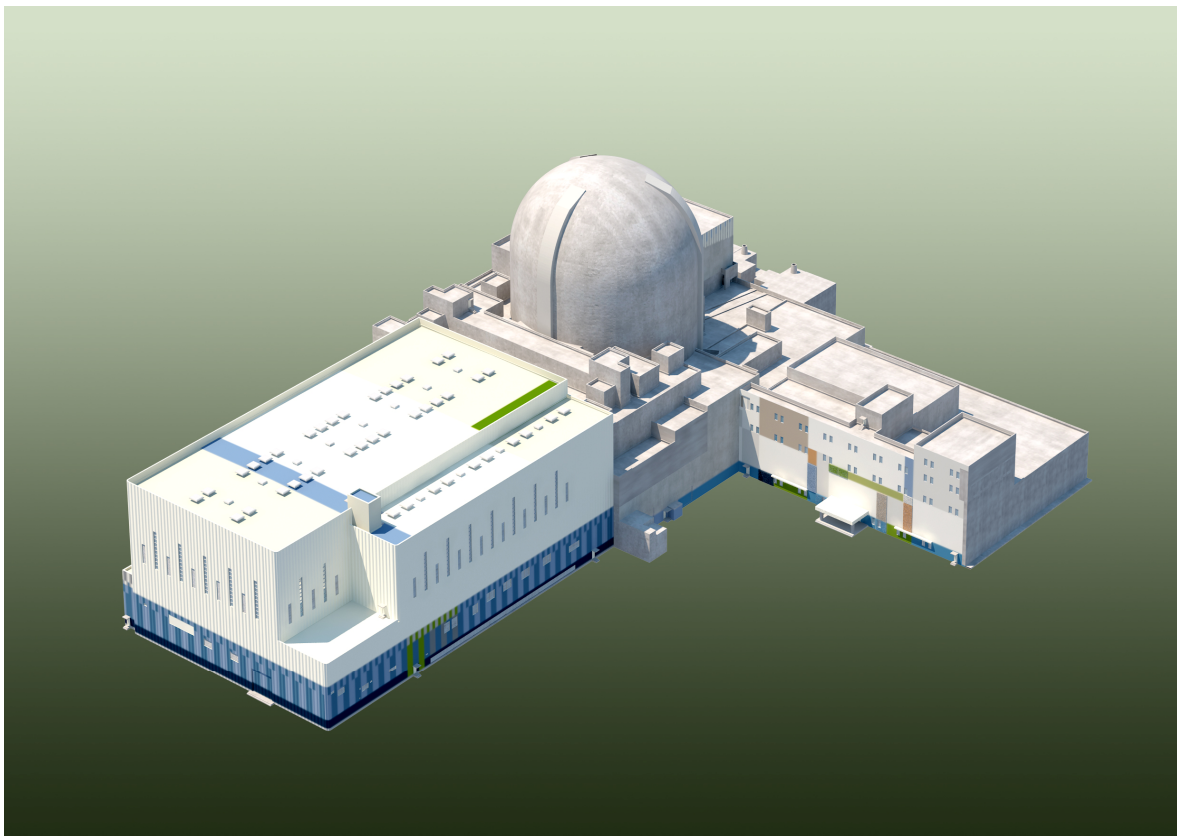


APR1400
DESIGN CONTROL DOCUMENT TIER 2

CHAPTER 7
INSTRUMENTATION AND CONTROLS

APR1400-K-X-FS-13002
REVISION 0
SEPTEMBER 2013



© 2013

KEPCO and KHNP

All Rights Reserved

This document was prepared for the design certification application to the U.S. Nuclear Regulatory Commission and contains technological information that constitutes intellectual property.

Copying, using, or distributing the information in this document in whole or in part is permitted only by the U.S. Nuclear Regulatory Commission and its contractors for the purpose of reviewing design certification application materials. Other uses are strictly prohibited without the written permission of Korea Electric Power Corporation and Korea Hydro & Nuclear Power Co., Ltd.

CHAPTER 7 – INSTRUMENTATION AND CONTROLS

TABLE OF CONTENTS

CHAPTER 7 – INSTRUMENTATION AND CONTROLS	7.1-1
7.1 Introduction.....	7.1-1
7.1.1 Identification of Safety Systems and Non-Safety Systems	7.1-3
7.1.1.1 Plant Protection System.....	7.1-3
7.1.1.2 Reactor Trip System	7.1-4
7.1.1.3 Engineered Safety Features Systems.....	7.1-4
7.1.1.4 Systems Required for Safe Shutdown	7.1-5
7.1.1.5 Information Systems Important to Safety.....	7.1-6
7.1.1.6 Interlock Systems Important to Safety	7.1-8
7.1.1.7 Control Systems Not Required for Safety	7.1-8
7.1.1.8 Diverse Instrumentation and Control Systems	7.1-9
7.1.1.9 Data Communication Systems	7.1-9
7.1.1.10 Auxiliary Support Features.....	7.1-10
7.1.2 Identification of Safety Criteria.....	7.1-10
7.1.2.1 Design Bases	7.1-10
7.1.2.2 Conformance with 10 CFR 50.55a(a)(1).....	7.1-11
7.1.2.3 Conformance with 10 CFR 50.55a(h)(2).....	7.1-11
7.1.2.4 Conformance with 10 CFR 50.55a(h)(3).....	7.1-11
7.1.2.5 Conformance with 10 CFR 50.34f(2)(v)	7.1-12
7.1.2.6 Conformance with 10 CFR 50.34f(2)(xi).....	7.1-12
7.1.2.7 Conformance with 10 CFR 50.34f(2)(xii).....	7.1-12
7.1.2.8 Conformance with 10 CFR 50.34f(2)(xiv).....	7.1-12
7.1.2.9 Conformance with 10 CFR 50.34f(2)(xvii).....	7.1-12
7.1.2.10 Conformance with 10 CFR 50.34f(2)(xviii).....	7.1-13
7.1.2.11 Conformance with 10 CFR 50.34f(2)(xix).....	7.1-13
7.1.2.12 Conformance with 10 CFR 50.34f(2)(xx)	7.1-13
7.1.2.13 Conformance with 10 CFR 50.62.....	7.1-13
7.1.2.14 Conformance with GDC 1	7.1-13
7.1.2.15 Conformance with GDC 2.....	7.1-13

APR1400 DCD TIER 2

7.1.2.16	Conformance with GDC 4.....	7.1-14
7.1.2.17	Conformance with GDC 10.....	7.1-14
7.1.2.18	Conformance with GDC 13.....	7.1-14
7.1.2.19	Conformance with GDC 15.....	7.1-14
7.1.2.20	Conformance with GDC 16.....	7.1-14
7.1.2.21	Conformance with GDC 19.....	7.1-14
7.1.2.22	Conformance with GDC 20.....	7.1-14
7.1.2.23	Conformance with GDC 21.....	7.1-15
7.1.2.24	Conformance with GDC 22.....	7.1-15
7.1.2.25	Conformance with GDC 23.....	7.1-15
7.1.2.26	Conformance with GDC 24.....	7.1-15
7.1.2.27	Conformance with GDC 25.....	7.1-15
7.1.2.28	Conformance with GDC 28.....	7.1-15
7.1.2.29	Conformance with GDC 29.....	7.1-16
7.1.2.30	Conformance with GDC 33.....	7.1-16
7.1.2.31	Conformance with GDC 34.....	7.1-16
7.1.2.32	Conformance with GDC 35.....	7.1-16
7.1.2.33	Conformance with GDC 38.....	7.1-16
7.1.2.34	Conformance with GDC 41.....	7.1-16
7.1.2.35	Conformance with GDC 44.....	7.1-16
7.1.2.36	Conformance with SECY 93-087 II.Q.....	7.1-16
7.1.2.37	Conformance with SECY 93-087 II.T.....	7.1-17
7.1.2.38	Conformance with NRC RG 1.22.....	7.1-18
7.1.2.39	Conformance with NRC RG 1.47.....	7.1-19
7.1.2.40	Conformance with NRC RG 1.53, as Augmented by IEEE Std. 379.....	7.1-19
7.1.2.41	Conformance with NRC RG 1.62.....	7.1-19
7.1.2.42	Conformance with NRC RG 1.75, as Augmented by IEEE Std. 384.....	7.1-20
7.1.2.43	Conformance with NRC RG 1.97.....	7.1-21
7.1.2.44	Conformance with NRC RG 1.105.....	7.1-21
7.1.2.45	Conformance with NRC RG 1.118, as Augmented by IEEE Std. 338.....	7.1-22

APR1400 DCD TIER 2

7.1.2.46	Conformance with NRC RG 1.151	7.1-22
7.1.2.47	Conformance with NRC RG 1.152	7.1-22
7.1.2.48	Conformance with NRC RG 1.168	7.1-23
7.1.2.49	Conformance with NRC RG 1.169	7.1-24
7.1.2.50	Conformance with NRC RG 1.170	7.1-24
7.1.2.51	Conformance with NRC RG 1.171	7.1-24
7.1.2.52	Conformance with NRC RG 1.172	7.1-24
7.1.2.53	Conformance with NRC RG 1.173	7.1-24
7.1.2.54	Conformance with NRC RG 1.180	7.1-25
7.1.2.55	Conformance with NRC RG 1.189	7.1-25
7.1.2.56	Conformance with NRC RG 1.204	7.1-25
7.1.2.57	Conformance with NRC RG 1.206	7.1-25
7.1.2.58	Conformance with BTP 7-1	7.1-25
7.1.2.59	Conformance with BTP 7-2	7.1-25
7.1.2.60	Conformance with BTP 7-3	7.1-26
7.1.2.61	Conformance with BTP 7-4	7.1-26
7.1.2.62	Conformance with BTP 7-5	7.1-26
7.1.2.63	Conformance with BTP 7-6	7.1-26
7.1.2.64	Conformance with BTP 7-8	7.1-26
7.1.2.65	Conformance with BTP 7-9	7.1-26
7.1.2.66	Conformance with BTP 7-10	7.1-26
7.1.2.67	Conformance with BTP 7-11	7.1-27
7.1.2.68	Conformance with BTP 7-12	7.1-27
7.1.2.69	Conformance with BTP 7-13	7.1-27
7.1.2.70	Conformance with BTP 7-14	7.1-27
7.1.2.71	Conformance with BTP 7-17	7.1-27
7.1.2.72	Conformance with BTP 7-18	7.1-28
7.1.2.73	Conformance with BTP 7-19	7.1-28
7.1.2.74	Conformance with BTP 7-21	7.1-28
7.1.2.75	Conformance with DI&C-ISG-04	7.1-28
7.1.3	Digital Instrumentation and Control Systems Software Design Process	7.1-28

APR1400 DCD TIER 2

7.1.4	Combined License Information.....	7.1-29
7.1.5	References	7.1-29
7.2	Reactor Trip System	7.2-1
7.2.1	System Description.....	7.2-1
7.2.1.1	Reactor Protection System Variables.....	7.2-3
7.2.1.2	Reactor Protection System Logic	7.2-9
7.2.1.3	Initiation Circuits.....	7.2-11
7.2.1.4	Reactor Trip Initiation Signals.....	7.2-12
7.2.1.5	Manual Reactor Trip and Actuated Devices	7.2-21
7.2.1.6	Bypasses	7.2-22
7.2.1.7	Interlocks	7.2-23
7.2.1.8	Redundancy	7.2-25
7.2.1.9	Defense-In-Depth and Diversity.....	7.2-25
7.2.1.10	Vital Instrument Power Supply	7.2-26
7.2.1.11	System Arrangement	7.2-26
7.2.2	Design Basis Information.....	7.2-26
7.2.2.1	Single Failure Criterion	7.2-26
7.2.2.2	Quality of Components and Modules.....	7.2-27
7.2.2.3	Independence.....	7.2-27
7.2.2.4	Defense-in-Depth and Diversity	7.2-28
7.2.2.5	System Testing and Inoperable Surveillance.....	7.2-28
7.2.2.6	Use of Digital Systems	7.2-30
7.2.2.7	Setpoint Determination.....	7.2-30
7.2.2.8	Equipment Qualification	7.2-30
7.2.3	Analysis.....	7.2-31
7.2.3.1	Failure Modes and Effects Analysis	7.2-31
7.2.3.2	Safety Analysis	7.2-32
7.2.3.3	Test and Inspection	7.2-32
7.2.3.4	Restrictive Setpoints.....	7.2-32
7.2.3.5	Conformance to GDC.....	7.2-32
7.2.3.6	Conformance to IEEE Std. 603	7.2-32
7.2.3.7	Conformance to IEEE Std. 7-4.3.2	7.2-32

APR1400 DCD TIER 2

7.2.4	Combined License Information.....	7.2-33
7.2.5	References	7.2-33
7.3	Engineered Safety Features Systems	7.3-1
7.3.1	System Description.....	7.3-1
7.3.1.1	ESFAS Measurement Channels.....	7.3-3
7.3.1.2	ESFAS Bistable and Coincidence Logic	7.3-3
7.3.1.3	Actuation Logic	7.3-4
7.3.1.4	Component Control Logic	7.3-8
7.3.1.5	Bypasses	7.3-16
7.3.1.6	Interlocks	7.3-16
7.3.1.7	Redundancy	7.3-17
7.3.1.8	EDG Loading Sequencer	7.3-17
7.3.1.9	Actuated Systems	7.3-20
7.3.1.10	Vital Instrument Power Supply	7.3-24
7.3.1.11	Component Interface Module and Interface Logic	7.3-24
7.3.2	Design-Basis Information.....	7.3-24
7.3.2.1	Single Failure Criterion	7.3-24
7.3.2.2	Quality of Components and Modules.....	7.3-25
7.3.2.3	Independence.....	7.3-25
7.3.2.4	Defense-in-Depth and Diversity	7.3-26
7.3.2.5	System Testing and Inoperable Surveillance.....	7.3-26
7.3.2.6	Use of Digital Systems	7.3-28
7.3.2.7	Setpoint Determination.....	7.3-28
7.3.2.8	Equipment Qualification	7.3-29
7.3.2.9	System Drawings.....	7.3-29
7.3.3	Analysis	7.3-30
7.3.3.1	Failure Modes and Effects Analysis	7.3-30
7.3.3.2	Conformance to IEEE Std. 603	7.3-30
7.3.3.3	Conformance to IEEE Std. 7-4.3.2.....	7.3-30
7.3.3.4	Analysis for Additional Postulated Failure.....	7.3-30
7.3.3.5	Periodic Testing Method.....	7.3-31
7.3.4	Combined License Information.....	7.3-31

APR1400 DCD TIER 2

7.3.5	References	7.3-31
7.4	Systems Required for Safe Shutdown	7.4-1
7.4.1	Description	7.4-1
7.4.1.1	System Description.....	7.4-2
7.4.2	Design-Basis Information.....	7.4-9
7.4.2.1	Single Failure Criterion	7.4-9
7.4.2.2	Quality of Components and Modules.....	7.4-10
7.4.2.3	Independence.....	7.4-10
7.4.2.4	Periodic Testing	7.4-10
7.4.2.5	Use of Digital Systems	7.4-10
7.4.2.6	System Drawings.....	7.4-10
7.4.3	Analysis	7.4-10
7.4.3.1	Conformance with IEEE Std. 603 and IEEE Std. 7-4.3.2	7.4-10
7.4.3.2	Conformance with General Design Criterion 19	7.4-11
7.4.3.3	Consideration of Selected Plant Contingencies.....	7.4-11
7.4.4	References	7.4-11
7.5	Information Systems Important to Safety	7.5-1
7.5.1	System Description.....	7.5-1
7.5.1.1	Accident Monitoring Instrumentation	7.5-2
7.5.1.2	Inadequate Core Cooling Monitoring Instrumentation	7.5-5
7.5.1.3	Bypassed and Inoperable Status Indication.....	7.5-7
7.5.1.4	Alarm System	7.5-9
7.5.1.5	Safety Parameter Display System	7.5-10
7.5.1.6	Information Systems Associated with the ERF and ERDS	7.5-11
7.5.2	Design Basis Information.....	7.5-11
7.5.2.1	Accident Monitoring Instrumentation	7.5-11
7.5.2.2	Inadequate Core Cooling Monitoring.....	7.5-14
7.5.2.3	Bypassed and Inoperable Status Indication.....	7.5-14
7.5.2.4	Alarm System	7.5-14
7.5.2.5	Safety Parameter Display System	7.5-15

APR1400 DCD TIER 2

7.5.2.6	Information Systems Associated with the ERF and ERDS	7.5-15
7.5.3	Analysis	7.5-15
	Combined License Information	7.5-15
7.5.4	7.5-15	
7.5.5	References	7.5-16
7.6	Interlock Systems Important to Safety	7.6-1
7.6.1	System Description	7.6-1
7.6.1.1	SCS Suction Line Isolation Valve Interlocks	7.6-1
7.6.1.2	SCS Suction Line Relief Valve Interlocks	7.6-2
7.6.1.3	SIT Isolation Valve Interlocks	7.6-3
7.6.1.4	CCW Supply and Return Header Tie Line Isolation Interlocks	7.6-4
7.6.1.5	Interlocks Required to Preclude Inadvertent Inter-ties between Redundant or Diverse Safety Systems	7.6-5
7.6.2	Design Basis Information	7.6-5
7.6.2.1	Applicable Codes and Regulations	7.6-5
7.6.2.2	Conformance to IEEE Std. 603	7.6-10
7.6.2.3	System Testing and Inoperable Surveillance	7.6-14
7.6.2.4	Use of Digital Systems	7.6-14
7.6.3	Analysis	7.6-14
7.6.3.1	Interlocks to Prevent Over-pressurization of Low-Pressure Systems	7.6-14
7.6.3.2	Interlocks to Prevent Over-pressurization of the Reactor Coolant System during Low-Temperature Operations of the Reactor Vessel	7.6-15
7.6.3.3	Interlocks for SIT Isolation Valves	7.6-15
7.6.3.4	Interlocks for Supply and Return Header Isolation Valves	7.6-15
7.6.4	Combined License Information	7.6-15
7.6.5	References	7.6-15
7.7	Control Systems Not Required for Safety	7.7-1
7.7.1	Description	7.7-1

APR1400 DCD TIER 2

7.7.1.1	Control Systems.....	7.7-1
7.7.1.2	MCR Facility	7.7-19
7.7.1.3	LDP.....	7.7-23
7.7.1.4	IPS.....	7.7-24
7.7.1.5	NSSS Integrity Monitoring System.....	7.7-33
7.7.2	Design Basis Information.....	7.7-34
7.7.2.1	Safety Classification	7.7-34
7.7.2.2	Effects of Control System Operation upon Accidents.....	7.7-34
7.7.2.3	Effects of Control System Failures.....	7.7-34
7.7.2.4	Effects of Control System Failures Caused by Accidents	7.7-34
7.7.2.5	Environmental Control System	7.7-35
7.7.2.6	Use of Digital Systems	7.7-35
7.7.2.7	Independence.....	7.7-35
7.7.2.8	Defense-in-Depth and Diversity	7.7-35
7.7.2.9	Potential for Inadvertent Actuation	7.7-36
7.7.2.10	Control of Access	7.7-36
7.7.3	Analysis.....	7.7-37
7.7.4	Combined License Information.....	7.7-37
7.7.5	References	7.7-37
7.8	Diverse Instrumentation and Control Systems	7.8-1
7.8.1	System Description.....	7.8-2
7.8.1.1	Diverse Protection System	7.8-2
7.8.1.2	Diverse Manual ESF Actuation Switch.....	7.8-4
7.8.1.3	Diverse Indication System.....	7.8-4
7.8.2	Design Bases	7.8-5
7.8.2.1	Diverse Protection System	7.8-5
7.8.2.2	Diverse Manual ESF Actuation Switch.....	7.8-8
7.8.2.3	Diverse Indication System.....	7.8-10
7.8.3	Analysis.....	7.8-12
7.8.3.1	General	7.8-12
7.8.3.2	Scope of Evaluation.....	7.8-13

APR1400 DCD TIER 2

7.8.3.3	Evaluation of Design Basis Events.....	7.8-13
7.8.4	Combined License Information.....	7.8-14
7.8.5	References	7.8-14
7.9	Data Communication Systems.....	7.9-1
7.9.1	System Description.....	7.9-1
7.9.1.1	SDN for Safety Systems	7.9-2
7.9.1.2	SDL for Safety Systems	7.9-3
7.9.1.3	DCN-I for Non-safety Systems	7.9-5
7.9.1.4	Data Communication for Safety and Non-Safety Systems.....	7.9-6
7.9.2	Design-Basis Information.....	7.9-9
7.9.2.1	Quality of Components and Modules.....	7.9-9
7.9.2.2	Data Communication Systems Software Quality	7.9-9
7.9.2.3	Performance Requirements	7.9-10
7.9.2.4	Potential Hazards.....	7.9-12
7.9.2.5	Control of Access	7.9-12
7.9.2.6	Single Failure Criterion	7.9-13
7.9.2.7	Independence.....	7.9-13
7.9.2.8	Fail Safe Failure Modes.....	7.9-13
7.9.2.9	System Testing and Surveillances	7.9-13
7.9.2.10	Bypass and Inoperable Status Indications	7.9-14
7.9.2.11	EMI/RFI Susceptibility	7.9-14
7.9.2.12	Defense-In-Depth and Diversity.....	7.9-14
7.9.2.13	Seismic Hazards	7.9-14
7.9.3	Analysis	7.9-14
7.9.4	Combined License Information.....	7.9-15
7.9.5	References	7.9-15

APR1400 DCD TIER 2

LIST OF TABLES

<u>NUMBER</u>	<u>TITLE</u>	<u>PAGE</u>
Table 7.1-1	Regulatory Requirements Applicability Matrix.....	7.1-35
Table 7.2-1	Reactor Protection System Operating Bypass Permissive	7.2-35
Table 7.2-2	Reactor Protection System Monitored Plant Variable Ranges	7.2-36
Table 7.2-3	Reactor Protection System Sensors.....	7.2-37
Table 7.2-4	Reactor Protection System Design Inputs.....	7.2-38
Table 7.2-5	Reactor Protective Instrumentation Response Time	7.2-40
Table 7.2-6	Critical Function Success Path Diversity	7.2-42
Table 7.2-7	Failure Mode and Effects Analysis for the Plant Protection System.....	7.2-43
Table 7.3-1	ESFAS Operating Bypass Permissive.....	7.3-34
Table 7.3-2	Design Basis Events Requiring ESF System Action	7.3-35
Table 7.3-3	Monitored Variables for ESFAS Signals	7.3-36
Table 7.3-4	ESFAS Sensors	7.3-37
Table 7.3-5A	NSSS ESFAS Setpoints and Margins to Actuation	7.3-38
Table 7.3-5B	BOP ESFAS Setpoints and Margin to Actuation.....	7.3-39
Table 7.3-6	ESFAS Variable Ranges	7.3-40
Table 7.3-7	ESF Response Time	7.3-41
Table 7.3-8	Engineered Safety Feature – Component Control System Failure Modes and Effects Analysis	7.3-44
Table 7.4-1	Remote Shutdown Console Instrumentation and Controls for Hot Shutdown.....	7.4-13
Table 7.4-2	Remote Shutdown Controlled Functions for Cold Shutdown.....	7.4-17
Table 7.5-1	Accident Monitoring Instrumentation Variables	7.5-18
Table 7.6-1	Shutdown Cooling System and Safety Injection Tank Interlock	7.6-17
Table 7.6-2	CCW Supply and Return Header Tie Line Isolation Interlocks	7.6-18
Table 7.7-1	Controller Grouping in the NSSS Control System	7.7-39
Table 7.7-2	Control Limit and Interlocks on Digital Rod Control System	7.7-40

APR1400 DCD TIER 2

Table 7.8-1	Diverse Protection System Parameter	7.8-16
Table 7.8-2	Diverse Functions Remain Available After the CCF	7.8-17
Table 7.8-3	Diverse Actuation Signals.....	7.8-18
Table 7.8-4	Display and Control Parameters for the DIS.....	7.8-19

