis, Tables 7.5-6 through 7.5-10 show specific PAM variables and their required functions.

The COL Applicant is to provide a description of site-specific PAM variables, which are type D variables for monitoring the performance of the UHS and type E variables for monitoring the meteorological parameters.

Instrumentation for monitoring severe accidents is discussed in Subsection 19.2.3.3.7, which summarizes the necessary equipment survivability for achieving and maintaining shutdown of the plant and maintaining containment integrity for severe accidents. A detailed description of the analysis on equipment survivability, including instruments required for severe accident monitoring, is provided in Chapter 15 of PRA Technical Report, MUAP-07030 (Reference 7.5-15)

#### **7.5.1.1.1 Variable Classifications and Signal Processing Design**

The following clarifications are provided for the design attributes identified in Tables 7.5-1 and 7.5-2:

1. Single Failure: The design ensures that at least one measurement channel is available after each single failure. Process measurement channels are interfaced to redundant trains of the RPS. Component status signals are interfaced to redundant trains of the SLS. PAM information is then interfaced to redundant safety grade HSI and non-safety HSI for display.
2. Seismic Qualification: RPS, SLS, and safety grade HSI are seismically qualified, as previously described. PAM measurement channels are generically qualified by the instrument OEM. Specific analysis for the US-APWR demonstrates this qualification bounds the seismic levels for the specific instrument location.
3. Environmental Qualification: RPS, SLS, and safety grade HSI are environmentally qualified, as previously described. These systems are located in a mild environment; therefore, the qualification duration is not applicable. PAM measurement channels are generically qualified by the instrument OEM. Specific analysis for the US-APWR demonstrates this qualification bounds the environmental conditions for the specific instrument location and required qualification duration. The qualification duration requirements are defined in Section 3.11 for all variable types. For Type C variables monitoring fission product barriers, the qualification duration is a minimum of one hundred days. Qualification testing does not encompass severe accident conditions however, a qualitative evaluation provides reasonable assurance that the instruments will operate in the severe operating environment for which they are intended over the time span for which they are needed. The qualification of PAM equipment is the

---

scope of Section 3.11 and Technical Report MUAP-08015, "US-APWR Equipment Environmental Qualification Program" (Reference 7.5-16).

4. Power Supply: Class 1E UPS is provided to redundant trains of RPS, SLS, safety grade HSI, and PAM measurement channel instrumentation.
5. QA: RPS, SLS, safety grade HSI and PAM measurement channel instrumentation meet all Class 1E quality requirements.
6. Independence and Separation: Independence and physical separation are provided between redundant safety systems and between the safety and non-safety systems. Safety-related PAM variables are interfaced between safety system and non-safety system via the unit bus as illustrated in Figure 7.5-1. This design meets the requirements of DI&C-ISG-04(Reference 7.5-17). More detail for the unit bus is described in Subsection 7.9.1.
7. Information Ambiguity: The PCMS automatically identifies instrument channels that are out of range. Where there are at least three redundant measurements, the PCMS also automatically identifies a drifting instrument. Where there are only two instruments, the PCMS can identify when the measurement values have drifted apart; the operator can then manually access other related instrumentation to specifically identify which of the two instrument channels has failed.
8. Testability: PAM measurement channels are continuously tested to identify ambiguity as discussed above. RPS, SLS, and safety grade HSI are continuously tested, as discussed in Subsection 7.1.3.10. In addition, input channels are periodically calibrated, including HSI testing, as discussed in Subsection 7.1.3.14. Measurement uncertainty calculations are as described in Subsection 7.2.2.7.
9. Continuous Display: Type A and B variables are continuously displayed, as described in Subsection 7.5.1.1.2.
10. Recording: PAM variables are continuously recorded within the PCMS. The PCMS also provides trend displays on operational VDUs.

Figures 7.5-1 and 7.5-2 show the signal processing for safety-related and non safety-related variables, respectively. PAM parameters are displayed on the VDUs and LDP, supported by the PCMS and PSMS. If a software common cause failure (CCF) in the PCMS and PSMS were occur, they will be disabled including PAM indications on the VDUs and LDP. The diverse actuation system (DAS) provides the diverse actuation and indications to cope with this failure mode. Diverse indications are provided on the diverse HSI panel (DHP). The variables indicated on the DHP are determined from the best estimate D3 analysis. The US-APWR complies with BTP 7-19(Reference 7.5-18) for coping with CCF. For this compliance the DHP provides diverse indications for variables needed to prompt credited manual operator actions (Type A variables) and variables to monitor critical safety functions (Type B variables). BTP 7-19 does not require diverse indications for monitoring fission product barriers (Type C variables). More detailed discussions are provided in Section 7.8, Topical Report MUAP-07006 (Reference 7.5-19), and Technical Report MUAP-07014 (Reference 7.5-20). Therefore, the indication for CCF

is out of scope of the PAM design criteria. The DHP demonstrates that defense-in-depth exists against the consequences of a software CCF in the PCMS and PSMS systems that would disable PAM indications.

#### **7.5.1.1.2 Variables Display Design**

PAM Type A, B, and C variables have redundant instrumentation and are displayed on at least two redundant safety VDUs. Type A and B variables are continuously displayed on the LDP. During most normal operating conditions, a complete set of Type A and B variables for at least one train is also continuously displayed on safety VDUs. A second complete set of Type A and B variables for a second train may be displayed on demand. There are limited times, during normal operating conditions, when the safety VDUs are used for monitoring other variables or for control or testing. During these limited time-periods, the Type A and B variables are always continuously visible on the LDP. In addition, the display for Type A and B variables can be recalled on the safety VDU from any other safety VDU display, using one touch access. This one touch access feature is most useful during degraded HSI conditions, such as loss of all non-safety HSI, when the safety VDU may be the only HSI available for monitoring and control. Table 7.5-4 describes the configuration of this display.

#### **7.5.1.1.3 Inadequate Core Cooling Monitoring**

This section provides a description of the instrumentation provided to monitor the following inadequate core cooling (ICC) information:

- Degrees of subcooling
- Reactor vessel water level (RVWL)
- Core exit temperature

The Degrees of Subcooling indicates the loss of subcooling, occurrence of saturation and achievement of a subcooled condition following core recovery. The RVWL provides information to the operator on the decreasing liquid inventory in the reactor. The core exit temperature sensors monitor the increasing core exit temperatures associated with ICC and the decreasing core exit temperatures associated with recovery from ICC.

##### **7.5.1.1.3.1 Degrees of Subcooling**

The degrees of subcooling utilizes sensors for reactor coolant cold and hot leg temperatures, core exit temperature, and reactor coolant pressure.

The saturation temperature is calculated from the minimum pressure input. The temperature subcooled margin is the difference between saturation temperature and the sensor temperature input.

Two temperature subcooled margin presentations are available as follows:

- RCS saturation margin - the temperature saturation margin based on the difference between the saturation temperature and the maximum temperature from the resistance temperature detectors (RTDs) in the hot and cold legs.

- 
- Upper head saturation margin - temperature saturation margin based on the difference between the saturation temperature and the core exit temperature.

#### **7.5.1.1.3.2 Reactor Vessel Water Level**

The RVWL probe assembly measures reactor coolant liquid inventory above the fuel alignment plate with discrete heated junction thermocouple (HJTC) sensors located at different levels within a separator tube ranging from the top of the fuel alignment plate to the RV head. The basic principle of operation is the detection of a temperature difference between adjacent heated and unheated thermocouples.

The HJTC sensor consists of a thermocouple near a heater (or heated junction) and another thermocouple positioned away from the heater (or unheated junction). In a fluid with relatively good heat transfer properties, the temperature difference between the adjacent thermocouples is small. In a fluid with relatively poor heat transfer properties, the temperature difference between the thermocouples is large.

Two RVWL probe assemblies provide two channels of HJTC instruments. Each HJTC probe assembly includes six HJTC sensors. The two probe assemblies are assigned to two electrically independent trains.

The heater power for the HJTC is supplied by a dedicated heater power supply for HJTC.

#### **7.5.1.1.3.3 Core Exit Temperature**

There are 39 core exit thermocouples. Thermocouples are threaded into individual guide tubes that penetrate the RV closure head through seal assemblies and terminate at the exit flow end of the fuel assemblies. All thermocouples are arranged in two safety divisions and one non-safety division; the two safety divisions are independent. The two safety divisions interface with the RPS and provide signals for PAM. Core exit thermocouples provide a measure of core heat up via measurement of core exit fluid temperature.

#### **7.5.1.1.4 Performance Design**

The assessment of performance criteria of the PAM variables, based on Clause 5 of IEEE 497-2002, is provided in this subsection.

##### **1. Range**

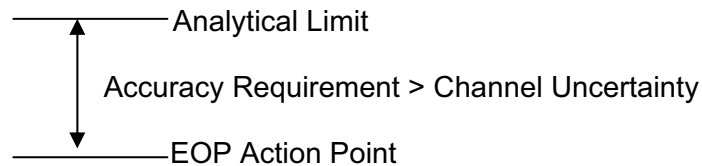
The range of each PAM channel described in Table 7.5-3 was established to ensure that it covers the AOOs and PAs. Instrument ranges were developed per the US-APWR system design and safety analysis, and have been confirmed to be consistent with similar instruments in operating plants. Instrument ranges are confirmed again during development of the emergency response guidelines (ERGs). Validation of the complete HSI, including instrument indicators and emergency operating procedures (EOPs) will be conducted during the HFE program.

##### **2. Accuracy**



The required accuracy of each PAM channel is established according to how the indication is to be used by control room personnel and is established in accordance with Annex A of IEEE 497-2002, which divides accuracy requirements into two groups.

The first group consists of those variables, that support credited manual actions and where the corresponding channel accuracy is specified in the accident analysis or licensing basis. These are the Type A PAM variables listed in Table 7.5-3. The function and action are defined as important safety function, thus the methodology for action point determination conforms to RG1.105(Reference 7.5-21) as same as other safety-related function. The following figure graphically depicts the relationship between the analytical limit, the operator action point (EOP action point), and channel uncertainty.



The second group consists of those variables that provide trend or plant stability information. In this case, it is of primary importance to know whether the variable is increasing, decreasing, or constant, and the exact value of the variable is only of secondary importance. All PAM variables, except for Type A variables, are categorized in this group. For linearly derived display instruments, the typical required accuracy is  $\pm 20$  percent or more. For logarithmic scale instruments, the typical required accuracy is  $\pm 50$  percent of the reading or alternatively plus/minus a half decade. Trend information for these variables is displayed on the operational VDUs as described in Subsection 7.5.1.1.1 and Figures 7.5-1 and 7.5-2.

### 3. Response Time

A PAM channel is designed to provide real time and timely information. PAM signals are transmitted from the sensors to the VDUs through a digital control system. The response time between detection and indication is approximately one to three seconds. The update frequency is less than one second. Thus, the PAM channel has sufficient capability to provide real time and timely information.

### 4. Required Instrumentation Duration

The operating time for each variable required for DBA conditions is addressed in the development of the qualification program, per Section 3.11 and Technical Report MUAP-08015. The design basis accident analyses provide the basis for the required durations.

- a. The duration for Type A variables is determined from required operator action by the accident analysis and emergency procedure which duration is less than four months. All Type A variables are also other type. Therefore, the duration for Type A variables is required to be four months consistent with the duration for other type.
- b. The duration for Type B variables is at least the duration associated with the longest-duration design basis event for that variable; four months is required by the accident analyses and emergency procedure of the US-APWR.

- 
- c. The duration for Type C variables is at least 100 days for instrument channels monitoring the fission product barriers; four months is required by the accident analyses and emergency procedure of US-APWR.
  - d. The duration for Type D and E is four months as required by the accident analyses and emergency procedure.

A shorter duration may be acceptable if equipment replacement or repair can be accomplished within an acceptable out-of-service time, taking into consideration the location and accessibility of the equipment. When PAM instrumentation is located inside containment, is inaccessible, or cannot be repaired, replaced, recalibrated or equivalent indication cannot be obtained, the required duration is one year.

## 5. Reliability

DCD Subsection 19.1.4.1.1, "Description of the Level 1 PRA for Operations at Power," states that for each component type and failure mode, the failure rates are extracted from available generic data sources. This section also makes two key assumptions related to component reliability:

- US generic data are applied for component reliability data
- US generic data are applied to component unavailability due to test and unplanned maintenance

The US-APWR PRA directly models instrument reliability using generic data, and the PRA is used to analyze the plant design to confirm that system reliability goals, such as those set for the maintenance rule, are acceptable. PAM instruments will be procured with sufficient reliability to be consistent with the generic reliability data used in the PRA, Chapter 7 of MUAP-07030. Therefore, assuring that system reliability goals are met.

### 7.5.1.2 Bypassed and Inoperable Status Indication

The system level BISI is provided based on RG 1.47 (Reference 7.5-4). These indications are displayed as the spatially dedicated continuously visible (SDCV) information on LDP in the MCR. The system level BISI is discussed in detail in Topical Report MUAP-07007 (Reference 7.5-3) Section 4.9.

#### 7.5.1.2.1 Design of Bypassed and Inoperable Status Indication

BISI functions are provided from the status of PCMS and PSMS systems. BISI is a non-safety function implemented within the PCMS. The interface of BISI data signals from safety to non-safety systems uses the Unit Bus and therefore meets DI&C-ISG-04 in the same manner as other safety to non-safety data communications. Independence and physical separation are provided between redundant safety systems and between the safety and non-safety systems.

The system level BISI is provided in the "OK monitor" area on the LDP for inoperable conditions that result in inoperability of any ESF or RT system function at the train level. The BISI is color-coded so that the indication for each function is lighted in yellow color when one train is bypassed, and lighted in red color when two or more trains are

---

bypassed. When the system level BISI are displayed on the LDP, operators can drill down to specific inoperable information in the train level on the operational VDU in the MCR.

With regard to certain items performed at least once per fuel cycle (i.e., up to 24 months while RG 1.47 recommends “per one year”), the system level BISI is automatically initiated by a signal from the PSMS and is not removed by any method until the initiating signal is reset from the PSMS. In addition, to the automatic initiation conditions listed below, the operator can manually initiate the system level BISI from the operational VDU.

- Connecting PSMS controller to the maintenance network |
- PSMS input bypass to accommodate input calibration and testing
- ESFAS train bypass for testing
- RPS bypass for shunt trip testing
- Component bypass from SLS (to perform component maintenance)
- Bypass or alignment of the components and equipment of the following fluid system in positions that would bypass the safety function (that are tested at least once per 24 months during plant operation)
  - ECCS
  - CS/RHR System
  - EFWS
  - CCWS
  - ESWS
  - HVAC

#### **7.5.1.2.2 Bypassed and Inoperable Status Indication Functions**

System level indication for each of the following safety function is displayed.

- RT
- ECCS
- Containment spray
- MCR isolation
- Containment purge isolation
- Containment isolation phase A

- 
- Containment isolation phase B
  - Main feedwater isolation
  - Main steam line isolation
  - Emergency feedwater initiation
  - Emergency feedwater isolation
  - CVCS isolation
  - Interlock systems import to safety (Refer to Section 7.6)

#### 7.5.1.3 Plant Annunciator (Alarm) System

The primary purpose of the alarm system is to alert operators that the plant is in an abnormal status. Alarms are used not only to draw operator's attention, but also to identify the extent of the abnormal status. The alarm system is also designed taking into consideration functional and ergonomic aspects, facilitating appropriate operator response.

The main features of the alarm system are as follows:

- Adequate display to acknowledge and recognize alarm information.
- Application of alarm prioritization to avoid alarm avalanche.
- Request function from alarm display to relevant system display and alarm response procedures.

These functions help operators to identify and diagnose transients. Plant alarm system functional design is discussed in details in Topical Report MUAP-07007 Section 4.7.

Alarm annunciations are provided by the PCMS on the alarm VDUs and the LDP, and displayed on the operational VDUs. Safety-related sensors for alarms are interfaced between safety system and non-safety system via the unit bus as illustrated in Figure 7.5-4. This communication meets the requirements of DI&C-ISG-04. More detail for the unit bus is described in Subsection 7.9.1. The alarm VDU computer and all alarm HSI components, including audible and visual devices, are redundant to ensure operation is not adversely affected by credible malfunctions. The digital portion of the alarm system integrity is checked by self-diagnosis which does not affect the operation of alarms. Failures in the redundant visual portions of the alarm system are easily identified by operators, since the LDP and alarm VDUs are used routinely by operators for all tasks in the MCR. Failures in the redundant audible portions of the alarm system are easily identified by operators, since distinct alarm sounds normally originate from different locations within the MCR. Alarm signals originate in plant instrumentation or within the controllers of the PCMS and PSMS. These signals are interfaced to the PCMS via the redundant unit bus, described in Section 7.9. The data interface to the PSMS is physically and functionally isolated so as not to affect the safety system in case of failure of the alarm system.

---

As for all PCMS components, the alarm system is powered by redundant UPSs. The alarm system is designed and tested to a similar environmental, seismic, and EMI/RFI requirement as the PSMS.

The highly reliable design of the alarm system makes it suitable for prompting operator attention to all abnormal plant conditions, including those requiring manual operator actions credited in the plant safety analysis. The alarms for credited manual operator actions are developed through an augmented quality program, which includes software V&V.

#### **7.5.1.4 Safety Parameter Display System**

The SPDS provides a display of key plant parameters from which the plant's critical safety function status may be assessed. The primary function of the SPDS is to help operators and emergency response personnel make quick assessments of plant safety status. The SPDS is operated during normal operations as well as during all classes of emergencies. The functions and design of SPDS are included as a part of the overall HSI design. Following is list of SPDS parameters for each critical safety function.

1. Reactivity Control
  - Neutron flux
  - Status of RTBs
  - Control rod position
2. RCS Inventory
  - Pressurizer water level
  - Reactor coolant hot leg temperature (wide range)
  - Reactor coolant cold leg temperature (wide range)
  - Reactor coolant pressure
3. Core Cooling
  - Reactor coolant hot leg temperature (wide range)
  - Reactor coolant cold leg temperature (wide range)
  - Degrees of subcooling
  - Core exit temperature
  - Reactor coolant pressure
4. Secondary Heat Sink
  - SG water level (narrow range)

- 
- SG water level (wide range)
  - EFW flow
  - MFW flow
5. RCS Integrity
- Reactor coolant pressure
  - Reactor coolant hot leg temperature (wide range)
  - Reactor coolant cold leg temperature (wide range)
  - Degrees of subcooling
  - Core exit temperature
6. Containment Integrity
- Containment pressure
  - Containment temperature
  - CS/RHR pump discharge flow
  - Status of Containment isolation valves

The SPDS is discussed in MUAP-07004 (Reference 7.5-5) Section 4.2.5.b. |

The SPDS is provided by the PCMS on operational VDUs, alarm VDUs, and the LDP. The LDP provides a continuous display of the status of each critical safety function. The status displayed for each critical safety function corresponds to the critical safety function status algorithm defined in the emergency operating procedures (EOPs).

The computer that processes SPDS functions and all related HSI components are redundant, to ensure operation is not adversely affected by credible malfunctions. SPDS signals originate in plant instrumentation or within the controllers of the PCMS and PSMS. These signals are interfaced to the PCMS via the redundant unit bus, described in Section 7.9. The data interface to the PSMS is physically and functionally isolated so as not to affect the safety system in the event of SPDS component failure. The SPDS is developed through an augmented quality program, which includes software V&V.

#### **7.5.1.5 Credited Manual Operator Actions**

The plant safety analysis credits manual operator actions where there are no automated actions. The manual operator actions credited in the safety analysis for accident mitigation are identified in Table 7.5-5.

HSI to support all credited manual operator actions is provided on safety VDUs. Operational VDUs and interfaces to the SLS, which may also be used for credited manual

---

operator actions, are developed through an augmented quality program, which includes software V&V, and seismic and environmental testing to levels consistent with the PSMS.

All credited manual operator actions are included in the human factor engineering (HFE) program described in Chapter 18.

#### **7.5.1.5.1 Quality of Alarms**

The reliability of all PSMS alarms is ensured based on the following design aspects:

- Redundancy is provided for all alarm HSI components including audible and visual devices to ensure no adverse affects by credible malfunctions.
- Separation between redundant segments is provided so that a failure in one segment does not result in the failure of both redundant segments.
- Testability is provided from self-diagnosis of MELTAC and HSI computers.
- An augmented qualification program is provided for alarms for credited related to SPDS.
- Similar environmental, seismic, and EMI/RFI specifications are provided as for the PSMS. Conformance testing differs with respect to the QA level and documentation.

The PCMS provides a highly reliable design for all audible and visual alarms. The reliability of alarms credited for manual action in the safety analysis is further ensured from the following additional design aspects.

- Prompts for credited manual operator actions are provided on PCMS non-safety VDUs and PSMS safety VDUs.
- The PCMS alarms for credited manual operator actions are developed through an augmented quality program, which includes software V&V.
- Diverse alarms from DHP address CCF in PSMS and/or PCMS.
- The parameters for credited manual operator actions are indicated on the safety VDU to accommodate degraded HSI conditions (i.e., loss of PCMS VDUs), since restricted, continued operation with complete loss of PCMS VDUs is within the US-APWR HSI design basis. Indications on the safety VDU are spatially dedicated and continuously visible (SDCV) and include alarm color coding. The safety VDUs provide notification of the plant accident condition to the operator in case of malfunction of the PCMS VDUs.

SECY-93-087 requires the annunciator to meet “applicable” requirements of Class 1E equipment, not all requirements. The intent is to ensure high reliability. Complete IEEE 603 conformance is not appropriate, since most aspects of IEEE Std 603-1991 pertain to the sense, command and execute features of the RPS and ESFAS. PCMS indications and alarms, together with safety VDU indications, provide a highly reliable HSI system to prompt credited manual operator actions.

---

The alarm system configuration including alarms credited for manual actions in safety analysis with safety sensors and non-safety sensors are shown in Figures 7.5-4. In addition to the sufficient reliable PCMS alarm, the parameters for credited manual operator actions are indicated on safety VDU to accommodate degraded HSI conditions (i.e., loss of PCMS VDUs). Restricted, continued operation with complete loss of PCMS VDUs is within the US-APWR HSI design basis. Indications on the safety VDU are spatially dedicated and continuously visible (SDCV), which enables notification of the plant accident condition to the operator in case of malfunction of PCMS VDUs.

PCMS indications and alarms, together with safety VDU indications, provide a highly reliable HSI system to prompt credited manual operator actions.

#### **7.5.1.6 Facilities**

PAM, BISI, plant alarms, and SPDS information is displayed on non-safety HSI equipment at all operations support facilities, including the MCR, RSR, TSC, and EOF. The information displayed in all locations is identical. Duplication of all information important to safety at all operations support locations improves the exchange of information between these facilities and the MCR and assists corporate and plant management in the decision-making process.

A subset of this information is also transmitted to the U.S. Nuclear Regulatory Commission (NRC) via the ERDS.

##### **7.5.1.6.1 Technical Support Center**

The onsite TSC provides the following functions:

- Provides plant management and technical support to plant operations personnel during emergency conditions
- Relieves the reactor operators of peripheral duties and communications not directly related to reactor system manipulations
- Prevents congestion in the MCR
- Performs EOF functions for alert emergency class, for site area emergency class, and for general emergency class until the EOF is functional

Adequate working space for the personnel assigned to the TSC at the maximum level of occupancy is approximately 75 sq ft/person. The TSC working space is sized for a minimum of 25 persons, including 20 persons designated by the licensee and five NRC personnel. The TSC arrangement drawing is shown in Figure 7.5-3. The size and layout of TSC gives necessary space to maintain and repair TSC equipment, and is sufficient for storage of plant records and historical data.

The TSC is the primary onsite communications center for the plant during an emergency. The TSC facility consists of PCMS operational VDUs (information only, no control) and the LDP, which receives plant information from the unit bus. The TSC also provides personal computers with interfaces to external information systems via the station bus. Refer to Section 7.9. PCMS equipment is redundant including its power supply. In



---

addition, the TSC provides telephones and facsimiles machines, which utilize multiple methods of telecommunication, refer to Subsection 9.5.2.

The TSC is located in the access building. Its location is close to the MCR, which is located in the reactor building. The walking time from the TSC to the MCR does not exceed two minutes.

The TSC ventilation system includes high-efficiency particulate air (HEPA) and charcoal absorbers.

The HSI display design is the same as that of the MCR. TSC is discussed in details in Topical Report MUAP-07007 Section 4.2.

#### **7.5.1.6.2 Emergency Operations Facilities**

The EOF is a near site or on-site support facility for the management of overall licensee emergency response (including coordination with federal, state, and local officials), coordination of radiological and environmental assessments, and determination of recommended public protective actions.

The EOF has suitable technical data displays and plant records to assist in the diagnosis of plant conditions and to evaluate the potential or actual release of radioactive materials to the environment. A senior licensee official in the EOF will organize and manage licensee offsite resources to support the TSC and the control room operators.

The COL Applicant is to provide a description of the site-specific EOF.

#### **7.5.1.6.3 Emergency Response Data System**

The ERDS, a data transmission system, is designed to send a set of variables from the plant to the NRC operations center. These data may be used for analyses by the NRC headquarters technical support groups and NRC executive team. The ERDS transmits information that will aid NRC in its role of providing advice and support to the nuclear power plant licensee, state and local authorities, and other federal officials.

Communication systems involved with the EOF and using the ERDS are further discussed in Section 7.9.

### **7.5.2 Design Basis Information**

#### **7.5.2.1 Post Accident Monitoring**

The PAM design for the US-APWR complies with the requirements of the following codes, standard and RG:

- 10 CFR 50, Appendix A: GDC 13 (Reference 7.5-6), 19 (Reference 7.5-7) and 64 (Reference 7.5-8), for specific requirement to provide adequate instrumentation to monitor PA condition(s).
- 10 CFR 50.34(f)(2) "Additional TMI-Related Requirements" (Reference 7.5-9)

- 
- (xi): regarding direct indication of relief and safety valve position.
  - (xii): regarding auxiliary feedwater system flow indication.
  - (xvii): regarding accident monitoring instrumentation.
  - (xviii): regarding inadequate core cooling instrumentation.
  - (xix): regarding instruments for monitoring plant conditions following core damage.
  - (xx): regarding power for pressurizer level indication.
  - RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants" and BTP 7-10 (Reference 7.5-10).
  - IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations"

IEEE Std 497-2002 contains functional and design requirements for accident monitoring instrumentation for nuclear plant. RG 1.97 endorses IEEE Std 497-2002. For the US-APWR, specific PAM variables comply with the selection criteria described in IEEE Std 497-2002.