APR1400 DCD TIER 2

LIST OF FIGURES

<u>NUMBER</u>	<u>TITLE</u>	<u>PAGE</u>
Figure 7.1-1	APR1400 I&C System Overview Architecture	7.1-41
Figure 7.1-2	Symbol & Legend Diagram	7.1-42
Figure 7.2-1	PPS Basic Block Diagram	7.2-108
Figure 7.2-2	Typical PPS Measurement Channel Functional Diagram (Pressurizer Pressure Wide Range)	7.2-109
Figure 7.2-3	Reed Switch Position Transmitter Assembly Schematic	7.2-110
Figure 7.2-4	CEA Position Signal Flow for CPCS	7.2-111
Figure 7.2-5	Ex-Core Neutron Monitoring System (Safety Channel)	7.2-112
Figure 7.2-6	Reactor Coolant Pump Shaft Sensing System	7.2-113
Figure 7.2-7	Core Protection Calculator System Functional Block Diagram	7.2-114
Figure 7.2-8	PPS Bistable Trip Logic Functional Block Diagram	7.2-115
Figure 7.2-9	Reactor Trip Switchgear System Interface Diagram	7.2-116
Figure 7.2-10	PPS Channel A Trip Path Diagram	7.2-117
Figure 7.2-11	PPS Testing Overlap	7.2-118
Figure 7.2-12	Interface and Test Processor Block Diagram	7.2-119
Figure 7.2-13	PPS Channel Contact Bistable Interface Diagram	7.2-120
Figure 7.2-14	Plant Protection System Interface Logic Diagram for Channel A	7.2-121
Figure 7.2-15	Reactor Trip Initiation Diagram	7.2-122
Figure 7.2-16	Typical Manual Reactor Trip Initiation Diagram	7.2-123
Figure 7.2-17	Functional Logic Diagram for Variable Overpower	7.2-124
Figure 7.2-18	Functional Logic Diagram for High Logarithmic Power Level	7.2-125
Figure 7.2-19	Functional Logic Diagram for High Local Power Density	7.2-126
Figure 7.2-20	Functional Logic Diagram for Low Departure from Nucleate Boiling Ratio	7.2-127
Figure 7.2-21	Functional Logic Diagram for High Pressurizer Pressure	7.2-128
Figure 7.2-22	Functional Logic Diagram for Low Pressurizer Pressure	7.2-129
Figure 7.2-23	Functional Logic Diagram for Low Steam Generator Water Level	7.2-130

APR1400 DCD TIER 2

Figure 7.2-24	Functional Logic Diagram for Low Steam Generator Pressure	7.2-131
Figure 7.2-25	Functional Logic Diagram for High Containment Pressure	7.2-132
Figure 7.2-26	Functional Logic Diagram for High Steam Generator Water Level	7.2-133
Figure 7.2-27	Functional Logic Diagram for Low Reactor Coolant Flow.....	7.2-134
Figure 7.2-28	Functional Logic Diagram for Reactor Trip Signal Generation.....	7.2-135
Figure 7.2-29	Functional Logic Diagram for DNBR, LPD Operating Bypass Permissive	7.2-136
Figure 7.2-30	Functional Logic Diagram for Low Pressurizer Pressure Operating Bypass Permissive	7.2-137
Figure 7.2-31	Functional Logic Diagram for High Logarithmic Power Level Operating Bypass Permissive	7.2-138
Figure 7.2-32	Functional Logic Diagram for CPC CWP Operating Bypass	7.2-139
Figure 7.3-1A	ESFAS Functional Logic (SIAS).....	7.3-57
Figure 7.3-1B	ESFAS Functional Logic (CSAS, CIAS)	7.3-58
Figure 7.3-1C	ESFAS Functional Logic (AFAS-1, AFAS-2)	7.3-60
Figure 7.3-1D	ESFAS Functional Logic (MSIS).....	7.3-61
Figure 7.3-1E	ESFAS Functional Logic (General Legend).....	7.3-63
Figure 7.3-1F	ESF Functional Logic (FHEVAS).....	7.3-64
Figure 7.3-1G	ESF Functional Logic (CPIAS).....	7.3-65
Figure 7.3-1H	ESF Functional Logic (CREVAS).....	7.3-66
Figure 7.3-2	ESF-CCS Simplified Logic Diagram for Typical 2 out of 4 Actuation.....	7.3-67
Figure 7.3-3A	Simplified Functional Diagram of Engineered Safety Features Component Control System (ESF-CCS)	7.3-68
Figure 7.3-3B	ESF-CCS Block Diagram	7.3-69
Figure 7.3-4	Loading Sequencer - Control Logic Diagram	7.3-70
Figure 7.3-5	ESF-CCS Simplified Test Logic Diagram	7.3-74
Figure 7.3-6	Typical CLD for a Solenoid Operated Valve	7.3-75
Figure 7.3-7	Typical CLD for a Modulating Valve with Solenoid Operator	7.3-76
Figure 7.3-8	Typical Motor Operated Valve Functional Interface Design	7.3-77

APR1400 DCD TIER 2

Figure 7.3-9	Typical CLD for a Full Stroke Motor Operated Valve.....	7.3-78
Figure 7.3-10	Typical CLD for a Throttling Motor Operated Valve	7.3-79
Figure 7.3-11	Typical CLD for a Non-reversing Motor Starter Operated Component	7.3-80
Figure 7.3-12	Typical CLD for a Circuit Breaker Operated Component.....	7.3-81
Figure 7.3-13A	Typical CLD for a Modulating Component	7.3-82
Figure 7.3-13B	Typical CLD for an Electro Hydraulic Motor Damper	7.3-83
Figure 7.4-1	Interface Diagram for Division A Transfer Switches.....	7.4-18
Figure 7.4-2	Interface Diagram for Division AB Transfer Switches	7.4-19
Figure 7.4-3	Channel Transfer Logic	7.4-20
Figure 7.4-4	Layout of Remote Shutdown Room	7.4-21
Figure 7.5-1	Diverse Display of Accident Monitoring Type A, B, and C Variables.....	7.5-23
Figure 7.5-2	QIAS-N Block Diagram	7.5-24
Figure 7.6-1A	Interlocks for Shutdown Cooling System Suction Line Isolation Valve.....	7.6-19
Figure 7.6-1B	Interlocks for Shutdown Cooling System Suction Line Isolation Valve.....	7.6-20
Figure 7.6-1C	Interlocks for Shutdown Cooling System Suction Line Isolation Valve.....	7.6-21
Figure 7.6-2	Interlocks for Safety Injection Tank Isolation Valve	7.6-22
Figure 7.6-3	Interlocks for CCW Supply and Return Header Isolation Valve	7.6-23
Figure 7.7-1	Reactor Regulating System Block Diagram	7.7-41
Figure 7.7-2	Digital Rod Control System - Reactor Protection System Interface Block Diagram.....	7.7-42
Figure 7.7-3	Pressurizer Pressure Control System Block Diagram	7.7-43
Figure 7.7-4	Pressurizer Level Control System Block Diagram.....	7.7-44
Figure 7.7-5	Feedwater Control System Block Diagram	7.7-45
Figure 7.7-6	Steam Bypass Control System Block Diagram	7.7-46
Figure 7.7-7	Simplified Block Diagram Reactor Power Cutback System	7.7-47
Figure 7.7-8	Process-Component Control System Simplified Block Diagram.....	7.7-48
Figure 7.7-9	Core Operation Limit Supervisory System Functional Diagram	7.7-49

APR1400 DCD TIER 2

Figure 7.7-10	Ex-Core Neutron Flux Monitoring System Startup and Control Channel Flow Diagram.....	7.7-50
Figure 7.7-11	N-16 Detection and Alarm Logic	7.7-51
Figure 7.7-12	HSI Information Processing Block Diagram	7.7-52
Figure 7.7-13	Typical Main Control Room Overview	7.7-53
Figure 7.7-14	Layout of Main Control Room	7.7-54
Figure 7.8-1	Diverse Protection System Block Diagram	7.8-21
Figure 7.8-2	Diverse Reactor Trip, Turbine Trip, AFWS, and SIS Actuation.....	7.8-22
Figure 7.8-3	Diverse Reactor Trip and Turbine Trip	7.8-23
Figure 7.8-4	Diverse AFWS Actuation	7.8-24
Figure 7.8-5	Diverse SIS Actuation	7.8-25
Figure 7.9-1	Data Communication Block Diagram	7.9-16

APR1400 DCD TIER 2

ACRONYM AND ABBREVIATION LIST

AAC	alternate alternating current
AC	alternating current
ACU	air cleaning unit
AFAS	auxiliary feedwater actuation signal
AFW	auxiliary feedwater
AFWS	auxiliary feedwater system
AFWST	auxiliary feedwater storage tank
AI	analog input
ALMS	acoustic leak monitoring system
ALWR	Advanced Light Water Reactor
AMI	accident monitoring instrumentation
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	anticipated operational occurrence
APC-S	auxiliary process cabinet-safety
APR	advanced power reactor
ASI	axial shape index
ASIC	application specific integrated circuit
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without scram
AUX	auxiliary
AWP	automatic withdrawal prohibit
BDAS	boron dilution alarm system
BIOB	backplane input output bus
BISI	bypassed and inoperable status indication
BOP	balance of plant
BP	bistable processor
BTP	Branch Technical Position
CBP	computer-based procedure
CCF	common-cause failure
CCG	control channel gateway
CCW	component cooling water
CCWS	component cooling water system
CEA	control element assembly

APR1400 DCD TIER 2

CEAC	control element assembly calculator
CEDM	control element drive mechanism
CET	core exit thermocouple
CFR	Code of Federal Regulations
CFS	cavity flooding system
CI	containment isolation
CIAS	containment isolation actuation signal
CIM	component interface module
CIS	containment isolation system
CIV	containment isolation valve
CLD	control logic diagram
CNMT	containment
COL	combined license
COLSS	core operating limit supervisory system
CPC	core protection calculator
CPCS	core protection calculator system
CPIAS	containment purge isolation actuation signal
CPM	control panel multiplexer
CPP	CEA position processor
CPU	central processing unit
CRC	cyclical redundancy check
CREVAS	control room emergency ventilation actuation signal
CS	1) containment spray, 2) communication section
CSAS	containment spray actuation signal
CSS	containment spray system
CVCS	chemical and volume control system
CWP	CEA withdrawal prohibit
DAS	diverse actuation system
DBE	design basis event
DC	direct current
DCD	design control document
DCN-I	data communication network-information
DCS	distributed control system
DI	digital input
DIS	diverse indication system
DMA	diverse manual ESF actuation

APR1400 DCD TIER 2

DNBR	departure from nucleate boiling ratio
DO	digital output
DPS	diverse protection system
DRCS	digital rod control system
DVI	direct vessel injection
EDESS	emergency diesel engine starting system
EDG	emergency diesel generator
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOF	emergency operation facility
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ERDS	emergency response data system
ERF	emergency response facility
ESCM	ESF-CCS soft control module
ESF	engineered safety features
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety features-component control system
ESW	essential service water
ESWS	essential service water system
FAP	fuel alignment plate
FC	fully closed
FHEVAS	fuel handling area emergency ventilation actuation signal
FIDAS	fixed in-core detector amplification system
FMEA	failure modes and effects analysis
FO	fully open
FOM	fiber optic modem
FPD	flat panel display
FWCS	feedwater control system
GC	group controller
GDC	General Design Criteria
GTG	gas turbine generator
HDSR	historical data storage and retrieval
HFE	human factors engineering
HJTC	heated junction thermocouple
HMS	hydrogen mitigation system

APR1400 DCD TIER 2

HSI	human system interface
HVAC	heating, ventilation, and air conditioning
HVT	holdup volume tank
I&C	instrumentation and control
ICC	inadequate core cooling
ICCM	inadequate core cooling monitoring
ID	identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical And Electronics Engineers
IFPD	information flat panel display
IPS	information processing system
IRWST	in-containment refueling water storage tank
ISA	Instrument Society of America
ISG	Interim Staff Guidance
ITA	important to availability
ITP	interface and test processor
ITS	important to safety
IVMS	internal vibration monitoring system
LBD	licensing basis documentation
LC	loop controller
LCL	local coincidence logic
LCO	limiting conditions for operation
LDP	large display panel
LEL	lower electrical limit
LGS	lower group stop
LOCA	loss of coolant accident
LOOP	loss of offsite power
LPD	local power density
LPMS	loose parts monitoring system
LTOP	low temperature over-pressurization protection
LWR	light water reactor
MCC	motor control center
MCR	main control room
MFIV	main feedwater isolation valve
MG	motor generator
MI	minimum inventory

APR1400 DCD TIER 2

MOV	motor-operated valve
MSADV	main steam atmospheric dump valve
MSIS	main steam isolation signal
MSIV	main steam isolation valve
MSLB	main steam line break
MSS	main steam system
MTP	maintenance and test panel
NA	not applicable
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OM	operator module
OSC	operational support center
P&ID	piping and instrumentation diagram
PA	postulated accident
PC	personal computer
P-CCS	process-component control system
PCS	power control system
PF	penalty factor
PLC	programmable logic controller
PLCS	pressurizer level control system
PM	processor module
POSRV	pilot operated safety relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
PRV	process representative value
PS	processing section
PSCEA	part-strength CEA
PZR	pressurizer
QA	quality assurance
QAPD	quality assurance program description
QIAS	qualified indication and alarm system
QIAS-N	qualified indication and alarm system - non-safety
QIAS-P	qualified indication and alarm system - P
RAM	random access memory

APR1400 DCD TIER 2

RCC	remote control console
RCGV	reactor coolant gas vent
RCGVS	reactor coolant gas vent system
RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
RCPS	reactor power cutback system
RCPVMS	reactor coolant pump vibration monitoring system
RCS	reactor coolant system
RFI	radio frequency interference
RG	Regulatory Guide
RMS	radiation monitoring system
RPCB	reactor power cutback
RPCS	reactor power cutback system
RPS	reactor protection system
RRS	reactor regulating system
RSC	remote shutdown console
RSPT	reed switch position transmitter
RSR	remote shutdown room
RT	reactor trip
RTCB	reactor trip circuit breaker
RTD	resistance temperature detector
RTOTT	reactor trip on turbine trip
RTS	reactor trip system
RTSG	reactor trip switchgear
RTSS	reactor trip switchgear system
RV	reactor vessel
SBCS	steam bypass control system
SC	safety critical
SCP	shutdown cooling pump
SCS	shutdown cooling system
SDL	serial data link
SDN	safety system data network
SDS	safety depressurization system
SDVS	safety depressurization and vent system
SECY	Office of the Secretary of the Commission
SG	steam generator

APR1400 DCD TIER 2

SGTR	steam generator tube rupture
SI	safety injection
SIAS	safety injection actuation signal
SIP	safety injection pump
SIS	safety injection system
SIT	safety injection tank
SMS	seismic monitoring system
SODP	shutdown overview display panel
SOE	sequence of event
SPADES+	safety parameter display and evaluation system+
SPDS	safety parameter display system
SRM	Staff Requirements Memorandum
T _{AVG}	average temperature
TBV	turbine bypass valve
TCB	trip circuit breaker
T _{COLD}	cold leg temperature
TCS	turbine control system
TMI	Three Mile Island
T _{REF}	reference temperature
TSC	technical support center
UEL	upper electrical limit
UGS	upper guide structure
UV	under voltage
V&V	verification and validation
Vac	voltage alternating current
VBPSS	vital bus power supply system
Vdc	voltage direct current
VOPT	variable overpower trip
VSP	variable setpoint
WDT	watchdog timer
WR	wide range

CHAPTER 7 – INSTRUMENTATION AND CONTROLS

7.1 Introduction

The APR1400 instrumentation and control (I&C) system uses advanced design features such as digital data communication, a network-based distributed digital control system, and a compact workstation-based human-system interface (HSI) in the control room.

The I&C architecture of the APR1400 is implemented by two major independent and diverse platforms: (1) safety-qualified programmable logic controller (PLC) platform for safety systems and (2) a non-qualified distributed control system (DCS) platform for the data processing system and non-safety control systems. In addition, self-standing systems such as the turbine/generator (T/G) control and protection system, the nuclear steam supply system (NSSS), and the balance of plant (BOP) monitoring system perform the required functions of a portion of the I&C systems.

Table 3.2-1 provides the safety classifications and quality groups of the APR1400 systems.

Safety Systems

The safety systems are implemented by safety-grade hardware and previously developed software components that are dedicated or qualified for use in nuclear power plants. The PLC platform is loaded with the APR1400-specific application software to implement various nuclear plant safety functions.

The components of the safety system are qualified to satisfy nuclear requirements such as environmental, seismic, electromagnetic interference (EMI), and radio frequency interference (RFI) qualifications. The safety system software is designed, verified, and validated using the industry standard for software development and the verification and validation (V&V) process in accordance with the *[Software Program Manual Technical Report (Reference 1)]**. The qualified PLC platform applies to the following safety systems:

- a. Plant protection system (PPS)
- b. Core protection calculator system (CPCS)
- c. Engineered safety features – component control system (ESF-CCS)

APR1400 DCD TIER 2

- d. ESF-CCS soft control module (ESCM)
- e. Qualified indication and alarm system – P (QIAS-P)

The Safety I&C System Technical Report (Reference 2) describes the functional requirements and design features, and the *[Software Program Manual Technical Report]** describes the software design process of the safety I&C system, particularly the PPS, CPCS, ESF-CCS, and QIAS-P.

The following safety I&C systems are implemented on self-standing platforms that are diverse from the safety-qualified PLC platform: ex-core neutron flux monitoring system (ENFMS), auxiliary process cabinet – safety (APC-S), safety portion of radiation monitoring system (RMS), component interface module (CIM), and emergency diesel sequencer.

Non-Safety Systems

Most of the non-safety I&C systems are implemented by a DCS-based common platform that has been proven in operating experience in the nuclear industry and other industries. The DCS conducts the functions of operator interface, component level control, automatic process control, high-level group control, and data processing for normal operation. The DCS is designed with a redundant and fault-tolerant architecture for high reliability and to prevent the failure of a single component from causing a spurious plant trip.

The following systems are implemented on the DCS platform:

- a. Process-component control system (P-CCS), which includes NSSS process control system (NPCS)
- b. Power control system (PCS)
- c. Information processing system (IPS)

The qualified indication and alarm system – non-safety (QIAS-N) is also implemented on the common PLC platform, even though it is a non-safety system, because it displays the plant's important parameters and maintains diversity from the IPS.

APR1400 DCD TIER 2

Some I&C functions are not installed on a common PLC and DCS platform. These functions are implemented in self-standing systems to fulfill system design requirements. Non-standard systems include the diverse protection system (DPS), diverse indication system (DIS), NSSS integrity monitoring system (NIMS), radiation-monitoring system (RMS), and seismic monitoring system (SMS).

Data Communications

Data communications within and between I&C systems are designed to provide reasonable assurance that any error in data communication does not spuriously actuate a function or prevent the safety functions from being performed. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, and a network between qualified PLC and non-qualified DCS. The qualified PLC data communications network is independent and diverse from the non-qualified DCS data network.

Human-System Interface

The APR1400 HSI is designed based on a compact workstation using the soft control and digital DCS. The compact workstation, which is based on HSI, provides a convenient operating environment to facilitate the display of plant status information to the operator so that operability is enhanced by using advanced display, alarm, and procedure systems. The HSI has sufficient diversity to demonstrate defense-in-depth protection against common-cause failure of the safety system.

7.1.1 Identification of Safety Systems and Non-Safety Systems

Safety and non-safety I&C systems, including supporting systems, are identified in the following subsections.

7.1.1.1 Plant Protection System

The plant protection system (PPS) is a safety system that includes electrical, electronic, network, circuit, and mechanical devices and performs the following protective functions:

APR1400 DCD TIER 2

a. Reactor protection system (RPS)

The RPS is the portion of the PPS that acts to trip the reactor when required. The RPS is described in Subsection 7.1.1.2 and Section 7.2.

b. Engineered safety features actuation system (ESFAS)

The ESFAS is the portion of the PPS that activates the engineered safety features (ESF) systems listed in Subsection 7.1.1.3 and described in Section 7.3.

7.1.1.2 Reactor Trip System

The reactor trip system (RTS) is a safety system that initiates reactor trips. The RTS consists of four channels of sensors, APC-S cabinets, ENFMS cabinets, CPCS cabinets, the RPS portion of the PPS cabinets, and reactor trip switchgear system (RTSS) cabinets. The RTS initiates a reactor trip based on the signals from the sensors that monitor various NSSS parameters and the containment pressure.

When a safety limit is approached, the RPS function in the PPS cabinet initiates a signal that opens the reactor trip breakers. This action removes power from the control element drive mechanism (CEDM) coils, permitting the rods to fall by gravity into the core. The rapid negative reactivity insertion causes the reactor to shutdown.

7.1.1.3 Engineered Safety Features Systems

An ESF system is a safety system that includes the actuation systems of ESF and the components that perform protective actions after receiving a signal from the ESFAS or the operator.

The ESF system consists of the following systems:

- a. Containment isolation system
- b. Main steam isolation system
- c. Safety injection system (SIS)
- d. Auxiliary feedwater system (AFWS)
- e. Containment spray system (CSS)

APR1400 DCD TIER 2

- f. Fuel handling area heating, ventilation, and air conditioning (HVAC) system
- g. Containment purge system
- h. Control room HVAC system
- i. Containment combustible gas control system (manual)
- j. Supporting systems

The ESF system also includes sensors, APC-S cabinets, the ESFAS portion of the PPS, and the ESF-CCS, as described in Section 7.3.

7.1.1.4 Systems Required for Safe Shutdown

The safety systems that are required for a safe shutdown are defined as the systems that are essential for pressure and reactivity control, coolant inventory makeup, and removal of residual heat once the reactor has been brought to a subcritical condition. These safety systems are categorized according to the following shutdown modes:

- a. Hot shutdown

Systems that maintain the primary system at, or near, operating temperature and pressure

- b. Cold shutdown

Systems that cool down and maintain the primary system at, or near, ambient conditions

The safety systems that are required for a safe shutdown are listed below and described in Section 7.4.

- a. Shutdown cooling system (SCS)
- b. Safety injection system (SIS)
- c. Auxiliary feedwater system (AFWS)
- d. Main steam system (MSS) – atmospheric dump

APR1400 DCD TIER 2

- e. Safety depressurization and vent system (SDVS)
- f. Reactor coolant gas vent system (RCGVS)

The auxiliary supporting safety systems that are required for a safe shutdown are as follows:

- a. Class 1E emergency diesel generator system
- b. Emergency diesel generator fuel storage and transfer system
- c. Essential service water system (ESWS)
- d. Component cooling water system (CCWS)
- e. Class 1E power system
- f. Heating, ventilation, and air conditioning (HVAC) systems

In addition, remote shutdown console (RSC) equipment and systems are provided to allow for an emergency shutdown from outside the main control room (MCR).

The safe shutdown systems or portions of systems required to place the reactor into a cold shutdown include the systems listed above and the shutdown cooling system (SCS).

7.1.1.5 Information Systems Important to Safety

Information systems important to safety provide information that is needed to mitigate the consequences of anticipated operating occurrences (AOOs) and postulated accidents (PAs). Information systems important to safety are listed below. Further details are provided in Section 7.5

- a. Accident monitoring instrumentation (AMI)

The AMI provides the operator with information that is used to assess the state of the plant following PAs. AMI variables are displayed in the MCR by the QIAS-P, QIAS-N, and IPS. The design is implemented in accordance with the guidance of Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 1.97 (Reference 3), as depicted in Figure 7.5-1.

APR1400 DCD TIER 2

The QIAS-P processors and display processors are dedicated to continuously monitor and display NRC RG 1.97 Type A, B, and C variables. Class 1E conventional indicators present continuous indications for NRC RG 1.97 Type A variables.

The QIAS-N provides NRC RG 1.97 Type A, B, and C variables. The QIAS-N also displays selected Type D and E variables.

The IPS provides displays for all NRC RG 1.97 variables through signal paths that are isolated from the QIAS-P and QIAS-N.

b. Inadequate core cooling (ICC) monitoring instrumentation

The ICC monitoring instrumentation provides an unambiguous, easy-to-interpret indication of ICC. The design is in accordance with the guidance of II.F.2 of NUREG-0737 (Reference 4). The SPDS displays ICC variables as a primary display. The QIAS-P displays the ICC monitoring signals as a backup.

c. Bypassed and inoperable status indication

The BISI is monitored on the large display panel (LDP) and information flat panel display (FPD). The BISI provides an indication of bypassed or deliberately introduced inoperability of the protection system at the system level, which is required for safe operation of the plant.

d. Alarm system

The alarm system is implemented in both the IPS and QIAS-N. The IPS and QIAS-N are independent and diverse from each other. Therefore, the implemented alarm functions have redundancy and diversity features in the alarm system, as specified in SECY-93-087, Item II.T (Reference 5).

e. Safety parameter display system

SPDS functions are implemented in the safety parameter display and evaluation system+ (SPADES+), which is designed to meet the criteria for SPDS in NUREG-0696 (Reference 6) and NUREG-0737, Supplement 1.

APR1400 DCD TIER 2

- f. Information systems associated with the emergency response facilities (ERF) and emergency response data system (ERDS)

The ERF consists of the technical support center (TSC), operation support center (OSC), emergency operation facility (EOF), SPDS, and ERDS.

The ERDS is a data transmission system designed to send a set of variables from the plant to the NRC operations center in accordance with NUREG-0737, Supplement 1, and NUREG-0696.

7.1.1.6 Interlock Systems Important to Safety

Interlock systems important to safety include the interlocks required to prevent overpressurization of the SCS and to provide reasonable assurance of safety injection availability. The interlock systems important to safety are also required to isolate the non-essential supply and return headers from the essential supply and return headers, and to supply component-cooling water flow between two separate divisions. The interlock systems important to safety are listed below and are described in Section 7.6.

- a. Shutdown cooling system suction line isolation valve interlocks
- b. Shutdown cooling system suction line relief valve interlocks
- c. Safety injection tank (SIT) isolation valve interlocks
- d. Component cooling water (CCW) supply and return header tie line isolation valve interlocks
- e. Interties between redundant or diverse safety system isolation valve interlocks

7.1.1.7 Control Systems Not Required for Safety

Control systems not required for safety include plant information, monitoring, and control systems that are not essential for the safety of the plant. The primary function of the non-safety control system is to maintain variables and the systems within normal operational limits. The non-safety control systems consist of the PCS and the P-CCS.

7.1.1.8 Diverse Instrumentation and Control Systems

The diverse actuation system (DAS) is a non-safety system and is provided to meet the diverse methods required to cope with AOOs concurrent with potential common-cause failure (CCF) of the safety systems. The DAS is also provided to mitigate certain PAs concurrent with a postulated software CCF in the safety system. The basis for the DAS functions is provided in the Diversity and Defense-in-Depth Technical Report (Reference 7).

The DAS consists of the following systems, which are independent and diverse from the safety system:

- a. Diverse protection system (DPS)
- b. Diverse manual ESF actuation (DMA) switches
- c. Diverse indication system (DIS)

Diverse I&C systems are described in Section 7.8.

7.1.1.9 Data Communication Systems

Data communication systems provide high-speed reliable communications between each segment of a channel, between channels, and between systems. The systems consist of hardware, protocols, and interfacing cabling. The systems are designed to provide the accurate, reliable, and timely transfer of data between control, protection, and information systems or within information systems. Input modules in cabinets acquire plant data, and the acquired data are transmitted to control and protection systems. The IPS and QIAS-N acquire information from data communication networks, process the data, and provide information to the display devices and other peripherals. The major components of the data communication systems within the I&C architecture are shown in Figure 7.1-1.

Data communication systems consist of the following three kinds of data communication networks or links with different protocols:

- a. Safety system data network (SDN) for safety systems
- b. Serial data link (SDL) for safety systems
- c. Data communication network – information (DCN-I) for non-safety systems

7.1.1.10 Auxiliary Support Features

Auxiliary supporting features and other auxiliary features are safety systems or components of systems that provide the services that are required for the safety systems to accomplish their safety functions. HVAC and electrical power systems are examples of auxiliary supporting features. The I&C aspects of auxiliary supporting features are described primarily in Chapters 8 and 9. Examples of other auxiliary features are built-in test equipment and isolation devices.

7.1.2 Identification of Safety Criteria

Subsections 7.1.2.2 through 7.1.2.75 and Sections 7.2 through 7.6 contain comparisons of the design with the applicable NRC regulatory guides and a description of the degree of compliance with the appropriate design bases, General Design Criteria (GDC) of Appendix A of 10 CFR 50, standards, and other documents used in the design of the systems listed in Subsection 7.1.1.

7.1.2.1 Design Bases

The design bases for each safety I&C system are presented in the relevant sections of this chapter.

7.1.2.1.1 Systems Required for Plant Protection

The design bases for plant protection systems are described in Sections 7.2 and 7.3.

7.1.2.1.2 Systems Required for Safe Shutdown

The design bases for the systems required for safe shutdown are described in Section 7.4.

7.1.2.1.3 Information Systems Important to Safety

The design bases for information systems important to safety are described in Section 7.5.

7.1.2.1.4 All Other Systems Required for Safety

The design bases for all other systems required for safety are described in Section 7.6.

APR1400 DCD TIER 2

7.1.2.1.5 Interlocks

The interlocks for safety instrumentation are described in Subsection 7.2.1.7, 7.3.1.6, and 7.6.

7.1.2.1.6 Bypasses

The bypasses for safety instrumentation are described in Subsection 7.2.1.6 and 7.3.1.5.

7.1.2.1.7 Diversity

The diversity for safety instrumentation is described in Subsection 7.2.1.9, 7.2.2.4, and 7.3.2.4.

7.1.2.1.8 Instrumentation Protection

The safety instrumentation protection is described in Chapter 3.

7.1.2.2 Conformance with 10 CFR 50.55a(a)(1)

The I&C systems that are applicable to 10 CFR 50.55a(a)(1) (Reference 8), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.55a(a)(1) by complying with IEEE Std. 603 (Reference 9), Clause 5.3.

7.1.2.3 Conformance with 10 CFR 50.55a(h)(2)

The I&C systems that are applicable to 10 CFR 50.55a(h)(2) (Reference 10), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.55a(h)(2) except that the CPCS has two channels of a reed switch position transmitter (RSPT) for each control element assembly. The alternative to Clause 5.6 of IEEE Std. 603 is described in the Safety I&C System Technical Report.

7.1.2.4 Conformance with 10 CFR 50.55a(h)(3)

The I&C systems that are applicable to 10 CFR 50.55a(h)(3) (Reference 11), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.55a(h)(3).

APR1400 DCD TIER 2

7.1.2.5 Conformance with 10 CFR 50.34f(2)(v)

The I&C systems that are applicable to 10 CFR 50.34f(2)(v) (Reference 12), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(v). Display instrumentation provides accurate, complete, and timely information to safety system status by compliance to Clause 5.8.2 (system status indication) and Clause 5.8.3 (indication of bypasses) of IEEE Std. 603. Conformance to IEEE Std. 603 is described in the Safety I&C System Technical Report. Information regarding bypassed and inoperable status is provided in Subsection 7.5.1.3.

7.1.2.6 Conformance with 10 CFR 50.34f(2)(xi)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xi) (Reference 13), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xi), as described in Subsection 7.5.1.1.

The seismically qualified QIAS-N provides pilot-operated safety relief valve (POSRV) position indication.

7.1.2.7 Conformance with 10 CFR 50.34f(2)(xii)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xii) (Reference 14), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xii). The automatic and manual initiation of the auxiliary feedwater system is described in Subsection 7.3.1.9.

7.1.2.8 Conformance with 10 CFR 50.34f(2)(xiv)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xiv) (Reference 15), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xiv). The containment isolation function, including reset of the function, is described in Subsection 7.3.1.9.

7.1.2.9 Conformance with 10 CFR 50.34f(2)(xvii)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xvii) (Reference 16), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xvii), as described in Subsection 7.5.1.

APR1400 DCD TIER 2

7.1.2.10 Conformance with 10 CFR 50.34f(2)(xviii)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xviii) (Reference 17), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xviii), as described in Subsection 7.5.1.1.

7.1.2.11 Conformance with 10 CFR 50.34f(2)(xix)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xix) (Reference 18), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xix).

7.1.2.12 Conformance with 10 CFR 50.34f(2)(xx)

The I&C systems that are applicable to 10 CFR 50.34f(2)(xx) (Reference 19), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.34(f)(2)(xx).

7.1.2.13 Conformance with 10 CFR 50.62

The I&C systems that are applicable to 10 CFR 50.62 (Reference 20), as shown in Table 7.1-1, are designed in accordance with 10 CFR 50.62, which states in part, “Each pressurized water reactor manufactured by Combustion Engineering must have a diverse scram system from the sensor output to interruption of power to the control rods.” The compliance with 10 CFR 50.62 is described in the Diversity and Defense-in-Depth Technical Report.

7.1.2.14 Conformance with GDC 1

The I&C systems that are applicable to GDC 1 (Reference 21), as shown in Table 7.1-1, are designed in accordance with GDC 1 in compliance with IEEE Std. 603, Clause 5.3. The quality assurance program description (QAPD) complies with the requirements of 10 CFR 50, Appendix B (Reference 22).

7.1.2.15 Conformance with GDC 2

The I&C systems that are applicable to GDC 2, as shown in Table 7.1-1, are designed in accordance with GDC 2 in compliance with IEEE Std. 603, Clause 5.4.

APR1400 DCD TIER 2

7.1.2.16 Conformance with GDC 4

The I&C systems that are applicable to GDC 4, as shown in Table 7.1-1, are designed in accordance with GDC 4 in compliance with IEEE Std. 603, Clause 5.4.

7.1.2.17 Conformance with GDC 10

The I&C systems that are applicable to GDC 10, as shown in Table 7.1-1, are designed in accordance with GDC 10.

7.1.2.18 Conformance with GDC 13

The I&C systems that are applicable to GDC 13, as shown in Table 7.1-1, are designed in accordance with GDC 13.

7.1.2.19 Conformance with GDC 15

The I&C systems that are applicable to GDC 15, as shown in Table 7.1-1, are designed in accordance with GDC 15.

7.1.2.20 Conformance with GDC 16

The I&C systems that are applicable to GDC 16, as shown in Table 7.1-1, are designed in accordance with GDC 16.

7.1.2.21 Conformance with GDC 19

The I&C systems that are applicable to GDC 19, as shown in Table 7.1-1, are designed in accordance with GDC 19. The capabilities with regard to the safe operation of the plant from the MCR during normal and accident conditions are described in Section 7.4.

7.1.2.22 Conformance with GDC 20

The I&C systems that are applicable to GDC 20, as shown in Table 7.1-1, are designed in accordance with GDC 20. The protection function is described in Sections 7.2 and 7.3.

APR1400 DCD TIER 2

7.1.2.23 Conformance with GDC 21

The I&C systems that are applicable to GDC 21, as shown in Table 7.1-1, are designed in accordance with GDC 21. The protection system is designed to comply with the requirements of IEEE Std. 603. No credible single failure would result in a loss of the protection function.

7.1.2.24 Conformance with GDC 22

The I&C systems that are applicable to GDC 22, as shown in Table 7.1-1, are designed in accordance with GDC 22. The protection systems comply with the independence requirements of IEEE Std. 603 except for the CEA position inputs described in Subsection 7.1.2.3.

7.1.2.25 Conformance with GDC 23

The I&C systems that are applicable to GDC 23, as shown in Table 7.1-1, are designed in accordance with GDC 23. Failure modes and effects analysis (FMEA) for protection systems is described in Subsections 7.2.3.1 and 7.3.3.1.

7.1.2.26 Conformance with GDC 24

The I&C systems that are applicable to GDC 24, as shown in Table 7.1-1, are designed in accordance with GDC 24. Electrical isolation, physical separation, and communication independence are maintained between redundant safety channels and between the safety system and non-safety system.

7.1.2.27 Conformance with GDC 25

The I&C systems that are applicable to GDC 25, as shown in Table 7.1-1, are designed in accordance with GDC 25.

7.1.2.28 Conformance with GDC 28

The I&C systems that are applicable to GDC 28, as shown in Table 7.1-1, are designed in accordance with GDC 28.

APR1400 DCD TIER 2

7.1.2.29 Conformance with GDC 29

The I&C systems that are applicable to GDC 29, as shown in Table 7.1-1, are designed in accordance with GDC 29.

7.1.2.30 Conformance with GDC 33

The I&C systems that are applicable to GDC 33, as shown in Table 7.1-1, are designed in accordance with GDC 33.

7.1.2.31 Conformance with GDC 34

The I&C systems that are applicable to GDC 34, as shown in Table 7.1-1, are designed in accordance with GDC 34.

7.1.2.32 Conformance with GDC 35

The I&C systems that are applicable to GDC 35, as shown in Table 7.1-1, are designed in accordance with GDC 35.

7.1.2.33 Conformance with GDC 38

The I&C systems that are applicable to GDC 38, as shown in Table 7.1-1, are designed in accordance with GDC 38.

7.1.2.34 Conformance with GDC 41

The I&C systems that are applicable to GDC 41, as shown in Table 7.1-1, are designed in accordance with GDC 41.

7.1.2.35 Conformance with GDC 44

The I&C systems that are applicable to GDC 44, as shown in Table 7.1-1, are designed in accordance with GDC 44.

7.1.2.36 Conformance with SECY 93-087 II.Q

Analyses and design features for diversity and defense-in-depth for the PPS and ESFAS are provided in accordance with SECY-93-087 Item II.Q (Reference 23), as referenced by

APR1400 DCD TIER 2

NUREG-0800 (Reference 24). The analyses and design features address postulated safety system CCFs, and are described in the Diversity and Defense-in-Depth Technical Report.

7.1.2.37 Conformance with SECY 93-087 II.T

The alarm systems are required to meet the redundancy, independence, and safety alarm system requirements in accordance with SECY-93-087, Item II.T. The APR1400 design complies with the requirements as follows:

a. Redundancy

The alarm systems are implemented in the software driven IPS and QIAS-N. The alarm functions in the IPS and QIAS-N are non-safety.

Major equipment of the IPS such as the computational server, alarm server, historical data storage and retrieval (HDSR) server, and data communication are configured to primary and standby processors.

The QIAS-N controllers also provide redundant processing in a hot standby configuration. Multi-channel information displayed by the QIAS-N is independently processed and displayed by the IPS. The QIAS-N receives the processed information via the multi-channel gateway and alarms any discrepancies from its own corresponding multi-channel information calculations.

Therefore, the implemented alarm function complies with the intent of the redundancy requirement. The redundant processor configuration enhances the availability of alarm systems.

b. Independence

The IPS and QIAS-N in which the alarm function is implemented are designed as independent and diverse.

The non-safety IPS and QIAS-N are isolated from each other with qualified isolation devices so the failure of the IPS would not affect the QIAS-N.

c. Safety alarm system requirements

APR1400 DCD TIER 2

This requires the alarms to be safety related when safety functions need to be manually performed with no safety automatic control functions available.

7.1.2.38 Conformance with NRC RG 1.22

The I&C systems that are applicable to NRC RG 1.22 (Reference 25), as shown in Table 7.1-1, conform to the guidance of NRC RG 1.22. Conformance is as follows:

- a. Provisions are made to permit periodic testing of the complete PPS, ESF-CCS, and RTSS with the reactor operating at power or when shutdown. These tests cover the trip action from sensor input to the actuated devices. ESF-actuated devices that could affect operations are tested when the reactor is shut down but not when the reactor is operating.
- b. No provisions are made in the design of the PPS, ESF-CCS, or RTSS at the system level to intentionally bypass an actuation signal that may be required during power operation. All-bypasses are on a channel level to prevent an operator from inadvertently bypassing a trip function. Bypass methods are described in Subsections 7.2.1.6 and 7.3.1.5.
- c. The manual testing for an RPS channel is performed administratively to prevent testing more than one redundant channel simultaneously. When a channel is bypassed for manual testing, the bypass is automatically indicated in the MCR.
- d. When an ESFAS is bypassed for manual testing, the bypass is automatically indicated in the MCR.
- e. Actuated devices that cannot be tested during reactor operation are tested when the reactor is shut down.
- f. The DPS is not a safety system. Therefore, NRC RG 1.22 is not applicable to the DPS design. However, the DPS is designed to provide system testing features as described in Subsection 7.8.2.1.

APR1400 DCD TIER 2

7.1.2.39 Conformance with NRC RG 1.47

The I&C systems that are applicable to NRC RG 1.47 (Reference 26), as shown in Table 7.1-1, comply with the recommendations of NRC RG 1.47. A discussion of application for BISI is described in Subsection 7.5.1.3.

7.1.2.40 Conformance with NRC RG 1.53, as Augmented by IEEE Std. 379

The I&C systems that are applicable to NRC RG 1.53 (Reference 27), as augmented by IEEE Std. 379 (Reference 28) and shown in Table 7.1-1, comply with the requirements of IEEE Std. 379 as endorsed by NRC RG 1.53. A discussion of the application of the single failure criterion is provided in Subsections 7.2.2.1 and 7.3.2.1.

7.1.2.41 Conformance with NRC RG 1.62

Manual initiation of the RPS is described in Subsection 7.2.1.5. Manual initiation of the ESFAS is described in Subsections 7.3.1.3 and 7.3.1.4. Compliance with NRC RG 1.62 (Reference 29) is as follows:

- a. The RPS and ESFAS can be manually actuated.
- b. Manual initiation of a protective action is provided at the system level and causes the same actions to be performed by the protection system as would be performed if the protection system had been initiated by automatic action.
- c. Manual switches are located on the safety console in the MCR. Some ESF functions also have manual actuation at the remote shutdown room (RSR).
- d. The amount of equipment common to the manual and automatic initiation paths is kept to a minimum, usually only the actuation devices. No single credible failure in the manual, automatic, or common portions of the protective system would prevent initiation of a protective action by manual or automatic means.
- e. Manual initiation requires a minimum of equipment consistent with the needs of Items a, b, c, and d above.
- f. Once initiated, a manual protective action goes to completion.

APR1400 DCD TIER 2

7.1.2.42 Conformance with NRC RG 1.75, as Augmented by IEEE Std. 384

The instrumentation for the safety electric systems complies with the requirements of IEEE Std. 384 (Reference 30) as endorsed by NRC RG 1.75 (Reference 31) with the exception of the CEA position inputs described in Subsection 7.1.2.3. The physical independence is described in this subsection and includes compliance with Clause 5.6 of IEEE Std. 603, GDC 3, and GDC 21.

The PPS is connected to Class 1E buses, which are divided into four assemblies that are physically located in different geographic fire zones. Each assembly contains one of the four redundant channels of the RPS and ESFAS, which provides the separation and independence necessary to meet the requirements of Clause 5.6 of IEEE Std. 603.

The independence and separation of redundant Class 1E circuits within and between the PPS assemblies or ESF-CCS assemblies is accomplished primarily using fiber-optic technology. The optical technology provides reasonable assurance that no single credible electrical fault in a PPS channel prevents the circuitry in any other redundant channel from performing its safety function.

The ESF-CCS cabinets provide separation and independence for the 2-out-of-4 actuation and component control logic of the channels in the redundant ESF systems. The component control logic for each channel is contained in a separate cabinet. The redundant cabinets are physically separated from each other by locating them in separate zones. Redundant channel remote input/output (I/O) controller is located to maintain physical separation.

The RTSS consists of two sets of four reactor trip switchgears (RTSGs). Each RTSG and associated switches, contacts, and relays is contained in a separate cabinet. Each cabinet is physically separate from the other cabinets. This method of construction provides reasonable assurance that a single credible failure in one RTSG cannot cause malfunction or failure in another cabinet.

The separation and independence of the power supplies is described further in Subsection 8.3.1.

The analog and digital signals sent from the protection system to non-Class 1E systems (e.g., IPS, QIAS-N) for status monitoring, alarm, and display are isolated from the protection system. Fiber-optic isolation and other techniques are used to provide

APR1400 DCD TIER 2

reasonable assurance that no credible failures on the non-Class 1E side of the isolation device will affect the PPS side and that independence of the PPS is not jeopardized.

7.1.2.43 Conformance with NRC RG 1.97

The design of the accident monitoring instrumentation and information display via the QIAS-P, QIAS-N, and IPS is described in Subsections 7.5.1.1. The design complies with NRC RG 1.97.

NRC RG 1.97 endorses IEEE Std. 497 (Reference 32). IEEE Std. 497, Clause 9, states in part, “Microprocessor based instrumentation development including software verification and validation shall be in accordance with the requirements of IEEE Std. 7-4.3.2.” NRC RG 1.152, Rev. 3 (Reference 34), endorses IEEE Std. 7-4.3.2 (Reference 33).

Clause 5.3 of IEEE Std. 7-4.3.2 requires verification and validation (V&V) of software in accordance with IEEE Std. 1012 (Reference 35), which requires software integrity level 4 V&V. The design criteria specified in IEEE Std. 497 are the same for Type A, B, and C variables. The design criteria consider Type A, B, and C variables to be equivalent to safety system variables. Therefore, the design criteria meet the guidance of IEEE Std. 7-4.3.2, and the software for Type A, B, and C variables are qualified as a safety critical software class.

The QIAS-P processes Type A, B, and C variables. The software for the QIAS-P is classified as important to safety (ITS) software. ITS software is defined as “software whose function is necessary to perform DPS control actions, or software that is relied on to monitor or test protection functions, or software that monitors plant critical safety function.” The ITS software meets the software integrity level 3 V&V requirements of IEEE Std. 1012. The design, verification, and validation for safety critical and ITS software are described in the *[Software Program Manual Technical Report]**.

7.1.2.44 Conformance with NRC RG 1.105

The setpoint methodology follows the methodology in ISA-S67.04 (Reference 36) as endorsed by NRC RG 1.105 (Reference 37).

The environment considered when determining errors is the most detrimental realistic environment calculated or postulated to exist until the worst-case time of the required reactor trip or engineered safety features actuation. This environment may be different for

APR1400 DCD TIER 2

different events analyzed. For the setpoint calculation, the accident environment error calculation for process equipment uses the environmental conditions up to the longest required time of trip or actuation that results in the largest errors, thus providing additional conservatism to the resulting setpoints.

7.1.2.45 Conformance with NRC RG 1.118, as Augmented by IEEE Std. 338

The I&C systems that are applicable to NRC RG 1.118 (Reference 38), as augmented by IEEE Std. 338 (Reference 39) and shown in Table 7.1-1, are designed so that they can be tested periodically in accordance with the criteria of IEEE Std. 338 as endorsed by NRC RG 1.118. The response time of individual instrumentation and control components is obtained from the performance verification tests and is provided to the site operator. It is the site operator's responsibility to test the integrated response time of each protection system after installation. Testing criteria are specified in Subsections 7.2.2.5 and 7.3.2.5. Minimum testing frequency requirements are provided in the Technical Specifications (Chapter 16).

Complete channels in the ESFAS can be tested individually without initiating protective action and without inhibiting the operation of the system.

The system can be checked from the sensor signal to the actuated equipment or devices. The sensors can be checked by comparison with redundant signals from other channels.

The actuated equipment or devices that are not tested during reactor operation are tested during the scheduled reactor shutdown to demonstrate that they are capable of performing the necessary functions.

7.1.2.46 Conformance with NRC RG 1.151

Instrument sensing lines comply with NRC RG 1.151 (Reference 40). Compliance with NRC RG 1.151 is described in Section 1.9.

7.1.2.47 Conformance with NRC RG 1.152

NRC RG 1.152 states that the requirements set forth in IEEE Std. 7-4.3.2 provide methods for designing, verifying, and implementing software and for validating computer systems in safety systems in nuclear power plants.

APR1400 DCD TIER 2

The software development plan is described in the *[Software Program Manual Technical Report]**.

Clause 5.3.3 of IEEE Std. 7-4.3.2 requires V&V of software in accordance with IEEE Std. 1012, which requires software integrity level 4 V&V. The safety I&C system meets the requirements of IEEE Std. 7-4.3.2, and the software for these systems are qualified as safety critical software class as defined in the Software Program Manual Technical Report.

- a. The CPCS described in Subsection 7.2.1.1 is a digital computer system that generates reactor trip signals for low departure from nucleate boiling ratio (DNBR) and high local power density (LPD). The core protection calculator(CPC) software is developed and tested in accordance with NRC RG 1.152.
- b. The PPS described in Section 7.2 is a digital system that generates RPS and ESF initiation signals. The PPS software is developed and tested in accordance with NRC RG 1.152.
- c. The ESF-CCS described in Section 7.3 is a digital system that controls and actuates ESF fluid system components. The ESF-CCS software is developed and tested in accordance with NRC RG 1.152.

Some of the safety I&C system software such as the QIAS-P in Subsection 7.5.1.1 is classified as ITS software class. ITS software is defined as “software whose function is necessary to perform DPS control actions, or software that is relied on to monitor or test protection functions, or software that monitors plant critical safety functions” in the *[Software Program Manual Technical Report]**. ITS software meets the software integrity level 3 V&V requirements of IEEE Std. 1012. The description of safety critical and ITS software design, verification, and validation for is provided in the *[Software Program Manual Technical Report]**.