#### **7.5.2.2 Bypassed and Inoperable Status Indication**

The BISI design for the US-APWR complies with the requirements of the following code and RG:

- RG 1.47, "Bypassed and inoperable Status Indication for Nuclear Power Plant Safety Systems."
- 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements" regarding BISI

#### **7.5.2.3 Plant Annunciators**

The Plant Annunciators design for the US-APWR complies with the following regulatory guidance:

- Staff Requirements Memorandum (SRM) SECY-93-087, Item II.T, "Control Room Annunciator (Alarm) Reliability. (Reference 7.5-11)

#### **7.5.2.4 Safety Parameter Displays System**

The SPDS design for the US-APWR complies with the requirements of the following code and NUREG:

- 10 CFR 50.34 (f)(2)(iv), "Additional TMI-Related Requirements" regarding the SPDS console

- 
- NUREG 0737 Supplement 1, "Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability", with respect to SPDS (Reference 7.5-12)

#### 7.5.2.5 Facilities

The emergency response facility design for the US-APWR complies with the requirements of the following code:

- 10 CFR 50.34 (f)(2)(xxv), "Additional TMI-Related Requirements" regarding emergency response facilities

#### 7.5.3 Analysis

Detailed compliance with the GDC, IEEE Std 603-1991 (Reference 7.5-13) and IEEE Std 7-4.3.2-2003 (Reference 7.5-14) are described in MUAP-07004 Section 3.0, Appendix A and B.

For most accident conditions, RPS and ESFAS are designed to perform required protective functions automatically without any credit for manual action(s). Manual operator actions are credited for mitigating some accident conditions, as defined in the safety analysis. Manual operator actions are also credited for achieving safe shutdown for normal and post accident conditions.

The HFE program described in Chapter 18 includes the design and evaluation process for HSIS to determine the adequacy of the alarms, indications, controls and procedures for all credited manual actions. The results of the HFE program demonstrate that:

1. The operator has sufficient information to perform required manual safety functions (e.g., manual ESF operations, possible unanticipated post accident operations, and monitoring the status of safety equipment).
2. The operator has sufficient time to make reasoned judgments and take action where operator action is essential for maintaining the plant in a safe condition.
3. The HSI is designed in compliance with HFE criteria.
4. The HSI includes all required indications for monitoring conditions in the reactor, the RCS, the containment and safety-related process systems, including ESFs.
5. The HSI includes all required indications for monitoring operating conditions of the plant, including AOOs, PAs, and post-accident conditions, including indications required for PAM.
6. Documentation available to the operator includes the design criteria, the Type of displayed information, number of channels provided, and information of variables including range, accuracy and location.

- 
7. Documentation available to the operator confirms that the system design is adequate to meet its design objectives, and the range and accuracy of displays are consistent with system requirements.

#### 7.5.4 Combined License Information

COL 7.5(1) *The COL Applicant is to provide a description of site-specific PAM variables.*

COL 7.5(2) *The COL Applicant is to provide a description of the site-specific EOF.*

#### 7.5.5 References

- 7.5-1 Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, Regulatory Guide 1.97 Revision 4, June 2006.
- 7.5-2 Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE Std 497 -2002.
- 7.5-3 HSI System Description and HFE Process, MUAP-07007-P Rev.3 (Proprietary) and MUAP-07007-NP Rev.3 (Non-Proprietary), October 2009.
- 7.5-4 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems, Regulatory Guide 1.47 Revision 0, May 1973.
- 7.5-5 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.5-6 Instrumentation and Control, General Design Criteria for Nuclear Power Plant 13, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.
- 7.5-7 Control Room, General Design Criteria for Nuclear Power Plant 19, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.
- 7.5-8 Monitoring Radioactivity Releases, General Design Criteria for Nuclear Power Plant 64, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.
- 7.5-9 Additional TMI-Related Requirements, NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50.34(f)(2).
- 7.5-10 Guidance on Application of RG. 1.97, BTP 7-10 Revision 5, March 2007.
- 7.5-11 Control Room Annunciator (Alarm) Reliability, SECY-93-087, Item II.T.
- 7.5-12 Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability, NUREG 0737 Supplement No. 1, January 1983.

- 
- 7.5-13 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.
- 7.5-14 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.
- 7.5-15 US-APWR Probabilistic Risk Assessment, MUAP-07030 Rev.2 (Proprietary), December 2009.
- 7.5-16 US-APWR US-APWR Equipment Environmental Qualification Program, MUAP-08015 Rev.0, February 2009.
- 7.5-17 Task Working Group #4: High-Integrated Control Rooms –Communication Issues(HICRc), Interrim Staff Guidance, DI&C-ISG-04 Revision 1, March 2009.
- 7.5-18 Guidance for Evaluation of Diversity and Defence-in-Depth in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.
- 7.5-19 Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.
- 7.5-20 Defense in Depth and Diversity Coping Analysis, MUAP-07014-P Rev.2 (Proprietary) and MUAP-07014-NP Rev.2 (Non-Proprietary), December 2009.
- 7.5-21 Setpoint for Nuclear Safety-Related Instrumentation, Regulatory Guide 1.105 Revision 3, December 1999.

**Table 7.5-1 Summary of PAM Variable Types and Source Documents**

<b>Variable Type</b>	<b>Selection Criteria for the Variable Type</b>	<b>Source Documents</b>
A	- Planned manually controlled actions for accomplishment of safety-related functions for which there is no automatic control.	- Plant accident analysis licensing basis - Emergency procedure guidelines (EPGs) or EOPs - Plant abnormal operating procedures (AOPs)
B	- Assess the process of accomplishing or maintaining plant critical safety functions.	- Functional restoration EPGs or - Plant critical safety functions related EOPs - Plant critical safety function status trees
C	- Indicate potential for a breach of fission product barriers - Indicate an actual breach of fission product barriers	- Plant accident analysis licensing basis - Design basis documentation for the fission product barriers - EPGs or EOPs
D	- Indicate performance of safety systems - Indicate the performance of required auxiliary support features - Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition - Verify safety system status	- Plant accident analysis licensing-basis - Event specific EPGs or EOPs - Functional restoration EPGs or EOPs - Plant AOPs
E	- Monitor the magnitude of releases of radioactive materials through identified pathways - Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature) - Monitor radiation levels and radioactivity in the plant environments - Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery	- Procedures for determining radiological releases through plant identified pathways (See Note.) - Procedures for determining plant environs radiological concentration (See Note.) - Procedures for determining plant habitability (See Note.)

Note: These site-specific procedures are to be developed by the COL Applicant in accordance with the guidance provided in DCD Section 13.5.

**Table 7.5-2 PAM Main Design Criteria for Each Variable Type**

Requirements	Type				
	A	B	C	D	E
1. Single Failure	Yes	Yes	Yes	—	—
2. Seismic Qualification	Yes	Yes	Yes	Yes	—
3. Environmental Qualification	Yes	Yes	Yes	Yes	—
4 Power Supply	Yes	Yes	Yes	If required	if required
5. QA	Yes	Yes	Yes	—	—
6. Independence and Separation	Yes	Yes	Yes	—	—
7. Information Ambiguity	Yes	Yes	Yes	—	—
8. Testability	Yes	Yes	Yes	Yes	Yes
9. Continuous Display	Yes	Yes	—	—	—
10. Recording	Yes	Yes	Yes	—	Yes

Note: Yes means it is required.

Table 7.5-3 PAM Variables (Sheet 1 of 3)

Variable	Range	Monitored Function or System	Quantity	Type
Reactor Coolant Hot Leg Temperature (Wide Range)* <sup>1</sup>	32 to 752°F	Core Cooling	1 per Loop	A,B,D
Reactor Coolant Cold Leg Temperature (Wide Range)* <sup>1</sup>	32 to 752°F	Core Cooling	1 per Loop	A,B,D
Reactor Coolant Pressure	0 to 3000 psig	Core Cooling Maintaining RCS Integrity	2	A,B,C, D
Degrees of Subcooling	360°F Subcooling to 360°F Superheat	Core Cooling	2	A,B,D
Pressurizer Water Level* <sup>2</sup>	0 to 100% of Span	Primary Coolant System	4	A,B,D
SG Water Level (Wide Range)* <sup>3</sup>	0 to 100% of Span	Secondary System (SG)	1 per SG	B,D
SG Water Level (Narrow Range)* <sup>2</sup>	0 to 100% of Span	Secondary System (SG)	4 per SG	A,B,D
Main Steam Line Pressure* <sup>2</sup>	0 to 1400 psig	Secondary System (SG)	4 per SG	A,B,D
EFW Flow* <sup>3</sup>	0 to 250% Design Flow	Emergency Feedwater System	1 per Line	A,B,D
Wide Range Neutron Flux	1E-6 to 100% Full Power	Reactivity Control	2	B,D
Core Exit Temperature	200 to 2300°F	Core Cooling Fuel Cladding	2 Train (8 thermocouples for each train)	B,C
Containment Pressure* <sup>2</sup>	-7 to 80 psig	Maintaining RCS Integrity Maintaining Containment Integrity	4	B,C,D
RV Water Level	Bottom of Hot Leg to Top of Vessel	Core Cooling	2	B,D
Containment Isolation Valve Position (Excluding Check Valves)	Open/Closed	Maintaining Containment Integrity	1 per Valve	B,D
Reactor Coolant Soluble Boron Concentration	0 to 4000 ppm	Reactivity Control	-(sampling)	B
CS/RHR Pump Discharge Flow* <sup>4</sup>	0 to 130% Design Flow	RHR or Decay Heat Removal System	1 per Line	D
CS/RHR Pump Minimum Flow* <sup>4</sup>	0 to 110% Design Flow	RHR or Decay Heat Removal System	1 per Line	D
Accumulator Pressure	0 to 1000 psig	Safety Injection System	1 per Tank	D
Accumulator Water Level	0 to 100% Span	Safety Injection System	1 per Tank	D
Safety Injection Pump Discharge Flow	0 to 110% Design Flow	Safety Injection System	1 per Line	D



**Table 7.5-3 PAM Variables (Sheet 2 of 3)**

Variable	Range	Monitored Function or System	Quantity	Type
Safety Injection Pump Minimum Flow	0 to 110% Design Flow	Safety Injection System	1 per Line	D
Refueling Water Storage Pit Water Level (Wide Range)	0 to 100% Span	Safety Injection System	2	B,D
Refueling Water Storage Pit Water Level (Narrow Range)	0 to 100% Span	Safety Injection System	2	B,D
EFW Pit Water Level	0 to 100% Span	Emergency Feedwater System	2 per Pit	B,D
Containment Temperature	32 to 428°F	Containment Cooling Systems	1	D
CCW Header Pressure	0 to 220 psig	Cooling Water System	1 per Line	D
ESW Header Pressure	Plant Specific	Cooling Water System	1 per Line	D
Status of Standby Power and Other Energy Sources Important to Safety		Power Supplies		
• Class 1E ac Bus Voltage	0 to 9 kV ac		1 per Bus	D
• Class 1E dc Bus Voltage	0 to 150 V dc		1 per Bus	D
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	1/2 Tech Spec Limit to 100 Times Tech Spec Limit	Fuel Cladding	-(sampling)	C
Containment High Range Area Radiation* <sup>2</sup>	1 to 1E-7 R/hr	Containment Radiation	4	C,E
MCR Area Radiation	1E-5 to 1 mR/hr	Area Radiation	1	E
TSC Area Radiation	1E-4 to 1E+1 mR/hr	Area Radiation	1	E
Plant Vent Radiation Gas Radiation* <sup>5</sup> (Including High Range)	5E-8 to 1E+5 µCi/cc	Airborne Radioactive Materials Released from Plant	1	E
Main Steam Line Radiation	1E-1 to 1E+3 µCi/cc	Airborne Radioactive Materials Released from Plant	1 per Line	E
GSS Exhaust Fan Discharge Line Radiation* <sup>5</sup> (Including High Range)	5E-8 to 1E+5 µCi/c	Airborne Radioactive Materials Released from Plant	1	E
Condenser Vacuum Pump Exhaust Line Radiation* <sup>5</sup> (Including High Range)	5E-8 to 1E+5 µCi/cc	Airborne Radioactive Materials Released from Plant	1	E
Plant Air Vent High Concentration Sampling System	1E-3 to 1E+2 µCi/cc	Airborne Radioactive Materials Released from Plant Particulates and Halogens	-(sampling)	E

**Table 7.5-3 PAM Variables (Sheet 3 of 3)**

Variable	Range	Monitored Function or System	Quantity	Type
Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	1E-9 to 1E-3 $\mu\text{Ci/cc}$	Environs Radiation and Radioactivity	-(sampling)	E
Plant and Environs Radiation (Portable Instrumentation)	1E-3 to 1E+4 R/hr, photons 1E-3 to 1E+4 rads/hr, beta Radiations and low-energy photons	Environs Radiation and Radioactivity	At least 1	E
Plant and Environs Radioactivity (portable instrumentation)	(Isotopic Analysis)	Environs Radiation and Radioactivity	At least 1	E
MCR Outside Air Intake Radiation	1E-7 to 1E-2 $\mu\text{Ci/cc}$ (Gas) 1E-11 to 1E-5 $\mu\text{Ci/cc}$ (Iodine) 1E-12 to 1E-7 $\mu\text{Ci/cc}$ (Particulate)	Airborne Radioactive Materials taken into MCR	1 for each	E
TSC Outside Air Intake Radiation	1E-7 to 1E-2 $\mu\text{Ci/cc}$ (Gas) 1E-11 to 1E-5 $\mu\text{Ci/cc}$ (Iodine) 1E-12 to 1E-7 $\mu\text{Ci/cc}$ (Particulate)	Airborne Radioactive Materials taken into TSC	1 for each	E
Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	Site specific	Meteorology	1 for each	E

Note:

1. The number of quantity for Reactor Coolant Hot Leg Temperature (Wide Range) and Reactor Coolant Cold Leg Temperature (Wide Range) are one per loop because of having a diversity monitoring of each other.
2. An additional channel is assigned for a single failure concurrent with one channel unlimited instrument bypass for RT and ESF function, while the number of quantity required for Type A, B and C redundant PAM variables is two.
3. The number of quantity for SG Water Level (Wide Range) and EFW Flow is one per loop because of having a diversity monitoring function of each other.
4. CS Flow can be monitored to confirm the CS/RHR System Flow due to the sharing feature of RHR system and CS system flow line.
5. These monitors consist of two normal range monitors, one accident mid range monitor and one accident high range monitor. To function as a PAM variable, these monitors need one normal range, one accident mid range and one accident high range.

**Table 7.5-4 Display Concept for Type A, B PAM Variables**

	Status and Condition for PAM Variable Display	VDU Displays			
Safety VDU not in use for monitoring or control	<p>Type A, B and C variables can be displayed on at least two redundant safety VDUs.</p> <p>A Complete set of Type A and B variables are continuously displayed on safety VDUs in most normal conditions. In this case, a complete set of Type A and B variables are assumed to display in Train A and D safety VDUs.</p> <p>A second complete set of Type A and B variables may be displayed on demand.</p> <p>LDP also displays Type A and B variables.</p>	Safety VDU Train A	Safety VDU Train B	Safety VDU Train C	Safety VDU Train D
		<div>PAM Type A&amp;B</div>	<div>PAM</div>	<div>PAM</div>	<div>PAM Type A&amp;B</div>
Safety VDU in use for monitoring or control	<p>Type A, B and C variables can be displayed on at least two redundant safety VDUs.</p> <p>When any safety VDU (one or more) is changed to operational status for monitoring, control, or testing, Type A and B variables remain continuously displayed on the LDP.</p> <p>Type A and B variables can be recalled for continuous display on any safety VDU through one touch access.</p>	Safety VDU Train A	Safety VDU Train B	Safety VDU Train C	Safety VDU Train D
		<div>Operation</div>	<div>PAM</div>	<div>PAM</div>	<div>PAM</div>
Safety VDU in use for monitoring or control	<p>Type A, B and C variables can be displayed on at least two redundant safety VDUs.</p> <p>When any safety VDU (one or more) is changed to operational status for monitoring, control, or testing, Type A and B variables remain continuously displayed on the LDP.</p> <p>Type A and B variables can be recalled for continuous display on any safety VDU through one touch access.</p>	LDP			
		<div>Type A and B variables</div>			

**Table 7.5-5 List of Accidents and Credited Manual Actions**

<b>Accident</b>	<b>Alarm</b>	<b>Credited Manual Action</b>
Inadvertent Decrease in Boron Concentration in RCS (Subsection 15.4.6)	<ul style="list-style-type: none"><li>- Control Rod Insertion Limit Alarm</li><li>- High Source Range Neutron Flux Alarm</li></ul>	Closure of Charging Flow Isolation Valve or Closure of Primary Makeup Water Control Valve or Stop of Primary Makeup Water Pump
CVCS Malfunction that Increases Reactor Coolant Inventory (Subsection 15.5.2)	High Pressurizer Water Level Alarm	Closure of Charging Line Isolation Valve or Charging Line Containment Isolation Valve
Radiological Consequences of a SG Tube Failure (Subsection 15.6.3)	<ul style="list-style-type: none"><li>- Main Steam Line Radiation (N-16) Alarm</li><li>- Low Pressurizer Water Level against Programmed Water Level Alarm</li></ul>	<ul style="list-style-type: none"><li>- Manual reactor trip</li><li>- Isolation of Affected SG</li><li>- Cooldown of Primary Coolant System by using Main Steam Depressurization Valve</li><li>- Equilibrium of Pressure between Primary and Secondary Coolant System by using Safety Depressurization Valve</li><li>- Stop of Injection from ECCS</li></ul>
Rod Ejection Accidents (Subsection 15.4.8)	Containment High Range Area Radiation Alarm	<ul style="list-style-type: none"><li>- Manual C/V Spray System Operation</li><li>- Manual Annulus Emergency Exhaust System Operation</li></ul>
Failure of Small Lines Carrying Primary Coolant Outside C/V (Subsection 15.6.2)	Low Volume Control Tank Water Level Alarm	RCS Sample Lines or CVCS Letdown Line Isolation

**Table 7.5-6 Function of Type A PAM Variables**

Variable	Monitored Function or System	Required Function
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	- SGTR Safety Analysis - RCS Depressurization based on EOPs in SGTR event
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Reactor Coolant Pressure	- Core Cooling - Maintaining RCS Integrity	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	- SGTR Safety Analysis - Manual action based on EOPs such as Safety injection termination in SGTR event
SG Water Level (Narrow Range)	Secondary System (SG)	
EFW Flow	Emergency Feedwater System	

**Table 7.5-7 Function of Type B PAM Variables**

Variable	Monitored Function or System	Required Function
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	Assess process of accomplishing manual RCS cooling
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	
Reactor Coolant Pressure	- Core Cooling - Maintaining RCS Integrity	Assess process of manual RCS depressurization
SG Water Level (Wide Range)	Secondary System (SG)	Assess maintaining SG Heat Removal Function
SG Water Level (Narrow Range)	Secondary System (SG)	
EFW Flow	Emergency Feedwater System	
Wide Range Neutron Flux	Reactivity Control	- Assess maintaining sub-critical state - Monitoring neutron flux decreasing after reactor trip
Core Exit Temperature	- Core Cooling - Fuel Cladding	Assess maintaining Core Cooling
RV Water Level	Core Cooling	
Containment Pressure	- Maintaining RCS Integrity - Maintaining Containment Integrity	- Assess maintaining CV Integrity - Monitoring CV pressure response
Containment Isolation Valve Position (Excluding Check Valves)	Maintaining Containment Integrity	Assess the process of accomplishing or maintaining CV Isolation
Reactor Coolant Soluble Boron Concentration	Reactivity Control	Indicate boron concentration (sampling)
Refueling Water Storage Pit Water Level (Wide Range)	Safety Injection System	Verifying safety injection source
Refueling Water Storage Pit Water Level (Narrow Range)	Safety Injection System	
EFW Pit Water Level	Emergency Feedwater System	Verifying EFW source

**Table 7.5-8 Function of Type C PAM Variables**

Variable	Monitored Function or System	Required Function
Core Exit Temperature	- Core Cooling - Fuel Cladding	- Indicate potential for a breach of fission product barriers - Indicate an actual breach of fission product barriers
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	Fuel Cladding	Indicate an actual breach of fission product barriers
Containment High Range Area Radiation	Containment Radiation	

**Table 7.5-9 Function of Type D PAM Variables**

<b>Variable</b>	<b>Monitored Function or System</b>	<b>Required Function</b>
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	Monitoring Long Term Core Cooling
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Reactor Coolant Pressure	- Core Cooling - Maintaining RCS Integrity	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	
RV Water Level	Core Cooling	
SG Water Level (Wide Range)	Secondary System (SG)	Monitoring Long Term SG Heat Removal
SG Water Level (Narrow Range)	Secondary System (SG)	
EFW Flow	Emergency Feedwater System	
EFW Pit Water Level	Emergency Feedwater System	
Wide Range Neutron Flux	Reactivity Control	Monitoring Long Term Reactor Shutdown State
Containment Pressure	- Maintaining RCS Integrity - Maintaining Containment Integrity	Monitoring CV Integrity
Containment Temperature	Containment Cooling Systems	
Containment Isolation Valve Position (Excluding Check Valves)	Maintaining Containment Integrity	Monitoring CV Isolation
CS/RHR Pump Discharge Flow	RHR or Decay Heat Removal System	Indicate performance of CV spray system
CS/RHR Pump Minimum Flow	RHR or Decay Heat Removal System	
Accumulator Pressure	Safety Injection System	Indicate performance of Accumulator
Accumulator Water Level	Safety Injection System	
Safety Injection Pump Discharge Flow	Safety Injection System	Indicate performance of Safety Injection system
Safety Injection Pump Minimum Flow	Safety Injection System	
Refueling Water Storage Pit Water Level (Wide Range)	Safety Injection System	
Refueling Water Storage Pit Water Level (Narrow Range)	Safety Injection System	
CCW Header Pressure	Cooling Water System	
ESW Header Pressure	Cooling Water System	Indicate performance of ESW system
Status of Standby Power and Other Energy Sources Important to Safety	Power Supplies	Verifying Energy Sources
Class 1E ac Bus Voltage		
Class 1E dc Bus Voltage		



**Table 7.5-10 Function of Type E PAM Variables**

<b>Variable</b>	<b>Monitored Function or System</b>	<b>Required Function</b>
MCR Area Radiation	Area Radiation	Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery
TSC Area Radiation	Area Radiation	
MCR Outside Air Intake Radiation	Airborne Radioactive Materials taken into MCR	
TSC Outside Air Intake Radiation	Airborne Radioactive Materials taken into TSC	
Plant Vent Radiation Gas Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	Monitor the magnitude of releases of radioactive materials through identified pathways
Main Steam Line Radiation	Airborne Radioactive Materials Released from Plant	
GSS Exhaust Fan Discharge Line Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	
Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	
Plant Air Vent High Concentration Sampling System	Airborne Radioactive Materials Released from Plant Particulates and Halogens	
Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	Environs Radiation and Radioactivity	Monitor radiation levels and radioactivity in the plant environs
Plant and Environs Radiation (Portable Instrumentation)	Environs Radiation and Radioactivity	
Plant and Environs Radioactivity (Portable Instrumentation)	Environs Radiation and Radioactivity	
Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	Meteorology	Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways

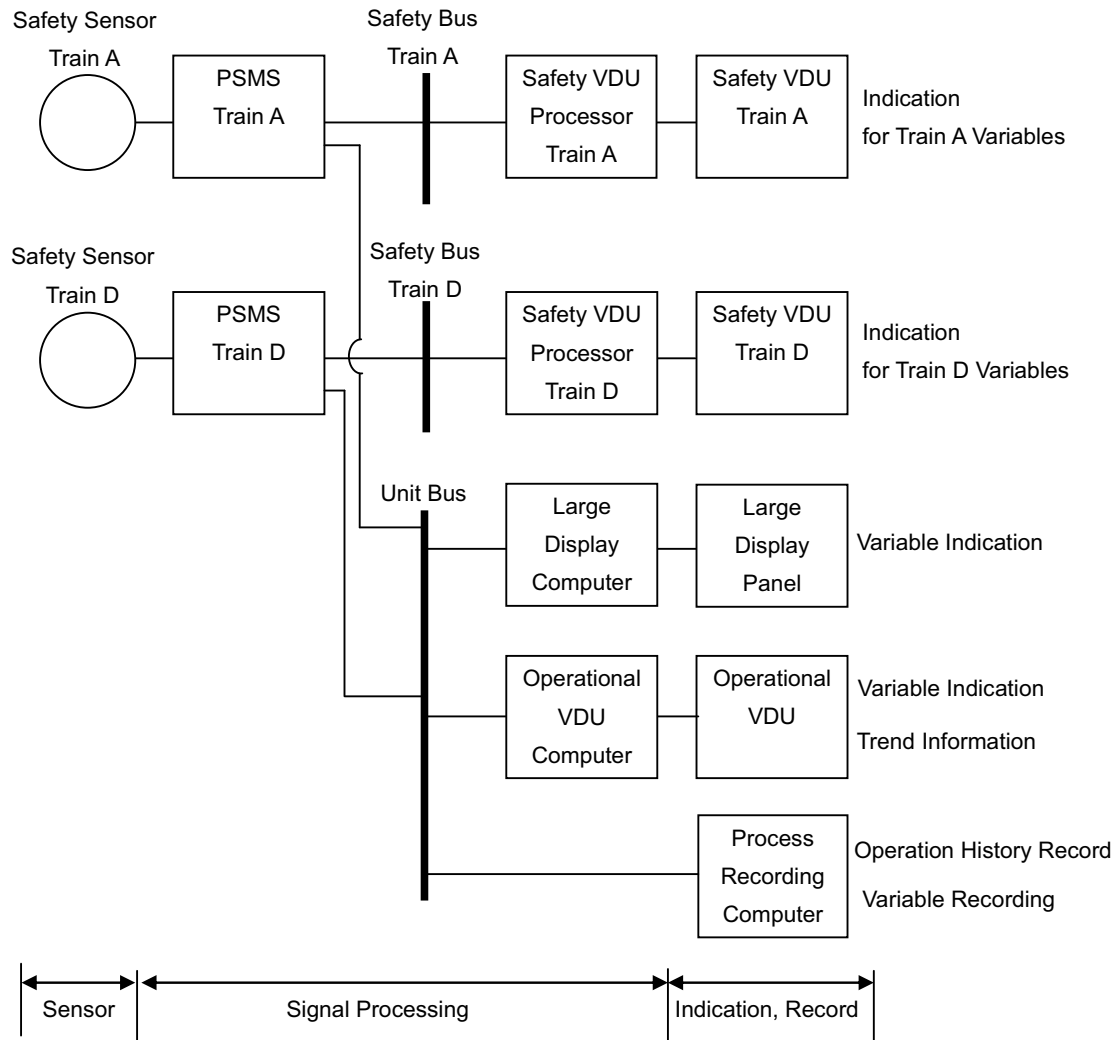
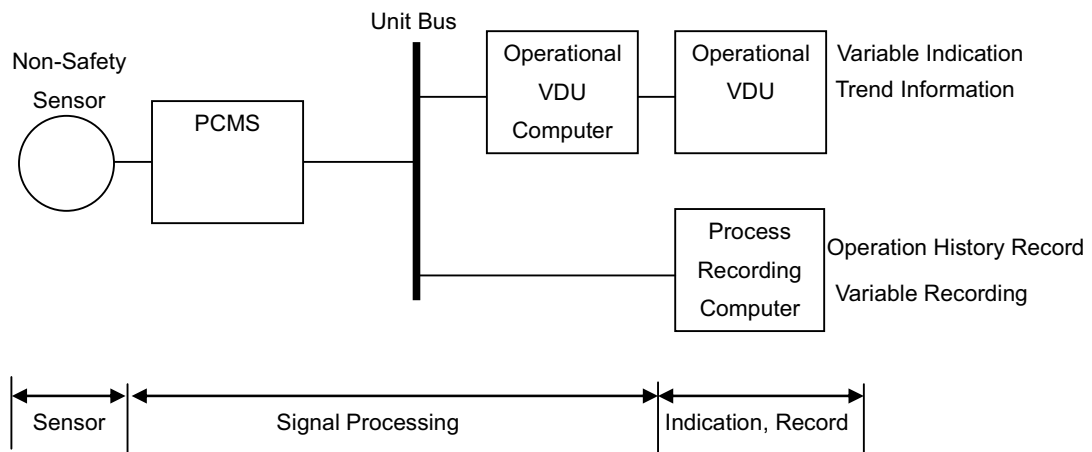
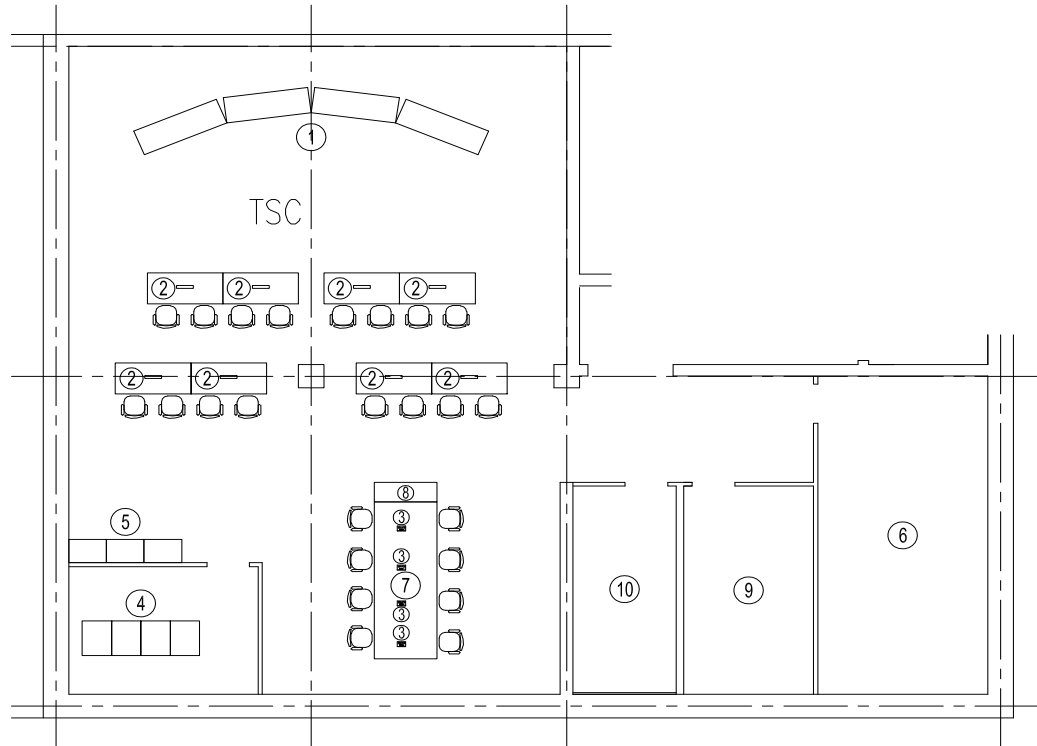


Figure 7.5-1 Configuration of Signal Processing for Safety PAM Variables

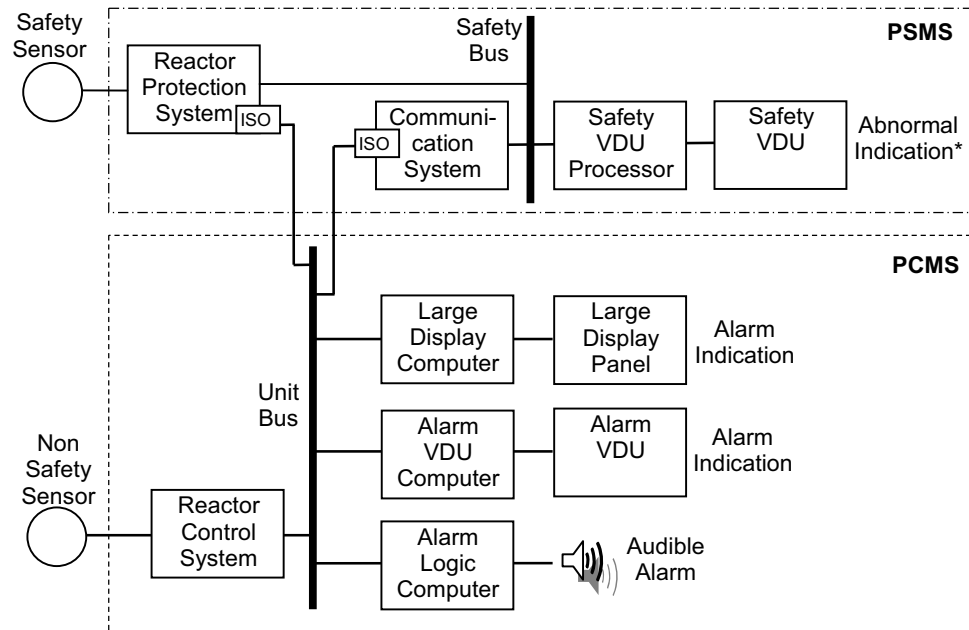


**Figure 7.5-2 Configuration of Signal Processing for Non-Safety PAM Variable**



	Contents
1	Large Display Panel
2	Plant Monitoring VDUs
3	Communication equipments (phone, facsimiles, etc.)
4	Display Processor Data Transmitter
5	Cabinet for plant records and historical data, etc.
6	NRC consultation rooms
7	Sufficient table and chairs for staffs
8	Printers/hardcopies
9	Kitchen
10	Rest room

**Figure 7.5-3 Layout of TSC**



\*1 Alarms to prompt credited manual actions in safety analysis are indicated on the safety VDU as abnormal indications.

**Figure 7.5-4 Alarm System Configuration**

## 7.6 Interlock Systems Important to Safety

This section describes interlock systems important to safety. These interlocks are provided to:

- Prevent accident conditions.
- Ensure availability of safety functions.

### 7.6.1 System Description

The PSMS provides the interlock systems important to safety for the plant, with the exception of electro-mechanical interlocks within the electrical distribution system.

Except as noted for specific interlocks described below:

Interlocks are tested using the input test, self-test and output test methods as described in Subsections 7.1.3.10 and 7.1.3.11.

Bypassed and inoperable status of all interlocks is provided via BISI. BISI is discussed in Section 7.5.

The following sections describe all interlock functions.

#### 7.6.1.1 CS/RHR Pump Hot Leg Isolation Valve Open Permissive Interlock

During RHRS operation, the CS/RHR pump takes suction from the RCS hot legs, routes the reactor coolant through the CS/RHR heat exchangers, and returns the reactor coolant back to the reactor via RCS cold legs. In general, compared to the RCS, RHRS is a low-pressure system. An inadvertent connection between the RCS and RHRS while reactor coolant pressure is greater than RHR design pressure could lead to over pressurization of the RHRS. Over-pressurization could damage and disable the RHRS, and could lead to inter-system loss of reactor coolant. The RHR system is designed with sufficient wall thickness to withstand normal operating RCS pressure without rupture when both CS/RHR pump hot leg isolation valves are inadvertently opened, as described in Subsection 5.4.7.1.

The US-APWR RHRS is placed in operation only when the pressure and temperature of the RCS are approximately at or below 400 psig and 350°F, respectively. To preclude over pressurization of the RHRS, a reactor coolant pressure interlock is provided for the MOVs that interconnect the RHRS to the RCS. Unless the reactor coolant pressure is less than the setpoint for RHR operation, these MOVs cannot be opened. If the MOVs open for RHR operation, and the reactor coolant pressure increases above the setpoint, an alarm is initiated. This interlock for CS/RHR pump hot leg isolation valves are shown in Figure 7.6-1. These valves are typically open at low-pressure conditions (i.e., during cold shutdown) while below the allowable pressure setpoint. During startup, the valves are manually locked closed (power is removed) to prevent these valves from opening and exposing the RHRS to an over-pressure condition. The valves will not be placed on service again until the subsequent plant cooldown.

The piping connecting the RCS hot leg to RHR pump suction is provided with two MOVs connected in series for each RHR train (8 valves total):

- For RHR train A, the valves are assigned to train A.
- For RHR train B, the valves are assigned to train B.
- For RHR train C, the valves are assigned to train C.
- For RHR train D, the valves are assigned to train D.

Redundant (two) valves in series, ensures that over pressurization will not occur even in presence of a single valve failure. The safety interlock prevents valve opening unless the reactor coolant pressure is less than the setpoint for RHR operation.

The signal path for this interlock is from the reactor coolant pressure transmitters to the RPS, and then to the SLS, which controls the MOVs via motor control centers.

CS/RHR pump hot leg isolation valves open permissive interlock does not have independence and diversity in each train, because the current design of RHR system has sufficiently high reliability against overpressurization or possible radioactive release. Moreover the valves cannot be opened inadvertently because power is normally removed as described above.

#### 7.6.1.2 CS/RHR Valve Open Block Interlock

Common CS/RHR pumps are shared between the CSS and RHRS. The CSS and RHRS will not be required at the same time. CSS will be required in the beginning of an AOO or PA to reduce the containment pressure, while the RHR will be employed in the later part of the event to remove decay heat.

- Simultaneous-open block interlock with RHR discharge line containment isolation valve and CS header containment isolation valve;

Valves are provided for CS/RHR pump discharge for each CS and RHR line. If CS and RHR lines are opened simultaneously, the CS/RHR pump will be loaded beyond its capacity. This could lead to a pump run-out condition, which would damage the CS/RHR pumps. To preclude opening both systems valves simultaneously an interlock is provided to block simultaneous opening of the RHR discharge line containment isolation valve and the CS header containment isolation valve. The interlock functions to prevent opening a valve that is closed. This interlock prevents CS and RHR system from operating simultaneously to prevent a pump run-out situation. The interlocks for these valves are shown in Figures 7.6-2 and 7.6-3. For RHS-MOV-021A, B, C, D, the piping diagrams for these valves are shown in Figure 5.4.7-2 in Chapter 5, and for CSS-MOV-004A, B, C, D in Figure 6.2.2-1 of Chapter 6.

- Simultaneous-open block interlock with CS/RHR pump hot leg isolation valve and CS header containment isolation valve;

Since the CS/RHR pumps are also used for containment spray, there is a potential for valve misalignment that could lead to pumping RCS inventory through the CS lines. This would result in the inadvertent depletion of RCS inventory. To prevent this condition an interlock is provided to block simultaneous opening of the RCS suction line valves to the CS/RHR pumps and the CS discharge line valves. This interlock prevents CS and RHR systems operating simultaneously, which could lead to inadvertent depletion of RCS inventory. The interlocks for these valves are shown in Figure 7.6-1 and 7.6-3. For RHS-MOV-001A, B, C, D, the piping diagrams for these valves are shown in Figure 5.4.7-2 in Chapter 5, for RHS-MOV-002A, B, C, D in Figure 5.4.7-2 of Chapter 5, and for CSS-MOV-004A, B, C, D in Figure 6.2.2-1 in Chapter 6.

All interlocks discussed above are between valves within the same division:

- For CS/RHR train A, the interlocked valves are assigned to train A.
- For CS/RHR train B, the interlocked valves are assigned to train B.
- For CS/RHR train C, the interlocked valves are assigned to train C.
- For CS/RHR train D, the interlocked valves are assigned to train D.

A single interlock failure may result in valve misalignment within a single division, but this will not adversely affect the other divisions. The safety related interlocks preclude multiple valve misalignment due to spurious commands from operational VDUs.

The signal path for this interlock is from the valve limit switches to the component control logic for each valve within the SLS.

#### **7.6.1.3 Primary Makeup Water Line Isolation Interlock**

The CVCS regulates boron concentration in the RCS by controlling the flow of reactor makeup water from sources that contain primary makeup water and borated water.

Redundant interlocks are provided to close two series isolation valves in the primary makeup water supply flow path. This interlock actuates when the monitored primary makeup water flow exceeds its high setpoint. This interlock blocks primary makeup water supply flow, preventing over dilution of the RCS. The interlocks for primary makeup water line isolation valves are shown in Figure 7.6-4. For CVS-FCV-128, 129 the piping diagrams for these valves are shown in (Figure 9.3.4-1 (Sheet 4 of 7)) in Chapter 9.

The two-train redundancy of this design provides over dilution protection even in the presence of a single failure. The safety related interlocks preclude multiple valve misalignment due to spurious commands from operational VDUs.

The signal path for this interlock is from local flow transmitters to the RPS, and then to the SLS, which controls each isolation valve.



#### 7.6.1.4 Accumulator Discharge Valve Open Interlock

Each of the four RCS loops is provided with a separate accumulator. Each ECCS accumulator discharge line connecting to the RCS cold leg is provided with a motor operated isolation valve. Normally the isolation valve is open; therefore, the accumulator system is normally available for its designed function.

The accumulator discharge valve can be closed manually. However, an interlock is provided to open this valve when the reactor coolant pressure is above the P-11 setpoint. The interlocks for these valves are shown in Figure 7.6-5. The safety related interlocks preclude multiple valve misalignment due to spurious commands from operational VDUs.

This interlock may be manually bypassed for test and maintenance to close the accumulator discharge valve by two deliberate operator actions. If this valve is closed and not selected to "Lock", then the ECCS actuation signal will automatically open the valve and make the accumulator system available. The "Lock" function is described in Topical Report MUAP-07007 (Reference 7.6-1) Section 4.5.3.a.

The accumulator system can be bypassed for test and maintenance by manually closing its discharge valve and selecting it to "Lock". In the "Lock" mode, the accumulator discharge valves will not automatically open, therefore the affected accumulator will be un-available for its designed ESF function. During this condition, the inoperable status of the accumulator is alarmed in the MCR and indicated continuously on the BISI system displays.

The signal path for this interlock is from the pressurizer pressure transmitters to the RPS, and then to the SLS, which controls these MOVs via motor control centers.

#### 7.6.1.5 CCW Supply and Return Header Tie Line Isolation Interlock

The CCW system consists of two independent subsystems. Each subsystem consists of two 50% trains. One subsystem consists of trains A & B, and the other subsystem consists of trains C & D, for a total of four 50% trains. There are cross-connections between trains A and B, and between trains C and D. Each subsystem supplies a non-essential safety class loop and a non-safety loop. There are two series motor-operated isolation valves for each supply and return tie line between separate trains. These isolation valves ensure each mechanical safety train is isolated from any potential passive failure in the non-safety portion or another mechanical safety train of the CCWS.

The two series isolation valves in each CCW header are automatically closed during the following conditions:

- ECCS actuation combined with LOOP
- CS actuation
- Low CCW surge tank water level

For NCS-MOV-007A, B and NCS-MOV-020A, B the piping diagrams for these valves are shown in Figure 9.2.2-1 (Sheet 1 of 9) in Chapter 9, and for NCS-MOV-007C, D and NCS-MOV-020C, D in Figure 9.2.2-1 (Sheet 2 of 9) of Chapter 9.

The interlocks for these valves are shown in Figure 7.6-6. These interlocks ensure the independence of each safety mechanical train of the CCWS thereby providing CCW coolant to ESF systems required for mitigating conditions of the event. The safety related interlocks preclude multiple valve misalignment due to spurious commands from operational VDUs.

These interlocks may be manually bypassed for reopening the valves to restore RCP seal and spent fuel pit heat exchanger cooling, if required. The bypass can be selected from the safety VDU. To select the bypass from the operational VDU, the Bypass Permissive for the respective train must be enabled.

Two series valves assigned to different trains ensures isolation even in the presence of a single failure.

The signal path for the ECCS and CS interlocks is from the ESFAS to the SLS that controls the isolation valves through motor control centers. The signal path for the surge tank interlock is from local level transmitters to the RPS to the SLS for control of these same valves.

#### **7.6.1.6 RCP Thermal Barrier HX CCW Return Line Isolation Interlock**

Each CCW subsystem supplies cooling water to the RCP thermal barrier heat exchanger. Two motor-operated valves and flow meters are located at the CCW outlet line of the RCP thermal barrier heat exchanger.

These valves close automatically upon a high flow rate signal at the outlet of this line in the event of in-leakage from the RCS through the thermal barrier heat exchanger, and prevent this in-leakage from further contaminating the CCWS.

The interlocks for these valves are shown in Figure 7.6-7. The safety related interlocks preclude multiple valve misalignment due to spurious commands from Operational VDUs.

These interlocks ensure isolation of in-leakage from the RCS through the thermal barrier heat exchanger.

The signal path for these interlocks is from the local flow transmitters to the RPS, and then SLS, which controls these MOVs via motor control centers.

#### **7.6.1.7 Low-pressure Letdown Line Isolation Interlock**

A single normally closed air-operated valve is placed in each of the two low pressure letdown lines connected to two of the four RHR trains. During the normal plant cool down operation, one of these valves is open to divert a portion of the RCS flow to the CVCS for the purpose of purification and RCS inventory control.

Additionally at mid-loop operation during plant shutdown, these valves are automatically closed and the CVCS is isolated from the RHRS after receiving the RCS loop low-level signal to prevent loss of RCS inventory.

The interlocks for these valves are shown in Figure 7.6-8. One of these valves of RHS-(AOV-024B,024C) the piping diagrams for these valves are shown in Figure 5.4.7-2 in

Chapter 5. The safety related interlocks preclude multiple valve misalignment due to spurious commands from Operational VDUs.

The signal path for these interlocks is from the local pressure transmitters to the RPS, and then SLS, which controls these MOVs via motor control centers.

### 7.6.2 Design Basis Information

The interlock systems important to safety comply with the following codes and standards:

1. 10 CFR 50.55a(a)(1), "Quality Standards."
2. 10 CFR 50.55a(h), "Protection and Safety Systems,"
3. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records."
4. GDC 2, "Design Bases for Protection Against Natural Phenomena."
5. GDC 4, "Environmental and Dynamic Effects Design Bases."
6. GDC 10 "Reactor Design"
7. GDC 13, "Instrumentation and Control."
8. GDC 15 "Reactor Coolant System Design"
9. GDC 16 "Containment Design"
10. GDC 19, "Control Room."
11. GDC 20 "Protection System Functions"
12. GDC 21 "Protection Systems Reliability and Testability"
13. GDC 22 "Protection System Independence"
14. GDC 23 "Protection System Failure Modes"
15. GDC 24, "Separation of Protection and Control Systems."
16. GDC 25 "Protection System Requirements for Reactivity Control Malfunctions"
17. GDC 28 "Reactivity Limits"
18. GDC 29 "Protection Against AOOs"
19. GDC 34 "Residual Heat Removal"
20. GDC 35 "Emergency Core Cooling"

- 
- |     |   |
|-----|---|
| 21. | GDC 38 "Containment Heat Removal"   |
| 22. | GDC 41 "Containment Atmosphere Cleanup"   |
| 23. | GDC 44 "Cooling Water"  |
| 24. | 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements, Bypass and Inoperable Status Indication" |

#### **7.6.2.1 Single Failure Criterion**

Compliance with the single failure criterion is discussed for each interlock in the sections above.

#### **7.6.2.2 Quality of Components and Modules**

All interlocks important to safety are implemented using Class 1E components with a corresponding quality program.

#### **7.6.2.3 Independence**

Redundancy and independent train assignments are specifically discussed for each interlock in the sections above.

#### **7.6.2.4 System Testing and Inoperable Surveillance**

System testing and inoperable surveillance for all interlocks is described in Subsection 7.6.1.

#### **7.6.2.5 Use of Digital Systems**

All interlocks important to safety are implemented in the PSMS, which is a digital system. This includes sensor monitoring and bistable functions, and interlock logic. The final SLS output (i.e., open or close), which interfaces to the controlled plant component, reflects the result of combining all manual, automatic and interlock control signals.

### **7.6.3 Analysis**

Detailed compliance to the GDC, IEEE Std 603-1991 (Reference 7.6-2) and IEEE Std 7-4.3.2-2003 (Reference 7.6-3) are described in MUAP-07004 (Reference 7.6-4) Section 3.0, Appendix A and B.

All the interlocks important to safety provide protection for plant mechanical systems or protection to prevent plant accident conditions. All the interlocks are implemented by the PSMS.

According to RG 1.206 (Reference 7.6-5) the following categories of interlocks are described:

- Interlocks to prevent overpressurization of low-pressure systems:
  - This is the RCS/RHR interlock discussed in Subsection 7.6.1.1.

- 
- Interlocks to prevent overpressurization of the primary coolant system during low-temperature operations of the RV:
    - There are no interlocks necessary to prevent overpressurization of the RCS during low-temperature operations of the RV. Refer to Subsection 5.2.2.
  - Interlocks for ECCS Accumulator Valves:
    - The ECCS accumulator valve Interlock is discussed in Subsection 7.6.1.4.
  - Interlocks required to isolate safety systems from non-safety systems:
    - This is the CCW Interlock discussed in Subsection 7.6.1.5.
  - Interlocks required to preclude inadvertent inter-ties between redundant or diverse safety systems:
    - There are no interlocks required to preclude inadvertent inter-ties in the US-APWR, except in the CCWS, since safety systems, such as safety injection system, residual heat removal system, containment spray system, and essential service water system, are mechanically separated in each train.
    - Redundant I&C trains are protected from inadvertent inter-ties, such as those cause by electrical faults, by qualified isolation devices described in Subsection 7.1.3.5.
    - Inadvertent inter-ties between safety systems and the DAS are discussed in Section 7.8.
    - Redundant mechanical trains (i.e., redundant CCW trains) are protected as discussed in Subsection 7.6.1.5.

#### 7.6.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

#### 7.6.5 References

- 7.6-1 HSI System Description and HFE Process, MUAP-07007-P Rev.3 (Proprietary) and MUAP-07007-NP Rev.3 (Non-Proprietary), October 2009.
- 7.6-2 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-1991.
- 7.6-3 IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2003.
- 7.6-4 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.

7.6-5      Combined License Applications for Nuclear Power Plants (LWR Edition),  
Regulatory Guide 1.206 Revision 0, June 2007.