7.1.2.48 Conformance with NRC RG 1.168

The I&C systems that are applicable to NRC RG 1.168 (Reference 41), as shown in Table 7.1-1, comply with IEEE Std. 1028 (Reference 42) and IEEE Std. 1012 as endorsed by NRC RG 1.168. The activities associated with compliance are described in the *[Software Program Manual Technical Report]**.

APR1400 DCD TIER 2

7.1.2.49 Conformance with NRC RG 1.169

The I&C systems that are applicable to NRC RG 1.169 (Reference 43), as shown in Table 7.1-1, comply with NRC RG 1.169, which endorses IEEE Std. 1042 (Reference 44). The activities associated with compliance to NRC RG 1.169 are described in the *[Software Program Manual Technical Report]**.

7.1.2.50 Conformance with NRC RG 1.170

The I&C systems that are applicable to NRC RG 1.170 (Reference 45), as shown in Table 7.1-1, comply with IEEE Std. 829 (Reference 46), as endorsed by NRC RG 1.170. The activities associated with compliance are described in the *[Software Program Manual Technical Report]**.

7.1.2.51 Conformance with NRC RG 1.171

The I&C systems that are applicable to NRC RG 1.171 (Reference 47), as shown in Table 7.1-1, comply with IEEE Std. 1008 (Reference 48), as endorsed by NRC RG 1.171. The activities associated with compliance are described in the *[Software Program Manual Technical Report]**.

7.1.2.52 Conformance with NRC RG 1.172

The I&C systems that are applicable to NRC RG 1.172 (Reference 49), as shown in Table 7.1-1, comply with IEEE Std. 830 (Reference 50), which is endorsed by NRC RG 1.172. The activities associated with compliance to NRC RG 1.172 are described in the *[Software Program Manual Technical Report]**.

7.1.2.53 Conformance with NRC RG 1.173

The I&C systems that are applicable to NRC RG 1.173 (Reference 51), as shown in Table 7.1-1, comply with IEEE Std. 1074 (Reference 52), as endorsed by NRC RG 1.173. The activities associated with compliance are described in the *[Software Program Manual Technical Report]**.

APR1400 DCD TIER 2

7.1.2.54 Conformance with NRC RG 1.180

The I&C systems that are applicable to NRC RG 1.180 (Reference 53), as shown in Table 7.1-1, are designed, tested, qualified, and installed to comply with the requirements and guidance specified in NRC RG 1.180 and EPRI TR-102323 (Reference 54), which is endorsed by the NRC. The equipment qualification plan is described in Section 6 of the Safety I&C System Technical Report.

7.1.2.55 Conformance with NRC RG 1.189

The I&C systems that are applicable to NRC RG 1.189 (Reference 55), as shown in Table 7.1-1, are designed in accordance with NRC RG 1.189. The details of compliance with NRC RG 1.189 are provided in Chapter 9.

7.1.2.56 Conformance with NRC RG 1.204

The I&C systems that are applicable to NRC RG 1.204 (Reference 56), as shown in Table 7.1-1, are designed in accordance with NRC RG 1.204. Details of compliance with NRC RG 1.204 are provided in Chapter 8.

7.1.2.57 Conformance with NRC RG 1.206

The APR1400 DCD including referenced technical reports is prepared in accordance with the guidance of NRC RG 1.206 (Reference 57) together with NUREG-0800 in order for NRC to evaluate and confirm the safety evaluation.

7.1.2.58 Conformance with BTP 7-1

The I&C systems that are applicable to BTP 7-1 (Reference 58), as shown in Table 7.1-1, are designed in accordance with BTP 7-1.

7.1.2.59 Conformance with BTP 7-2

The I&C systems that are applicable to BTP 7-2 (Reference 59), as shown in Table 7.1-1, are designed in accordance with BTP 7-2.

APR1400 DCD TIER 2

7.1.2.60 Conformance with BTP 7-3

The reactor is not permitted to operate with reactor coolant pump out of service. The PPS trips the reactor by low reactor coolant flow. Therefore, BTP 7-3 (Reference 60) is not applicable.

7.1.2.61 Conformance with BTP 7-4

The I&C systems that are applicable to BTP 7-4 (Reference 61), as shown in Table 7.1-1, are designed in accordance with BTP 7-4.

7.1.2.62 Conformance with BTP 7-5

The I&C systems that are applicable to BTP 7-5 (Reference 62), as shown in Table 7.1-1, are designed in accordance with BTP 7-5.

7.1.2.63 Conformance with BTP 7-6

The APR1400 does not have a recirculation mode. Therefore, BTP 7-6 (Reference 63) is not applicable.

7.1.2.64 Conformance with BTP 7-8

The I&C systems that are applicable to BTP 7-8 (Reference 64), as shown in Table 7.1-1, are designed in accordance with BTP 7-8.

7.1.2.65 Conformance with BTP 7-9

The I&C systems that are applicable to BTP 7-9 (Reference 65), as shown in Table 7.1-1, are designed in accordance with BTP 7-9.

7.1.2.66 Conformance with BTP 7-10

The I&C systems that are applicable to BTP 7-10 (Reference 66), as shown in Table 7.1-1, are designed in accordance with BTP 7-10, as described in Subsection 7.1.2.43.

APR1400 DCD TIER 2

7.1.2.67 Conformance with BTP 7-11

The I&C systems that are applicable to BTP 7-11 (Reference 67), as shown in Table 7.1-1, are designed in accordance with BTP 7-11.

7.1.2.68 Conformance with BTP 7-12

The I&C systems that are applicable to BTP 7-12 (Reference 68), as shown in Table 7.1-1, are designed in accordance with BTP 7-12.

7.1.2.69 Conformance with BTP 7-13

The I&C systems that are applicable to BTP 7-13 (Reference 69), as shown in Table 7.1-1, are designed in accordance with BTP 7-13.

7.1.2.70 Conformance with BTP 7-14

The I&C systems that are applicable to BTP 7-14 (Reference 70), as shown in Table 7.1-1, are designed in accordance with BTP 7-14.

7.1.2.71 Conformance with BTP 7-17

The I&C systems that are applicable to BTP 7-17 (Reference 71), as shown in Table 7.1-1, are designed in accordance with BTP 7-17. Test provisions for RPS and ESFAS are described in Subsections 7.2.2.5 and 7.3.2.5.

BTP 7-17 states, “The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system. The design should maintain channel independence, maintain system integrity, and meet single-failure criterion during testing.” The maintenance and test panel (MTP) and interface and test processor (ITP) are used to perform the periodic testing of the safety system. Hence, the MTP, ITP, and associated communication path software should be qualified in accordance with IEEE Std. 7-4.3.2, as endorsed by NRC RG 1.152, and be classified as safety critical software class.

The justification for this deviation is described in Subsection 7.1.2.47.

APR1400 DCD TIER 2

7.1.2.72 Conformance with BTP 7-18

The I&C systems that are applicable to BTP 7-18 (Reference 72), as shown in Table 7.1-1, are designed in accordance with of BTP 7-18. The safety I&C systems are based on a common platform that is manufactured in accordance with 10 CFR 50, Appendix B. The hardware is qualified to satisfy the nuclear requirements such as environmental, seismic, and EMI/RFI qualifications. The software is designed, verified, and validated with codes and industry standards for software development and V&V processes in accordance with the *[Software Program Manual Technical Report]**.

7.1.2.73 Conformance with BTP 7-19

The I&C systems that are applicable to BTP 7-19 (Reference 73), as shown in Table 7.1-1, are designed in accordance with BTP-19. Compliance to this standard is addressed in the Diversity and Defense-in-Depth Technical Report.

7.1.2.74 Conformance with BTP 7-21

The I&C systems that are applicable to BTP 7-21 (Reference 74), as shown in Table 7.1-1, are designed in accordance with BTP 7-21. Real-time performance is determined by performing response time analysis for all safety functions. An analysis for each function is performed to demonstrate that the actual system response time is less than the response time requirements. *[The response time requirements are described in the Setpoint Methodology for Plant Protection System Technical Report (Reference 75).]**

7.1.2.75 Conformance with DI&C-ISG-04

The compliance of the safety I&C systems with DI&C-ISG-04 (Reference 76) is addressed in Appendix C of the Safety I&C System Technical Report.

7.1.3 Digital Instrumentation and Control Systems Software Design Process

The processes for developing and implementing software comply with the regulatory requirements and industry standards governing those activities. The software quality assurance program is implemented in accordance with 10 CFR 50, Appendix B. Compliance with safety criteria for software is described in the *[Software Program Manual Technical Report]**.

APR1400 DCD TIER 2

[The software design throughout the software life cycle is implemented in accordance with various software development plan documents described in the Software Program Manual Technical Report. After the planning phase, the subsequent software development process is carried out throughout the general software life cycle as follows:

- a. Concept (planning) phase*
- b. Requirements phase*
- c. Design phase*
- d. Implementation phase*
- e. Testing phase*
- f. Installation and checkout phase*
- g. Operation and maintenance phase*

Software is classified based on the Software Program Manual Technical Report, which includes selecting the adequate implementation method for the target system functionality. The software that is used in the APR1400 is classified as one of the following:

- a. Protection (safety critical)*
- b. Important to safety*
- c. Important to availability*
- d. General purpose]**

7.1.4 Combined License Information

No COL information is required with regard to Section 7.1.

7.1.5 References

1. *[APR1400-Z-J-NR-13003-P, “Software Program Manual Technical Report,” September 2013.]**

APR1400 DCD TIER 2

2. APR1400-Z-J-EC-13001-P, "Safety I&C System Technical Report," September 2013.
3. NRC RG 1.97, Rev. 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," 2006.
4. NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements," 1982.
5. SECY 93-087 II.T, "Control Room Annunciator (Alarm) Reliability."
6. NUREG-0696, "Functional Criteria for Emergency Response Facilities," 1981.
7. APR1400-Z-J-EC-13002-P, "Diversity and Defense-in-Depth Technical Report," September 2013.
8. 10 CFR 50.55a(a)(1), "Domestic Licensing of Production and Utilization Facilities, Codes and Standards, Quality Standards for Systems Important to Safety."
9. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
10. 10 CFR 50.55a(h)(2), "Codes and Standards, Protection Systems."
11. 10 CFR 50.55a(h)(3), "Codes and Standards, Safety Systems."
12. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3]
13. 10 CFR 50.34(f)(2)(xi), "Direct Indication of Relief and Safety Valve Position," [II.D.3].
14. 10 CFR 50.34(f)(2)(xii), "Auxiliary Feedwater System Automatic Initiation and Flow Indication," [II.E.1.2].
15. 10 CFR 50.34(f)(2)(xiv), "Containment Isolation Systems," [II.E.4.2].
16. 10 CFR 50.34(f)(2)(xvii), "Accident Monitoring Instrumentation," [II.F.1].
17. 10 CFR 50.34(f)(2)(xviii), "Instrumentation for Detection of Inadequate Core Cooling," [II.F.2].

APR1400 DCD TIER 2

18. 10 CFR 50.34(f)(2)(xix), “Instruments for Monitoring Plant Conditions Following Core Damage,” [II.F.3].
19. 10 CFR 50.34(f)(2)(xx), “Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves,” [II.G.1].
20. 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water Cooled Nuclear Power Plants.”
21. 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”
22. 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants.”
23. SECY 93-087 II.Q, “Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems.”
24. NUREG-0800, “Standard Review Plan,” March 2007.
25. NRC RG 1.22, “Periodic Testing of Protection System Actuation Functions,” 1972.
26. NRC RG 1.47, Rev. 1, “Bypassed and Inoperable Status indication for Nuclear Power Plant Safety Systems,” 2010.
27. NRC RG 1.53, Rev. 2, “Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems,” 2003.
28. IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”
29. NRC RG 1.62, Rev. 1, “Manual Initiation of Protective Actions,” 2010.
30. IEEE Std. 384-1992, “IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.”
31. NRC RG 1.75, Rev. 3, “Criteria for Independence of Electrical Safety Systems,” 2005.
32. IEEE Std. 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.”

APR1400 DCD TIER 2

33. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
34. NRC RG 1.152, Rev. 3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," 2011.
35. IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation Plans."
36. ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related instrumentation.
37. NRC RG 1.105, Rev. 3, "Setpoints for Safety-Related Instrumentation," 1999.
38. NRC RG 1.118, Rev. 3, "Periodic Testing of Electrical Power and Protection Systems," 1995.
39. IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems."
40. NRC RG 1.151, Rev. 1, "Instrument Sensing Lines," 2010.
41. NRC RG 1.168, Rev. 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 2004.
42. IEEE Std. 1028-1997, "IEEE Standard for Software Reviews and Audits."
43. NRC RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.
44. IEEE Std. 1042-1987, "IEEE Guide to Software Configuration Management."
45. NRC RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety systems of Nuclear Power Plants," 1997.
46. IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation."
47. NRC RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.
48. IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing."

APR1400 DCD TIER 2

49. NRC RG 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.
50. IEEE Std. 830-1993, "IEEE Recommended Practice for Software Requirements Specifications."
51. NRC RG 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1997.
52. IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes."
53. NRC RG 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," 2003.
54. EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants," 1997.
55. NRC RG 1.189, Rev. 2, "Fire Protection for Nuclear Power Plants," 2009.
56. NRC RG 1.204, "Guidelines for Lightning Protection of Nuclear Power Plants," 2005.
57. NRC RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," 2007.
58. BTP 7-1, Rev.5, "Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System," March 2007.
59. BTP 7-2, Rev. 5 "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines," March 2007.
60. BTP 7-3, Rev. 5 "Guidance on Protection System Trip Point Changes for the Operation With Reactor Coolant Pumps Out of Service," March 2007.
61. BTP 7-4, Rev. 5 "Guidance on Design Criteria for Auxiliary Feedwater Systems," March 2007.
62. BTP 7-5, Rev. 5 "Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors," March 2007.

APR1400 DCD TIER 2

63. BTP 7-6, Rev. 5 “Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode,” March 2007.
64. BTP 7-8, Rev. 5 “Guidance for Application of NRC RG 1.22,” March 2007.
65. BTP 7-9, Rev. 5 “Guidance on Requirements for Reactor Protection System Anticipatory Trips,” March 2007.
66. BTP 7-10, Rev. 5 “Guidance on Application of NRC RG 1.97,” March 2007.
67. BTP 7-11, Rev. 5 “Guidance on Application and Qualification of Isolation Devices,” March 2007.
68. BTP 7-12, Rev. 5 “Guidance on Establishing and Maintaining Instrument Setpoints,” March 2007.
69. BTP 7-13, Rev. 5 “Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors,” March 2007.
70. BTP 7-14, Rev. 5 “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” March 2007.
71. BTP 7-17, Rev. 5 “Guidance on Self-Test and Surveillance Test Provisions,” March 2007.
72. BTP 7-18, Rev. 5 “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems,” March 2007.
73. BTP 7-19, Rev. 6 “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” July 2012.
74. BTP 7-21, Rev. 5 “Guidance on Digital Computer Real-Time Performance,” March 2007.
75. [APR1400-Z-J-NR-13005-P, “Setpoint Methodology for Plant Protection System Technical Report,” April 2013.]*
76. DI&C-ISG-04, Rev. 1, “Highly Integrated Control Rooms – Communications Issues (HICRc),” 2009.

Table 7.1-1 (1 of 6)

Regulatory Requirements Applicability Matrix

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
10 CFR 50										
1	50.55a(a)(1)	Quality Standards and Records for Systems Important to Safety	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
2	50.55a(h)(2)	Protection Systems	×	×						7.2, 7.3, 7.9
3	50.55a(h)(3)	Safety Systems	×	×	×					7.2, 7.3, 7.5, 7.6, 7.9
4	50.34(f)(2)(v)	Bypass and Inoperable Status Indication	×	×	×	×				7.2, 7.3, 7.5, 7.6, 7.9
5	50.34(f)(2)(xi)	Direct Indication of Relief and Safety Valve Position			×					7.5
6	50.34(f)(2)(xii)	Auxiliary Feedwater System Automatic Initiation and Flow Indication	×	×	×					7.2, 7.3, 7.5
7	50.34(f)(2)(xiv)	Containment Isolation Systems	×	×	×					7.2, 7.3, 7.5
8	50.34(f)(2)(xvii)	Accident Monitoring Instrumentation			×	×				7.5
9	50.34(f)(2)(xviii)	Instrumentation for the Detection of Inadequate Core Cooling			×					7.5
10	50.34(f)(2)(xix)	Instruments for Monitoring Plant Conditions Following Core Damage			×					7.5
11	50.34(f)(2)(xx)	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves			×					7.4, 7.5
12	50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram							×	7.8
10 CFR 50, Appendix A GDC										
13	GDC 1	Quality Standards and Records	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
14	GDC 2	Design Bases for Protection against Natural Phenomena	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9

7.1-35

APR1400 DCD TIER 2

Table 7.1-1 (2 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
15	GDC 4	Environmental and Dynamic Effects of Design Bases	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
16	GDC 10	Reactor Design	×	×			×	×		7.2, 7.3, 7.6, 7.7
17	GDC 13	Instrumentation and Control	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
18	GDC 15	Reactor Coolant System Design	×	×			×	×		7.2, 7.3, 7.6, 7.7
19	GDC 16	Containment Design		×						7.3, 7.6
20	GDC 19	Control Room	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
21	GDC 20	Protection System Functions	×	×						7.2, 7.3
22	GDC 21	Protection System Reliability and Testability	×	×						7.2, 7.3, 7.9
23	GDC 22	Protection System Independence	×	×						7.2, 7.3, 7.9
24	GDC 23	Protection System Failure Modes	×	×						7.2, 7.3, 7.9
25	GDC 24	Separation of Protection and Control Systems	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
26	GDC 25	Protection System Requirements for Reactivity Control Malfunctions	×							7.2, 7.6
27	GDC 28	Reactivity Limits					×			7.6, 7.7
28	GDC 29	Protection against Anticipated Operational Occurrences	×	×			×	×		7.2, 7.3, 7.7, 7.9
29	GDC 33	Reactor Coolant Makeup	×	×						7.2, 7.3, 7.6
30	GDC 34	Residual Heat Removal	×	×						7.2, 7.3, 7.4, 7.6
31	GDC 35	Emergency Core Cooling	×	×						7.2, 7.3, 7.4, 7.6
32	GDC 38	Containment Heat Removal	×	×						7.2, 7.3, 7.4, 7.6
33	GDC 41	Containment Atmosphere Cleanup	×	×						7.2, 7.3, 7.6
34	GDC 44	Cooling Water		×						7.3, 7.6

APR1400 DCD TIER 2

7.1-36

Table 7.1-1 (3 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
Staff Requirements Memoranda										
35	SECY 93-087 II.Q	Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems	×	×					×	7.2, 7.3, 7.8, 7.9
36	SECY 93-087 II.T	Control Room Annunciator (Alarm) Reliability				×				7.5, 7.9
NRC Regulatory Guides										
37	NRC RG 1.22	Periodic Testing of Protection System Actuation Functions	×	×						7.2, 7.3,, 7.9
38	NRC RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems	×	×		×				7.2, 7.3, 7.5, 7.6, 7.9
39	NRC RG 1.53	Application of the Single-Failure Criterion to Safety Systems	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6, 7.9
40	NRC RG 1.62	Manual Initiation of Protective Actions	×	×					×	7.2, 7.3, 7.8
41	NRC RG 1.75	Criteria for Independence of Electrical Safety Systems	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
42	NRC RG 1.97	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants			×	×				7.5
43	NRC RG 1.105	Setpoints for Safety-Related Instrumentation	×	×	×	×				7.2, 7.3, 7.4, 7.5, 7.6, 7.9
44	NRC RG 1.118	Periodic Testing of Electric Power and Protection Systems	×	×	×	×				7.2, 7.3, 7.4, 7.5, 7.6, 7.9
45	NRC RG 1.151	Instrument Sensing Lines	×	×	×					7.2, 7.3, 7.5,
46	NRC RG 1.152	Criteria for Digital Computers in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9

7.1-37

APR1400 DCD TIER 2

Table 7.1-1 (4 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
47	NRC RG 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
48	NRC RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
49	NRC RG 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
50	NRC RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
51	NRC RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
52	NRC RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9
53	NRC RG 1.180	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6, 7.9
54	NRC RG 1.189	Fire Protection for Nuclear Power Plants								Refer to Chapter 9 (Subsection 9.5.1)
55	NRC RG 1.200	An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities								See BTP 7-12 for applicability
56	NRC RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants								Refer to Chapter 8 (Subsection 8.3.1.1.8)

Table 7.1-1 (5 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
57	NRC RG 1.206	Combined License Applications for Nuclear Power Plants (LWR Edition)	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
Branch Technical Positions										
58	BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System		×						7.6
59	BTP 7-2	Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines		×						7.6
60	BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service								Not Applicable
61	BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems		×						7.3
62	BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	×				×			7.2, 7.7
63	BTP 7-6	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode								Not Applicable
64	BTP 7-8	Guidance for Application of NRC RG 1.22	×	×						7.2, 7.3, 7.9
65	BTP 7-9	Guidance on Requirements for Reactor Protection System Anticipatory Trips	×							7.2
66	BTP 7-10	Guidance on Application of NRC RG 1.97			×	×				7.5
67	BTP 7-11	Guidance on Application and Qualification of Isolation Devices	×	×	×					7.2, 7.3, 7.5, 7.9
68	BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6,

7.1-39

APR1400 DCD TIER 2

Table 7.1-1 (6 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			PPS	ESF-CCS	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
69	BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	×	×	×					7.2, 7.3, 7.4, 7.5
70	BTP 7-14	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6, 7.9
71	BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6, 7.9
72	BTP 7-18	Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems	×	×	×	×				7.2, 7.3, 7.5, 7.9
73	BTP 7-19	Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
74	BTP 7-21	Guidance on Digital Computer Real-Time Performance	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 7.9

7.1-40

APR1400 DCD TIER 2

APR1400 DCD TIER 2

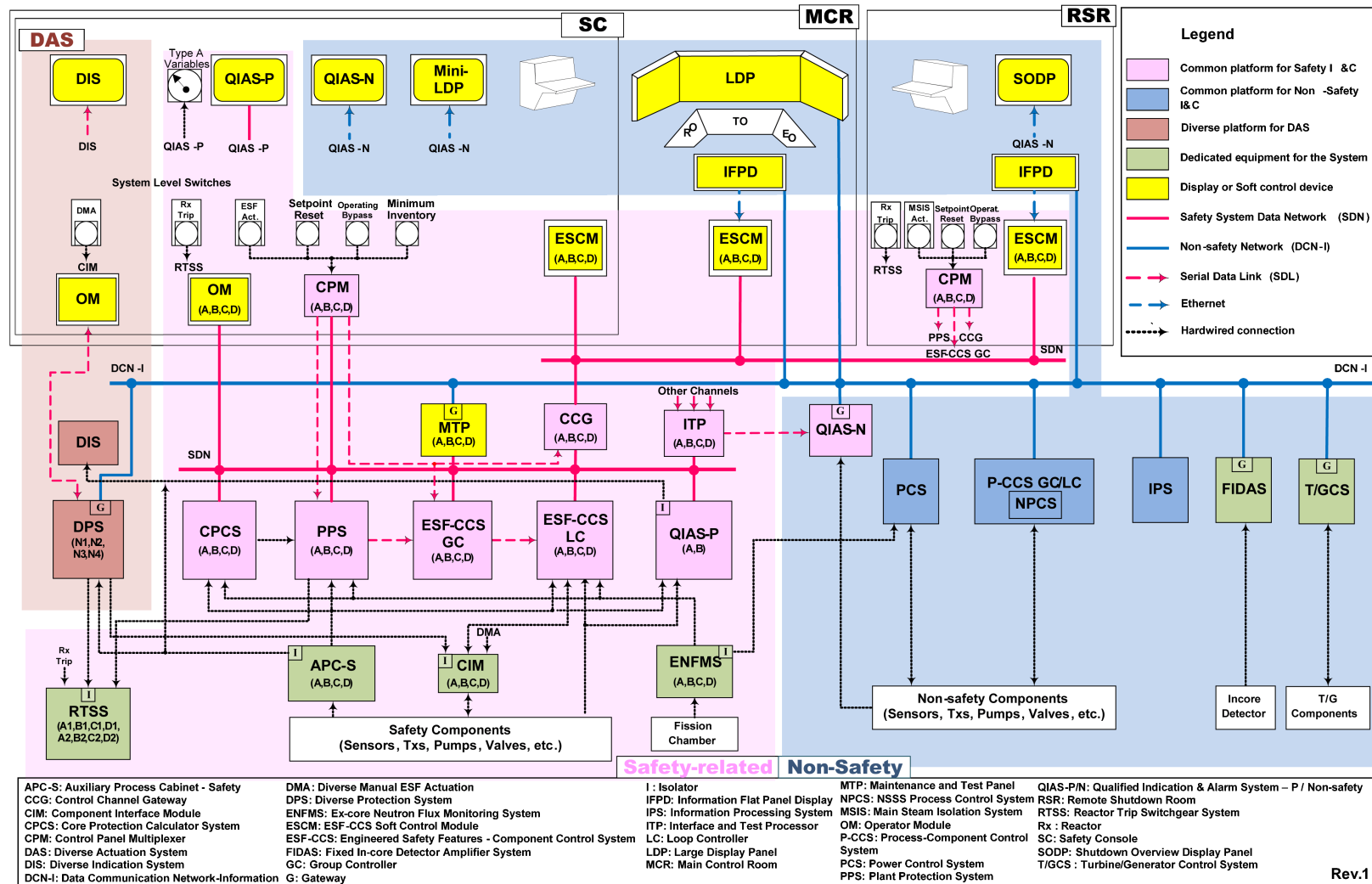


Figure 7.1-1 APR1400 I&C System Overview Architecture

APR1400 DCD TIER 2

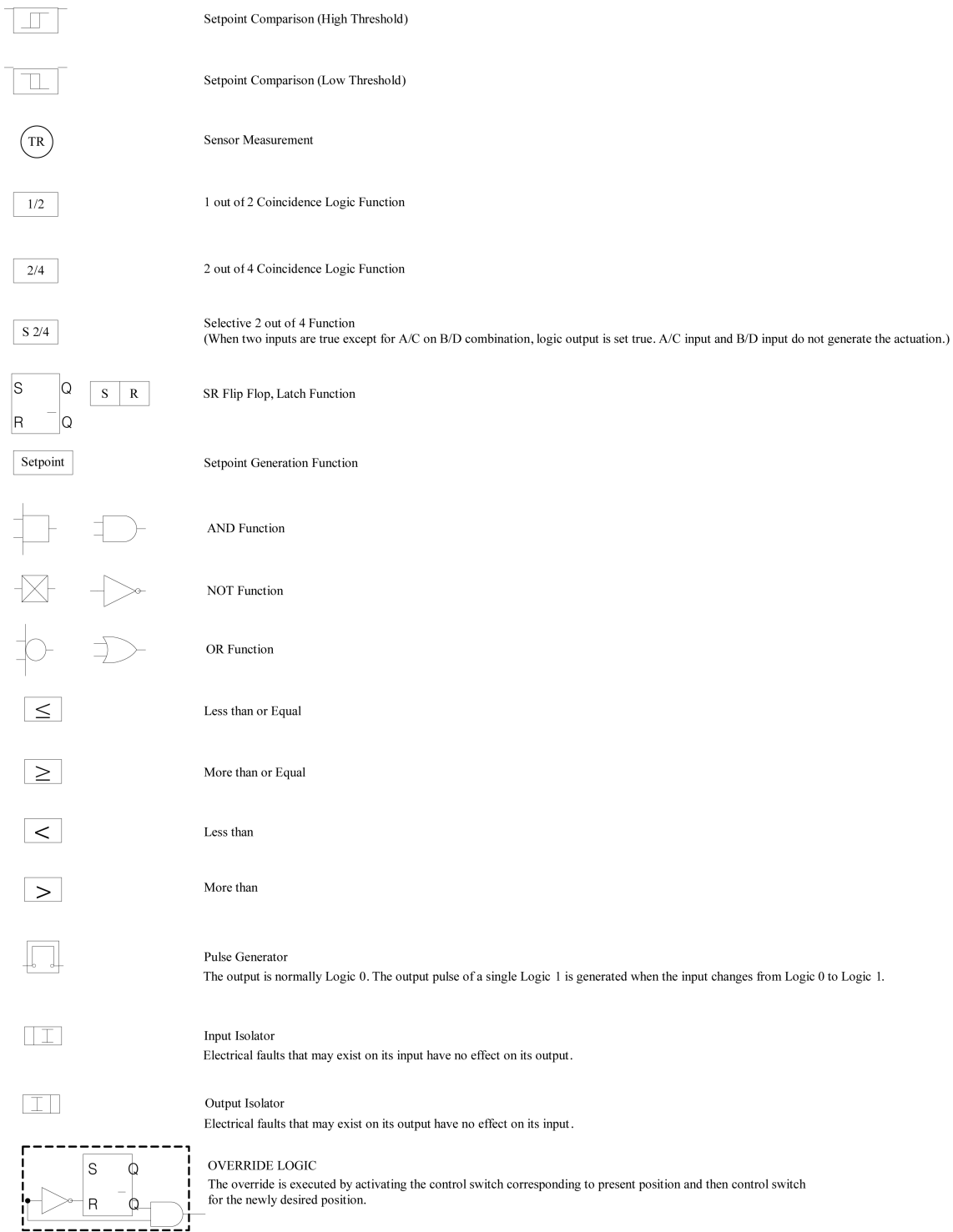


Figure 7.1-2 Symbol & Legend Diagram

7.2 Reactor Trip System

7.2.1 System Description

The reactor trip system (RTS) is a safety system that initiates reactor trips. The RTS consists of four channels of sensors, auxiliary process cabinet-safety (APC-S) cabinets, ex-core neutron flux monitoring system (ENFMS) cabinets, core protection calculator system (CPCS) cabinets, the reactor protection system (RPS) portion of the plant protection system (PPS) cabinets, and reactor trip switchgear system (RTSS) cabinets, as shown in Figure 7.2-1.

The PPS performs the RPS function, and the engineered safety features (ESF) initiation function. The engineered safety features (ESF) system consists of four channels of sensors, APC-S cabinets, the ESF initiation portion of the PPS cabinets, and the engineered safety features – component control system (ESF-CCS). The ESF system is described in Section 7.3.

The RPS functions protect the core fuel design limits and the reactor coolant system (RCS) pressure boundary following anticipated operational occurrences (AOOs) and provides assistance in mitigating the consequences of postulated accidents. Four measurement channels with electrical isolation and physical separation are provided for each parameter to generate the trip signals, with the exception of the control element assembly (CEA) position indication used in the CPCS.

The RPS portion of the PPS includes the following functions: bistable trip logic, local coincidence logic (LCL), reactor trip initiation, and testing.

The PPS consists of four channels. Each PPS channel is located in a channelized I&C equipment room. The cabinets contain the input and output module, bistable processor (BP), LCL processor, and other hardware for the interface with other PPS channels.

Each channel is designed based on a programmable logic controller (PLC) platform. The BPs (two redundant processors per channel) generate trip signals if the process values exceed their respective setpoints. The BP provides trip signals to the LCL processors in the four redundant channels, as shown in Figure 7.2-10.

The LCL processors (four redundant processors per channel) determine the LCL output state based on the state of the eight bistable trip signals and their respective trip channel

APR1400 DCD TIER 2

bypasses. For the RPS, the LCL outputs are transmitted to the RTSS through the selective 2-out-of-4 initiation circuit. For the engineered safety features actuation system (ESFAS), the initiation signals are provided to the ESF-CCS.

The 2-out-of-4 LCL generates four reactor trip signals per channel. The four reactor trip signals are combined using redundant selective 2-out-of-4 logic to generate two reactor trip signals that are transmitted to the two reactor trip circuit breaker (RTCB) undervoltage (UV) trip devices (A1 and A2) in the respective channel (A1 to RTSS-1 A1, and A2 to RTSS-2 A2), as shown in Figure 7.2-10. The reactor trip signals de-energize the UV trip devices, which results in opening the respective RTCB. The reactor trip signal interrupts power to the control element drive mechanism (CEDM) coils, allowing all control element assemblies (CEAs) to drop into the core by gravity.

The CPCS consists of four redundant channels. Each channel is located in a channelized I&C equipment room. Each cabinet contains the device signal conditioner, the control element assembly calculator (CEAC), the CEA position processor (CPP), and the core protection calculator (CPC). The CPCS sends a low departure from nucleate boiling ratio (DNBR) and a high local power density (LPD) trip signals to the PPS.

The PPS receives variable overpower and high log power for the reactor trip from the ENFMS.

The operator modules (OMs) of each channel shared by the PPS, CPCS, and ESF-CCS are located on the safety console in the main control room (MCR) (Figure 7.1-1). Each OM provides the HSI displays and controls needed to support the operation of the PPS, CPCS, and ESF-CCS.

The OM provides an indication of trip, pre-trip, initiation, trip channel bypasses, and operating bypasses of the PPS and an indication of the status of the CPC/CEAC variables and the CPC/CEAC calculations.

The maintenance and test panel (MTP) and the interface and test processor (ITP) cabinet are located in a channelized I&C equipment room. The MTP and ITP are shared by the PPS, ESF-CCS, CPCS, and the qualified indication and alarm system-P (QIAS-P).

The bistable trip channel bypasses, all-bypass, operating bypass, and setpoint reset switches are provided on the MTP switch panel. These switches are directly connected to the digital input module of the BPs or LCL processors. The MTP also provides a unidirectional data

APR1400 DCD TIER 2

communication gateway function to send a selected safety system channel status to the information processing system (IPS). The MTP is used to initiate manual surveillance testing based on operator input.

The ITP monitors the status of the safety systems. The ITP has interfaces with the BPs, LCL processors, MTP, CPCS, and ESF-CCS for status indications and surveillance testing feedback, as shown in Figure 7.2-12. The ITP serves as a data communication gateway to send a selected safety system channel status to the qualified indication and alarm system – non-safety (QIAS-N) using a one-way serial data link (SDL). The MCR safety console and remote shutdown console (RSC) provide the means to manually initiate reactor shutdown.

7.2.1.1 Reactor Protection System Variables

a. Process measurements

Various process parameters (e.g., pressures, levels, temperatures) are continuously monitored to provide signals to the BPs. These process protective parameters, as shown in Table 7.2-2, are measured with four redundant and independent process instrument channels with the exception of the CEA position indication used in the CPCS. The number of RPS sensors is listed in Table 7.2-3.

A typical protective channel, as shown in Figure 7.2-2, consists of a sensor/transmitter, signal converter, and logic part. MCR and RSR displays are provided from the IPS and the QIAS-N via the MTP and ITP, respectively.

Each process measurement channel is physically separated and electrically independent from the other channels.

b. CEA position measurements

The position of each CEA is an input to the CPCS. The positions are measured by two reed switch assemblies on each CEA.

Each reed switch assembly consists of a series of magnetically actuated reed switches spaced at fixed intervals along the CEA housing and wired with precision resistors in a voltage divider network (see Figure 7.2-3). A magnet attached to the CEA extension shaft actuates the adjacent reed switches, causing voltages

APR1400 DCD TIER 2

proportional to position to be transmitted for each assembly. The two assemblies and wiring are physically and electrically separated from each other.

The signals of the reed switch position transmitter (RSPT) are transmitted to CEACs through CPPs in all four CPCS channels. The CEAC1 and CEAC2 monitor RSPT1 and RSPT2 of all CEAs, respectively.

The CEAs in control groups that are moved in response to operator or control system demand are arranged into subgroups. Within each subgroup, the CEAs are symmetric about the core centerline. Subgroups within a control group are designed to move together and comply with the fixed insertion order for the control group.

Each CEAC monitors the position of all CEAs within each control subgroup. If a CEA position deviates from its subgroup position, the CEAC monitors the event, activates alarms, and transmits the appropriate penalty factors to the CPCs. If needed, the penalty factors result in a reduction in the margins-to-trip for a low departure from the nucleate boiling ratio (DNBR) and a high LPD. This function provides reasonable assurance of the conservative operation of the RPS in case of an anticipated operational occurrence (AOO), which requires a reactor trip.

The positions of each regulating, shutdown, and part-strength CEA are displayed on the IPS. The operator is able to select a channel from the four CPCS channels for display. If channel A or B is selected, CEA position RSPT1 is displayed. If channel C or D is selected, CEA position RSPT2 is displayed.

The CPC uses the designated 23 CEA RSPT signals to measure the position of the group and subgroup. The CPC uses one penalty factor from two CEACs to get the conservative result from CEA deviation calculated in CEACs. The analog signals of the RSPT are converted into digital signals in two CPPs of each channel and are transmitted to the associated CPPs and CEAC of all channels. The CPPs transmit the designated 23 CEA position signals to the CPC in the same channel using data communication between the CPC and CPP, and the isolated data communication is used to interface with the other channels. The detailed signal paths of CEA position information within the CPCS are shown in Figure 7.2-4. The functional block diagram for the CPCS is shown in Figure 7.2-7.

- c. Ex-core neutron flux measurements

APR1400 DCD TIER 2

The ENFMS consists of four redundant safety channels and two redundant startup/control signal processing drawers. The startup/control signal processing drawers are independent from the four safety channels through the qualified isolation devices.

The ENFMS includes neutron detectors located around the reactor core, and signal processing equipment located within the auxiliary building. There are four channels of safety instrumentation as shown in Figure 7.2-5.

The four safety channels provide neutron flux information from near startup neutron flux levels (2×10^{-8} percent) to 200 percent (10 decades) of rated power. Each safety channel consists of a detector assembly, a preamplifier assembly, and a signal processing drawer. These signal processing drawers provide the logarithmic power, linear power, and rate-of-change of power for the DNBR; local power density; overpower protection; and display of the rate-of-change of power.

The detector assembly provided for each safety channel consists of three identical fission chambers stacked vertically along the length of the reactor core. The use of multiple subchannel detectors in this arrangement permits the determination of axial power shape during power operation.

The fission chambers are mounted in detector holder assemblies, which are located in four dry instrument wells (thimbles) at or in the primary shield. The wells are spaced radially around the reactor vessel to provide optimum neutron flux information.

Four safety channel preamplifier assemblies and signal drawers for the fission chambers are mounted in the ENFMS cabinets in the electrical equipment rooms. Physical separation and electrical isolation between redundant channels are provided.

d. Reactor coolant flow measurements

The speed of each reactor coolant pump (RCP) is measured for calculation of reactor coolant flow through each pump. Two metal discs, each with 44 uniformly spaced slots about its periphery, are scanned by proximity sensors. The metal discs are attached to the pump motor shaft; one to the upper portion and one to the lower portion as shown Figure 7.2-6. Each scanning device produces a voltage

APR1400 DCD TIER 2

pulse signal. The pulse train that is input to the CPCS to calculate flow rate is based upon every n-th pulse from the scanning sensor. The frequency of this pulse train is proportional to pump speed. Physical separation between proximity sensors is provided.

The mass flow rate is obtained using the pump speed inputs from the four RCPs, the cold leg temperatures, and the hot leg temperatures. The volumetric flow rate through each RCP is dependent on the rotational speed of the pump and the pump head. Calibration of the calculated mass flow rate is performed periodically using instrumentation that is not part of the RCP shaft speed sensing system.

The mass flow rate is calculated for each pump using a correction factor based on the pump speed, the density of cold leg coolant, and the hot leg temperature. The mass flow rates calculated for each pump are summed to give a core mass flow rate. This flow rate is then used in the CPC DNBR and ΔT power algorithms.

e. Core protection calculators

One CPC per channel is provided. The DNBR and LPD are calculated in each CPC using the input signals described below. The DNBR and the LPD are compared with trip setpoints for initiation of the low DNBR trip and the high LPD trip. A trip signal from a CPC in each channel is hard-wired to the BP in the respective PPS channel. The CPC also provides pre-trip output signals.

Two independent CEACs are provided in each channel of the CPCS to calculate individual CEA deviations from the position of the other CEAs in their subgroup. RSPT signals of all core quadrants are transmitted to the CEAC through CPPs of each channel, and the specified CEA position signals used in the CPC of the corresponding channel are provided from the CPPs to the CPC through the CEAC. CPP channels A and B provide the position signals of RSPT1 to CEAC1 through CPPs in the other channels, and CPP channels C and D provide the position signals of RSPT2 to CEAC2 through CPPs in the other channels.

The data communications between CPPs and CEACs of the other channels use the isolated one-way SDL communication.

Each CPC receives the following inputs:

APR1400 DCD TIER 2

- 1) Core cold leg and hot leg temperature
- 2) Pressurizer pressure
- 3) RCP speed
- 4) Ex-core neutron flux power
- 5) Selected CEA position
- 6) Penalty factors for CEA deviations within a subgroup from each CEAC

The following calculations are performed in the CPC or CEACs and are described further in the Functional Design Requirements for the Core Protection Calculator System for the APR1400 (Reference 1):

- 1) CEA deviations
- 2) Correction factor for ex-core flux power for shape annealing and CEA shadowing
- 3) Reactor coolant flow change rate from RCP speeds, and temperatures and DNBR penalty for pump speeds less than a setpoint
- 4) ΔT power from reactor coolant temperatures, pressure, and flow information
- 5) Ex-core flux power signals are summed and corrected for CEA shadowing, shape annealing, and cold leg temperature shadowing. This corrected flux power is periodically calibrated to the actual core power measured independently of the RPS.
- 6) Axial power distribution from the corrected ex-core flux power signals
- 7) Radial peaking factors based on CEA positions
- 8) DNBR
- 9) Comparison of DNBR with a fixed trip setpoint
- 10) LPD

APR1400 DCD TIER 2

- 11) Comparison of LPD with a fixed trip setpoint
- 12) CEA deviation alarm
- 13) Calculation of cold leg temperature for asymmetric steam generator transient trip determination
- 14) Comparison of core power with CPC variable overpower trip setpoint

The outputs of each CPC are as follows:

- 1) DNBR low trip and pre-trip
- 2) Local power density high trip and pre-trip
- 3) CEA withdrawal prohibit
- 4) CPC auxiliary trips (Table 7.2-4)

The outputs to the IPS are as follows:

- 1) DNBR margin
- 2) Local power density margin
- 3) Calibrated neutron flux power
- 4) CPC measurement factor and calculation results values
- 5) Trip-buffer and snapshot reports

The outputs to the QIAS-N are as follows:

- 1) DNBR margin
- 2) Local power density margin
- 3) Axial shape index
- 4) DNBR
- 5) Compensated LPD

APR1400 DCD TIER 2

The CPCS consists of four channels, and each channel is installed in an independent cabinet. The operator can monitor all calculators, including inputs and calculated outputs from the OMs. The operator can change CPC addressable constants according to administrative procedures.

7.2.1.2 Reactor Protection System Logic

a. Bistable logic

The bistable logic compares input signals from the process measurement instrumentation to fixed or variable setpoints. The bistable logic initiates a channel trip when any monitored parameter exceeds the trip setpoint, as shown in Figure 7.2-8. The analog input signals are assigned to different analog input modules in each channel considering mitigating a transient, as shown in Figure 7.2-10. There are two redundant BPs per channel (A1 and A2 in channel A, B1 and B2 in channel B, C1 and C2 in channel C, and D1 and D2 in channel D) that receive the same process variable inputs.

The trip output signal of the bistable logic is sent to the LCL processors via the SDL in the four protective channels. A pre-trip output signal is also provided as part of the bistable logic output signals.

In addition to the trip and pre-trip functions, the BPs contains testing logic. The testing logic allows testing of the following signals:

- 1) Analog input
- 2) Trip setpoint
- 3) Pre-trip setpoint
- 4) Status information (pre-trip, trip, operating bypass)

The setpoint for bistable logic is adjustable from the MTP. The setpoint can be changed only if the function enable keyswitch is enabled. The setpoint change is restricted by a cabinet door open alarm, door keylock, and administrative procedure. The actual setpoint value can be monitored through the MTP, IPS, and OM.

APR1400 DCD TIER 2

The setpoint type for each trip parameter is provided in Table 7.2-4.

Bistable logic with fixed setpoint

For the bistables with a fixed setpoint (i.e., digital), the setpoint can be changed at the MTP. Setpoint change is controlled by administrative procedure. All of the fixed setpoints are monitored by the ITP.

Bistable logic with variable setpoint

Bistable logic with variable setpoints is provided to permit safe and orderly plant startup and shutdown. Two types of variable setpoints are as follow:

1) Variable setpoint with manual reset

This type of variable setpoint is a function of the input signal to the bistable logic. The design permits manually initiated automatic decrementing of the setpoint. Decrementing of the setpoint can be initiated by setpoint reset switches on the safety console and remote shutdown console (RSC).

When the signal decreases, the setpoint resets itself to a fixed value less than the actual input signal that exists at that time. By continuing to reset the setpoint whenever the pre-trip setpoint is reached, the plant can be shut down without the initiation of any unnecessary protective actions.

2) Variable setpoint with automatic rate limiting

The variable setpoint with automatic rate limiting permits the automatic incrementing and decrementing of the setpoint based on the action of the bistable input variable. The design allows for maintaining a fixed difference between the bistable input and the setpoint. If the input signal changes at a rate greater than the preset setpoint changing rate, the difference between the two values eventually becomes zero and creates a bistable trip. When the bistable trip occurs, it prevents the setpoint change until the bistable trip clears.

b. Local coincidence logic

The function of the local coincidence logic (LCL) is to generate a coincidence trip signal based on the BP outputs that are transmitted using SDLs. There are two

APR1400 DCD TIER 2

sets of two redundant LCL processors for the RPS in each channel. For example, the first set of two LCL processors generates two redundant trip signals based on the following logic combination: 2-out-of-4 of [(1-out-of-2 of A1 and A2), (1-out-of-2 of B1 and B2), (1-out-of-2 of C1 and C2), (1-out-of-2 of D1 and D2)].

The four LCL redundant processor outputs are combined in the initiation circuits, as shown in Figures 7.2-10 and 7.2-15.

In addition to a coincidence trip signal, each LCL also provides trip channel bypass status outputs. The bypass status is provided to verify that a bypass has actually been entered into the coincidence logic. The bypass status is available for display at the MTPs, OMs, and IPS.

7.2.1.3 Initiation Circuits

The initiation circuit is located in each channel of the PPS. The initiation circuit for the RPS function is composed of initiation relays, interposing relays, contacts from the manual initiation switches, and wiring.

The initiation circuit implements the following logical expression, as shown in Figure 7.2-10:

$(A1 \text{ OR } A3) \text{ AND } (A2 \text{ OR } A4)$ where A1, A2, A3, and A4 are the output signals of the redundant LCLs (A1 and A3 from one rack; A2 and A4 from the other rack).

Figure 7.2-9 illustrates the interface between the initiation circuit outputs and the reactor trip breakers and the reactor trip breaker configuration applied to the RPS function.

There are separate initiation circuits for undervoltage and shunt-trip initiation. The PPS provides the undervoltage trip signals, and the DPS provides the shunt-trip signals to each RTSG for diversity.

If an initiation circuit fails, it is set as fail-safe (i.e., in a trip state), resulting in a partial trip (1 of 4) in the reactor trip breaker arrangement. The partial trip activates the alarm by opening one reactor trip breaker and is indicated by the IPS. The partial trip cannot be bypassed.

APR1400 DCD TIER 2

7.2.1.4 Reactor Trip Initiation Signals

Figure 7.2-14 illustrates the logic for the RPS and ESFAS function. The nominal trip setpoints are provided in Table 7.2-4. The trip parameters for the RPS are as follows:

- a. Variable overpower
- b. High logarithmic power level
- c. High local power density
- d. Low departure from the nucleate boiling ratio
- e. High pressurizer pressure
- f. Low pressurizer pressure
- g. Low steam generator -1 water level
- h. Low steam generator -2 water level
- i. Low steam generator-1 pressure
- j. Low steam generator-2 pressure
- k. High containment pressure
- l. High steam generator water level-1
- m. High steam generator water level-2
- n. Low reactor coolant flow-1
- o. Low reactor coolant flow-2

In addition, the PPS generates the turbine trip signal to the turbine control system (TCS) when any variable trip initiation occurs.