1st CS/RHR Pump Hot Leg Isolation Valve  
2nd CS/RHR Pump Hot Leg Isolation Valve

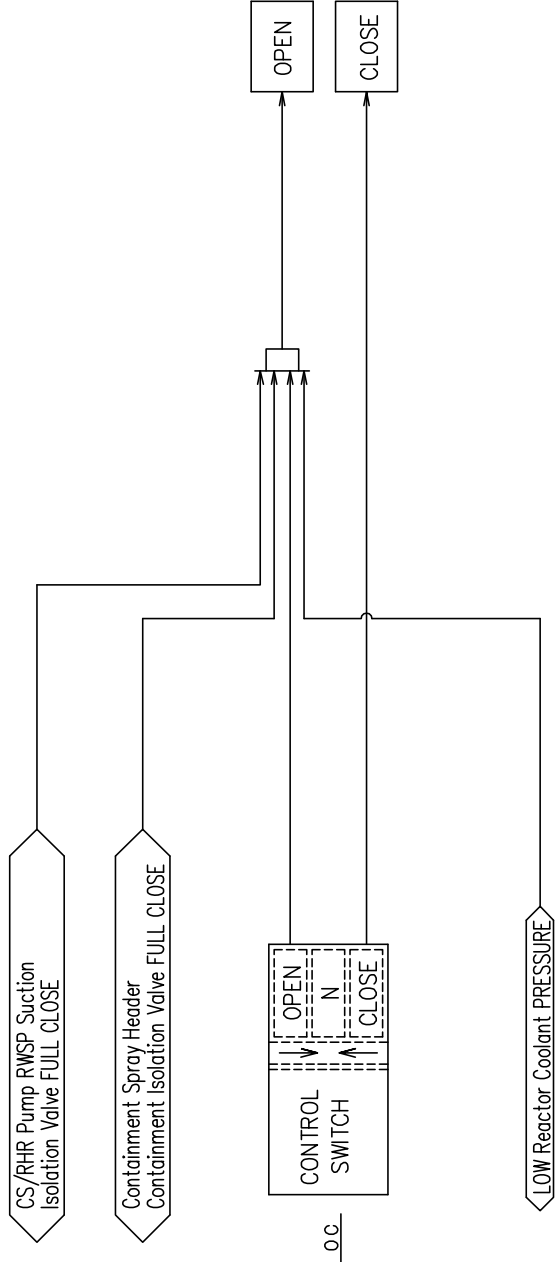


Figure 7.6-1 Interlocks for CS/RHR Pump Hot Leg Isolation Valves

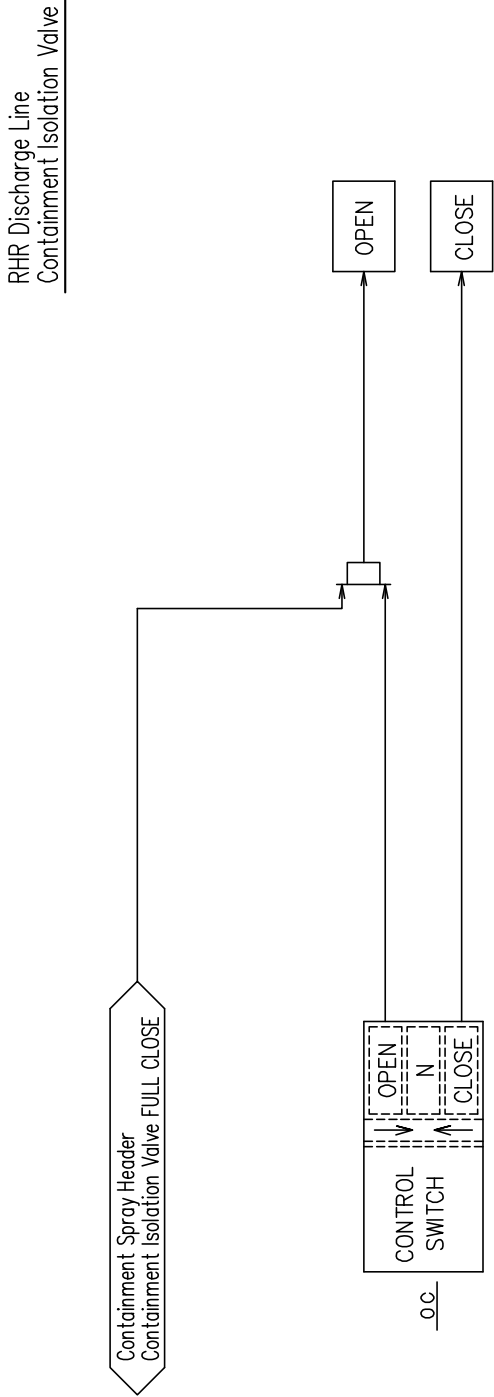


Figure 7.6-2 Interlocks for RHR Discharge Line Containment Isolation Valve



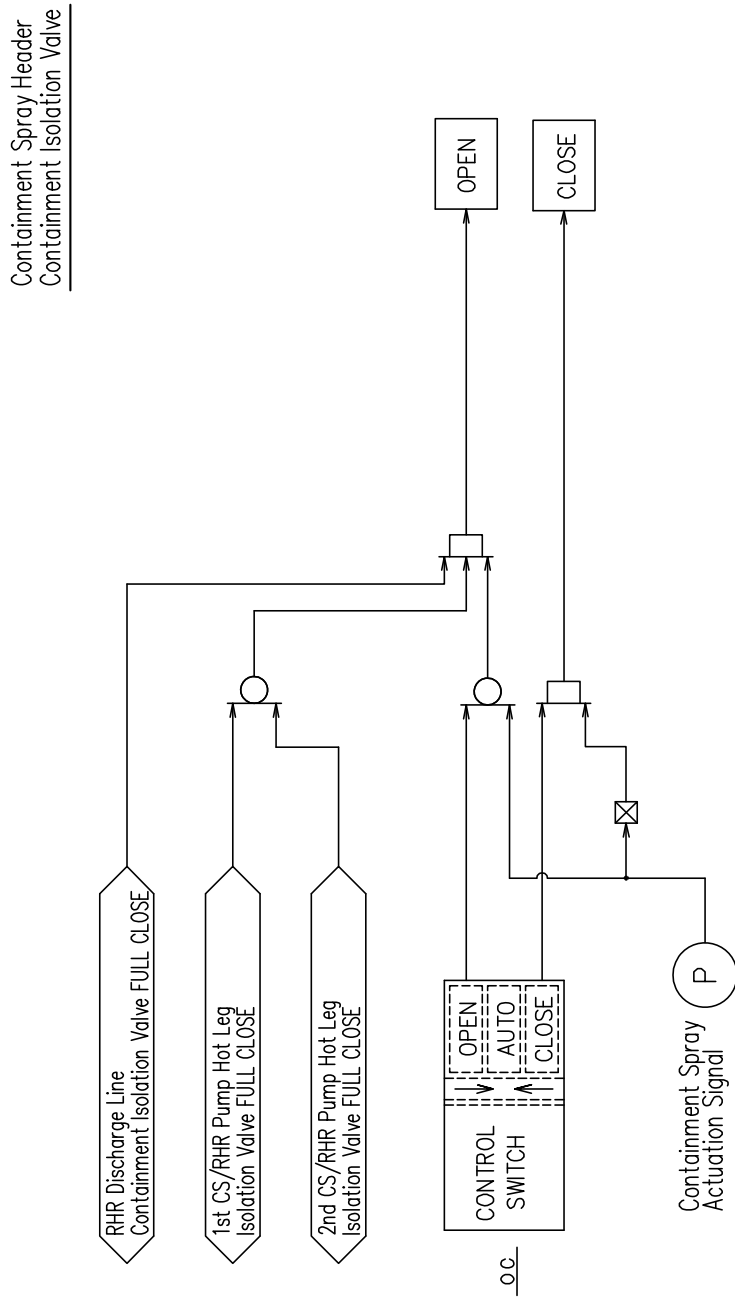


Figure 7.6-3 Interlocks for Containment Spray Header Containment Isolation Valve

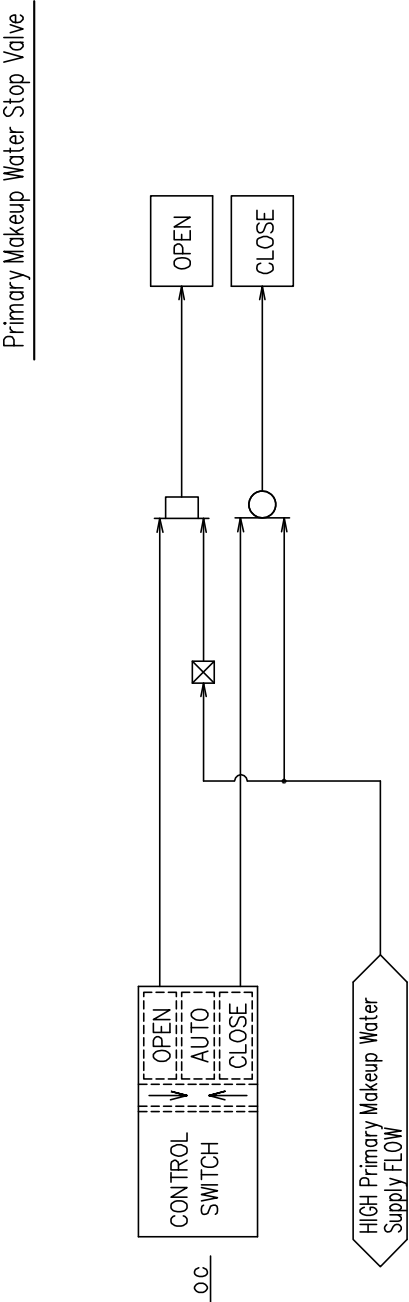


Figure 7.6-4 Interlocks for Primary Makeup Water Stop Valve

Accumulator Discharge Valve

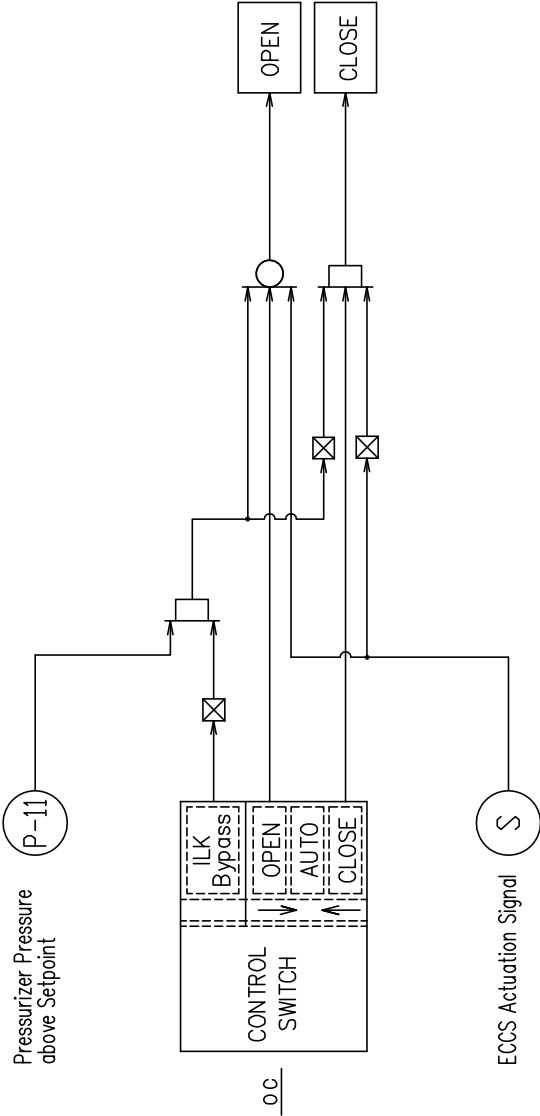


Figure 7.6-5 Interlocks for Accumulator Discharge Valve

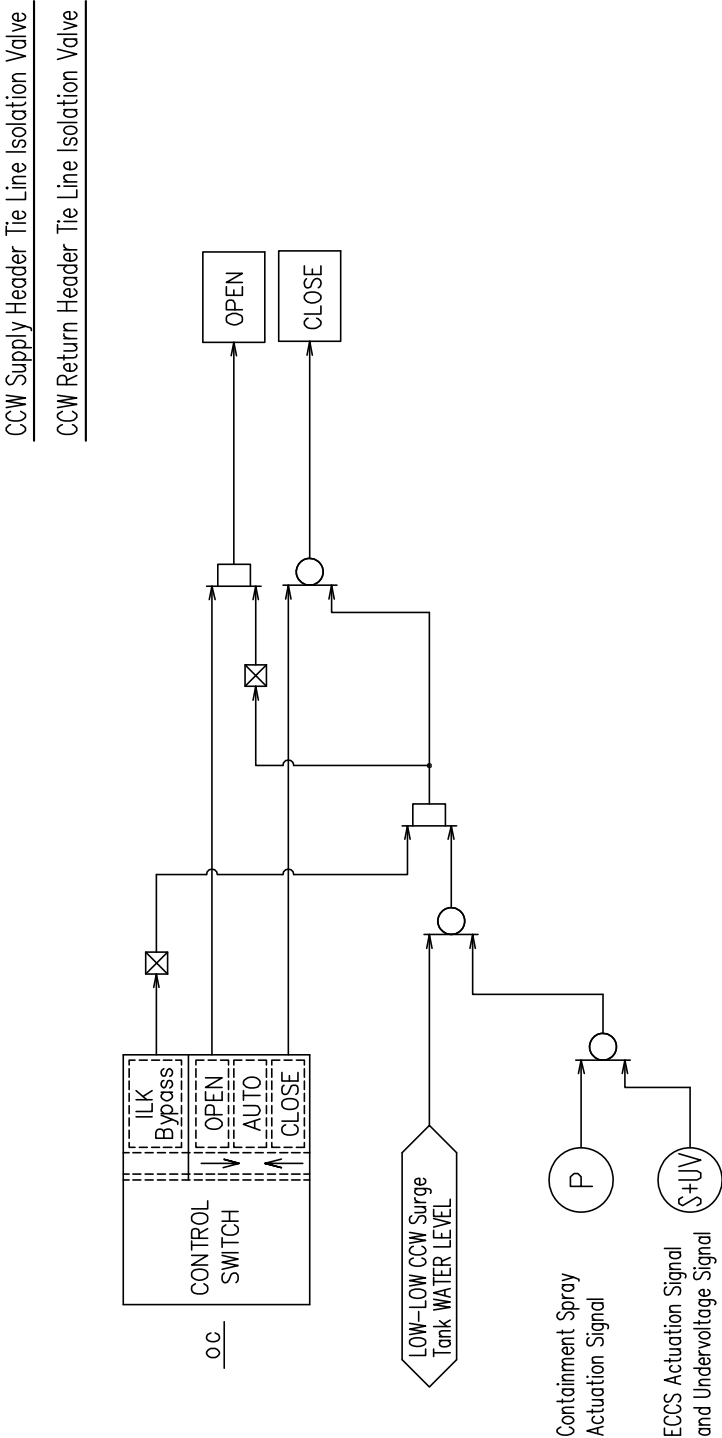


Figure 7.6-6 Interlocks for CCW Header Tie Line Isolation Valves

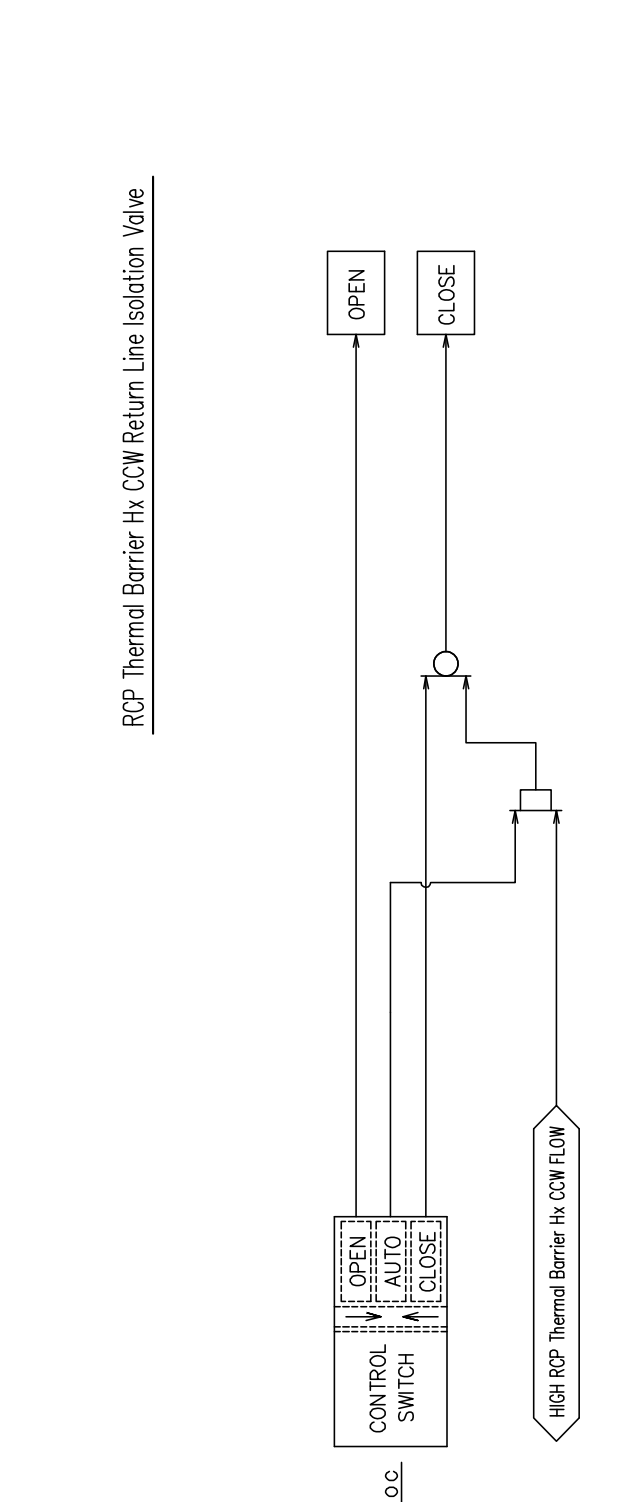


Figure 7.6-7 Interlocks for RCP Thermal Barrier Hx CCW Return Line Isolation Valve

Low Pressure Letdown Line Isolation Valve

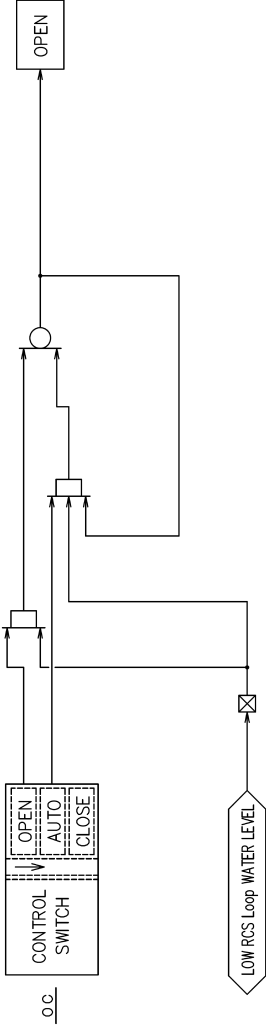


Figure 7.6-8 Interlocks for Low Pressure Letdown Line Isolation Valve

### 7.7 Control Systems Not Required for Safety

The function of the US-APWR control systems not required for safety is to establish and maintain the plant operating conditions within prescribed limits. These control systems improve plant safety by minimizing the frequency of protection responses required and relieve the operator from routine tasks.

The control functions not required for safety are implemented by the PCMS. The PCMS regulates conditions in the plant automatically in response to changing plant conditions and changes in plant load demand. These operating conditions include the following:

- Step load changes of plus or minus 10% while operating in the range of 15 to 100% of full power.
- Ramp load changes of plus or minus 5% per minute while operating in the range of 15 to 100% of full power (subject to core power distribution limits)
- Full load rejection from 100% power

These capabilities are accomplished without a reactor trip. Full load rejection is an event in which the main generator is cut off from the transmission system by a tripping of the main transformer breaker or the switchgear breaker without causing a turbine trip. In a load rejection scenario, the turbine governor valves are immediately fully closed, and the turbine bypass valves are opened fully, dumping the excess steam in the condenser. Reactor power is decreased by the automatic insertion of the control rods.

The AOOs defined in the plant safety analysis that must be considered in the control function design are listed in Table 7.7-1. To ensure the PCMS failures do not cause the concurrent AOOs that have not been considered in the plant safety analysis, control functions are distributed to separate the PCMS controller groups as shown in Table 7.7-2. The following sections describe the control functions and the features of those functions that ensure credible control system failures are bounded by the plant safety analysis.

#### 7.7.1 Description

The following sections describe US-APWR control functions not required for safety that can affect the performance of critical safety functions.

##### 7.7.1.1 Reactor Control System

The reactor control system section in the PCMS provides the following automatic functions to respond to the load changes described above.

##### 7.7.1.1.1 Rod Control

The rod control function controls the reactor coolant average temperature ( $T_{avg}$ ) by sending control signals to the CRDM control system to adjust control rod bank positions, refer to Figure 7.2-2 sheet 16. For any RCS loop, the  $T_{avg}$  is the average value of the reactor coolant hot leg and cold leg temperatures.

The difference between the programmed reference temperature (which is based on turbine inlet pressure), and the lead/lag compensated value of the  $T_{avg}$  signal from all four reactor coolant loops becomes the primary demand signal for the rod control. This primary demand signal is further varied using an additional control input signal, which is derived from the reactor power versus turbine load mismatch signal. This mismatch signal improves system performance by enhancing response and reducing transient peaks. The programmed coolant temperature increases linearly with turbine load from the zero-power to the full-power condition. As the temperature difference increases, the demanded rod speed also increases. A dead band is included in the system to preclude rod motion when the temperature error is within the dead band.

The  $T_{avg}$  input signals for the rod control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for rod control function.

The output signals from the rod control function of the PCMS are interfaced to the CRDM control system via the data links.

The PCMS provides the following HSI signals for rod control function.

- Rod control auto/manual - Allows transfer between the Automatic control mode of the control rod control banks by rod control or Manual control mode.
- Control rod bank selector - Allows selection of the desired control rod bank for manual motion demand when in the manual mode.
- Control rod lift coil disconnection selector - Allows disconnection of lift coil signal for a selected control rod to achieve test and maintenance condition.
- Rods out/in - Allows manual control of control rod banks and individual control rods at a fixed speed when in the manual mode.

#### **7.7.1.1.2 Over Power and Over Temperature Interlocks**

Interlocks are provided to prevent abnormal power and temperature conditions that could result from excessive control rod withdrawal initiated either by a control system malfunction or by an operator violation of operating procedures. Refer Table 7.7-3 for the rod control interlocks and Figure 7.2-2 sheet 15.

These interlocks are generated by the following signals:

- Power range neutron flux
- Intermediate range neutron flux
- Over power  $\Delta T$
- Over temperature  $\Delta T$



- Turbine inlet pressure
- Control rod bank D position

To generate these interlocks the PCMS receives neutron flux signals from the RPS via the unit bus. Two high intermediate range neutron flux signals are used in 1-out-of-2 logic, since there are only two intermediate range neutron flux detectors for low power conditions. Four power range neutron flux signals are used for normal power conditions. The power range neutron flux logic is 1-out-of-4 to ensure rod withdrawal is stopped to prevent abnormal flux distribution in local areas of the core, which may occur as a result from other rod control malfunctions (i.e., rod withdrawal after compensating from a dropped rod event). The CRDM control system performs this function by receiving this signal (via the path above). This ensures that one detector can prevent this abnormal flux distribution quickly, since the other detectors may realize this event later than the excore detector affected by the local flux distribution.

The over power  $\Delta T$  and over temperature  $\Delta T$  input signals are interfaced from the RPS to the PCMS via the unit bus. Within the PCMS, signals from each of the four RPS trains, corresponding to each of the four RPS loops, are processed through the SSA within the PCMS before being used to generate these interlocks.

The turbine inlet pressure input signal is interfaced from the RPS to the PCMS via the unit bus. Within the PCMS, signals from each of the four RPS trains are processed through the SSA within the PCMS before being used to generate these interlocks.

All interlocks block automatic or manual control rod withdrawal. These interlocks are provided from the reactor control section of the PCMS to the CRDM control system.

The over power  $\Delta T$  and over temperature  $\Delta T$  interlock also initiates a turbine runback. These interlocks are provided from the reactor control system in the PCMS to the BOP control system.

The over power and over temperature interlocks which block rod withdrawal, are generated from a separate controller group from the rod control function discussed above which generates rod control withdrawal demands. This improves the potential for stopping inadvertent rod withdrawals that may be generated due to failures in the CRDM control group.

Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

#### 7.7.1.1.3 Control Rod Bank Insertion Limit Alarms

The PCMS generates control rod bank insertion limit alarms to alert the operator of excessive rod insertion, refer to Figure 7.2-2 sheet 16. The alarms prompt the operator to manually terminate rod insertion. The control rod bank insertion limit alarm setpoints ensure sufficient core reactivity shutdown margin following a RT to accommodate all accident conditions.

The following two control rod bank insertion limit alarms are provided for each control rod control bank:

- A "low" alarm warns the operator that the rod insertion limits are being approached
- A "low-low" alarm warns the operator the rod insertion limits have been reached.

These alarms prompt the operator to terminate automatic or manual rod insertion. The operator may also adjust required concentration of boron in the RCS, in accordance with operating procedures.

The control rod bank insertion limit alarm setpoints are calculated from reactor power, as measured by the  $\Delta T$ , according to the following equations:

$$Z_{LL} = A + B \Delta T$$

where:

$Z_{LL}$  = Maximum permissible insertion limit for the affected control bank

$\Delta T$  = Valid  $\Delta T$  measurements

A,B = Constants chosen to maintain  $Z_{LL}$ , which equal to or more than the actual limit based on physics calculations

The control rod bank demand position (Z), refer to Subsection 7.7.1.3, for the control rod control banks is compared to the respective  $Z_{LL}$  as follows:

- If  $Z - Z_{LL} \leq C$  (setpoint), a low alarm is actuated.
- If  $Z - Z_{LL} \leq D$  (setpoint), a low-low alarm is actuated.

These alarm limits ensure that adequate shutdown margin is maintained for all accident conditions. The control rod insertion limit alarm setpoint also provides a limit on the maximum inserted rod worth for the hypothetical rod ejection event. Insertion limits provide confidence that acceptable nuclear peaking factors are always maintained. The allowable rod insertion limits are increased (the rods must be withdrawn further) with increasing power because the amount of shutdown reactivity required for the design shutdown margin following a reactor trip increases with increasing power.

The reactor control system in the PCMS receives rod position signals from the CRDM control system based on control rod demand position.

$\Delta T$  input signals for control rod bank insertion limits are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS divisions, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for control rod bank insertion limits.

The control rod bank insertion limit alarms are generated from a separate controller group from the CRDM controls discussed above, which generates rod control insertion demands. This improves the potential for stopping inadvertent rod insertions that may be generated due to failures in the CRDM control group.

**7.7.1.1.4 Control Rod Position Monitoring**

The reactor control system in the PCMS receives signals from the rod position indication (RPI) system, refer to Subsection 7.7.1.4.

Alarms are generated if any control rod shutdown bank is detected to have left its fully withdrawn position, or if any control rods are detected at the bottom position, except as part of the normal insertion sequence. An alarm is also generated whenever the position of an individual rod deviates from the other rods in the bank by a preset limit. The alarm is set to accommodate appropriate core design limits, including allowance for instrument error.

Subsection 7.7.1.3 describes the CRDM Control System.

**7.7.1.1.5 Pressurizer Pressure Control**

The pressurizer pressure control function maintains the pressurizer pressure at its nominal operating value during normal operation and transients, refer to Figure 7.2-2 sheet 19.

During normal plant operation, the primary system pressure is monitored and controlled to prevent pressure from increasing to a limit where actuation of the PSMS is required to prevent design limits from being encroached. Additionally, the primary system pressure is prevented from decreasing to a value that may encroach on thermal design limits.