- a. Variable overpower

The variable overpower trip is provided to trip the reactor when the neutron flux positive power rate or neutron flux power exceeds the preset value. The neutron

APR1400 DCD TIER 2

flux value is the average of the three linear subchannel flux values from each ENFMS safety channel. A pre-trip alarm is initiated below the trip setpoint to provide an audible and visible indication of approach to a trip condition.

1) Input

Neutron flux power from the ENFMS

2) Purpose

To provide a reactor trip in the event of uncontrolled CEA withdrawal; the functional logic for variable overpower is shown in Figure 7.2-17

b. High logarithmic power level

The high logarithmic power level trip is provided to trip the reactor when indicated neutron flux power reaches a preset value. The flux signal used is the logarithmic power signal originating in each ex-core neutron flux monitoring system safety channel. The trip is manually bypassed by the operator if power is equal to or greater than a preset value. The operating bypass is removed automatically when the power decreases below the preset value. The operating bypass setpoint is provided in Table 7.2-1.

A pre-trip alarm is initiated below the trip setpoint to provide audible and visible indications of an approach to a trip condition. The pre-trip alarm is bypassed when the trip is bypassed.

1) Input

Neutron flux power from the ENFMS

2) Purpose

To provide reasonable assurance of the integrity of the fuel cladding and RCS boundary in the event of unplanned criticality from a shutdown condition, resulting from either the dilution of the soluble boron concentration or the uncontrolled withdrawal of CEAs

APR1400 DCD TIER 2

If CEAs are in the withdrawn position, automatic trip action is initiated. If all CEAs are inserted, an alarm is provided to alert the operator to take the appropriate action in the event of an unplanned criticality.

The functional logic for high logarithmic power level is shown in Figure 7.2-18. The functional logic for operating bypass permissive is shown in Figure 7.2-31.

c. High local power density

The high LPD trip is provided to trip the reactor when the calculated core peak local power density reaches a preset value. The preset value is less than that value that would cause fuel centerline melting. The calculation of the peak local power density is performed by the CPCs, which compensates the calculated peak local power density to account for the thermal capacity of the fuel.

The calculation considers axial distribution, average power, radial peaking factors (based on target CEA position), and CEAC penalty factors to calculate the current value of compensated peak local power density.

The calculated trip provides reasonable assurance that the core peak local power density is below the safety limit for peak linear heat rate (W/cm or kW/ft). The effects of core burnup are considered in the determination of the local power density trip. The trip may be manually bypassed by the operator if power is equal to or less than a preset value. The bypass is automatically removed when the power is greater than the preset value. The operating bypass setpoint is provided in Table 7.2-1.

A pre-trip alarm is initiated below the trip value to provide audible and visible indications of an approach to a trip condition. The pre-trip alarm is bypassed when the trip is bypassed.

The high LPD trip signal is also generated based on the CPC auxiliary trips identified in Table 7.2-4.

1) Input

APR1400 DCD TIER 2

- a) Neutron flux power and hot pin axial power distribution from the ENFMS
- b) Radial peaking factors from CEA position measurement system (reed switch assemblies)
- c) ΔT power from coolant temperatures, pressure and flow measurements
- d) Penalty factors from CEACs for CEA deviation within a subgroup
- e) Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence

2) Purpose

To prevent the linear heat rate (W/cm or kW/ft) of fuel pin in the core from exceeding fuel design limits in the event of AOOs

The functional logic for the high local power density is shown in Figure 7.2-19. The functional logic for operating bypass permissive is shown in Figure 7.2-29.

d. Low departure from nucleate boiling ratio

The low DNBR trip is provided to trip the reactor when the calculated DNBR approaches a preset value. The calculation of DNBR is performed by the CPC based on core average power, reactor coolant pressure, reactor cold leg temperature, reactor coolant flow, and the core power distribution. The calculations include allowances for sensor, processing time delays and inaccuracies such that a trip is generated within the CPC before violation of the DNBR safety limit during an AOO.

The trip may be manually bypassed by the operator if power is equal to or less than a preset value. The bypass is automatically removed when the power is greater than a preset value. The bypass setpoint is provided in Table 7.2-1.

A pre-trip alarm is initiated above the trip value to provide audible and visible indications of an approach to a trip condition. Pre-trip alarm is bypassed when the trip is bypassed.

APR1400 DCD TIER 2

A combined low pressure and low DNBR trip provides a trip signal when the DNBR and pressurizer pressure reach their respective setpoints at the same time.

The low DNBR trip signal is also generated based on the CPC auxiliary trips identified in Table 7.2-4.

1) Input

- a) Neutron flux power and hot pin axial power distribution from the ex-core neutron flux monitoring system.
- b) RCS pressure from pressurizer pressure measurement
- c) ΔT power from coolant temperatures, pressure and flow measurements
- d) Radial peaking factors from CEA position measurement (reed switch assemblies).
- e) Reactor coolant mass flow from RCP speeds and temperatures
- f) Core inlet temperature from reactor coolant cold leg temperature measurements
- g) Penalty factors from CEACs for CEA deviation within a subgroup
- h) Penalty factors generated within the CPC for subgroup deviation and groups out-of-sequence

2) Purpose

To prevent the DNBR of the coolant channel in the core from exceeding the fuel design limit in the event of AOOs. In addition, this trip provides a reactor trip to assist the ESF systems in limiting the consequences of the steam line break outside the containment, steam generator tube rupture, and RCP shaft seizure accidents

The functional logic for low departure from the nucleate boiling ratio is shown in Figure 7.2-20. The functional logic for the operating bypass permissive is shown in Figure 7.2-29.

APR1400 DCD TIER 2

e. High pressurizer pressure

The high pressurizer pressure trip is provided to trip the reactor when the measured pressurizer pressure reaches a high preset value.

A pre-trip alarm is initiated below the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

Reactor coolant pressure from narrow range pressurizer pressure measurement

2) Purpose

To provide reasonable assurance of the integrity of the RCS boundary for any defined AOO that could lead to an over-pressurization of the RCS

The functional logic for the high pressurizer pressure is shown in Figure 7.2-21.

f. Low pressurizer pressure

The low pressurizer pressure trip is provided to trip the reactor when the measured pressurizer pressure falls to a low preset value. At pressures below the normal operating range, this setpoint can be manually decreased to a fixed increment below the existing pressurizer pressure down to a minimum value. The incremental and minimum values are given in Table 7.2-4. This provides the capability of a trip when required during plant cooldown.

The trip is manually bypassed by the operator if the pressure decreases below a preset value. The bypass is automatically removed as pressure is increased above the preset value and the low-pressure setpoint automatically increases, maintaining the fixed increment between the plant pressure and the setpoint. The bypass setpoint is provided in Table 7.2-1.

A pre-trip alarm is initiated above the trip setpoint to provide audible and visible indications of an approach to a trip condition. The pre-trip alarm is bypassed when the trip is bypassed.

1) Input

APR1400 DCD TIER 2

Reactor coolant pressure from wide range pressurizer pressure measurements

2) Purpose

To provide a reactor trip to assist the ESF Systems in the event of reduction in system pressure such as a LOCA

The functional logic for low pressurizer pressure is shown in Figure 7.2-22. The functional logic for operating bypass permissive is shown in Figure 7.2-30.

g. Low steam generator water level

The low SG water level trip is provided to trip the reactor when the measured SG water level falls below a preset value. Separate trips are provided for each SG.

A pre-trip alarm is initiated above the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

The level of water in each SG downcomer region from wide range differential pressure measurements

2) Purpose

To provide a reactor trip to assist the ESF systems to provide reasonable assurance that there is sufficient time for actuating the auxiliary feedwater pumps to remove decay heat from the reactor in the event of a reduction of steam generator water inventory

The functional logic for low steam generator level is shown in Figure 7.2-23.

h. Low steam generator pressure

The low SG pressure trip is provided to trip the reactor when the measured SG pressure falls below a preset value. At SG pressure below normal, the operator has the ability to manually decrease the setpoint to a fixed increment below existing system pressure. This is used during plant cooldown. During startup, this setpoint is automatically increased and remains at the fixed increment below SG pressure. This fixed increment is provided in Table 7.2-4.

APR1400 DCD TIER 2

A pre-trip alarm is initiated above the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

Steam pressure in each SG

2) Purpose

To provide a reactor trip to assist the ESF systems in the event of a steam line break accident

The functional logic for low steam generator pressure is shown in Figure 7.2-24.

i. High containment pressure

The high containment pressure trip is provided to trip the reactor when the measured containment pressure reaches a high preset value. The high containment pressure trip setpoint is selected in conjunction with the high-high containment pressure setpoint to prevent exceeding the containment design pressure during a loss of coolant accident (LOCA) or main steam line break (MSLB) accident.

A pre-trip alarm is initiated below the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

Pressure inside containment

2) Purpose

To assist the ESF systems by tripping the reactor coincident with the initiation of safety injection caused by excessive pressure in containment

The functional logic for high containment pressure is shown in Figure 7.2-25.

j. High steam generator water level

A high SG water level trip is provided to trip the reactor when the measured SG water level rises to a high preset value. Separate trips are provided for each SG.

APR1400 DCD TIER 2

A pre-trip alarm is initiated below the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

Level of water in each SG downcomer region from narrow range differential pressure measurements

2) Purpose

To assist the ESF systems by tripping the reactor coincident with the initiation of the main steam isolation caused by a high SG water level

The functional logic for high steam generator water level is shown in Figure 7.2-26.

k. Low reactor coolant flow

The low reactor coolant flow trip is provided to trip the reactor when the differential pressure across the primary side of either SG decreases below a rate-limited variable setpoint or below a preset value.

A separate trip is provided for each SG. This function is used to provide a reactor trip in an RCP-sheared shaft event.

A pre-trip alarm is initiated above the trip setpoint to provide audible and visible indications of an approach to a trip condition.

1) Input

Pressure differential measured across the steam generator primary side

2) Purpose

To provide a reactor trip in the event of an-RCP sheared shaft

The functional logic for low reactor coolant flow is shown in Figure 7.2-27.

l. Turbine trip

APR1400 DCD TIER 2

The turbine trip signal is generated whenever any RPS initiation signal is generated.

The time delay is implemented in the RPS so the turbine trip signal occurs 3 seconds following a reactor trip to prevent core damage from a single CEA withdrawal.

1) Input

All RPS initiations including manual reactor trip

2) Purpose

To provide a turbine trip in the event of a single CEA withdrawal

The functional logic for a turbine trip on a reactor trip is shown in Figure 7.2-14.

7.2.1.5 Manual Reactor Trip and Actuated Devices

Manual trip switches (two pairs in the MCR and one pair in the RSR) are provided to open the RTSS as shown in Figures 7.2-16 and 7.2-28. Actuation of any pair of switches opens the trip circuit breakers resulting in interruption of the ac power to the CEDMs. Both manual trip switches in a pair must be actuated to initiate a reactor trip. The manual trip signals completely bypass the automatic trip logic in accordance with NRC RG 1.62 (Reference 2).

A minimum of two channels of RPS trips are required for a reactor trip. The RPS initiation relays in each channel interface with the undervoltage devices to trip the circuit breakers of the RTSS while the DPS interfaces with the shunt trip devices to trip the RTSGs. The final actuation logic for the RPS is connected to the RTSS, which connects or interrupts the power to the digital rod control system (DRCS).

Power for CEAs comes from two full capacity motor generator (MG) sets so that the loss of either set does not cause a release of the CEAs.

The RTSS is housed in separate cabinets from the RPS cabinet. The cabinet also contains current monitoring devices for testing purposes and pushbuttons on each trip switchgear that allow manual opening of the circuit breaker.

7.2.1.6 Bypasses

The design provides for two types of bypasses such as operating bypasses and trip channel bypasses as shown in Table 7.2-1. The bypass status is indicated at the MTP and OM in the MCR. In addition, all bypass information in each channel is available for the displays on the QIAS-N and IPS.

a. Operating bypasses

Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The following operating bypasses are provided:

1) DNBR/LPD trip bypass

The DNBR and LPD bypass, which bypasses the low DNBR and high LPD trips from the CPC, is provided to allow system tests at low power and to allow CEA withdrawal at a subcritical condition during pre-power ascension. The bypass can be manually initiated if power falls below the permissive setpoint and is automatically removed when the power level increases above the bypass setpoint, as shown in Figure 7.2-13. In addition, manual operation of the bypass removal function is provided.

2) Low pressurizer pressure bypass

The RPS/ESFAS pressurizer pressure bypass is provided for two conditions:

a) System tests at low pressure

b) Heatup and cooldown with shutdown CEAs withdrawn

The bypass may be manually initiated if pressurizer pressure is below the bypass setpoint and is automatically removed when the pressurizer pressure increases above the bypass setpoint. In addition, manual operating bypass removal function is provided.

3) High logarithmic power level bypass

The high logarithmic power level bypass is provided to allow the reactor to be brought to the power range during a reactor startup. The bypass may be

APR1400 DCD TIER 2

manually initiated above the bypass setpoint and is automatically removed when power decreases below the bypass setpoint, as shown in Figure 7.2-13. In addition, manual operating bypass removal function is provided.

4) CPC CWP bypass

For each channel, an automatic bypass is provided for the CPC CEA withdrawal prohibit (CWP) signals to the CWP logic if the power level is less than 10^{-4} percent full power, as shown in Figures 7.2-13 and 7.2-32. The high pressurizer pressure pre-trip to the CWP logic is unaffected by this bypass. The permissive status (energized when the power is below 10^{-4} percent full power) is provided on the ENFMS safety channel drawer.

b. Trip channel bypasses

A trip channel bypass prevents a bistable trip. The bistable logic bypass converts the LCL to a 2-out-of-3 coincidence.

An individual trip channel bypass is possible on each MTP switch panel for each bistable trip. Trip channel bypass is used when removing a trip channel input from service for maintenance or testing. The trip channel bypass signal is distributed to the LCLs in the four redundant channels.

The process sensor (or transmitter) signal can be bypassed using the trip channel bypass described above.

An all-bypass function for all RPS variables is provided to bypass all parameters in one channel. An all-bypass switch is connected to LCL digital input module. The PPS initiation logic and initiation circuit outputs cannot be bypassed.

7.2.1.7 Interlocks

The following interlocks are provided:

a. Trip channel bypass interlock

Bypassing the same parameter in more than one channel is restricted by an administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. The all-bypass function for bypassing all parameters in one channel is

APR1400 DCD TIER 2

interlocked in an LCL algorithm to prevent the simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on an analog circuit through hard-wired cable between LCLs in all channels. The purpose of the all-bypass functions is to support testing and maintenance of the BP whereas the trip channel bypass is used against sensor failure.

b. Manual bistable logic test interlock

The manual bistable test function is performed after implementing the trip channel bypass administratively so that only one of the four channels can be selected for manual bistable testing at one time. The function enable key switch is interlocked for testing.

c. Initiation circuit test interlock

Testing of the initiation circuit is restricted to one channel at a time administratively. The function enable key switch is interlocked for testing.

d. ENFMS test interlock

The ENFMS generates an ENFMS test interlock to the PPS whenever the ENFMS is in test mode or trouble has occurred. The ENFMS test interlock generates a low DNBR RPS bistable and high LPD RPS bistable trips in the PPS channel.

e. CPCS test interlock

Both the low DNBR and the high LPD channel trips are bypassed to test a CPCS channel.

f. CEA withdrawal prohibit interlock

The CPCS generates a CWP input to the PPS to generate a CWP signal to the digital rod control system (DRCS) for the following events:

- 1) Low DNBR pre-trip
- 2) High LPD pre-trip
- 3) Reactor power cutback

APR1400 DCD TIER 2

- 4) CEA deviation within a subgroup beyond a preset limit
- 5) CEA group out-of-sequence or subgroup deviations within a group beyond a preset limit

The PPS provides the CWP signal to DRCS when the 2-out-of-4 coincidence logic is met for CPC CWP input or high pressurizer pressure pre-trip.

7.2.1.8 Redundancy

Redundant features of the RPS include:

- a. Four redundant channels of process sensors
- b. Four redundant channels of bistable logics
- c. Redundant BPs in each channel
- d. Four redundant channels of coincidence logics
- e. Redundant coincidence logics in each channel
- f. Four redundant channels of initiation circuits
- g. Three pairs of manual trip pushbuttons with one pair being sufficient to cause a reactor trip
- h. Four redundant AC power supplies from vital instrument buses
- i. Four redundant DC power supplies for the RTSG control circuit

Four redundant channels of RPS allow a channel functional test during power operation while still meeting the single failure criteria.

7.2.1.9 Defense-In-Depth and Diversity

The PPS is designed to minimize credible multiple channel failures originating from a postulated software common cause failure. The diversity features for the PPS are as follows:

APR1400 DCD TIER 2

- a. The software execution orders in the redundant BPs in a channel are different. In each channel, one BP executes a trip function in sequence 1 through N while the other BP executes trip functions in the reverse sequence (N through 1). The reverse trip function execution orders between redundant BPs provide software trajectory diversity for the PPS.
- b. Each RTSS circuit breaker has diverse methods of being automatically opened via the shunt trip and undervoltage trip devices. The PPS interfaces with the UV trip device and the DPS interfaces with the shunt trip device. For additional diversity, the RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2) with diverse design features.
- c. The PPS and the DPS are designed using different hardware and software to address postulated software common cause failures, as described in Section 7.8.

The RPS provides the reactor trip echelon of defense, as described in the Diversity and Defense-in-Depth Technical Report (Reference 3).

The critical function success path for diversity is shown in Table 7.2-6.

7.2.1.10 Vital Instrument Power Supply

The vital instrument power supply is described in Subsection 8.1.3.2.

7.2.1.11 System Arrangement

RPS components are arranged to comply with the separation and independence criteria specified in this chapter. The safety components are located to provide access for maintenance, testing, and operation as required.

The redundant channels of the RPS and RTSS cabinets are designed to be located in separate I&C equipment rooms.

7.2.2 Design Basis Information

7.2.2.1 Single Failure Criterion

The RPS is designed so that any single failure within the system does not prevent proper protective action at the system level in accordance with NRC RG 1.53 (Reference 4).

APR1400 DCD TIER 2

The RPS meets the single failure criteria through four redundant and independent channels. One input channel may be out of service (or bypassed), and the duration is limited by the Technical Specifications.

The 2-out-of-4 voting logic prevents a system-level spurious actuation due to single failure.

7.2.2.2 Quality of Components and Modules

All safety functions of the RPS are implemented using Class 1E components.

The instrumentation and controls used for the RPS are designed in accordance with the QA program in accordance with ASME NQA-1 (Reference 5).

*[The integration of RPS software and hardware including software development, tool, verification, validation, and configuration management is performed according to the Software Program Manual Technical Report (Reference 6).]**

7.2.2.3 Independence

a. Independence between redundant portions of a safety system

The routing of Class 1E and associated cabling and sensing lines from sensors comply with NRC RG 1.75 (Reference 7) and NRC RG 1.151 (Reference 8). The cablings for the four safety channels are routed separately.

The PPS channel receives ac power from the vital bus power supply system. The PPS does not share the power between channels.

b. Independence between safety systems and effects of design basis events

Independence between the components of the RPS and the effects of design basis event is provided by qualifying the equipment in accordance with the requirements in Subsections 7.2.2.2 and 7.2.2.8.

c. Independence between safety systems and non-safety systems

The PPS and non-safety systems are isolated using a qualified isolator or fiber-optic cable so that any failure in a non-safety system does not cause loss of the

APR1400 DCD TIER 2

safety system function. The PPS signals transmitted to the IPS/QIAS-N are isolated using fiber-optic cable.

Data flow is unidirectional from Class 1E systems to non-Class 1E systems.

7.2.2.4 Defense-in-Depth and Diversity

The defense-in-depth and diversity analysis is described in Reference 3. The diversity feature of the PPS is described in Subsection 7.2.1.9.

7.2.2.5 System Testing and Inoperable Surveillance

The system integrity is confirmed through self-diagnostics and surveillance testing. Testing features are provided for RPS testing during power operation or shutdown.

The RPS testing covers the trip path from the sensor input to the RTSG, as shown in Figure 7.2-11. The system test does not affect the protective functions. The testing system complies with the criteria of IEEE Std. 338 (Reference 9), which is endorsed by NRC RGs 1.22 (Reference 10) and 1.118 (Reference 11).

The test intervals are specified in the Technical Specifications (Chapter 16).

The test equipment consists of channelized MTP, ITP, and the associated interface circuits. Test results are displayed at the MTP.

Bypasses and inoperable status of safety systems are displayed at the MTP and OM in accordance with NRC RG 1.47 (Reference 12).

RPS manual testing consists of the following tests:

a. Sensor check

During power operation, measurement channels for the RPS are checked in the IPS by comparing process input values between channels.

b. Bistable logic test

Manual bistable logic testing is performed to verify bistable logic functions.

APR1400 DCD TIER 2

Manual testing is interlocked administratively for testing only one channel at a time.

c. CPCS test

The predetermined test inputs are entered into one CPCS at a time. The outputs of CPCS are checked against specific values.

The checks of trip logic by trip signal generated from CPCS are performed by tripping CPCS and monitoring the trip indication of each bistable logic.

d. LCL test

The LCL test is performed manually. The trip path of 2-out-of-4 coincidence logic is tested for all input combinations.

e. Initiation logic and circuit test

The initiation “OR” logic is tested simultaneously with the initiation circuit test.

Input signals are injected from the MTP, and the results are verified with the expected contact status of the initiation circuit.

f. Manual trip test

The manual trip test is performed by using one of the four manual trip pushbuttons on the safety console or one of the two manual trip pushbuttons on the RSC, observing an RTSG trip, and closing the RTSG prior to the next manual trip test.

The RTSG can be closed from the MTP.

g. Response time test

Response time from sensor to the RTSG is tested during shutdown to verify that the measured system response time is less than or equal to the response time assumed in the Chapter 15 safety analysis.

7.2.2.6 Use of Digital Systems

All RPS functions are implemented by digital systems. Manual RTs from the MCR and RSR are hardwired directly to the RTSGs.

7.2.2.7 Setpoint Determination

The RPS nominal trip setpoints are determined based on the analysis setpoints in the Chapter 15 safety analysis, in which analysis setpoints exist for the parameters.

*[When determining uncertainties, the worst environment considering a reactor trip or ESF actuation is assumed based on the bounding initiating event. The methodology for calculating uncertainty is provided in the Uncertainty Methodology and Application for Instrumentation Technical Report (Reference 13).]**

*[The methodology for combining uncertainty in a channel and determining the final trip setpoint is provided in the Setpoint Methodology for Plant Protection System Technical Report (Reference 14).]**

The setpoint methodology includes the relationship between the analytical limit, setpoint, and channel uncertainty. The setpoint methodology also provides the channel uncertainty calculations associated with the setpoints used for the RT and ESF actuation functions.

The setpoint methodology follows the methodology in ANSI/ISA-S67.04 (Reference 15) as endorsed by NRC RG 1.105 (Reference 16).

The instrumentation channel response time is the signal propagation time from the process sensor to the final actuation device. The response time for the RPS meets the response time assumed in Chapter 15. The reactor protective instrumentation response times assumed in the safety analysis in Chapter 15 are shown in Table 7.2-5.

The methodology for calculating system response time is provided in Reference 14.

7.2.2.8 Equipment Qualification

The RPS is designed and tested in accordance with the requirements of IEEE Std. 323 (References 17 and 18) for environmental qualification, IEEE Std. 344 (Reference 19) for seismic qualification, NRC RG 1.89 (Reference 20), and NRC RG 1.209 (Reference 21).

APR1400 DCD TIER 2

The RPS is designed and tested to minimize both the emission and susceptibility of EMI and RFI in accordance with NRC RG 1.180 (Reference 22).

The RPS is designed and tested to have immunity to electrostatic discharge in accordance with IEC-61000-4-2 (Reference 23).

7.2.3 Analysis

This section provides analyses, including a failure mode and effects analysis (FMEA), to demonstrate how the analyses satisfy the requirements of the applicable GDC (refer to Table 7.1-1), IEEE Std. 603 (Reference 24), and IEEE Std. 7-4.3.2 (Reference 25).

Compliance with applicable GDC, IEEE Std. 603, and IEEE Std. 7-4.3.2 is described in the Safety I&C System Technical Report (Reference 26).

7.2.3.1 Failure Modes and Effects Analysis

The failure modes and effects analysis (FMEA) follows the methods of IEEE Std. 352 (Reference 27) as referenced by IEEE Std. 603, IEEE Std. 7-4.3.2, and IEEE Std. 379 (Reference 28).

The RPS is designed with four independent redundant channels. Independence provides reasonable assurance that single failure cannot propagate between channels within the safety system or between the safety system and non-safety system.

The FMEA demonstrates that:

- a. As a result of the 4-channel redundancy, any single failure does not prevent a system-level RPS reactor trip,
- b. No single failure results in a spurious reactor trip.
- c. Any single failure is detected by diagnostic or periodic testing.

The FMEA is prepared assuming that one bistable trip channel is bypassed for maintenance.

The results of system-level FMEA are shown in Table 7.2-7.

7.2.3.2 Safety Analysis

The RPS is designed to provide the following protective functions:

- a. Automatic protective action is initiated by the RPS to provide reasonable assurance of adequate protection of the fuel, fuel cladding, and RCS boundary during specified anticipated operational occurrences.
- b. Automatic protective action is initiated by the RPS to aid the ESF systems in limiting the consequences of the accidents.

The Chapter 15 safety analysis addresses postulated accidents and AOOs including single CEA ejection, load rejection, and turbine trip. Control functions to mitigate the consequences of a plant load rejection and turbine trip are addressed in Subsection 7.7.1.1. The RPS has no reliance on plant instrument air or cooling water to vital equipment.

7.2.3.3 Test and Inspection

The RPS complies with the test requirements of IEEE Std. 338. Test intervals and their bases are included in the Technical Specifications (Chapter 16).

Periodic testing complies with NRC RG 1.22 and NRC RG 1.118.

7.2.3.4 Restrictive Setpoints

Restrictive setpoints are not used for the RPS.

7.2.3.5 Conformance to GDC

Compliance with the applicable GDC is described in Reference 26, and cross references to relevant information are provided in Table 7.1-1.

7.2.3.6 Conformance to IEEE Std. 603

Compliance to IEEE Std. 603 is described in Reference 26.

7.2.3.7 Conformance to IEEE Std. 7-4.3.2

Compliance to IEEE Std. 7-4.3.2 is described in Reference 26.

APR1400 DCD TIER 2

7.2.4 Combined License Information

No COL information is required with regard to Section 7.2.

7.2.5 References

1. APR1400-F-C-NR-13001-P, "Functional Design Requirements for the Core Protection Calculator System for the APR1400."
2. NRC RG 1.62, "Manual Initiation of Protection Action."
3. APR1400-Z-J-EC-13002-P, "Diversity and Defense-in-Depth Technical Report," September 2013.
4. NRC RG 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Protection Systems."
5. ASME NQA-1-1994, "Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage, and Handling of Items for Nuclear Power Plants."
6. *[APR1400-Z-J-NR-13003-P, "Software Program Manual Technical Report," September 2013.]**
7. NRC RG 1.75, "Criteria for Independence of Electrical Safety Systems."
8. NRC RG 1.151, "Instrument Sensing Lines."
9. IEEE Std. 338-1987, "IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
10. NRC RG 1.22, "Periodic Testing of Protection System Actuation Functions."
11. NRC RG 1.118, "Periodic Testing of Electric Power and Protection Systems."
12. NRC RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."
13. *[APR1400-Z-J-NR-13004-P, "Uncertainty Methodology and Application for Instrumentation Technical Report," April 2013.]**

APR1400 DCD TIER 2

14. [APR1400-Z-J-NR-13005-P, “Setpoint Methodology for Plant Protection System Technical Report,” April 2013.]*
15. ANSI/ISA-67.04-1994, “Setpoint for Nuclear Safety-Related Instrumentation.”
16. NRC RG 1.105, “Setpoints for Safety-Related Instrumentation.”
17. IEEE Std. 323-1974, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”
18. IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.”
19. IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.”
20. NRC RG 1.89, “Qualification for Class 1E Equipment for Nuclear Power Plants.”
21. NRC RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants.”
22. NRC RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control.”
23. IEC 61000-4-2, “Electromagnetic Compatibility – Testing and Measurement Techniques – Electrostatic Discharge Immunity Test.”
24. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”
25. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
26. APR1400-Z-J-EC-13001-P, “Safety I&C System Technical Report.” September 2013.
27. IEEE Std. 352-1987, “IEEE Guide for General Principles of Reliability Analysis of Nuclear Generating Station Protection Systems”
28. IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

APR1400 DCD TIER 2

Table 7.2-1

Reactor Protection System Operating Bypass Permissive

Title	Operating Bypass Function	Operating Bypass Permissive	Removed By	Notes
DNBR and LPD	Disable low DNBR and high LPD trips by manual operation of bypass switch	If power is $\leq 10^{-4} \%$	Automatic if power is $> 10^{-4} \%$	Allows low power testing and CEA withdrawal under non-critical state
Pressurizer pressure operating bypass permissive	Disables low pressurizer pressure trip, SIAS, and CIAS by manual operation of bypass switch	If pressure is $\leq 28.12 \text{ kg/cm}^2\text{A}$ (400 psia)	Automatic if pressure is $> 35.15 \text{ kg/cm}^2\text{A}$ (500 psia)	—
High log power level operating bypass permissive	Disables high logarithmic power level trip by manual operation of bypass switch	If power is $\geq 10^{-3} \%$	Automatic if power is $< 10^{-3} \%$	Bypassed during reactor startup
CPC CWP operating bypass permissive	Disables CPCS CWP signals by automatic operation of bypass	If power is $\leq 10^{-4} \%$	Automatic if power is $> 10^{-4} \%$	CWP by Hi PZR pressure is not affected by bypass

APR1400 DCD TIER 2

Table 7.2-2

Reactor Protection System Monitored Plant Variable Ranges

Monitored Variable	Minimum	Nominal (full power)	Maximum
Neutron flux power, % of full power	Near 2×10^{-8}	100	200
Cold leg temperature, °C (°F)	230 (446)	291 (555)	330 (626)
Hot leg temperature, °C (°F)	250 (482)	324 (615)	350 (662)
Pressurizer pressure (narrow range), kg/cm ² A (psia)	105 (1,494)	158 (2,250)	175 (2,489)
Pressurizer pressure (wide range), kg/cm ² A (psia)	0 (0)	158 (2,250)	211 (3,000)
CEA positions	Full in	NA	Full out
Reactor coolant pump speed, rpm	100	1,190	1,320
Steam generator water level (wide range), % ⁽¹⁾	0	77	100
Steam generator water level (narrow range), % ⁽²⁾	0	60	100
Steam generator pressure, kg/cm ² a (psia)	0 (0)	70.3 (1,000)	105.0 (1,494)
Containment pressure, cm/H ₂ O (psig)	−300 (−4)	0 (0)	1,200 (17)
Steam generator primary pressure differential, cm/H ₂ O (psig)	0 (0)	2,180 (31)	5,000 (70)

(1) Percentage of the distance between the wide range level instrument nozzles (above the lower nozzle)

(2) Percentage of the distance between the narrow range level instrument nozzles (above the lower nozzle)

APR1400 DCD TIER 2

Table 7.2-3

Reactor Protection System Sensors

Monitored Variable	Type	Number of Sensors	Location	Receiving System
Neutron flux power	Fission chamber	12	Shield of primary side	ENFMS (for generating VOPT and High Log Power)
Cold leg temperature	Precision RTD	8	Cold leg piping	CPCS (for generating High LPD and Low DNBR)
Hot leg temperature	Precision RTD	8	Hot leg piping	CPCS (for generating High LPD and Low DNBR)
Pressurizer pressure (narrow range)	Pressure transmitter	4	Pressurizer	PPS, CPCS (for generating High LPD and Low DNBR)
Pressurizer pressure (wide range)	Pressure transmitter	4 ⁽¹⁾	Pressurizer	PPS
CEA positions	Reed switch position transmitter	2/CEA	Control element drive mechanism	CPCS (for generating High LPD and Low DNBR)
Reactor coolant pump speed	Proximity sensor	4/pump	Reactor coolant pump	CPCS (for generating High LPD and Low DNBR)
Steam generator 1/2 level (narrow range)	Differential pressure transmitter	4/steam generator ⁽¹⁾	Steam generators	PPS
Steam generator 1/2 pressure (wide range)	Differential pressure transmitter	4/steam generator ⁽¹⁾	Steam generators	PPS
Containment pressure	Pressure transmitter	4 ⁽¹⁾	Containment structure	PPS
Steam generator 1/2 primary differential pressure	Differential pressure transmitter	4/steam generator	Steam generators	PPS

(1) Common with the engineered safety features actuation system

APR1400 DCD TIER 2

Table 7.2-4 (1 of 2)

Reactor Protection System Design Inputs

Type		Nominal Value at Full Power	Nominal Trip Setpoint	Setpoint Type ⁽¹⁾	Nominal Margin to Trip
High logarithmic power level		NA	0.018 % power	Fixed	NA
Variable Overpower (Ex-core)	Ceiling	100 % power	109.6 % power	Rate limited variable	9.6 % power
	Rate	0 % / min	6.0 % / min		6.0 % / min
	Step	NA	12.5 % band ⁽²⁾		NA
Low DNBR		> 1.98 ⁽³⁾	≥ 1.29	Fixed	≥ 0.69
High local power density, W/cm (kW/ft)		≤ 485 (peak) (14.8)	656 (20)	Fixed	≥ 171 (5.2)
High pressurizer pressure, kg/cm ² A (psia)		158.0 (2,250)	167.1 (2,377)	Fixed	9.1 (127)
Low pressurizer pressure, kg/cm ² A (psia)		158 (2,250)	127.3 ^{(4),(5)} (1,810)	Variable	30.7 (440)
Low steam generator water level, WR % ⁽⁶⁾		77.0	45.0	Fixed	32
Low steam generator pressure, kg/cm ² A (psia)		70.3 (1,000)	60.1 (855) ⁽⁴⁾	Variable	10.2 (145)
High containment pressure, cmH ₂ O (psig)		0	133.6 (1.9)	Fixed	133.6 (1.9)
High steam generator water level, NR % ⁽⁷⁾		60.0	90.0	Fixed	30.0
Low reactor coolant flow, cmH ₂ O (psid)	Min	2,180 (31)	763.7 (10.8)	Rate limited Variable	1,416.3 (20.2)
	Rate	0/second	3.4/second (0.048)		3.4/second (0.048)
	Step	NA	616.7 band (8.8)		NA

APR1400 DCD TIER 2

Table 7.2-4 (2 of 2)

Type	Nominal Value at Full Power	Nominal Trip Setpoint	Setpoint Type ⁽¹⁾	Nominal Margin to Trip
CPC Auxiliary Trips				
Cold leg temperature, °C (°F)	291 (555)	262.2 (504) to 310.6 (591)	Fixed	+19.6 (36) –28.8 (51)
Primary pressure, kg/cm ² A (psia)	158 (2,250)	127.3 (1,810) to 168.0 (2,390)	Fixed	+10.0 (140) –30.7 (440)
Hot pin ASI	0.0	–0.5 to +0.5	Fixed	+0.5; –0.5
One pin radial peak	1.6	1.28 to 7.0	Fixed	+5.4; +0.32
Hot leg temperature, °C (°F)	324 (615)	Thot > Tsat-11.1 °C (20 °F)	Fixed	10 (18)
Asymmetric steam generator transient, °C (°F)	0 (0)	8.33(15)	Fixed	8.33 (15)
Pump speed, %	100	95.0	Fixed	5.0
Variable overpower	100 % Power	110 % Power	Variable	10 % Power
Increasing Rate	0	12 % / min		12 % / min
Decreasing Rate	0	300 % / min		300 % / min
Band ⁽²⁾	NA	15 % band		NA
Low P\pressure, kg/cm ² A (psia) and DNBR	158 (2,250) and 2.0	141.7 (2,015) and 1.52	Fixed	16.3 (235) and 0.48

- (1) Type of setpoint generation
- (2) % band is percent above measured ex-core power level.
- (3) Calculated value of DNBR provides reasonable assurance of a trip conservatively considering all sensor and processing time delays and inaccuracies. Calculated DNBR is less than or equal to actual core DNBR.
- (4) Setpoint can be manually decreased to a fixed increment below existing pressure as pressure is reduced during controlled plant cooldown and is automatically increased as pressure is increased maintaining a fixed increment. This fixed increment is 28 kg/cm² (400 psi) for pressurizer pressure and 14 kg/cm² (200 psi) for steam generator pressure.
- (5) Trip setpoint has a minimum value of 7 kg/cm²A (100 psia).
- (6) Percentage of the distance between steam generator upper and lower level wide range instrument nozzle.
- (7) Percentage of the distance between steam generator upper and lower level narrow range instrument nozzle.

APR1400 DCD TIER 2

Table 7.2-5 (1 of 2)

Reactor Protective Instrumentation Response Time

Function	Response Time
I. Trip Generation	
A. Process	
1. Pressurizer Pressure – Low	≤ 1.15 seconds
2. Pressurizer Pressure – High	≤ 0.85 second
3. Steam Generator Level – Low	≤ 1.25 seconds
4. Steam Generator Level – High	≤ 1.15 seconds
5. Steam Generator Pressure – Low	≤ 1.15 seconds
6. Containment Pressure – High	≤ 1.15 seconds
7. Reactor Coolant Flow – Low	≤ 0.85 second
8. Local Power Density – High	
a. Neutron Flux Power from Ex-core Neutron Detectors	≤ 0.65 second ⁽¹⁾
b. CEA Positions	≤ 1.45 seconds ⁽²⁾
c. CEA Positions: CEAC Penalty Factor	≤ 0.85 second ⁽²⁾
9. DNBR – Low	
a. Neutron Flux Power from Ex-core Neutron Detectors	≤ 0.65 second ⁽¹⁾
b. CEA Positions	≤ 1.45 seconds ⁽²⁾
c. Cold – Leg Temperature	≤ 8.65 seconds ⁽³⁾
d. Hot – Leg Temperature	≤ 8.65 seconds ⁽³⁾
e. Primary Coolant Pump Shaft Speed	≤ 0.45 second ⁽⁴⁾
f. Reactor Coolant Pressure from Pressurizer	≤ 0.95 second ⁽⁵⁾
g. CEA Positions: CEAC Penalty Factor	≤ 0.85 second ⁽²⁾

APR1400 DCD TIER 2

Table 7.2-5 (2 of 2)

Function	Response Time
B. Ex-core Neutron Flux	
1. Variable Overpower Trip	≤ 0.55 second ⁽¹⁾
2. Logarithmic Power Level – High	
a. Startup and Operating	≤ 0.55 second ⁽¹⁾
b. Shutdown	≤ 0.55 second ⁽¹⁾
C. Core Protection Calculator System	
1. CEA Calculators	Not Applicable
2. Core Protection Calculators	Not Applicable
D. Diverse Protection System	
1. Pressurizer Pressure – High	≤ 0.85 second
2. Containment Pressure – High	≤ 1.15 seconds
II. RPS Logic	
A. Coincidence Logic	
B. Initiation Logic	
III. RPS Actuation Devices	
A. Reactor Trip Breakers	
B. Manual Trip	

- (1) Neutron detectors are exempt from response time testing. The response time of neutron flux signal portion of the channel is measured from the detector output or from the input of first electronic component in channel.
- (2) Response time is measured from the output of the sensor. Acceptable CEA sensor response is demonstrated by compliance with Technical Specifications Subsection 3.3.1.
- (3) Response time is measured from the output of the resistance temperature detector (sensor). RTD response time is measured at least once per 18 months. The measured response time of the slowest RTD is less than or equal to 8.0 seconds.
- (4) The pulse transmitters measuring pump speed are exempt from response time testing. The response time is measured from the pulse shaper input.
- (5) Response time is measured from the output of the pressure transmitter. The transmitter response time is less than or equal to 0.3 second.

Table 7.2-6

Critical Function Success Path Diversity

Success Path/ Control Function	Reactivity Control	Inventory Control	RCS Pressure Control	Core Heat Removal	RCS Heat Removal	CNMT Isolation	CNMT Environment	Indirect Radiation Releases	Vital Auxiliaries
Normal Success Path ⁽¹⁾	1. CVCS (Boration) 2. CEA Drive Mechanism	CVCS	1. Pressurizer Heaters and Sprays 2. CVCS	RCPS	Main Feed	Control Valves	1. CNMT Fan Cooling 2. Hydrogen Recombiner	Monitoring Only	1. Non-vital ac from offsite source 2. Alternate ac source 3. Non-safety CCW
Alternate (Emergency or safety) Success Path ⁽²⁾	1. RPS 2. Safety Injection	1. Safety Injection 2. Rapid Depressuriza tion	1. Safety Injection 2. Rapid Depressuriza tion 3. Reactor Coolant Gas Vent	1. Shutdown Cooling 2. Safety Injection 3. Rapid Depressuriza tion	1. Auxiliary Feedwater 2. Atmospheric Dump Valves 3. Safety Injection 4. Rapid Depressuriza tion	CIAS Actuation	CNMT Spray	Monitoring Only	1. Vital ac and dc from onsite source 2. Emergency Diesel Generators 3. Safety - Related CCW

(1) Type 2 System: PCS or P-CCS

(2) Type 1 System: PPS or ESF-CCS

Table 7.2-7 (1 of 65)

Failure Mode and Effects Analysis for the Plant Protection System

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-1	Ex-core neutron flux detector	a) Low output	Loss of high power supply source	Data loss Incorrect data Detection failure of high neutron flux level	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Reactor trip logic on variable overpower, high logarithmic power, DNBR/LPD changes to 2-out-of-2 coincidence logic.	Loss of high power supply makes all three sub-channel detectors not work properly. Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) High output	Short circuit of detector Continuous ionization	Channel trip can occur due to variable overpower, low DNBR, high logarithmic power level or high LPD.	Occurrence of pre-trip and trip alarm for variable overpower, low DNBR, high logarithmic power level, or high LPD.	Three-channel redundancy	Reactor trip logic on variable overpower, high logarithmic power, DNBR/LPD changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

Table 7.2-7 (2 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-2	Pressurizer Pressure (wide range)	a) One signal turns on due to failure (high level signal)	Sensor failure Component failure	High-level pressure signal is input to bistable logic. Low pressurizer pressure bistable logic does not generate trip under trip condition.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Logic for reactor trip, CIAS, and SIAS changes to 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) One signal turns off due to failure (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level pressure signal input to bistable logic. Low pressurizer pressure bistable logic initiates channel trip.	Occurrence of pre-trip and trip alarm for low pressurizer pressure channel	Three-channel redundancy	Logic for reactor trip, CIAS and SIAS changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

Table 7.2-7 (3 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-3	Pressurizer Pressure (narrow range)	a) Signal turns on (high level signal)	Sensor failure Component failure	High-level pressure signal is input to bistable logic. High pressurizer pressure bistable logic initiates channel trip.	Occurrence of pre-trip and trip alarm for high pressurizer pressure channel	Three-channel redundancy	Reactor trip logic on low DNBR changes to 2-out-of-2 coincidence logic. Reactor trip logic on high pressurizer pressure changes to 1-out-of-2 coincidence logic. CWP logic on high pressurizer pressure changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level pressure lowers margin of DNBR and initiates low DNBR channel trip. High pressurizer pressure bistable logic does not generate trip under trip condition.	Occurrence of pre-trip and trip alarm for low DNBRchannel	Three-channel redundancy	Reactor trip logic on low DNBR changes to 1-out-of-2 coincidence logic. Reactor trip logic on high pressurizer pressure changes to 2-out-of-2 coincidence logic. CWP logic on high pressurizer pressure changes to 2-out-of-2 coincidence logic	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

Table 7.2-7 (4 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-4	Steam generator-1 level signal, Steam generator-2 level signal (Wide range)	a) Signal turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level signal is input to bistable logic. Low steam generator level bistable logic generates channel trip on affected steam generator by changing logic state.	Occurrence of pre-trip and trip alarm for low steam generator level channel	Three-channel redundancy	Logic for reactor trip and AFAS on affected low steam generator level changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns on (high level signal)	Sensor failure Component failure	High-level signal is input to bistable logic. Low steam generator level bistable logic does not generate trip on affected steam generator.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Logic for reactor trip and AFAS on affected low steam generator level changes to 2-out-of-2 coincidence logic. System on normal steam generator level still operates.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

7.2-46

APR1400 DCD TIER 2

Table 7.2-7 (5 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-5	Steam generator-1 level signal, Steam generator-2 level signal (Narrow range)	a) Signal turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level signal is input to bistable logic on affected steam generator. Bistable logic does not generate trip signal from actual signal value of high steam generator level.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Logic for reactor trip and MSIS on high steam generator level changes to 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns on (high level signal)	Sensor failure Component failure	Incorrect high-level signal is input to bistable logic on affected steam generator. Bistable logic does not trip applicable channel of steam generator by changing logic state.	Occurrence of pre-trip and trip alarm for high steam generator level channel	Three-channel redundancy	Logic for reactor trip and MSIS on affected high steam generator level changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

7.2-47

APRI400 DCD TIER 2

Table 7.2-7 (6 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-6	Steam generator-1 pressure signal, Steam generator-2 pressure signal	a) One signal unnecessarily turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level pressure signal is input to bistable logic. Bistable logic initiates channel trip of low steam generator pressure on reactor trip and MSIS.	Occurrence of pre-trip and trip alarm for low steam generator pressure channel	Three-channel redundancy	Logic for reactor trip and MSIS on steam generator pressure changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) One signal unnecessarily turns on (high level signal)	Sensor failure Component failure	High-level pressure signal is input to bistable logic. One channel of low steam generator pressure on affected steam generator at low-pressure state does not generate channel trip.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Logic for reactor trip and MSIS on low steam generator pressure changes to 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

7.2-48

APRI400 DCD TIER 2

Table 7.2-7 (7 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-7	Steam generator-1 pressure difference signal, Steam generator-2 pressure difference signal	a) One signal turns on due to failure (high level signal)	Sensor failure Component failure	High or normal pressure difference signal is input to one bistable logic on affected steam generator. One channel is not tripped at actually low steam generator flow on affected steam generator.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Reactor trip logic on affected low steam generator flow changes to 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) One signal turns off due to failure (low level signal)	Sensor failure DC power supply failure Open circuit	Low-pressure difference signal is input to bistable logic on affected steam generator. Bistable logic changes logic initiates channel trip.	Occurrence of pre-trip and trip alarm for low steam generator flow channel	Three-channel redundancy	Reactor trip logic on affected low steam generator flow changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

7.2-49

APRI400 DCD TIER 2

Table 7.2-7 (8 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-8	Containment pressure signal (Narrow range)	a) Signal turns on (high level signal)	Component failure	High-level pressure signal is input to bistable logic. Bistable logic initiates channel trip of high containment pressure for RPS, SIAS, CIAS, and MSIS.	RPS and ESF channel indication and pre-trip/alarm for high containment pressure channel	Three-channel redundancy	Reactor trip logic on high containment pressure changes to 1-out-of-2 coincidence logic. Logic for CIAS, SIAS, and MSIS on high containment pressure changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low-level pressure signal is input to bistable logic. Bistable logic does not change logic state, and no trip occurs at actual condition of high containment pressure.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	RPS trip logic on high containment pressure changes to 2-out-of-2 coincidence logic. Logic for CIAS, SIAS, and MSIS regarding high containment pressure changes to 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

Table 7.2-7 (9 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-9	Containment pressure signal (Wide range)	a) Signal turns on (high level signal)	Sensor failure Component failure	High-level pressure signal is input to bistable logic. Bistable logic initiates channel trip for CSAS.	ESF channel indication and pre-trip/alarm for high-high containment pressure channel	Three-channel redundancy	CSAS logic changes to 1-out-of-2.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns off (low level signal)	Sensor failure DC power supply failure Open circuit	Low level or normal containment pressure signal is input to bistable logic. Bistable logic does not initiate channel trip at actual condition of high-high containment pressure.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	CSAS logic changes to 2-out-of-2.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

Table 7.2-7 (10 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-10	Ex-core Neutron Flux Measurement Channel (ENFMS)	a) ENFMS test interlock contact turns off due to failure.	Open circuit Mechanical failure	Relay output for ENFMS test interlock is de-energized. Unnecessary channel trip of LPD and DNBR.	Alarm	Three-channel redundancy on LPD and DNBR	RPS trip logic on LPD and DNBR changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) ENFMS test interlock contact turns on due to failure.	Contact arc and fixing	Relay output for ENFMS test interlock is not de-energized upon failure of signal processing drawer of or test for ENFMS. Loss of failure alarm Bistable logic of LPD and DNBR does not generate trip signal. Bistable logic of LPD and DNBR may not generate trip signal due to incorrect data during nuclear measurement system test.	Periodic test	Three-channel redundancy	RPS trip logic on LPD and DNBR can change to 2-out-of-2 coincidence logic.	