The pressurizer pressure control function is designed to provide a stable and accurate control of pressure to its predetermined setpoint.

Small or slowly varying changes in pressure are regulated by modulation of the proportional heaters. Reset (integral) action is included to maintain pressure at its setpoint. A fast pressure increase is controlled by reducing the proportional heater output and actuating pressurizer spray. Spray continues until pressure decreases to a point where the proportional heaters alone can regulate pressure.

For normal transients including a full-load rejection, the pressurizer pressure control function acts promptly to prevent reaching the high pressurizer pressure RT setpoint. A decrease in pressure, greater than that which can be handled only by controlling the proportional heaters, will result in the actuation of the backup heaters. These backup heaters are switched-off automatically when the proportional heaters alone are able to restore the falling pressure. During normal steady-state plant operation, proportional heater output is regulated to compensate for pressurizer heat loss. During normal transient operation, the pressure is regulated to provide adequate margin to ESF systems actuation or reactor trip.

The automatic pressure control function can be manually selected by the operator when nominal pressure is established during plant startup. Automatic pressure control function can be maintained from zero to 100% power.

Pressurizer pressure input signals for pressurizer pressure control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are

---

processed through the SSA within the PCMS before being used for pressurizer pressure control function.

Pressurizer pressure control function output signals are provided from the reactor control system in the PCMS to switchgear for the backup heaters, power controllers for the proportional heaters, and electro-pneumatic positioners for the pressurizer spray valves.

The PCMS provides the following HSI signals for pressurizer pressure control function:

- Pressurizer pressure control auto/manual - Allows transfer between the automatic control mode by pressurizer pressure input signals or function level manual control mode. In manual mode pressurizer heaters are controlled directly by the operator, but control signal to pressurizer spray valves may be in auto or manual mode.
- Pressurizer spray valve A auto-manual - Allows transfer between the automatic control mode by pressurizer pressure control or component level manual control mode for each pressurizer spray valve. In the manual mode the operator can fix the spray valve position.
- Pressurizer spray valve B auto-manual - Same as for pressurizer spray valve A.

#### **7.7.1.1.6 Pressurizer Spray Interlock**

An interlock is provided to prevent excessive depressurization of the RCS that could result from excessive spray, from a control system malfunction or operator violation of operating procedures, refer to Figure 7.2-2 sheet 19.

To generate this interlock the PCMS receives pressurizer pressure signals from the RPS and processes these signals through SSA, as discussed above.

The interlock blocks automatic or manual pressurizer spray valve opening. It interlock is provided from the Reactor control system in the PCMS to permissive solenoids on the Pressurizer Spray Valves.

The pressurizer spray Interlock is generated from a separate controller group from the pressurizer pressure control function discussed above, which generates pressurizer spray valve opening demands. This improves the potential for preventing inadvertent pressurizer spray valve opening that may be generated due to failures in the PCMS pressurizer pressure control function group.

The pressurizer spray interlock may be manually bypassed to allow plant depressurization for cold shutdown.

Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

#### **7.7.1.1.7 Pressurizer Water Level Control**

The pressurizer water level control function maintains pressurizer water level at its programmed value, refer to Figure 7.2-2 sheet 20. The programmed value is determined

as a function of reactor coolant  $T_{avg}$  to minimize charging and letdown control operations. This arrangement minimizes potential challenges to the protection systems actuation during normal operational transients.

The Pressurizer provides a reservoir for the RCS inventory changes that occur due to changes in reactor coolant density. As the reactor coolant temperature is increased from hot zero-load to full-load values, the RCS fluid expands. The pressurizer water level control adjusts letdown and charging flow to allow the pressurizer to absorb this change.

The pressurizer water level control function provides a stable and accurate method of pressurizer water level control at the prescribed setpoint value, which is programmed by  $T_{avg}$ . Automatic level control may be manually selected from the point in the startup cycle where the hot zero-load level is established. Automatic pressurizer water level control can be maintained from zero through 100% power.

Pressurizer water level input signals for the pressurizer water level control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the pressurizer water level control function.

$T_{avg}$  input signals for pressurizer water level control are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for Pressurizer water level control.

The pressurizer water level control function output signals are provided from the reactor control system in the PCMS to electro-pneumatic positioners for the charging flow control valve.

The PCMS provides the following HSI signals for the pressurizer water level control function:

Charging flow control valve auto/manual - Allows transfer of the charging flow control valve between the automatic control mode by pressurizer water level control or manual control mode. In the manual mode the operator can fix the charging flow control valve position.

#### **7.7.1.1.8 Low Pressurizer Water Level Interlock**

An interlock is provided to prevent excessive low pressurizer water level conditions that could result from excessive letdown or inadequate charging initiated by either a control system malfunction or operator violation of operating procedures, refer to Figure 7.2-2 sheet 20.

To generate this interlock the PCMS receives pressurizer water level signals from the RPS and processes these signals through SSA, as discussed above.

This interlock automatically closes letdown line isolation valves #1 and #2. The interlock also de-energizes the backup heaters to prevent damage during low pressurizer water level conditions where they may become uncovered.

This interlock is provided from the reactor control system in the PCMS to backup heater switchgear and the control solenoid on letdown line isolation valve #1 and #2.

One of the low pressurizer water level interlocks is generated from a separate controller group from the pressurizer water level controls which generates charging flow demands. This improves the potential for preventing excessive low pressurizer water level conditions that may be generated due to failures in the PCMS pressurizer water level control group. Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

#### 7.7.1.1.9 Steam Generator Water Level Control

Water level in the shell side of the SGs is maintained by the SG water level control function at a pre-determined setpoint, refer to Figure 7.2-2 sheet 21. During normal plant transients, the SG water level is controlled to prevent an undesirable reactor trip.

Three modes of the SG water level control function are provided:

- During normal power operation, three-element feedwater control regulates flow of MFW flow into the SGs via the MFW line with the MFW regulation valve by continuously comparing the SG water level signal, the fixed level reference, the MFW flow signal, and the steam flow signal.
- During low-power operation, two-element feedwater control regulates the flow of MFW into the SGs, bypassing the MFW regulation valve with the MFW bypass regulation valve by continuously comparing the SG water level signal, the fixed level reference, and the reactor coolant  $\Delta T$  signal.
- During hot standby operation, single element feedwater control regulates the flow of MFW into the SGs, also bypassing the MFW regulation valve and MFW bypass regulation valve with SG water filling control valve by continuously comparing the SG water level signal, and the fixed level reference.

The transition from the MFW bypass regulation valve to the MFW regulation valve during low power startup operation or the transition from the MFW regulation valve to the MFW bypass regulation valve during low power shutdown operation can be done automatically or manually. Tracking is provided to allow a smooth transition between manual and automatic control.

The transition from the SG water filling control valve to the MFW bypass regulation valve during low power startup operation is manual.

The SG water level control function is separate for each SG, the following description is applicable to each SG:

The SG water level input signals for the SG water level control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the SG water level control.

$\Delta T$  input signals for the SG water level control function are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains, corresponding to each RPS loop, are processed through the SSA within the PCMS before being used for the SG water level control function.

Redundant main steam flow and MFW flow input signals are interfaced directly to the PCMS. For main steam line flow, the PCMS validates these signals by cross-checking the signals between two SG loops. For MFW flow, the PCMS validates these signals by cross-checking to the main steam line flow in the same loop. After the input signals are validated, the PCMS selects the higher of the two valid inputs for use in the SG water level control function. Inputs determined to be invalid are not included in this selection.

The SG water level control function output signals are provided from the reactor control system in the PCMS to electro-pneumatic positioners on all MFW regulation valves described above.

The PCMS provides the following HSI signals for the SG water level control function:

- MFW regulation valve auto/manual - Allows transfer between the automatic control mode by SG water level control or component level manual control mode. In the manual mode the operator can fix the MFW regulation valve position.
- MFW bypass regulation valve auto-manual - Same as for MFW regulation valve.
- SG water filling control valve auto/manual - Same as for MFW regulation valve.

#### **7.7.1.1.10 High Steam Generator Level Interlock**

An interlock is provided to prevent excessive high SG water level conditions that could result from excessive feedwater initiated by either a control system malfunction or operator violation of operating procedures, refer to Figure 7.2-2 sheet 21.

This interlock is generated when the PCMS receives the SG water level signals from the RPS and processes these signals through SSA logic as discussed above.

This interlock is generated separately for each SG and automatically closes the MFW regulation valve and MFW bypass regulation valve for the associate SG.

This interlock is provided from the reactor control system in the PCMS to a permissive solenoid valve on each MFW regulation valve and MFW bypass regulation valve.

The high SG water level interlock is generated from a separate controller group from the SG water level control function above, which generates feedwater flow demands. This improves the potential for preventing excessive high SG water level conditions that may be generated due to failures in the PCMS SG water level control group.

Plant operators are alerted by alarms and indications to conditions of control system malfunctions and/or abnormal operating conditions.

**7.7.1.1.11 Turbine Bypass Control**

During startup and shutdown conditions when steam flow is blocked to the main turbine generator, the turbine bypass control function is used to bypass steam to the condenser. During normal operation, the turbine bypass control function is in a standby condition to modulate the bypass valves to maintain  $T_{avg}$ . Following a sudden loss of load, the turbine bypass control function prevents a reactor trip by opening the turbine bypass valves to dump excess steam from the SG to the condenser. For all operating modes, the turbine bypass control function prevents lifting the main steam safety valves. The functional operation of the turbine bypass control function for each plant-operating mode is described in the sections below; refer to Figure 7.2-2 sheet 17.

The turbine bypass control function input signals for turbine inlet pressure,  $T_{avg}$  and power range neutron flux are interfaced from the RPS to the PCMS via the unit bus. Signals from each of the four RPS trains are processed through the SSA within the PCMS before being used for the Turbine Bypass Control function.

The turbine bypass control function input signals for the turbine trip signal are interfaced from the RPS to the PCMS via the unit bus.

The turbine bypass control function input signals for steam header pressure signals, condenser available signals, and condensate booster pumps status are interfaced directly from non-safety field instrumentation to the PCMS.

The turbine bypass control function output signals are provided from the reactor control system in the PCMS to electro-pneumatic positioners and trip open solenoids for the turbine bypass valves.

The PCMS provides the following HSI for the turbine bypass control function:

- $T_{avg}$  control or steam header pressure control - Allows transfer between the two distinct turbine bypass control operating modes for heatup/cooldown operation (steam header pressure control) and normal power operation ( $T_{avg}$  control).
- Turbine bypass valves auto/manual - When turbine bypass control is in steam header pressure control mode, allows transfer between the automatic control mode by turbine bypass control or function level manual control for turbine bypass valves. In the manual mode, the operator can set the turbine bypass valve positions.
- Steam header pressure reference - When turbine bypass control is in steam header pressure control mode, allows adjustment of the steam header pressure setpoint used in the turbine bypass valves automatic mode.
- Loss of load reset - Allows manual reset of the load rejection operating mode after load rejection stabilization, refer to Subsection 7.7.1.1.12.



**7.7.1.1.11.1 Plant Startup and Shutdown**

During plant startup and shutdown, the difference between measured steam header pressure and a pressure setpoint is used to generate a turbine bypass demand signal. This mode is used for low-power conditions (up through turbine synchronization). This mode is also used during plant cooldown for decay heat removal between hot standby and entry conditions for the RHR system.

The steam header pressure control mode is manually selected by the operator. The pressure setpoint is manually adjusted by the operator to obtain the desired reactor coolant temperature.

**7.7.1.1.11.2 Normal Operation**

In this mode, the turbine bypass control function is in a standby condition to modulate the turbine bypass valve to control  $T_{avg}$  to a reference temperature derived from turbine inlet pressure.

**7.7.1.1.11.3 Load Rejection**

The US-APWR is designed to sustain a full load rejection, without generating a RT, atmospheric steam relief, or actuating a pressurizer or main steam line safety relief valve(s).

Full load rejection means an event when the main generator is cut off from transmission system either by tripping the main transformer breaker or the switchgear breaker without causing a turbine trip or the main generator trip. In this scenario, the main turbine control valve is immediately fully closed, and four banks of turbine bypass valves are tripped opened, to fully dump excess steam to the condenser.

Reactor power is decreased by automatic control of control rods. The automatic turbine bypass control function, in conjunction with other control systems, is provided to accommodate this abnormal load rejection and to reduce the effects of the transient imposed on the RCS. By bypassing main steam to the condenser, an artificial load is maintained on the primary system. This artificial load makes up the difference between reactor power and the turbine load for load rejections.

The turbine bypass control function is sized to pass approximately 68 percent of nominal steam flow at nominal steam pressure. This capacity, in conjunction with the response of the reactor control system, is sufficient to handle load rejections equivalent to a step load decrease of 100% of the rated load.

The turbine bypass control function prevents a large increase in reactor coolant temperature following a large, sudden load decrease. The error signal is the difference between the lead-lag compensated selected  $T_{avg}$  and the reference  $T_{avg}$  (designated  $T_{ref}$ ), which is based on turbine inlet pressure and a difference between the nuclear power signal and the turbine inlet pressure. The lead-lag compensation for the  $T_{avg}$  signal compensates for lags in the plant thermal response and in valve positioning. The addition of the difference between the nuclear power signal and the turbine inlet pressure with a

rate-lag compensation allows for a decrease in gain in the load rejection controller, thereby increasing stability.

Following a sudden load decrease,  $T_{ref}$  and turbine inlet pressure are immediately decreased and  $T_{avg}$  tends to increase. This generates an immediate demand signal for the turbine bypass control function. Following the initial trip opening the error signal reduces in magnitude, indicating that the  $T_{avg}$  is reduced toward the reference  $T_{avg}$  and power range neutron flux is reduced by an insertion of control rods. At this point, the turbine bypass valves are modulated and the rod control function commands the control rods to insert in a controlled manner to reduce the reactor power to match the turbine load. On a load rejection resulting in a turbine runback, the turbine bypass terminates when the reactor power matches the turbine load and the temperature error is within the maneuvering capability of the control rods. On a grid disconnect, the turbine bypass control function modulates closed in response to the control rods reducing nuclear power to approximately 15% power. At this point, the rod control function is transferred to manual mode to maintain the nuclear power by the operator and the plant stabilizes in preparation for a turbine/generator restart and/or grid synchronization with the turbine bypass partially open.

#### 7.7.1.1.11.4 Turbine Trip

For the US-APWR, a turbine trip will lead to a reactor trip and a reactor trip will lead to a turbine trip. Following a turbine trip, the load rejection control function is defeated and the turbine trip control function becomes active. The demand signal for the turbine bypass control function is the error signal between the lead-lag compensated  $T_{avg}$  and the no-load reference  $T_{avg}$ . When the error signal exceeds a predetermined setpoint, two banks of the turbine bypass valves are tripped opened in a prescribed sequence. As the error signal reduces in magnitude, indicating that the  $T_{avg}$  is being reduced toward the reference no-load value, the turbine bypass valves are modulated. This regulates the rate of decay heat removal and establishes the equilibrium hot shutdown condition.

#### 7.7.1.1.12 Turbine Bypass Interlock

Low-low  $T_{avg}$  turbine bypass block:

The turbine bypass control functions are prevented by the interlock from the PSMS, which controls redundant non-Class 1E permissive solenoids on each turbine bypass valve from SLS trains A and D. Excessive  $T_{avg}$  cooldown is blocked by this function as described in Subsection 7.3.1.12.

Loss of load interlock:

Actuation of turbine bypass on small load perturbations is prevented by an independent load rejection sensing circuit. This circuit senses the rate of decrease in the turbine load as detected by turbine inlet pressure. It unblocks the turbine bypass valves only when the rate of load rejection exceeds the preset value corresponding to a 10% step load decrease or a sustained ramp load decrease of greater than 5% per minute. The unblocking of the turbine bypass valves is latched to enable the load rejection operating

mode. This latch is manually reset by the operator after plant stabilization using the loss of load reset switch.

Condenser not available interlock:

This non-safety interlock is implemented in the PSMS to simplify the interface with the non-Class 1E turbine bypass valve permissive solenoids used for the  $T_{avg}$  interlock described above. Turbine bypass valve permissive solenoids are controlled by the PSMS to achieve high reliability of block turbine bypass function as described in Subsection 7.3.1.12.

These interlocks improve the potential for preventing inadvertent turbine bypass conditions that may be generated due to failures in the PCMS turbine bypass control group.

#### 7.7.1.2 Nuclear Instrumentation System

The RT signals derived from the nuclear instrumentation are described in Section 7.2. The control functions which use these same safety-related nuclear instrumentation signals are described in the sections above.

In addition, the reactor control system in the PCMS provides the following non-safety nuclear instrumentation monitoring functions:

- Indicated nuclear power.
- Indicated axial flux difference.
- Upper radial power tilt alarm on signal levels from the upper half of the power range neutron flux detector.
- Lower radial power tilt alarm on signal levels from the lower half of the power range neutron flux detector.
- Axial flux difference alarm deviation exceeds the limits.

In the MCR, provisions are made to continuously indicate and record nuclear power, axial flux imbalance and signal levels for each power range neutron flux detector.

#### 7.7.1.3 Control Rod Drive Mechanism Control System

The CRDM control system in the PCMS adjusts the position of the control rod banks in the reactor core. Each control rod bank is divided into two or more groups to obtain smaller incremental reactivity changes per step. The control rod groups within the same bank are moved such that the relative position of the groups does not differ by more than one-step. Each control rod in a group is paralleled so that rods of the same group move simultaneously.

Power to the CRDMs is supplied by two motor-generator sets operating from two separate 480 V, three-phase busses. Each generator is the synchronous type, and is

driven by an induction motor. The ac power is distributed to the CRDM control system power cabinet through the RTBs.

The CRDM control system consists of a logic cabinet and power cabinet, both located in close proximity to the CRDM motor generator sets. The PCMS controller group of the CRDM control system is located within the logic cabinet. The controller group controls solid-state CRDM power supplies that are located in the power cabinet.

Manual control is provided from the OC to move individual control rods or entire control rod banks in or out of the core. Control rod speed for manual control is fixed at approximately 48 steps per minute. The length of a step is described in Subsection 3.9.4.

The CRDM control system provides control for control rod shutdown banks and control rod control banks.

There are four control rod shutdown banks. The control rod shutdown banks are manually withdrawn to the full-out position prior to the reactor becoming critical. The control rod shutdown banks are always in the fully withdrawn position until the reactor is tripped or shutdown.

There are four control rod control banks, which are positioned to control reactor power after the control rod shutdown banks are fully withdrawn. The control rod control banks may be manually controlled or automatically controlled by the rod control function, refer to Subsection 7.7.1.1.1. In the manual mode, control banks may be moved individually or in a pre-determined overlap sequence. In the automatic mode, the control banks are withdrawn or inserted in the same predetermined overlapped sequence.

The following is a summary of the control rod control bank sequencing characteristics:

- The control rod control banks are programmed so that rod withdrawal is sequenced in a predetermined order. The programmed insertion sequence is the opposite of the withdrawal sequence. That is, the last inserted bank will be the first withdrawn.
- The control rod control bank withdrawals are programmed such that, when the first bank reaches a preset position, the next bank begins to move out simultaneously with the first bank. This preset position is pre-determined by the maximum allowable overlap between the banks. This withdrawal sequence continues until the reactor reaches to a desired power level. The control bank insertion sequence is the opposite of the withdrawal sequence.
- Overlap between successive control rod control banks is adjustable between 0 to 50%.

While in the automatic mode, the rod control function can vary the rod speed demand. The variable speed control function allows small changes in reactivity at low speed. This permits fine control of reactor coolant temperature. The variable speed control function allows large changes in reactivity at high speed. This permits control of reactor coolant temperature for transients such as large load rejections.

A RT signal causes the control rod shutdown banks and the control rod control banks to fall into the core by gravity.

The CRDM control system generates control rod position demand signals for display on operational VDUs. The demand position accuracy is  $\pm 0$  steps. This zero step accuracy is due to the fact that the demand is generated in the digital controller in the control system, and the readout is indicated in the operational VDU through the unit bus. The CRDM control system counts the motion demand signals during bank or individual rod motion, to provide a digital readout of the demanded position. The control rod position demand signals are used to generate alarms for incorrect control bank overlap and sequencing, and control rod bank insertion limit alarms, refer to Subsection 7.7.1.1.3.

#### **7.7.1.4 Rod Position Indication System**

The RPI system in the PCMS provides individual position indication for each control rod. The RPI system measures the position of each control rod using a detector consisting of discrete coils mounted outside the control rod pressure housing. These coils are located axially along the pressure housing. The RPI coils magnetically sense the movement of the rod drive shaft. Accuracy of digital RPI is  $\pm 12$  steps.

The RPI system consists of a remote I/O cabinet. The remote I/O cabinet is located in the C/V. The remote I/O cabinet interfaces to a PCMS controller group that is part of the reactor control system.

#### **7.7.1.5 Incore Instrumentation System**

The incore instrumentation system section of the PCMS consists of core exit temperature instrumentation and incore nuclear instrumentation. Core exit temperature instrumentation consists of thermocouples at fixed core outlet positions. Incore nuclear instrumentation consists of movable neutron detectors, which can be positioned in the instrumentation guide thimble of selected fuel assemblies anywhere along the length of the fuel assembly vertical axis.

##### **7.7.1.5.1 Core Exit Temperature Instrumentation**

There are a total of 39 core exit thermocouples. Thermocouples are threaded into individual guide tubes that penetrate the RV closure head through seal assemblies and terminate at the exit flow end of the fuel assemblies. All thermocouples are arranged in two safety divisions and one non-safety division. Core exit thermocouples provide a measure of core heat up via measurement of core exit fluid temperature.

All thermocouple readings are provided on operational VDUs to monitor radial temperature distribution. Safety-related thermocouples provide signals for PAM, refer to Subsection 7.5.1.1.3.3.

##### **7.7.1.5.2 Incore Nuclear Instrumentation**

Miniature fission chamber detectors can be remotely positioned in guide thimbles to provide flux mapping of the core. The detector guide thimbles penetrate the RV closure head through seal assemblies and terminate at the bottom of the fuel assemblies. The detector guide thimbles extend from the bottom of the fuel assemblies to the detector

drive unit in the C/V. The detector guide thimbles are distributed over the core nearly uniformly. The configuration of the main components of the system for insertion and withdrawal of these detectors is shown in Figure 7.7-1.

The thimble assemblies, which integrate the several detector guide thimbles, are mounted on the upper core support plate, as shown in Figure 7.7-1.

The main components of the system for insertion and withdrawal of the detectors are drive units and path selector assemblies, as shown in Figure 7.7-1. The drive system pushes hollow helical wrap drive cables into the core with the detectors attached to the leading ends of the cables and small diameter coaxial cables threaded through the hollow centers back to the end of the drive cables. Each drive unit consists of motors and storage wheels that accommodate the total drive cable length. The motor pushes a helical drive cable and a detector through a selective thimble path by means of the path selectors. Every thimble location can be accessed by each detector controlled from different drive units. A common path is provided for cross-calibration of the detectors.

The incore nuclear instrumentation data acquisition and drive motor control equipment are located inside the non-Class 1E I&C equipment room.

The incore nuclear instrumentation HSI is located inside the I&C equipment room. This HSI provides means for manually or automatically inserting and withdrawing the detectors and recording neutron flux data from the detectors. The control and readout system consists of the necessary equipment for control, position indication, and flux recording for each detector.

A flux mapping consists of selecting thimbles in given fuel assemblies at various core locations. Signals from the detectors are recorded as the detectors are repositioned in the core. A plot of position versus neutron flux levels is provided from this data. In a similar manner, other core locations are selected and scanned. Flux mappings are conducted periodically in accordance with technical specification surveillance requirements.

The incore nuclear instrumentation data is communicated via the unit management computer and station bus, refer to Figure 7.1-1, to external computer applications, which are used by reactor engineers to construct an accurate three-dimensional core power distribution. The data are used periodically for accurately detecting whether the reactor power distribution is within the technical specifications operating limits. The reactor engineers and plant operators communicate to make appropriate power distribution adjustments.

In addition, this flux map is used for periodically calibrating the excore nuclear detectors in accordance with technical specifications.

#### **7.7.1.6 Balance of Plant Control**

The BOP control system in the PCMS controls BOP systems such as service water, circulating water, feedwater, HVAC, and non-essential CCW. The system receives inputs from field process instrumentation and manual operation signals from the OC to control and monitor modulating control valves, discrete components such as MOVs, solenoid operated valves, and pumps. Refer to Chapters 9 and 10 for related details.

**7.7.1.7 Turbine Electro Hydraulic Governor Control System**

The turbine electro-hydraulic governor control system (EHGS) in the PCMS provides the following functions:

- Speed control
- Load control
- Over-speed protection
- Automatic turbine startup control

**7.7.1.8 Turbine Supervisory Instrumentation System**

The turbine supervisory instrument system in the PCMS monitors important parameters of the turbine such as vibration, temperature, and rotor position. This system interfaces to the BOP control system to provide PCMS alarms.

**7.7.1.9 Turbine Protection Control**

The turbine protection system in the PCMS receives signals regarding the turbine-generator and provides appropriate trip actions when it detects undesirable operating conditions of the turbine-generator.

**7.7.1.10 Electrical System Control**

The electrical system in the PCMS controls and monitors the non-safety plant electrical systems.

**7.7.1.10.1 Generator Transformer Protection System**

The generator transformer protection system in the PCMS monitors important parameters of the main generator such as vibration and temperature. The generator transformer protection system provides a generator trip in case of turbine trip. This system also controls related components (e.g., breakers) in case of undesirable operating conditions of the generator and associated transformer(s).

**7.7.1.10.2 Auto Voltage Regulator/Automatic Load Regulator System**

The auto voltage regulator (AVR)/automatic load regulator (ALR) system provides regulation of generator voltage.

**7.7.1.11 Radiation Monitoring System**

The radiation monitoring system (RMS) section of the PCMS provides non-safety area and process radiation monitoring to generate displays and alarms. Refer to Chapters 11 and 12 for additional related details.

---

#### 7.7.1.12 Auxiliary Equipment Control System

The auxiliary equipment control system section of the PCMS controls and monitors auxiliary systems (e.g., radioactive waste disposal system, CVCS water treatment).

HSI for the auxiliary equipment control system is located in the auxiliary equipment control room, which is located in the auxiliary building. This control room is manned periodically for auxiliary equipment operation (i.e., radioactive waste management). Key alarms are displayed on the alarm VDU, LDP and the operational VDU and key indications are provided on operational VDUs. Refer to Chapter 11 related details.

#### 7.7.2 Design Basis Information

The control systems include the necessary features for manual and automatic control of process variables within the prescribed normal operating limits.

The PCMS design is based on the following design considerations.

##### 7.7.2.1 Safety Classification

The PCMS is a non safety-related system. The plant accident analysis of Chapter 15 does not rely on the operability of any PCMS control functions to assure safety. Safe shutdown can be achieved without reliance on any PCMS control functions.

##### 7.7.2.2 Effects of Control System Operation on Accidents

For the transient response of the plant systems for AOOs and PAs, the safety analysis takes no credit for normal PCMS control actions that would lessen the affects of the event (e.g., reduction of feedwater by the SG water level control system during a SG tube rupture event). In addition, the safety analysis assumes normal control actions, that would aggravate the affects of the event and are not blocked by safety functions, will occur (e.g., increase of charging flow by the pressurizer water level control system during a SG tube rupture event).

##### 7.7.2.3 Effects of Control System Failures

The Chapter 15 analysis of AOOs bounds all single random failures within the PCMS. This includes single failures that result in:

- A fail as-is, fail de-energized or spurious actuation of a single PCMS hardware component (e.g., input module, or output module).
- A fail-as-is or fail de-energized condition of an entire PCMS control group; the control function to control group assignment are shown in Table 7.7-2.
- Spurious actuation of a single or multiple control functions (e.g., reactivity control, pressurizer control, or SG water level control) within a control group, resulting from a single software block failure.
- A spurious single command from an operational VDU.



- 
- Stuck or dropped control rod
  - Stuck control rod bank or overlap sequence error
  - Spurious actuation of a normal rod motion command (spurious motion of any single bank)
  - Spurious motion of multiple control banks in the predetermined overlap sequence.

The Chapter 15 analysis of AOOs, credits the affects of interlocks in PCMS control groups not affected by the failure, which limit the affects of a failed PCMS control group or control function.

The following types of failures are not considered credible, since they require a series of specific successive failures in multiple software blocks:

- Multiple spurious commands from an operational VDU. Since multiple spurious commands from an operational VDU are not credible, they are not considered in the analysis of bounding AOOs. However, multiple spurious commands from an operational VDU are analyzed for their effect on the safety functions, in MUAP-07004 Appendix D.
- Spurious actuation of multiple control functions in the same control group that do not rely on the same software block.
- Spurious actuation of un-programmed control actions (e.g., out of sequence motion for multiple control banks).
- Spurious motion of a single control rod.

MUAP-07004 (Reference 7.7-1) Section 5.1.8 describes the basis for the PCMS failures assumed in safety analysis.

#### **7.7.2.4 Effects of Control System Failures Caused by Accidents**

The PCMS controllers are in mild environment locations, which are not impacted by plant accidents. In addition, most PCMS inputs come from safety-related sensors, which are qualified for accident environments. To accommodate random PCMS failures and PCMS failures that may be caused by accident conditions, the Chapter 15 safety analysis assumes the worst case PCMS single failure, which would aggravate the accident condition and is not blocked by safety functions.

#### **7.7.2.5 Environmental Control System**

Environmental control systems that are credited in the safety analysis are controlled by the PSMS, not the PCMS. Environmental control systems controlled by the PCMS, such as non-essential area HVAC, heat tracing, and/or forced air-cooling or heating, are considered in the failure analyses described above, refer to Subsections 7.7.2.3 and 7.7.2.4.

**7.7.2.6 Use of Digital Systems**

The PCMS and PSMS utilize the same basic software. In addition, the PCMS application software is developed using a structured process similar to that applied to development of the PSMS application software. This process includes an augmented quality program, including software V&V, for the following functions:

- Safety functions controlled by operational VDUs
- SPDS
- Alarms for credited manual operator actions
- SSA

Therefore, the potential for control system failures that could challenge safety systems or impact plant safety functions has been minimized.

**7.7.2.7 Independence**

The PCMS is physically, electrically, and functionally independent of PSMS, refer to Subsection 7.1.3.4 and 7.1.3.5 for related details.

**7.7.2.8 Defense-In-Depth and Diversity**

PCMS and PSMS utilize the MELTAC digital platform, which is described in MUAP-07005 | (Reference 7.7-2). Maximum utilization of a common digital platform throughout a nuclear plant reduces maintenance, training, and changes due to obsolescence, thereby minimizing the potential for human error.

The potential for CCF in these systems is minimized by the following:

- Simplicity of the basic design.
- Maturity of the MELTAC platform.
- Design process including the elevated quality programs applied to both systems.
- Significant functional diversity within the numerous computers that compose these systems.

Regardless of this very low potential for CCF, the DAS is provided to accommodate beyond design basis CCFs that could adversely affect the PSMS and PCMS concurrent with an AOO or PA, refer to Section 7.8 for DAS details.

**7.7.2.9 Potential for Inadvertent Actuation**

The PCMS design limits the potential for inadvertent actuation and challenges to the PSMS as follows:

- The PCMS processes multiple redundant sensor signals through the SSA. The SSA ensures the PCMS does not take erroneous control actions based on a single instrument channel failure or single RPS train failure.
- The PCMS includes interlocks that limit erroneous control actions, refer to applicable Subsections in 7.7.1.1 above. These interlocks are assigned to control groups that are distinct from other control groups, which can initiate erroneous control actions.
- The PCMS control functions are distributed to multiple control groups such that erroneous actions resulting from a control group failure are bounded by the plant safety analysis.
- Operational VDUs generate control commands based on two distinct operator actions, in accordance with ISG-04 Position 3.1.5.

#### 7.7.2.10 Control of Access

**Security-Related Information – Withheld Under 10 CFR 2.390**

#### 7.7.3 Analysis

The Chapter 15 analysis for AOOs and PAs does not take credit for operability of the PCMS for accident/event mitigation or achieving and maintaining safe shutdown. In addition, PCMS failures are bounded by the Chapter 15 analysis. Refer to Subsections 7.7.2.2 through 7.7.2.4.

The plant transient analysis demonstrates the control systems are capable of safely controlling the plant, without the need for manual intervention and without violating plant protection or component limits, for the following:

- 10% step load change while operating in the range of 15% to 100% of full power without RT or turbine bypass system actuation.

- 
- Ramp load changes at 5% power per minute while operating in the range of 15% to 100% of full power without RT or turbine bypass system actuation (subject to core power distribution limits).
  - Full-load rejection without RT.

The control system permits maneuvering the plant through the above transients without actuation of the following:

- Main Steam safety valves
- Safety depressurization valves

In addition, these valves are not actuated during a normal plant trip.

#### 7.7.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

#### 7.7.5 References

- 7.7-1 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.7-2 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.4 (Proprietary) and MUAP-07005-NP Rev.4 (Non-Proprietary), September 2009.
- 7.7-3 Highly Integrated Control Rooms – Digital Communication Systems, DI&C-ISG-04 Revision 1, March 2009.

**Table 7.7-1 AOOs Due to the Control System Failures**

<b>Subsection</b>	<b>Title</b>	<b>Credible Event due to Control System Failure</b>
15.1.2	Increase in feedwater flow as a result of feedwater system malfunctions	Full open of any of the MFW regulation valve
15.1.4	Inadvertent opening of a steam generator relief or safety valve	Full open of any one of the main steam relief valve or turbine bypass valve
15.4.1	Uncontrolled control rod assembly withdrawal from a subcritical or low power startup condition	2 bank of control rod withdrawal according to bank overlap sequence
15.4.2	Uncontrolled control rod assembly withdrawal at power	2 bank of control rod withdrawal according to bank overlap sequence
15.5.1 15.5.2	Inadvertent operation of ECCS and chemical and volume control system malfunction that increases reactor coolant inventory	Full open of the charging flow control valve

Table 7.7-2 Controller Group Control System Distribution in the Reactor Control System

Group	Control System	Postulated Event Due to a Single Failure in the Corresponding Controller Group*1			
		Full open of any of the MFW regulation valves	Full open of any one of the main steam relief valves or turbine bypass valve	Two banks of control rod withdrawal according to bank overlap sequence	Full open of the charging flow control valve or pressurizer spray valve
Group 1	A-SG Feedwater Control	X			
	A-Main Steam Relief Valve Control		X*2		
Group 2	B-SG Feedwater Control	X			
	B-Main Steam Relief Valve Control		X*2		
Group 3	Pressurizer Pressure Control				X*2
	C-SG Feedwater Control	X			
	C-Main Steam Relief Valve Control		X*2		
	Pressurizer Water Level Control				X*2
Group 4	Control Rod Insertion Monitoring			X	
	D-SG Feedwater Control	X			
	D-Main Steam Relief Valve Control		X*2		
Group 5	Turbine Bypass Control		X*2		
	Reactor Makeup Control			X	
Group 6	Control Rod Control			X*2	

Note:

1. This table describes that one controller failure does not cause credible failures in other controller groups.
2. An interlock is provided (for this control system) in a separate controller group, to limit the effect of the single controller failure.

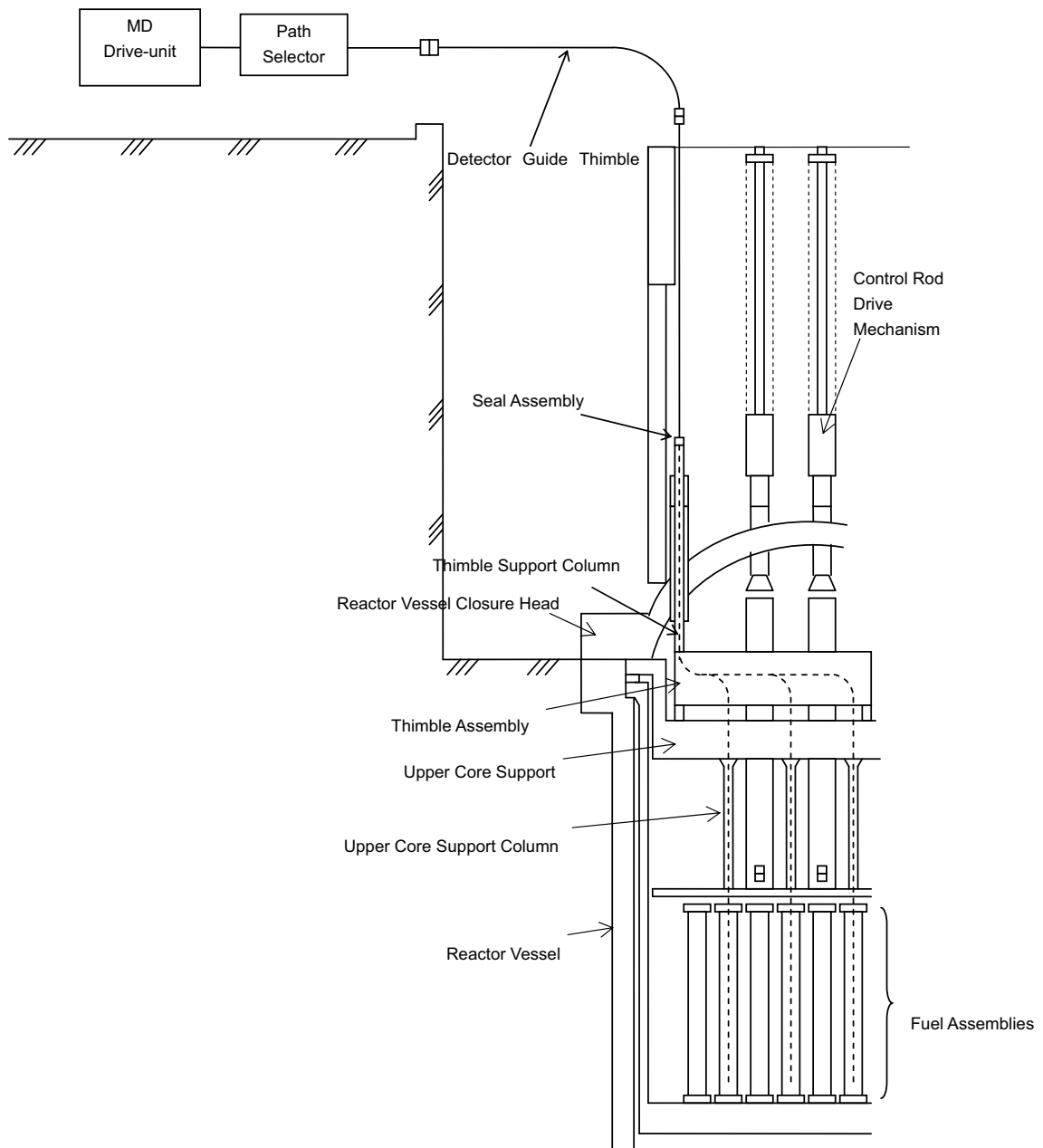
**Table 7.7-3 Rod Control System Interlocks**

Designation	Derivation	Function
C-1	1-out-of-2 Intermediate Range Neutron Flux above setpoint	Blocks automatic and manual control rod withdrawal
C-2	1-out-of-4 Power Range Neutron Flux above setpoint	Blocks automatic and manual control rod withdrawal
C-3	2-out-of-4 Over Temperature $\Delta T$ above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load reference
C-4	2-out-of-4 Over Power $\Delta T$ above setpoint	Blocks automatic and manual control rod withdrawal
		Actuates turbine runback via load Reference
C-5	Turbine Inlet Pressure (output of signal selector) below setpoint	Blocks automatic control rod Withdrawal

**Table 7.7-4 Process Control Parameters and Control Method Description**

Process control variables	How to control the process control variables
Reactor coolant average temperature (Tavg)	The Tavg is automatically controlled by the rod control function. (Refer to DCD Subsection 7.7.1.1.1)
Pressurizer pressure	The pressurizer pressure is automatically controlled by the pressurizer control function. (Refer to DCD Subsection 7.7.1.1.5)
Pressurizer water level	The pressurizer water level is automatically controlled by the pressurizer water level control function. (Refer to DCD Subsection 7.7.1.1.7)
Steam generator water level	The steam generator water level is automatically controlled by the steam generator water level control function. (Refer to DCD Subsection 7.7.1.1.9)
Steam header pressure	The steam header pressure is automatically controlled by the turbine bypass control function, when turbine bypass control is in steam header pressure control mode. (Refer to DCD Subsection 7.7.1.1.11)





**Figure 7.7-1 Basic System for Insertion of Movable Neutron Detectors**

---

### 7.8 Diverse Instrumentation and Control Systems

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The design basis and detailed system description for the DAS are described in Topical Report MUAP-07006 (Reference 7.8-1). Table 7.8-7 shows the supplemental information to Topical Report MUAP-07006-P-A, which is necessary to be clarified. The Defense in Depth and Diversity Coping Analysis, Technical Report MUAP-07014 (Reference 7.8-2), demonstrates the ability to maintain all critical safety functions and achieve hot standby using the DAS.

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is also designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety process inputs and outputs of the SLS are isolated within these safety systems. In addition, hardwired Class 1E logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function. For a figure of the DAS system architecture, refer to Figure 6.0-1 of Topical Report, MUAP-07006.

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions (Refer to Table 7.8-1). For conditions where there is insufficient time for manual operator action, the DAS provides automatic actuation of required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in two diverse automatic actuation cabinets (DAACs), each located in a separate room. Each DAAC is powered by a separate non-Class 1E UPS. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations.

#### 7.8.1 System Description

The DAS consists of manual HSI functions, which include automatic actuation functions. These functions are located in the DHP and the DAAC, respectively. In addition, the DAS consists of interfacing connections with the PSMS and CRDM motor-generator sets. The DAS receives inputs from qualified analog isolators located in the RPS or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified isolators located in the SLS or directly to plant components.

---

Once actuated, either manually or automatically, the DAS signals are latched at the system level. This ensures all DAS functions actuate to completion. The DAS latches can be reset from the defeat switch located on the OC.

The overall DAS architecture is described in Topical Report MUAP-07006 Section 4.0. For manual and automatic system level, actuations from the DAS refer to functional logic diagram Figure 7.2-2 sheet 14.

#### **7.8.1.1 Diverse HSI Panel**

The DHP, which is located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP installed equipment is used for manual control and actuations credited in the defense in depth and diversity coping analysis. Actuation status of each safety system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a non-Class 1E UPS and located in the MCR. Therefore, the DHP is qualified as Seismic Category II.

##### **7.8.1.1.1 Manual Actuation Switches**

System level manual actuation is provided on the DHP for all automated functions and for systems required to maintain critical safety functions, which may not be automatically actuated. The following manual actuations are provided from conventional switches on the DHP:

- Reactor trip/turbine trip/MFW isolation: one switch
- EFW actuation: one switch
- ECCS: one switch
- Containment isolation: one switch
- EFW isolation and flow control: four switches (one per SG)
- Control of main steam depressurization valve: four switches (one per SG)
- Control of safety depressurization valve: one switch

To prevent spurious actuation due to a failure of any of the above switches, a separate manual actuation permissive switch is provided. This is referred to as the "Permissive Switch for DAS HSI." The permissive switch is located in the MCR, but physically separated from the DHP to minimize the affect of fire propagation. The DAS permissive switch is powered by a non-Class 1E UPS that is separate from the power to the DHP. Signals from the manual actuation switches and permissive switch are interfaced separately from the MCR to each DAAC; refer to Topical Report MUAP-07006 Section 6.0. To prevent spurious DAS actuation due to the MCR fire, all DAS manual actuation signals are blocked when the MCR/RSR transfer is activated, refer to MUAP-07004 (Reference 7.8-3) Figure 4.2-1.

---

The manual actuation switches listed above are sufficient to take all manual actions credited in Technical Report MUAP-07014, which demonstrates the ability to maintain all critical safety functions and achieve hot standby. Hot standby can be maintained for an extended period-of-time by direct operation of local power distribution and switching devices that are not affected by the CCF in the PSMS.

#### **7.8.1.1.2 Alarms**

When the DAS system level actuation signals are generated for (1) reactor trip, turbine trip, and MFW isolation, or for (2) EFW actuation are generated, a summary alarm for these functions is also actuated on the DHP. The diverse audible alarm is activated to notify the operators. The first out alarm panel, on the DHP, indicates the specific input parameter that has caused the system level actuation.

Failure information about the DAS, such as power supply failure, or module de-energization or removal, is alarmed as a "DAS failure summary alarm" on the Alarm VDU in the MCR. The configuration of the DAS alarms is described in Topical Report MUAP-07006 Section 6.2.2.1. High main steam radiation (N16) and high-high steam generator water level are alarmed and indicated on DHP. Technical Report MUAP-07014 provides the specific information of the alarm credited for D3 coping analysis.

#### **7.8.1.1.3 Indicators**

The analog indicators provided on the DHP are identified in Table 7.8-2. These indicators are sufficient to support all manual control actions credited in Technical Report MUAP-07014, which demonstrates the ability to maintain all critical safety functions, and achieve and maintain hot standby.

#### **7.8.1.2 Diverse Automatic Actuation Cabinet**

Each DAAC provides for automatic actuation of critical systems, which are required to be actuated within first 10 minutes of an event (refer to Table 7.8-3 for system actuation times). The defense in depth and diversity coping analysis provides justification for manual operator actions credited after 10 minutes.

Safety sensors selected by the plant design for the DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP. The MELTAC input module design of the PSMS or PCMS is described in MUAP-07005 (Reference 7.8-4) Section 4.0.

The DAS has two analog logic subsystems, one each located in one of the two DAACs.

Within each DAAC, input signals are compared to their setpoint values and if the monitored value is greater than or less than its setpoint, a partial trip/actuation signal is generated. RT signals and/or ESF actuation signals are generated from each DAAC through voting logic of its input signals. The voting logic (2-out-of-4) for each specific

---

monitored parameter is shown in Table 7.8-4. Table 7.8-6 provides range, accuracy, and setpoint for each diverse actuation variables.

The DAS actuation signals from both DAAC subsystems are configured at their destination using 2-out-of-2 voting to execute actuation of RT and ESF systems.

The monitored signals are isolated from the PSMS and interfaced to the separate subsystems in each DAAC. Process variables monitored for automatic actuation functions are: (a) Pressurizer pressure (4 channels each for low and high-pressure signals), (b) SG water level (4 channels, one per each SG for low level signals).

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS.
- Unlimited bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions or prevent monitoring critical safety functions.

The defeat switch can be manually actuated during plant heatup and cooldown conditions to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.

The DAS functional logic diagram for automated actuation is included on Figure 7.2-2 sheet 14.

The DAACs are located in separate Class 1E Electrical Rooms. Therefore, the DAACs are qualified as Seismic Category II.

#### **7.8.1.2.1 Reactor Trip, Turbine Trip and Main Feedwater Isolation**

Reactor trip, turbine trip and MFW isolation are automatically actuated on the following signals:

- Low pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure low signals.
- High pressurizer pressure: 2-out-of-4 voting logic of the four pressurizer pressure high signals.
- Low SG water level: 2-out-of-4 voting logic of the one SG water level low signals from each SG.

The four pressurizer pressure signals are interfaced from each of the four PSMS trains. This configuration allows the DAS to meet the target reliability of the PRA with one channel continuously bypassed or inoperable.

To support the single failure criterion for all PSMS functions, there are four SG water level signals (one per each train A, B, C, and D) on each SG. However, for the DAS, which

does not need to meet the single failure criterion, only one water level signal is required from each SG.

The reactor trip is actuated by tripping the non-safety CRDM motor-generator set. This actuation leads to de-energizing the power for the CRDM by a means that is diverse from the RTB to release the control rods for gravity insertion into the reactor core. Diversity from the PSMS is maintained from sensor-inputs to final actuators.

The Turbine Trip is actuated by opening the solenoid valves for turbine trip. Diversity from the RT function in the PSMS is maintained from sensor-input up to the power interface module.

The MFW isolation is actuated by closing the MFW regulation valve. Diversity from the feedwater isolation function in the PSMS is maintained from sensor input up to the power interface module.

These DAS actuation functions are automatically blocked when all the following conditions are established:

- Status signals are received indicating that the minimum combination of the RTBs have actuated for the RT function. This is referred to as the P-4 interlock. The logic for the P-4 interlock is the same as in the PSMS, as shown in Figure 7.8-2. The P-4 interlock is processed independently in each DAAC. Signals from all RTBs are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1.
- The turbine emergency trip oil pressure trip signal is generated when oil pressure channels exceed the trip setpoint.

#### 7.8.1.2.2 Emergency Feedwater Actuation

EFW is automatically actuated on a low SG water level signal. 2-out-of-4 voting logic is utilized for the low SG water level signals from each SG.

The interface and configuration of the SG water level signals is as described above.

Diversity from the EFW actuation function in the PSMS is maintained from sensor input up to the power interface module. This automatic DAS EFW function is automatically blocked when status signals are received indicating that the PSMS EFW function has actuated correctly. Correct actuation is indicated when 2-out-of-4 status signals are received from limit switch contacts on the steam inlet valves to the turbine driven EFW pumps and from auxiliary contacts on the motor starters controlling the motor driven EFW pumps, as shown in Figure 7.8-3. The EFW pump status signals are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1.

## **7.8.2 Design Basis Information**

### **7.8.2.1 Single Failure**

Since the DAS is a non-safety system, it does not need to meet the single failure criterion for actuation. The DAS subsystems are arranged in a 2-out-of-2 configuration to ensure that the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions. Spurious actuation of single components due to single failures in SLS power interface modules has been considered in the plant safety analysis.

The two DAAC subsystems actuate all required plant components to achieve the required safety function. The number of actuated plant components does not consider additional single failures. For example, for containment isolation valves, only one of the two valves is actuated. This non-redundant configuration is considered in determining the allowable out of service time for plant equipment in the technical specifications. However, the out-of-service condition is considered for the numbers of safety injection pumps and EFW pumps. In addition, unavailable of main steam depressurization valve of the impaired SG line is considered. The DAS actuates all four of these pumps and valves for operability, while three is minimum-required. The number of actuated components for each DAS function is shown in Table 7.8-5.

### **7.8.2.2 Diversity to Digital Safety and Non-Safety Systems**

The DAS utilizes conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits). Therefore, a software CCF in the digital safety and non-safety systems (PSMS and PCMS), would not affect the DAS. In addition, the DAS hardware for anticipated transient without scram (ATWS) mitigation functions - Reactor trip, turbine trip, and EFW actuation, is diverse from the RT hardware used in the PSMS.

### **7.8.2.3 Separation and Independence**

The DAS is electrically and physically isolated from the PSMS. Isolation devices (isolation transformers, relays, optical fiber, photo couplers, etc.) are installed in the safety system for sharing sensors or transmitting signals between the PSMS and the DAS. These isolators are part of the safety system and are fully qualified.

Isolation devices are installed in the safety system for interfacing DAS outputs to power interface module in the SLS. These isolators are part of the safety system and are fully qualified.

### **7.8.2.4 Testability**

The DAS can be tested manually by injecting simulated input signals to confirm its function actuation setpoints, designed logic functions, and required system outputs. Spurious actuation from any one subsystem, during testing, is precluded by the system design of 2-out-of-2 logic that must be satisfied to generate an actuation signal. DAS output signals are tested to the inputs of the SLS power interface module. This testing overlaps with periodic testing of the SLS, which provides complete testing of all power interface module functions.

**7.8.2.5 Maintenance Bypass**

If an input sensor is failed, the failed sensor signal can be bypassed by a dedicated bypass switch. The switch bypasses only the sensor that has failed. Channel bypass is administratively controlled. Other maintenance bypass functions are not necessary based on the following DAS features:

- The DAS consists of two subsystems and DAS actuation requires coincident outputs of both subsystems.
- DAS electrical circuit is designed to actuate when energized. Therefore, loss of power or removal of module does not cause spurious actuation.

**7.8.2.6 Operating Bypass**

The DAS automatic functions can be manually bypassed by the defeat switch, which is a dedicated conventional switch on the OC. The defeat switch is shown in Figure 7.2-2 sheet 14. This switch bypasses both DAAC subsystems. The defeat switch prevents unnecessary automatic DAS actuations due to expected plant conditions during plant startup and shutdown. This operating bypass is reset only by operator action of the above switch. Actuation of the defeat switch is displayed in the MCR on the operational VDU.

Although failure of the defeat switch may result in spurious DAS actuation during startup or shutdown, durations for these plant modes are sufficiently small. Therefore, this failure mode is acceptable.

**7.8.2.7 Quality**

The DAS is a non-safety system designed with augmented quality, as defined by Generic Letter 85-06 (Reference 7.8-5). The following are the key attributes of the augmented quality program:

- Designed specially for nuclear applications using a nuclear quality program that meets the US-APWR QAP descriptions and the guidance in GL 85-06.
- Uses components with a long history of successful operation.
- Uses components that are common in conventional non-digital safety systems.
- Follow a design process that includes independent review by people that were not involved in the original design.

**7.8.2.8 Defense-In-Depth and Diversity**

The defense in depth and diversity approach is based on the following principles:

- Minimize the potential for CCF
- Cope with CCF for AOOs



---

Das is implemented to mitigate the adverse effects/impacts from digital I&C both hardware and software common cause failure (CCF). It is not to minimize the potential or extent of software CCF.

A detailed description of each principle is provided in Topical Report MUAP-07006 Section 5.0.

#### **7.8.2.9 Fire Protection**

Fire protection for the DAS is described in MUAP-07004 Sections 5.2.3 and 6.5.8.

### **7.8.3 Analysis**

#### **7.8.3.1 Anticipated Transient without Scram**

In accordance with 10 CFR 50.62 (Reference 7.8-6), the DAS is diverse from the RT system to initiate turbine trip and EFW actuation. Although not required by 10 CFR 50.62 for all reactors, MHI's defense in depth and diversity approach also includes a diverse RT function for ATWS mitigation.

A detailed discussion of conformance of to 10 CFR 50.62 is provided in Topical Report MUAP-07006 Appendix B.

#### **7.8.3.2 Adequacy of Manual Controls and Displays**

Technical Report MUAP-07014 defines the alarms, indicators and controls required on the DHP for the operator to take manual actions credited for mitigating each AOO and PA included in Chapter 15, place the nuclear plant in a hot standby condition, and monitor and control the following critical safety functions:

- Reactivity control
- Core heat removal
- Reactor coolant inventory control
- Containment integrity
- RCS inventory control
- Secondary heat sink

Technical Report MUAP-07014 also confirms that there is sufficient time for all credited manual operator actions. The HSI on the DHP is designed, verified, and validated in accordance with the HFE program described in Chapter 18.

#### **7.8.3.3 Conformance to BTP 7-19**

Topical Report MUAP-07006 Appendix A provides a detailed description for the conformance of BTP 7-19 (Reference 7.8-7).

---

**7.8.4 Combined License Information**

No additional information is required to be provided by a COL Applicant in connection with this section.

**7.8.5 References**

- 7.8-1 Defense-in-Depth and Diversity, MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.
- 7.8-2 Defense in Depth and Diversity Coping Analysis, MUAP-07014-P Rev.2 (Proprietary) and MUAP-07014-NP Rev.2 (Non-Proprietary), December 2009.
- 7.8-3 Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.
- 7.8-4 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.
- 7.8-5 Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related, Generic Letter 85-06.
- 7.8-6 Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants, NRC Regulations Title 10, Code of Federal regulations, 10 CFR Part 50.62.
- 7.8-7 Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, BTP 7-19 Revision 5, March 2007.
- 7.8-8 HSI System Description and HFE Process, MUAP-07007-P Rev.3 (Proprietary) and MUAP-07007-NP Rev.3 (Non-Proprietary), October 2009

**Table 7.8-1 Critical Safety Functions and Related Systems**

Critical Safety Function	Related System	Control
Reactivity Control	Reactor Trip Turbine Trip	Automatic & Manual
RCS Inventory	ECCS	Manual
Core Cooling	ECCS	Manual
Secondary Heat Sink	EFWS Isolation of Secondary System Secondary System Depressurization	Automatic & Manual
RCS Integrity	Primary System Depressurization	Manual
Containment Integrity	Containment Isolation CSS	Manual

**Note:**

The systems listed in this table are required to operate at different times for different events. Table 7.8-3 shows the expected action time measured from the prompting alarms for various events. These selected systems and expected action times establish the basis for DAS automation. The defense-in-depth and diversity coping analysis confirms the acceptability of DAS automation and credited manual operator action.

**Table 7.8-2 Variables Monitored by DAS**

Critical Safety Function	Variables	Number of Channel
Reactivity Control	Wide Range Neutron Flux	1
RCS Integrity	Pressurizer Pressure	1
	Reactor Coolant Pressure	1
Core Heat Removal	Reactor Coolant Cold Leg Temperature	1 per Loop
RCS Inventory Control	Pressurizer Water Level	1
Secondary Heat Sink	SG Water Level	1 per SG
	Main Steam Line Pressure	1 per SG
Containment Integrity	Containment Pressure	1

**Note:**

The DHP provides at least a single indicator for each parameter. The indication of parameter can be selectable between two channels to accommodate a channel that may be failed or in bypass.

**Table 7.8-3 System Actuation Times for Each Event**

Function	AOO	SGTR	MSLB	FLB	SBLOCA	DAS Req.
Reactor Trip	A	A	A	A	A	A
(Turbine Trip)	A					A
EFWS	A	C	C	A	C	A
(Isolation of MFW System)	A	A	A			A
(Isolation of EFW System)		C	C	B		B
ECCS		C			B	B
(Primary/Secondary Depressurize)		C				C
Isolation of Secondary System		C	C			C
CSS			C	C	C	C
Isolation of C/V					C	C

**Note:**

- A: need action within 10 minutes therefore DAS automation is provided.
- B: need action within 30 minutes therefore indications and manual controls are provided on the DHP.
- C: action after 30 minutes therefore indications and manual controls are provided outside the MCR.

All times are from the first prompting alarm. The defense in depth and diversity coping analysis considers the additional time from the event initiation to the prompting alarm.

AOOs are represented in a single column because most of them are terminated with reactor shutdown.

Table 7.8-4 Diverse Actuation Signals

Actuation Signal	Number of Sensors or Switches	Actuation Logic	Permissives and Bypasses
<b>1. Reactor Trip, Turbine Trip and MFW Isolation</b>			
Low Pressurizer Pressure	4 Pressure Sensors	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
High Pressurizer Pressure	4 Pressure Sensors	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
Low SG Water Level	1 Level Sensor per SG) (Shared with EFW Actuation)	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by P-4.
Manual Actuation	1 Switch	1/1	None
<b>2. Emergency Feedwater Actuation</b>			
Low SG Water Level	1 Level Sensor per SG (Shared with reactor trip, turbine trip and MFW isolation)	2/4	Manually bypassed by the actuation of a dedicated hardwired switch on the OC during plant startup and shutdown. Blocked by 2-out-of-4 signal of EFW Pump operation signals.
Manual actuation	1 Switch	1/1	None
<b>3. ECCS Actuation</b>			
Manual Actuation	1 Switch	1/1	None
<b>4. Containment Isolation</b>			
Manual actuation	1 Switch	1/1	None
<b>5. Open/Close Emergency Feedwater Control Valves</b>			
Manual Actuation	1 Switch per SG	1/1	None
<b>6. Open/Close Safety Depressurization Valve</b>			
Manual Actuation	1 Switch	1/1	None
<b>7. Open/Close Main Steam Depressurization Valves</b>			
Manual Actuation	1 Switch per SG	1/1	None

**Table 7.8-5 Components Actuated by DAS**

<b>Safety Function or Associated Components</b>	<b>Number of Components</b>	<b>Actuation Type</b>
Diverse Reactor Trip (Motor-Generator Set Trip)	2 M/G Sets	Automatic/Manual (MCR)
Turbine Trip	2 Trip Solenoids	Automatic/Manual (MCR)
EFW Pump	4 Pumps	Automatic/Manual (MCR)
Safety Injection Pump	4 Pumps	Manual (MCR)
Safety Depressurization Valve	1 Valve	Manual (MCR)
Main Steam Depressurization Valve	1 Valve per SG	Manual (MCR)
SG Blowdown Isolation Valve	1 Valve per SG	Automatic/Manual (MCR)
MFW Regulation Valve (Close)	1 Valve per SG	Automatic/Manual (MCR)
EFW Control Valve	1 Valve per SG	Manual (MCR)
Containment Isolation Valves	1 Train	Manual (MCR)

**Table 7.8-6 Diverse Actuation Variables, Ranges, Accuracies, and Setpoints (Nominal)**

Diverse Actuation Function	Variables to be monitored	Range of Variables	Instrument Accuracy* <sup>1,2</sup>	Time Delay	Setpoint** <sup>3</sup>
<b>Reactor Trip, Turbine Trip, and MFW Isolation</b>					
Low Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	10 sec	1825 psig
High Pressurizer Pressure	Pressurizer Pressure	1700 to 2500 psig	2.5% of span	10 sec	2425 psig
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	10 sec	7% of span
<b>Emergency Feedwater Actuation</b>					
Low SG Water Level	SG Water Level	0 to 100% of span (narrow range taps)	3% of span	10 sec	7% of span

Note:

1. Instrument accuracy calculation methodology refer to Subsection 7.2.2.7.
2. Instrument accuracies will be decided to take into account the specification of instruments.
3. Setpoints will be adjusted to compensate for loop accuracy.

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 1 of 6)**

<b>No.</b>	<b>Items to be clarified</b>	<b>Corresponding Section of SER for MUAP-07006-A</b>	<b>Resolution</b>	<b>Reference Document and Section</b>
1	The US-APWR design certification applicant shall demonstrate that the isolation devices are conventional (e.g., non software based devices) and completely testable in order to meet the independence and isolation requirements of IEEE Std and address fault-isolation criteria of IEEE-384.	3.1, 3.4	The isolation devices are conventional non software based devices, qualified by test to meet the independence and fault-isolation criteria of IEEE-384. Isolation devices are standard MELTAC platform components, described in MUAP-07005 Section 4.1.2.3. PSMS analog output isolation devices are functionally tested during the manual calibration described in Section 4.4.2 of MUAP-07004. The DAS test method described in Section 4.2.6 of MUAP-07004 includes functional testing of PSMS analog output isolation devices and binary input isolation devices.	Section 4.1.2.3 of MUAP-07005 Section 4.2.6 of MUAP-07004.
2	The US-APWR design certification applicant shall demonstrate the acceptability of all manual actions. Also, the concept and application-specific implementation of the priority alarms should be adequately demonstrated.	3.1.3	The acceptability of all manual actions and prompting alarms is demonstrated through analysis and preliminary verification, as documented in MUAP-07014; US-APWR D3 coping analysis. These manual actions and prompting alarms are completely verified and validated using a fully integrated full scope dynamic plant simulator, within the HFE V&V program element. The design process for the HFE V&V program element is described in Section 18.10 of the DCD and Section 5.10 of MUAP-07007(Reference 7.8-8). Completion of the HFE V&V program element is defined in Section 2.9 of DCD Tier 1.	MUAP-07014 Section 4.11.4 of DCD Ch.18 Section 18.10 and Section 5.10 of MUAP-07007 Section 2.9 of DCD Tier 1
3	The US-APWR design certification applicant shall demonstrate that the PIF Module is not susceptible to a software CCF.	3.2.1, 3.2.2	The interposing logic part and output part of the PIF Module, which are commonly used by the PSMS and DAS, utilize only conventional solid-state hardware components, as described in Section 4.1.2.4 of MUAP-07005. Therefore, these portions of the PIF module are not susceptible to a software CCF.	Section 4.1.2.4 of MUAP-07005



**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 2 of 6)**

No.	Items to be clarified	Corresponding Section of SER for MUAP-07006-A	Resolution	Reference Document and Section
4	The US-APWR design certification applicant shall identify the specific controls and indications for the DHP and address human factors aspects for the DAS and PSMS system-level manual actuation means.	3.2.1, 3.2.2, 3.2.3	The specific controls and indications for the DHP are identified in DCD Table 7.8-1 and Table 7.8-2, respectively. Since the PSMS system level actuation controls are located on the OC and the DAS system level actuation controls are located on the DHP, and the use of the DHP controls is prompted by unique DHP alarms, there is little potential for human performance error. The HFE V&V program element described in DCD Section 18.10 ensures that the system level manual actuation means provided in PSMS and DAS, are used appropriately and without human performance error.	DCD Table 7.8-1 and 7.8-2. DCD Section 18.10.
5	The US-APWR design certification applicant shall provide the final determination of the setpoints and the response time of the DAS.	3.2.2	The DAS setpoints and time delay settings are shown in DCD Table 7.8-6. These values are demonstrated to be acceptable in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis	DCD Table 7.8-6 MUAP-07014
6	The US-APWR design certification applicant shall demonstrate that the acceptability of the QA process used for the DAS meets the guidelines of GL 85-06.	3.2.2, 4.0	The QA process used for the DAS meets the guidelines of GL 85-06 as described in DCD Subsection 7.8.2.7. To comply with GL 85-06 the DAS QA program will comply with 10 CFR 50 Appendix B as described in MUAP-07006 Section 6.2.1.7.	DCD Subsection 7.8.2.7 MUAP-07006 Section 6.2.1.7

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 3 of 6)**

<b>No.</b>	<b>Items to be clarified</b>	<b>Corresponding Section of SER for MUAP-07006-A</b>	<b>Resolution</b>	<b>Reference Document and Section</b>
7	For each AOO in the design basis occurring in conjunction with each single postulated CCF, the US-APWR design certification applicant shall demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline value or violation of the integrity of the primary coolant pressure boundary.	3.2.3	Compliance to the BTP 7-19 acceptance criteria is demonstrated for each AOO in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	MUAP-07014
8	For each PA in the design basis occurring in conjunction with each single postulated CCF, the US-APWR design certification applicant should demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR Part 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).	3.2.3	Compliance to the BTP 7-19 acceptance criteria is demonstrated for each PA in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	MUAP-07014

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 4 of 6)**

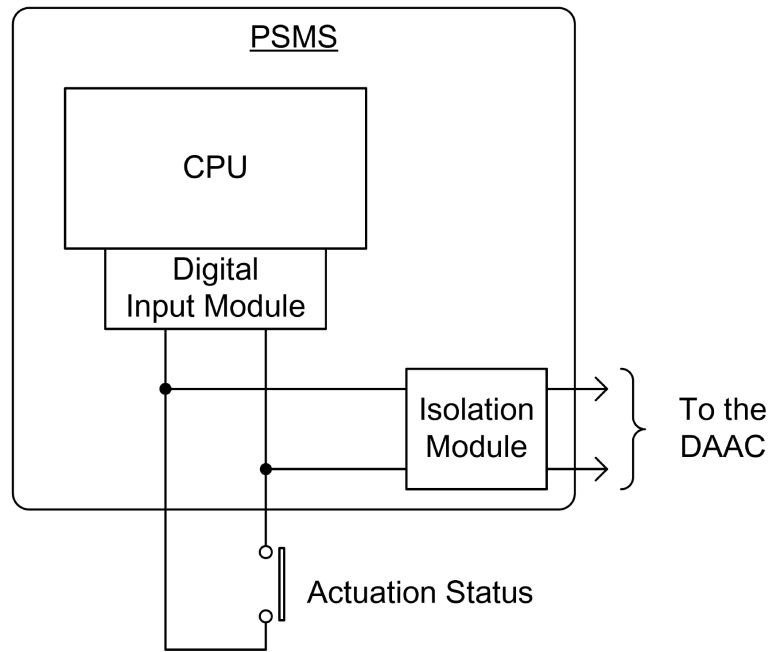
No.	Items to be clarified	Corresponding Section of SER for MUAP-07006-A	Resolution	Reference Document and Section
9	The US-APWR design certification applicant shall address the partial failures of the PCMS/ PSMS and demonstrate an adequate D3 strategy to cope with such failure modes.	3.2.3	Single failures that result in partial failure of the PSMS do not impact the PSMS safety functions, as demonstrated in DCD Tables 7.2-8 and 7.3-7. The evaluation of partial common-cause failures of the PCMS/ PSMS and an adequate D3 strategy to cope with such failure modes are provided in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	DCD Tables 7.2-8 and 7.3-7 MUAP-07014
10	The US-APWR design certification applicant shall provide an acceptable defense in depth and diversity strategy for a LBLOCA concurrent with a CCF of the PSMS.	3.3.2	An acceptable D3 strategy for a LBLOCA concurrent with a CCF of the PSMS is described in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	MUAP-07014
11	<b>Future Licensing Submittals</b> <b>(The resolution of Future Licensing Submittals described in Section 10 of MUAP-07006-A are follows)</b>			
11-1	Changes in implementation detail, as needed	1.0, 2.0	Application specific designs are described in Section 7.8	DCD Section 7.8
11-2	Specific description of the PSMS and the DAS functions	2.0	Subsection 7.2 and 7.3 describes specific description of the PSMS; the DAS functions are in Section 7.8	DCD Section 7.2, 7.3 and 7.8
11-3	Specific I&C functions implemented within the DAS	3.1 GDC 13	DCD Figure 7.2-2 Sheet 14 describes specific DAS functions.	DCD Figure 7.2-2

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 5 of 6)**

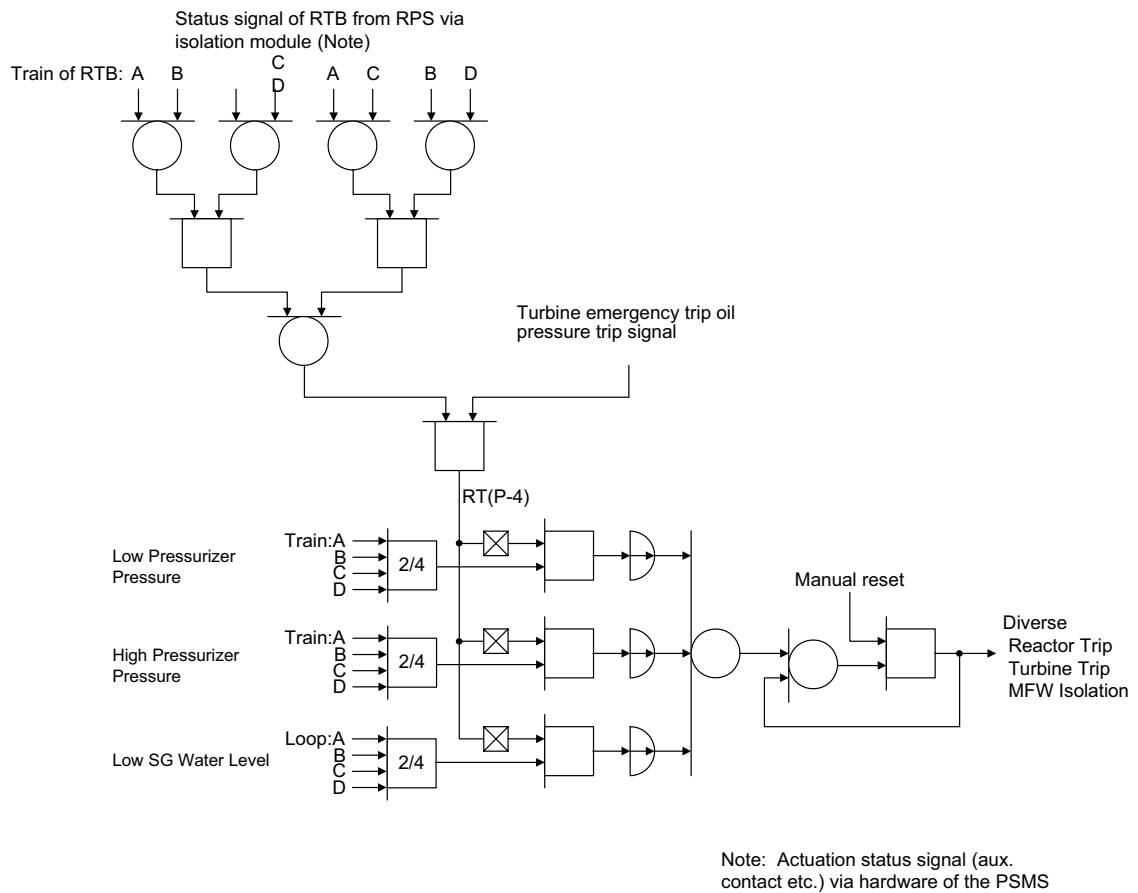
<b>No.</b>	<b>Items to be clarified</b>	<b>Corresponding Section of SER for MUAP-07006-A</b>	<b>Resolution</b>	<b>Reference Document and Section</b>
11-4	Electric power sources for the DAS and the plant components controlled by the DAS	3.1 GDC 17	DCD Section 7.8 describes electric power sources for the DAS. Each DAAC is powered by N11 or N12 UPS shown in DCD Fig 8.1-1, respectively. The DHP is powered only by UPS N11. The components actuated by DAS are safety related, therefore they are powered by safety power source discussed in DCD Section 8.3. The two control rod MG-set motor contactors are self-powered from their respective MG-sets.	DCD Section 7.8 DCD Section 8.1, 8.3
11-5	Conformance to the requirements in 10 CFR 52.47 Section (a)(1) items iv, vi, and vii.	3.1 10 CFR 52.47	The level of design information required by 10 CFR 52.47 is described in the DCD and its references.	DCD and references
11-6	Inspections, tests, analyses and acceptance criteria that demonstrate that the DAS has been constructed and will operate in conformity with the Commission's final safety conclusion	3.1 10 CFR 52.79	Resolved in DCD ITAAC Table 2.5.3-4.	DCD Tier 1 Table 2.5.3-4
11-7	Specific DAS functions of manual Initiation of Protective Actions	3.3 RG 1.62	DCD Subsection 7.8.1.1 describes DAS functions of manual initiation.	DCD Subsection 7.8.1.1
11-8	Specific accident monitoring instrumentation of the DAS	3.3 RG 1.97	DCD Subsection 7.8.1.2 describes specific accident monitoring instrumentation of DAS.	DCD Section 7.8.1.2
11-9	Instrument Sensing Lines	3.3 RG 1.151	Subsection 7.1.3.7 describes the conformance to RG1.151. The DAS uses the same instruments and instrument sensing lines as the PSMS.	DCD Subsection 7.1.3.7
11-10	Design Acceptance Criteria	3.4 BTP-16	BTP-16 has been withheld. There are no design acceptance criteria related to DAS. The ITAAC for DAS are defined in DCD Tier 1 Subsection 2.5.3	DCD Tier 1 Subsection 2.5.3

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 6 of 6)**

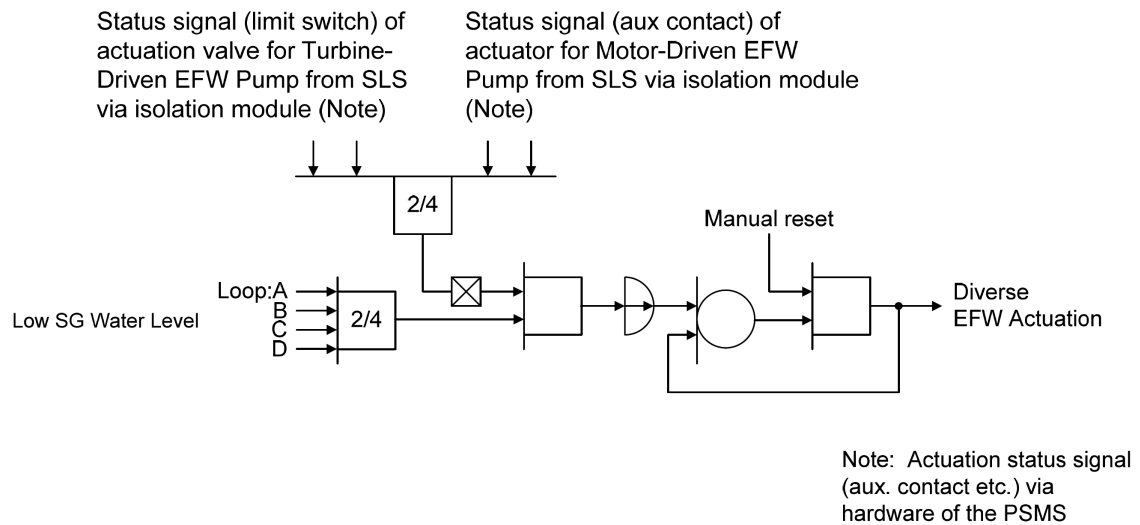
<b>No.</b>	<b>Items to be clarified</b>	<b>Corresponding Section of SER for MUAP-07006-A</b>	<b>Resolution</b>	<b>Reference Document and Section</b>
11-11	Coping for all AOOs and PAs	3.4 BTP-19	Described in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis	MUAP-07014
11-12	Descriptions of specific plant systems	3.5 NUREG-0800	The plant systems monitored and controlled by DAS to cope with AOOs and PAs with concurrent CCF are described in MUAP-07014	MUAP-07014
11-13	Specific DAS functions for other plants	6.0	DCD Figure 7.2-2 Sheet 14 describes specific DAS functions.	DCD Section 7.2
11-14	Specific functional logic for each plant	6.1	DCD Figure 7.2-2 Sheet 14 describes specific DAS functions.	DCD Section 7.2
11-15	Third method for RCS leak detection	6.2.3	Coping with LBLOCA, without crediting leak detection, is demonstrated in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis, therefore leak detection is not necessary.	N/A
11-16	Specific information of multiple reactor trip functions and ESF actuations	7.2.1	DCD Table 7.2-5 provides the multiple PSMS parameters.	DCD Table 7.2-5
11-17	Functional diversity within the PSMS	7.2.3	DCD Table 7.2-5 provides the functional diversity within the PSMS.	DCD Table 7.2-5
11-18	Sensor diversity within the PSMS for each AOO and PA	7.3.3	DCD Table 7.2-5 provides the sensor diversity within the PSMS.	DCD Table 7.2-5
11-19	Results of the D3 Coping Analysis for each event	8.1	Described in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis.	MUAP-07014
11-20	An analysis for each AOO and PA in SAR chapter 15 with a concurrent CCF that disables the PSMS and PCMS	Appendix A Point 2	Described in MUAP-07014, Defense-in-Depth and Diversity Coping Analysis	MUAP-07014



**Figure 7.8-1 The Signal Flow of the Status Signal to DAS**



**Figure 7.8-2 The Prevention Diagram of Reactor Trip, Turbine Trip and MFW Isolation in DAS**



**Figure 7.8-3 The Prevention Diagram of Emergency Feedwater Actuation in DAS**



---

## 7.9 Data Communication Systems

The DCS consists of the plant-wide unit bus, safety bus for each PSMS train, maintenance network for each PSMS train and the PCMS (five maintenance networks total), data links for point-to-point communication, and I/O bus for each controller. Figure 7.1-1 shows the involvement of each part of the DCS in the overall I&C architecture, with the exception of the maintenance network, which is shown in MUAP-07005 (Reference 7.9-1) Section 4.3.4. The DCS interfaces to the station bus, which is an information technology network (i.e., not I&C), as described in Subsection 7.9.1.6. The DCS interfaces to the HSIS and the unit bus are shown in Figure 7.9-1 and described in Table 7.9-1.

Although the DCS is a distributed and highly interconnected system, there is communication independence to prevent electrical and communication processing faults in one division (safety or non-safety) from adversely affecting the performance of safety functions in other divisions. To prevent electrical faults from transferring between divisions and between different plant fire areas for the MCR, RSR and I&C rooms, qualified fiber-optic isolators are used. Communication faults are prevented through a data integrity verification process that is described in MUAP-07005 Section 4.3.2.

### 7.9.1 System Description

#### 7.9.1.1 Control Network (Safety Bus and Unit Bus)

The control network technology is utilized for the plant-wide unit bus and the safety bus for each PSMS division.

The control network is a redundant bi-directional multi-node network that has automatic node detection and redirection features. The network provides the functionality to maintain communication even if a controller is powered down or if there is an unresponsive controller.

The Control Network is a fiber optic network, which interfaces to the control network interface module of each controller via qualified electrical to optical (E/O) converter. There is a separate E/O converter and control network interface module for each control network (i.e., unit bus and safety bus).

Details on the control network are described in MUAP-07005 Section 4.3.2.

##### 7.9.1.1.1 Safety Bus

The controllers of the SLS, ESFAS, and RPS, and the safety VDU processor communicate via the safety bus within each PSMS division. The signals transmitted on this network are described in Sections 7.2 through 7.6. The interconnections of these systems to the safety bus are shown in Figures 7.2-1 and 7.3-1.

There is one safety bus for each train. Each safety bus is used only within the same train.

---

**7.9.1.1.2 Unit Bus**

The unit bus provides non-safety data communication between all I&C systems. The main signals transmitted through the unit bus are:

- Manual operation signals transmitted from the operational VDUs in the MCR and RSR to the PSMS and PCMS. Signals to the PSMS are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic.
- Signals transmitted from the PCMS to PSMS for interlocks and automatic control of safety components during normal operation. These signals are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic.
- Process and alarm signals transmitted from the PSMS and PCMS to the LDP and VDUs in all operating locations, MCR, RSR, and TSC and to the computer systems such as process recording computer system, alarm processor system, etc.
- Shared sensor signals, such as pressurizer pressure, and shared calculated signals, such as  $T_{avg}$ , are transmitted from each PSMS division to the PCMS.

Signals interfaced between the PSMS and PCMS use qualified E/O isolators that are part of the safety system. In addition, communication and functional isolation are provided, within the PSMS, for signals sent from the PCMS to PSMS, such as process control signals and signals from operational VDUs. These signals are interfaced via redundant communication subsystems within the PSMS, referred to as the COM, which provide the communication interface between the unit bus and all PSMS controllers for non-safety control signals that originate in the PCMS.

Further details on communication independence are discussed in MUAP-07004 (Reference 7.9-2) Appendix B.5.6.

**7.9.1.2 Safety VDU Communication**

The safety VDU has two interfaces with the safety VDU processor:

- Conventional red/green/blue video signals are interfaced through a frame memory unit module within the safety VDU processor.
- The safety VDU touch panel is interfaced to the safety VDU processor through a touch panel interface module, which provides a conventional point-to-point data link.

Safety VDU processors are located in the Class 1E I&C room. There are separate safety VDU processors for the safety VDUs in the MCR and the safety VDUs in the RSR. Each safety VDU processor interfaces to the safety bus by a qualified E/O isolator. This

isolator ensures that electrical faults originating in the MCR or the RSR, which may adversely affect the respective safety VDU Processors, cannot propagate to the safety bus. Therefore, these faults cannot adversely affect safety bus communications or other controllers/processors on the safety bus. (The location of the safety VDU processors is different from the location described in MUAP-07005.)

Control commands from the safety VDU processors are interfaced to other PSMS processors in the same train via the Safety Bus and the COM. Within the COM, the safety VDU commands are combined with control commands from Operational VDUs. The priority logic in the COM ensures safety VDU commands always have priority over corresponding Operational VDU commands. In addition, this logic allows all Operational VDU commands to be blocked when the Safety VDU "Disconnect" command is selected, as shown in MUAP-07004 Figure 5.1-3.

#### 7.9.1.3 Data Links

Data link communication is used to transmit signals between the controllers in different divisions and within controllers of the same division, as follows:

- Between RPS controllers in all trains
- Between RPS and ESFAS controllers in all trains
- Between the reactor control system and CRDM control system controllers
- Between incore instrumentation system and the unit management computer

Data links use fiber optic interfaces to provide electrical isolation between divisions. Separate E/O conversion devices are used at the receiving end and sending end for each data link interface.

The data link interface provides unidirectional broadcast only communication with no data communication handshaking. Communication independence is assured by two port memory and specific attributes of the basic software within the controllers. These design features ensure that communication with external divisions cannot disrupt the deterministic processing of control functions, including the safety functions of the PSMS. MUAP-07005 Section 4.3.3 provides a detailed description of the data links including communication independence.

Data links are interfaced to the controller via the bus master module. The bus master module has four ports, which can be configured for either sending or receiving, as follows:

- Between RPS controllers in all trains - Each RPS controller includes one bus master module configured to broadcast its data to the RPS controllers in the three other trains (one of four ports utilized). This same bus master module receives broadcast data from the RPS controllers in the three other trains (three of four ports utilized).
- Between RPS and ESFAS controllers in all trains - Each RPS controller includes one bus master module configured to send its data to the two ESFAS controllers in its own train and the two ESFAS controllers in the three other trains (one of four

ports utilized). Each ESFAS controller includes two bus master modules to receive the broadcast data from the eight RPS controllers in all four trains. One bus master module receives data from RPS controllers A - Group 1, A - Group 2, B - Group 1, and B - Group 2 (four of four ports utilized), the second bus master module receives data from RPS controllers C - Group 1, C - Group 2, D - Group 1, and D - Group 2 (four of four ports utilized).

The failure of a bus master module and E/O conversion device is considered in the FMEA.

#### 7.9.1.4 I/O Bus

The I/O bus provides a bi-directional interface between a controller and its I/O modules. The I/O bus is interfaced via the bus master module in the controller and the repeater module within each I/O chassis. For single non-redundant controller configurations, the I/O bus is not redundant. For redundant controller configurations, the I/O bus is redundant. Various redundancy configurations are utilized as described in MUAP-07005 Section 4.1.1.1.

I/O can be located in close proximity to the controller or in locations remote from the controller. Remote I/O is utilized for both PCMS and PSMS applications.

#### 7.9.1.5 Maintenance Network

The maintenance network is a non-safety system that allows for monitoring the status of the PSMS and PCMS equipment failure indications and diagnostics, updating setpoints and constants, and the installation of new application software. PSMS controllers are normally not connected with the maintenance network. PSMS controllers that are temporarily connected to the maintenance network are declared inoperable and the affected inoperable functions of that controller are managed by the technical specifications. Access control for the maintenance network is described in MUAP-07004 Section 6.4.1. There is communication independence for the maintenance networks for each division. However, since all maintenance networks are non-safety, no electrical independence is required and there are locations in the plant where all maintenance networks are in close physical proximity. The following description is applicable to the maintenance network for any one division.

The major components of the maintenance network are the switching hub and the engineering tool. The maintenance network interfaces to the system management module of each controller via qualified E/O converters.

**Security-Related Information – Withheld Under 10 CFR 2.390**

(SRI)

---

**Security-Related Information – Withheld Under 10 CFR 2.390**

(SRI)

**7.9.1.6 Station Bus**

The station bus provides information to plant and corporate personnel and to the EOF and ERDS. The station bus receives information from the DCS via the unit management computer. The unit management computer provides a firewalled interface, which allows only outbound communication. There are no other connections from external sources to the DCS.

**7.9.1.7 External Network Interface**

The only interface from the PCMS and PSMS to external networks is via the firewall within the unit management computer. The unit management computer provides an outbound only interface to the plant Station Bus to allow communication to EOF computers, the NRC (via ERDS), corporate information systems and plant personnel computers.

**7.9.2 Design Basis Information**

**7.9.2.1 Quality of Components and Modules**

The PSMS includes the safety bus, data links, I/O bus, and safety VDU communications. The MELTAC platform is applied for all safety DCS components and follows the MELCO QA program. The quality of PSMS components and modules and the quality of the PSMS design process is controlled by a program that meets the requirements of ASME NQA-1-1994 (Reference 7.9-3). Conformance to ASME NQA-1-1994 is described further in Chapter 17.

The PCMS includes the unit bus, data links, I/O Bus, and the PCMS computers. The PCMS data communications uses the same hardware as the PSMS. The PCMS has a similar quality program to the PSMS, without the same level of documentation.

---

### 7.9.2.2 Software Quality

The safety related portions of the DCS are part of the PSMS. The non-safety related portions of the DCS are part of the PCMS. All portions of the DCS consist of MELTAC basic software, which handles the communication protocol and self-diagnostics, and application software, which handles the actual data being transmitted.

MHI applies its MELCO's safety system digital platform MELTAC to PSMS and PCMS systems of US-APWR. Details of the software quality program for the MELTAC basic software are discussed in MUAP-07005 Section 6.0. A summary of the software quality program for the PSMS application software is discussed in MUAP-07004 Section 6.0. A description of the application software quality program is provided in the Software Program Manual for US-APWR Technical Report MUAP-07017 (Reference 7.9-4).

The Software Program Manual Technical Report MUAP-07017, describes the processes, which ensure the reliability and design quality of the PSMS application software throughout its entire software lifecycle. MUAP-07017 also provides the software program plans based on the guidance of BTP 7-14. By following this SPM, the PSMS application software achieves high functionality and high quality including data communication systems as follows.

- Application software for the PSMS achieves a quality level expected for nuclear plant safety functions.
- Application software provides the required safety functions.
- The processes and procedures described in MUAP-07017 are based on established technical and document control requirements, practices, rules and industrial standards.

### 7.9.2.3 Performance Requirements

DCS in digital I&C system of the US-APWR meets the performance of required functions. The performance of the digital I&C system including DCS conforms to the guideline of BTP 7-21(Reference 7.9-15). Technical Report MUAP-09021 (Reference 7.9-16) provides the response time of safety I&C system. The report demonstrates that the safety I&C system meets the response time requirement from safety analysis. The simplified block diagrams of the RT and ESF functions propagation paths and response time of each path in the safety I&C system are provided. The conformance of BTP 7-21 and how the safety I&C system meets the performance requirements are also addressed in MUAP-09021.

#### 7.9.2.3.1 System Deterministic Timing

All DCS communication protocols allow calculation of a deterministic data communication response time. The time calculation includes the number of nodes on the network, data traffic, network topology, node processing cycle time, and network throughput. The methods used for real-time performance calculations are described in MUAP-07005 Section 4.4.

---

**7.9.2.3.2 Real-Time Performance**

Real-time performance is determined by performing response time analysis for all safety functions. For each safety function an analysis has been performed which demonstrates the actual system response time is less than the response time required by the plant safety analyses. Refer to MUAP-07004 Section 6.5.2 for the related details. Response times for the RPS and ESFAS functions are listed in Tables 7.2-3 and 7.3-4 respectively.

**7.9.2.3.3 Time Delays within the DCS**

Data propagation delays due to data communication in the DCS are incorporated into response time analysis. Response time calculations, which encompass the controller and all components connected to the DCS, include these data propagation delays. DCS response time calculations are validated through sample tests, during system integration testing, refer to MUAP-07004 Section 6.5.3.

**7.9.2.3.4 Data Rates and Bandwidth**

The data rates and bandwidths for the sections of the DCS are listed in MUAP-07005 as follows:

- Control network: Table 4.3-2.
- Data links: Section 4.3.3.
- Maintenance network: Section 4.1.4.2.
- I/O bus: Appendix A.3.
- Safety VDU communication: Appendix A.11 and A.12.

**7.9.2.3.5 Interfaces with other DCS**

**Security-Related Information – Withheld Under 10 CFR 2.390**

(SRI)

**7.9.2.3.6 Test Results**

MELTAC platform testing demonstrates that the DCS meets all generic qualification requirements, refer to MUAP-7005 Section 5.0. Qualification analysis demonstrates that the generic qualification testing bounds all US-APWR conditions.

The PCMS and PSMS factory test phase demonstrates that the DCS meets all US-APWR application performance requirements, refer to MUAP-07004 Section 6.1.

**7.9.2.3.7 Communication Protocols**

All communication protocols selected for the DCS are able to support all demands from interfacing systems. Refer to MUAP-07005 Section 4.0 and Appendix A for further details

on the specific communication protocols used in each network of the DCS including capabilities, bandwidth, and data rates.

#### 7.9.2.4 Potential Hazards and Single Failures

The self-diagnostic features described in MUAP-07004 Section 4.3, detect DCS errors or failures. The MELTAC controller has separate self-diagnostic features for each of the DCS related modules as described in MUAP-07005 Section 4.1.5 and Section 4.3. All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function. The FMEA identifies errors or failures that can result in failures or inadvertent actuation of single divisions, which are bounded by the plant safety analysis.

In addition, the safety controllers within the PSMS include electrical and communication isolation to ensure that the deterministic processing of the safety functions can not be affected due to failures or communication errors from the unit bus or maintenance network. Table 7.2-8 and Table 7.3-7 which shows the FMEA for reactor trip and ESF actuation in the PSMS include failure mode and effects of the DCSs.

#### 7.9.2.5 Control of Access

Security-Related Information – Withheld Under 10 CFR 2.390

#### 7.9.2.6 Cyber Security

The use of computer systems for various functions at nuclear power plants including digital I&C systems increases the potential for threats from cyber intrusions.

The COL Applicant is to provide a description of cyber security provisions.

#### 7.9.2.7 Independence

The DCS ensures electrical independence between PSMS divisions and between the PSMS and PCMS. In addition, electrical independence is maintained within the PSMS and PCMS, where the communication interfaces cross fire areas of the MCR and RSR.



Each PSMS and PCMS controller/processor protects itself against DCS errors or failures that could disrupt its internal application functions, thereby ensuring communications independence. For more detailed discussion on the methods used to ensure independence between digital systems in different safety trains and between safety and non-safety systems refer to Subsections 7.1.3.4 and 7.1.3.5, and MUAP-07004 Appendix A.5.6 and Appendix B.5.6.

All PSMS DCS cables, with the exception of its maintenance networks, are routed in accordance with IEEE Std 384-1992 (Reference 7.9-5) to ensure physical independence of each division. PSMS maintenance network cables, which are non-safety, are routed with other non-safety cables, including PCMS DCS cables.

#### **7.9.2.8 Fail Safe Failure Modes**

In general, controllers take no automatic fail-safe actions in response to failures in the unit bus, safety bus, data links, or I/O Bus. This means that inputs to control algorithms are considered to remain in the state prior to the DCS failure, and outputs from controllers remain in their state prior to the DCS failure. All DCS failures are alarmed so that operators can take appropriate manual actions. These actions may include setting signals to trip or maintenance bypass status, and declaring appropriate the technical specification inoperable status. Where failures affect only one of two redundant buses, actions may be limited to only initiating work orders for maintenance repairs.

The RPS controllers take fail-safe actions in response to failures in multiple data links, between the RPS trains, that result in loss of data to the 2-out-of-4 voting logic within each train. On the first failure (or bypassed data link) the voting logic becomes 2-out-of-3. On the second failure (or bypassed data link) the voting logic becomes 1-out-of-2. Failure (or bypass) of a third link will generate a trip based on this 1-out-of-2 logic. In addition, outputs from the RPS controllers to the RTBs will fail in a state that initiates opening of the RTBs if there is a failure of the I/O bus. This design satisfies the fail-safe requirements of 10 CFR 50 Appendix A, GDC 23 (Reference 7.9-6).

Alarms are provided for the DCS failures. Unique alarms are provided for DCS failures that affect inputs to the RPS voting logic from multiple divisions. For example, unique alarms are provided if an RPS controller detects two or more data link failures or a single data link failure when one of its own process parameters is already in a maintenance bypass condition.

#### **7.9.2.9 System Testing and Surveillances**

The MELTAC controller has separate self-diagnostic features for each of the DCS related modules; refer to MUAP-07005 Section 4.1.5 and Section 4.3. There are no periodic manual surveillance tests required for DCS functions.

#### **7.9.2.10 Bypass and Inoperable Status Indications**

There are no manual bypasses for any functions of the DCS. DCS failures are alarmed on the operational and alarm VDUs.

---

**7.9.2.11 EMI/RFI Susceptibility**

The PSMS DCS is qualified to the EMI/RFI testing requirements of RG 1.180 (Reference 7.9-7), refer to MUAP-07005 Section 5.3.

The PCMS DCS uses the same hardware and software components as the PSMS DCS.

**7.9.2.12 Defense-In-Depth and Diversity**

There is no credit for continued the DCS operability in the defense in depth and diversity coping analysis (i.e., the DCS is assumed to fail due to CCF). The DCS is not used by the conventional analog and hardwired DAS. A discussion on defense in depth and diversity is provided in Topical Report MUAP-07006 (Reference 7.9-8).

**7.9.2.13 Seismic Hazards**

All safety-related DCS components and hardware are Class 1E qualified and are in an appropriately qualified structure. Where non-safety portions of the DCS interface with the safety portions, qualified isolators are used which preserve the seismic qualifications of the safety-related portions. Refer to MUAP-07005 Section 4.1 and 5.2 for the related details.

The operational VDUs and unit bus are also tested to demonstrate operability after an SSE. In addition, the testing demonstrates that there are no erroneous signals generated that can adversely affect the PSMS or PCMS systems.

**7.9.3 Analysis**

Detailed compliance to the GDC, IEEE Std 603-1991 (Reference 7.9-9) and IEEE Std 7-4.3.2-2003 (Reference 7.9-10) are described in MUAP-07004 Section 3.0, Appendix A and B.

The FMEA demonstrates that failures in the DCS do not adversely affect the safety function of the PSMS or cause erroneous safety function actuation, refer to MUAP-07005 Section 7.4.

**7.9.4 Combined License Information**

COL 7.9(1)      *The COL Applicant is to provide a description of cyber security provisions.*

**7.9.5 References**

7.9-1      Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.

7.9-2      Safety I&C System Description and Design Process, MUAP-07004-P Rev.5 (Proprietary) and MUAP-07004-NP Rev.5 (Non-Proprietary), October 2010.

- 
- |        |  |  |
|--------|--|--|
| 7.9-3  | <u>Quality Assurance Program Requirements for Nuclear Facilities</u> , ASME NQA-1-1994.  |  |
| 7.9-4  | <u>US-APWR Software Program</u> , MUAP-07017-P Rev.3 (Proprietary) and MUAP-07017-NP Rev.3 (Non-Proprietary), January 2011.  |  |
| 7.9-5  | <u>Criteria for Independence of Class 1E Equipment and Circuits</u> , IEEE Std 384-1992.   |  |
| 7.9-6  | <u>Protection System Failure Modes, General Design Criteria for Nuclear Power Plant 23</u> , NRC Regulations Title 10, Code of Federal Regulations, 10 CFR Part 50, Appendix A.            |  |
| 7.9-7  | <u>Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems</u> , Regulatory Guide 1.180 Revision 1, October 2003. |  |
| 7.9-8  | <u>Defense-in-Depth and Diversity</u> , MUAP-07006-P-A Rev.2 (Proprietary) and MUAP-07006-NP-A Rev.2 (Non-Proprietary), September 2009.  |  |
| 7.9-9  | <u>IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations</u> , IEEE Std 603-1991.  |  |
| 7.9-10 | <u>IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations</u> , IEEE Std 7-4.3.2-2003.  |  |
| 7.9-11 | Intentionally Blanked.   |  |
| 7.9-12 | Intentionally Blanked.   |  |
| 7.9-13 | Intentionally Blanked.   |  |
| 7.9-14 | <u>Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems</u> , BTP 7-14 Revision 5, March 2007.  |  |
| 7.9-15 | <u>Guidance on Digital Computer Real-Time Performance</u> , BTP 7-21 Revision 5, March 2007.   |  |
| 7.9-16 | <u>Response Time of Safety I&amp;C System</u> , MUAP-08021-P Rev.1 (Proprietary) and MUAP-09021-NP Rev.1 (Non-Proprietary), April 2010.  |  |

**Table 7.9-1 Interface between HSIS and Other Systems  
(For Figure 7.9-1)**

<b>Interface Signals</b>	<b>Example of Signals</b>
(a) Safety operation signals to safety system [conventional switches]	RT signals, ESF actuation signals
(b) Safety operation signals from Safety VDU to safety system [soft controls on safety VDU]	Safety component manipulation signals, ECCS reset signals
(c) Safety information signals from safety system to safety VDU.	PAM signals, safety status signals
(d) Safety operation signals from operational VDU to safety system [soft controls on operational VDU]	Safety component manipulation signals, ECCS reset signals
(e) Safety information signals from safety system to operational VDU.	PAM signals, safety status signals, safety alarms
(f) Non-safety information signals from Non-safety system to operational VDU.	Plant parameter, component status signals, alarms
(g) Operation signals from operational VDU to non-safety system [soft controls on operational VDU]	Component manipulation signals
(h) Bypass signal to DAS [conventional switches]	Bypass signal from OC to DAS

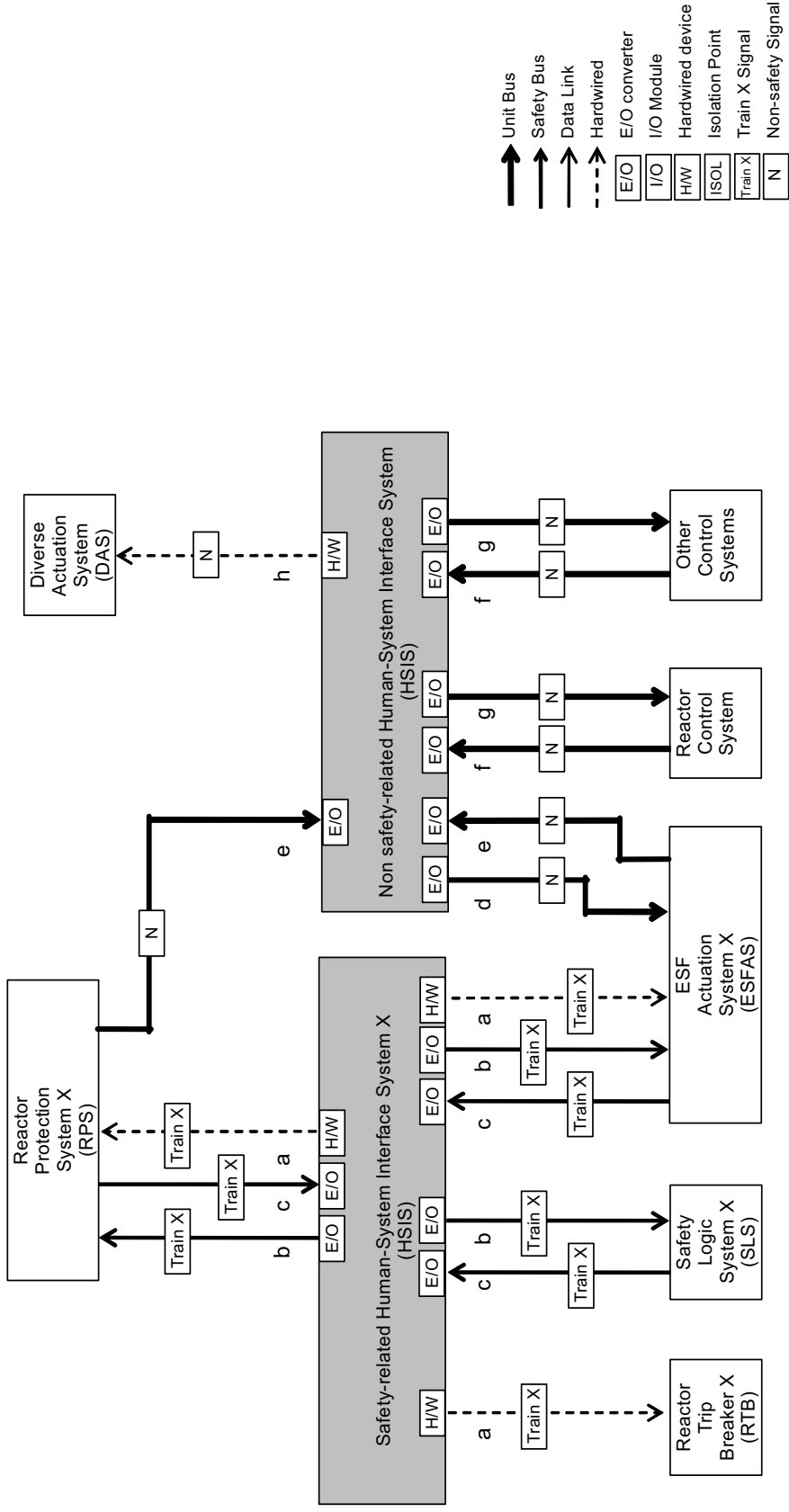


Figure 7.9-1 Interface between HSIS and Other Systems (for Table 7.9-1)