APR1400 DCD TIER 2

Table 7.2-7 (11 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-10	ENFMS (Continued)	c) Logarithmic power bistable contact of $10^{-3}\%$ turns off due to failure.	Open circuit Mechanical failure	Bistable fails to be energized with output power of over $10^{-3}\%$. Bypassing one high logarithmic power level trip channel is inapplicable resulting in channel trip on high logarithmic power level.	Periodic test Channel trip alarm No bypass permissive indication light for high logarithmic power	Three-channel redundancy	Channel trip occurs in one channel of high logarithmic power during power operation. Two other channels can still be bypassed.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic
		d) Logarithmic power bistable contact of $10^{-3}\%$ turns on due to failure.	Contact arc and fixing	Bistable relay is energized Operator can apply bypass on high logarithmic power bistable with power being below $10^{-3}\%$.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	RPS trip logic on high logarithmic power changes to 2-out-of-2 coincidence logic.	

Table 7.2-7 (12 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1-10	ENFMS (Continued)	e) Logarithmic power bistable contact of $10^{-4}\%$ turns off due to failure (CPCS, CWP).	Open circuit Mechanical failure	Bistable relay is not energized with power being below $10^{-4}\%$. Neither bypassing CWP nor bypassing CPC is applicable. Unnecessary channel trip of LPD and DNBR and unnecessary CWP at low output power.	Alarm: comparison of three channels Periodic test	Three-channel redundancy	Trip occurs in one channel on LPD, DNBR, and CWP at low power and trip logic changes to 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic
		f) Bistable for logarithmic power of $10^{-4}\%$ turns on due to failure (CPCS, CWP).	Contact arc and fixing	Bistable relay stays energized with output power exceeding $10^{-4}\%$. Operator can apply bypass on CPCS with power exceeding $10^{-4}\%$. One channel on CWP stays bypassed.	Bypass permission indication of CPCS Periodic test	Three-channel redundancy	RPS trip logic and CWP logic on LPD or DNBR changes to 2-out-of-2 coincidence logic.	

Table 7.2-7 (13 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-1	Analog Input Hot Leg Temperature	a) High level signal (out of range)	Sensor Failure	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC failed sensor indication and Channel Trouble OM and MTP indication, Channel Trouble annunciation.	For out of range failures: DNBR/LPD channel auxiliary trip, CPC sensor failure indication / annunciation, CPC trouble indication / annunciation. Sensor input cross channel comparison.	Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) High level signal (in range)	Sensor Failure	For in range failures, possible DNBR/LPD Channel Trip on Quality Margin. Likely Auxiliary trip on VOPT for rapid changes. CPC software generated sensor failure alarm if process exceeds high range limits.	For in range failures: Increase in delta T power, Sensor input cross channel comparison possible sensor failure alarm.	Three-channel redundancy	When trip occurs, DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	
		c) low level signal (out of range)	Sensor Failure	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC sensor failure indication and Channel Trouble OM and MTP indication, Channel Trouble annunciation.	For out of range failures: DNBR/LPD channel auxiliary trip, CPC Sensor Failure indication / annunciation, CPC Trouble indication/ annunciation Sensor input cross channel comparison	Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	

7.2-55

APRI400 DCD TIER 2

Table 7.2-7 (14 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-1	Analog Input Hot Leg Temperature (Continued)	d) Low level signal (in range)	Sensor Failure	For in range failures, Reduces Delta T power. NI-Delta T Power deviation alarm. CPC software generated sensor failure alarm if process exceeds low limits.	For in range failures: Sensor input cross channel comparison, possible NI-Delta T power deviation alarm. possible sensor failure alarm	Three-channel redundancy	If no action is performed after sensing the failure, the RPCS logic is remained 2-out-of-3 coincidence logic.	The bypassed channel is returned to operation. The failed channel is bypassed or placed in trip. Then the RPS logic is converted to 2-out-of-3 or 1-out-of-3 coincidence logic
2-2	Analog Input Cold Leg Temperature	a) High level signal (out of range)	Sensor Failure	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC sensor failure indication and Channel Trouble OM and MTP indication, CPC Channel Trouble annunciation.	DNBR/LPD channel auxiliary trip, CPC Sensor Failure indication / annunciation, CPC Trouble indication / annunciation	Single PPS channel trip Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to a 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) High level signal (in range)	Sensor Failure	For in range failures, reduces Delta T power. Lowers DNBR calculation. NI-Delta T Power deviation alarm Auxiliary Trip (DNBR/LPD) on High Tc; if only one Tc input failed, additional Delta Tc Auxiliary channel Trip. CPC software generated sensor failure alarm if process exceeds high limits.	For in range failures: Sensor input cross channel comparison, possible DNBR trip/pre-trip, NI-Delta T power deviation alarm. Possible aux trip possible sensor failure alarm	Single PPS channel trip Three-channel redundancy	DNBR /LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	

APRI400 DCD TIER 2

Table 7.2-7 (15 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-2	Analog Input Cold Leg Temperature (Continued)	c) Low level signal (out of range)	Sensor Failure	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC sensor failure indication and Channel Trouble OM and MTP indication, CPC Channel Trouble annunciation.	CPC Sensor Failure indication/annunciation, Increase in Delta T power, DNBR/LPD Channel Auxiliary Trip sensor input cross channel comparison CPC trouble indication / annunciation	Single PPS channel trip Three-channel redundancy	DNBR /LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed
		d) Low level signal (in range)	Sensor Failure	For in range failures: possible Auxiliary Trip (DNBR/LPD) on low Tc. If only one Tc input failed, additional Delta Tc auxiliary channels Trip. Increase in Delta T power. Possible NI-Delta T power deviation alarm. CPC software – generated sensor failure alarm if process exceeds low range limits.	For in range failures: Sensor input cross-channel comparison, possible DNBR Trip/pre-trip, NI-Delta T power deviation alarm. Possible aux. trip Possible sensor failure alarm	Single PPS channel trip Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.

7.2-57

APR1400 DCD TIER 2

Table 7.2-7 (16 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-3	Reactor Coolant Pump Flow	a) Low Pulse Rate Input, Loss of transmission (out of range)	Power Supply or pulse amplifier failure	Out of range interpreted as low flow. DNBR/LPD channel trip on Low Flow.	DNBR/LPD Channel trip Sensor input cross channel comparison	Single PPS channel trip Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) Low Pulse Rate Input (in range)	Power Supply or pulse amplifier failure	Decrease in thermal power. Change in calculated DNBR. Possible NI-Delta T Power deviation alarm.	Sensor cross channel comparison Possible NI-Delta T Power deviation alarm	Three-channel redundancy	For in range failures not resulting in a channel trip, RPS logic is converted to 2-out-of-2 coincidence logic.	
		c) High Pulse Rate Input (out of range)	Pulse amplifier failure	DNBR/LPD channel Trip on Low Flow. Excessively high Speed input exceeding module range limit interpreted as error.	DNBR/LPD channel Trip Sensor input cross channel comparison. CPCS sensor failure indication and annunciation	Single PPS channel trip Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	
		d) High Pulse Rate Input (in range)	Pulse amplifier failure	Increase in thermal power. Change in calculated DNBR. Possible NI-Delta T power deviation alarm.	Sensor cross channel comparison Possible NI-Delta T power deviation alarm	Three-channel redundancy	For in range failures not resulting in a channel trip, RPS logic is converted to 2-out-of-2 coincidence logic.	

7.2-58

APRI400 DCD TIER 2

Table 7.2-7 (17 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-4	Non-target CEA Position	a) Low level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction	Erroneous input to one of 2 CEACs in all four CPC channels. CEAC Sensor fail indication for out of range or rate of change failures. If more than three CEAs are affected, likely CEAC Fail condition. If failure occurs slowly, and multiple CEAs are affected, may get large PF to all operable CPC channels, causing a reactor trip.	CEAC sensor failure indication/annunciation. CEA Position display depiction CPC DNBR/LPD channel trips unlikely, but possible on slowly developing failure	Normally, no PF or trip on sensor failure. If failure is slow to develop, and is not recognized by CEAC as a sensor failure until after out of range, PF could occur. On excessive number of failures (as in the loss of RSPT power), a CEAC Fail condition occurs.	If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS. CEAC uses last valid position of the sensor in calculations. RPS remains in 2-out-of-3 coincidence logic. If sensor failure is not recognized by CEAC prior to sensor going out of range, reactor trip may occur on CEAC PF. Multiple CEA failures can cause CEAC Fail. CPC then selects last valid PF from failed CEAC, or current PF from operable CPC, whichever is larger. RPS logic is converted to a 2-out-of-2 coincidence logic on a channel trip.	

APR1400 DCD TIER 2

Table 7.2-7 (18 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-4	Non-target CEA Position (Continued)	b) Low level signal caused by 12 finger CEA failure (in range)	Shorted resistor, failed reed switches, power supply malfunction.	For in range failures, erroneous input to one of 2 CEACs in all four CPC channels. All channel DNBR and LPD trips due to subgroup deviation PFs unless sensor failure indication exists for out-of-range or rate of change failures.	All channel DNBR/LPD trips are possible for 12 finger CEAs Single PPS trip in the corresponding channel due to the PF and subgroup deviation alarm in the other channels for 4 finger CEAs RSPT input cross channel comparison within each channel	Normally, no PF or trip on sensor failure. If failure is slow to develop, and is not recognized by CEAC as a sensor failure with rate of change, PFs could occur. On excessive number of failures (as in the loss of RSPT power), a CEAC Fail condition occurs.	Plant is shutdown due to the DNBR and LPD trip for 12 finger CEAs. Single channel PPS trip for 4 finger CEAs and RPS logic is converted to a 1-out-of-2 coincidence logic on a channel trip. The RPCB flag may be set, to prevent the Plant shutdown.	
		c) Low level signal caused by 4 finger CEA failure (in range)	Shorted resistor, failed reed switches, power supply malfunction.	Subgroup deviation alarm occurs in all channels.	Subgroup deviation alarm occurs in all channels RSPT input cross channel comparison within each channel	Normally, no PF or trip on 4 finger CEA sensor failure. On excessive number of failures (as in the loss of RSPT power), a CEAC Fail condition occurs.	Normally, no PF or trip on 4 finger CEA sensor failure.	

Table 7.2-7 (19 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-4	Non-target CEA Position (Continued)	d) High level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction	Erroneous input to one of two CEACs in all four channels. CEAC sensor fail and channel trouble indication for out of range or deviation from normal change rate. If more than four CEAs are affected, likely CEAC fail condition. In case that the failure proceeds slowly and many CEAs are affected, the operating CPC receives a large PF and generates reactor trip.	CEAC sensor failure indication/annunciation on OM and MTP. CEA position display depiction CPCS channel trip unlikely, but possible on slowly developing failure from erroneous PF calculation	Sensor failure does not cause PF or trip. Until the range is deviated during the failure is developing slowly, the PF can be generated if not acknowledged as sensor failure by CEAC. On excessive number of failures (as in the loss of RSPT power), a CEAC fail condition occurs.	If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS. CEAC uses last valid position of the sensor in its calculations. RPS remains in 2-out-of-3 coincidence logic. If sensor failure is not recognized by CEAC prior to sensor going out of range, reactor trip may occur on CEAC PF. Multiple CEA failures can cause CEAC failure. CPC then selects last valid PF from failed CEAC, or current PF from operable CPC, whichever is larger. RPS logic is converted to a 2-out-of-2 coincidence logic on a channel trip.	.

Table 7.2-7 (20 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-4	Non-target CEA Position (Continued)	e) High level signal caused by failure (in range)	Shorted resistor, failed reed switches, power supply malfunction.	For in range failures, erroneous input to one of two CEACs in all four CPC channels. All channel DNBR and LPD trips due to subgroup deviation PFs unless sensor failure indication exists for out of range or rate of change failures.	All channel DNBR/LPD trips occur.	Normally, no PF or trip on sensor failure. If failure is slow to develop, and is not recognized by CEAC as a sensor failure with rate of change, subgroup deviation PFs could occur. On excessive number of failures (as in the loss of RSPT power), a CEAC Fail condition occurs.	Plant is shutdown due to the DNBR and LPD trip.	.

Table 7.2-7 (21 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-5	Target CEA position	a) Low level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction.	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC sensor failure indication and Channel Trouble OM indication, CPC Channel Trouble annunciation.	CPC sensor failure indication/ annunciation, DNBR/LPD channel trip	Single PPS channel trip Three-channel redundancy	RPS logic for function is converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) Low level signal caused by failure (in range)	Shorted resistor, failed reed switches, power supply malfunction.	For in range failures, CPC Channel Trip on DNBR and LPD due to subgroup deviation/PFs; CPC sensor failure indication/ annunciation. Affected CEAC also indicates sensor out of range, and respond as in the non-target CEA failure.	DNBR/LPD channel trips are possible. The RPCB flag is set, and a CWP generated. RSPT input cross channel comparison within each channel	Single PPS channel trip Three-channel redundancy	RPS logic for function is converted to 1-out-of-2 coincidence logic.	
		c) High level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction.	For failures beyond input module range limits: DNBR/LPD Channel Auxiliary Trip on sensor out of range failure; CPC sensor failure indication and Channel Trouble OM indication, CPC Channel Trouble annunciation.	CPC sensor failure indication/ annunciation, DNBR/LPD channel trip.	Single PPS channel trip Three-channel redundancy	RPS logic for function is converted to 1-out-of-2 coincidence logic.	
		d) Low level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction.	CPC Channel Trip on DNBR and LPD due to subgroup deviation/PFs only if group is inserted and is not the lead group. Possible sensor failure indication / annunciation.	RSPT cross channel comparison within each channel.	Three-channel redundancy	If no DNBR/LPD channel trip occurs, RPS logic for function is converted to 2-out-of-2 coincidence logic.	

Table 7.2-7 (22 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-6	CEA Calculator (CEAC)	a) Loss of data output	Loss of AC power, input/output failure, data link failure, logic or memory device failure	Loss of CEAC position indication	Annunciation on OM of CPC	Two channel redundancy	None	CPC uses input data from other CEAC and annunciates the failure. CPC compares data from two CEAC and generates alarm.
		b) Erroneous data output	CEA position sensor failure, input/output failure, data link failure, calculation, logic or memory device failure	Erroneous calculation value, DNBR or LPD trip possible	Annunciation on OM of CPC. CEA position indication comparison, same variable comparison in OM	CPC uses the conservative value in the two CEAC values.	DNBR or LPD trip possible	
2-7	Core Protection Calculator (CPC)	a) Tripped	Loss of AC power, input/output failure, logic or memory device failure, sensor failure	Loss of control panel control, erroneous calculation result	PPS alarm for channel trip, comparison of three channels, alarm of monitoring timer	Single RPS channel trip Three-channel redundancy logic	The RPS trip logic for DNBR/LPD, CWP is converted to 1-out-of-2 coincidence	Computer stops sequentially on AC power failure. To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.

Table 7.2-7 (23 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-7	Core Protection Calculator (CPC)	b) Stays in untripped state	Input/output failure, logic or memory device failure, sensor failure	Erroneous calculation result	Comparison of three channels, alarm of monitoring timer	Three-channel redundancy	The RPS trip logic for DNBR/LPD, CWP is converted to 2-out-of-2 coincidence logic.	Computer stops sequentially on AC power failure. To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
2-8	CEA withdrawal Prohibit logic (CWP)	a) The contact of CWP from CPC open due to failure	Open circuit, mechanical damage, contact corrosion	CWP contact open, unnecessary CWP channel trip	Visually indication	Three-channel redundancy	No effect on RPS channel trip logic. CWP logic is converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) CWP contact from CPC closed due to failure	Contact fixation	No CWP signal generated when CWP generation situation occurs.	Periodic test, DNBR/LPD pre-trip without any channel A CWP command	Three-channel redundancy	No effect on RPS channel trip logic. CWP logic is converted to 2-out-of-2 coincidence logic.	
		c) Discrete input ON (Untripped)	Contact failure	Bistable Logic not tripped	Periodic test	Three-channel redundancy	Coincidence logic is converted to 2-out-of-2 coincidence logic for the affected variable.	
		d) Discrete input OFF (tripped)	Contact failure, open cable	Bistable Logic tripped	Comparison logic trip alarm, comparison trip indication in cabinet and MCR	Initiated when tripped for the same variable in another channel.	Coincidence logic is converted to 1-out-of-2 coincidence logic for the affected variable.	

Table 7.2-7 (24 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-9	CPC Digital Output (DO) Module	DO module failure	Failures resulting in I/O Diagnostics indicating module failure	CPC WDT timeout. DNBR/LPD channel trips and pre-trips, CWP, "CPC Fail" annunciation	DNBR/LPD channel trip/pre-trip CPC Fail annunciators and indication at OM/MTP CPC Trouble indication at OM/MTP Diagnostics indicate DO module failure. Local DO Module Fault lamp on, green Run lamp off	Single PPS channel trip Three-channel redundancy	RPS logic for function is converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed. Module failures are monitored and cause CPC WDT timeouts.
2-10	CPC Processor Module (PM)	a) OFF; processor off. Failure of either the processor or communication section	Loss of module power; software execution stops	Watchdog timer timeout, DNBR and LPD trip/pre-trip/CWP output contact opening. Also CPC Fail OM/MTP indication.	Channel DNBR/LPD channel trip and pre-trip, CWP, also CPC Fail, annunciation CPC trouble indication on OM/MTP CPC processor fault lamp on, green Run lamp out	Single PPS channel trip Three-channel redundancy	The RPS logic is converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) ON; Processor running, CPC fails to trip for a bona fide trip condition.	Erroneous inputs, improper addressable constant, Unrecognized hardware or software malfunction.	Change in DNBR/LPD margin indication value of QIAS-N and IPS.	Four channel comparison DNBR/LPD margin indication of QIAS-N and IPS	Three-channel redundancy	The RPS logic is converted to 2-out-of-2 coincidence logic (assuming no channel trip)	

Table 7.2-7 (25 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-11	Aux CPC Processor Module (PM)	a) OFF; processor off	Loss of module power; software execution stops	Aux CPC Watchdog timer timeout input to CPC Processor to make Channel Trouble annunciation. OM/MTP monitors heartbeat, forcing OM/MTP Channel Trouble indication. Loss of trip buffer report and failed sensor array data.	Channel Trouble annunciation and indication on the OM/MTP Aux CPC processor Fault lamp on, green run lamp out	Aux CPC does not perform a safety function. No effect on PPS. No compensating provisions required.	None	CPC channel is operable with a failed Aux CPC processor. However, channel trip buffer report and failed sensor data are unavailable.
		b) ON; processor on	Unrecognized hardware or software malfunction.	Improper trip buffer data, failed sensor data, depending on failure.	After four-channel comparison of operating trip buffer data and failed sensor data, a normal condition is indicated.	Aux CPC does not perform a safety function. No effect on PPS. No compensating provisions required.	None	

7.2-67

APR1400 DCD TIER 2

Table 7.2-7 (26 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-12	CEAC 1 Processor Module (PM) Processor Section	a) OFF; processor off	Loss of module power; software execution stops	CEAC 1 Watchdog timer timeout, CEAC 1 Fail indication on OM/MTP. Channel Trouble indication / annunciation. CEAC 1 Fail flag to CPC in the same channel.	CEAC 1 Fail indication on OM/MTP Channel Trouble indication /annunciation CEAC 1 processor Fault lamp on, green run lamp out	Two redundant CEACs in each channel.	Affected CPC uses the last valid PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger. If the other CEAC is failed/declared inoperable/or in test, a large pre-assigned PF is assumed in that CPC.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Processor running, CEAC fails to detect proper CEA position, or otherwise fails to produce desired results.	Erroneous inputs, unrecognized hardware or software malfunction;	Possible inconsistency in CEA position with respect to other CEAC/pulse count. Failure to properly indicate CEA motion.	Cross channel comparison of CEA position	Two redundant CEACs in each channel.	Affected CPC uses the higher of the PFs from the two CEACs in the affected channel. CEAC 1 is the preferred source of Target CEA position to the CPC. If target CEA position is improper, could get improper channel response to a valid subgroup deviation or groups out of sequence. If so, only one CPC channel is affected. RPS logic is converted to a 2-out-of-2 coincidence logic.	To restore the PPS logic to 2-out-of-3 coincidence, the bypassed channel is returned to operation and the failed channels are bypassed. Note that on line diagnostics identify problems in CEAC module and generate CEAC failure.

APR1400 DCD TIER 2

Table 7.2-7 (27 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-13	CEAC 2 Processor Module (PM) Processor Section	a) OFF; processor off	Loss of module power; software execution stops	CEAC 2 Watchdog timer timeout, CEAC 2 Fail indication on OM/MTP. Channel Trouble annunciation. CEAC 2 Fail flag to CPC in the same channel.	CEAC 2 Fail indication on OM/MTP Channel Trouble annunciation CEAC 2 processor fault lamp on, green run lamp out	Two redundant CEACs in each channel.	Affected CPC uses the last valid PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger. If other CEAC is failed/declared inoperable/or in test, a large pre-assigned PF is assumed in that CPC.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Processor running, CEAC fails to detect proper CEA position, or otherwise fails to produce desired results.	Unrecognized hardware or software malfunction	Possible inconsistency in CEA position with respect to other CEAC/pulse count. Failure to properly indicate CEA motion.	Cross channel comparison of CEA position	Two redundant CEACs in each channel.	Affected CPC uses the higher of the PFs from the two CEACs in the affected channel. CEAC 2 is the alternate source of Target CEA position to the CPC. Therefore, Target CEA position errors are not passed on to CPC unless CEAC 1 is also inoperable.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3. After on-line diagnostic function is performed and the problem within CEAC module is identified, CEAC fail condition is generated.

Table 7.2-7 (28 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-14	CEA Position Processor 1 in Channels A or B. Processor and/or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	<p>CPP1 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation.</p> <p>Loss of alternate source of RSPT 1 CEA position transmission to CEAC 1 in all four channels.</p> <p>Loss of preferred source of Target CEA position in channel of origin.</p> <p>Loss of receive ports for alternate CEA position to CEAC 1.</p>	<p>CPP Trouble OM/MTP indication, Channel Trouble annunciation in all four channels and Channel Trouble indication on OM/MTP in all 4 channels due to loss of 1 of 2 redundant sources of CEA position input</p> <p>Run lamp out on affected CPP</p> <p>Diagnostics identify loss of SDL input to CPC.</p> <p>WDT in the affected CPP provide failure to CPC</p>	<p>CPPs 1 and 2 are redundant in each channel.</p> <p>CPP 2 in channels A and B is preferred source of CEAC 1 CEA position in all channels, and alternate source of Target CEA position.</p>	<p>None.</p> <p>CEAC 1 in all channels normally receives CEA position from CPP2.</p> <p>Target CEA position input in affected channel is switched from the CEAC 1 to CPC SDL to the CEAC 2 to CPC SDL.</p> <p>Loss of CPP 1 receives ports in channels A and B disables the alternate source of SDL input to CEAC 1.</p> <p>This has no effect on CEAC 1 since the preferred SDL input is directly to the CEAC processor receive port.</p>	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Erroneous CEA position transmitted	Un-recognized hardware or software malfunction	<p>Failure to provide proper alternate source of CEA position in CEAC 1 in all channels.</p> <p>Possible failure of preferred source of target CEA position transmission in channel of origin</p>	<p>Possible erroneous target CEA position indication</p> <p>If problem is due to processor failure, this is detected by on line diagnostics and a CPP Trouble/CPP WDT time out.</p>	<p>CPP1 is alternate source for CEAC 1 position indication, and is normally not selected.</p> <p>CPP1 is preferred source of Target CEA position, and Target CEA position may be improper in one CPC channel.</p> <p>3 channel redundancy.</p>	<p>None.</p> <p>If Target CEA position is improper, one CPC channel is inoperable, and RPS logic is in 2-out-of-2 coincidence logic.</p>	To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed

Table 7.2-7 (29 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-15	CEA Position Processor 2 in Channels C or D Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops	<p>CPP 2 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation.</p> <p>Loss of alternate source of RSPT 2 CEA position transmission to CEAC 2 in all four channels.</p> <p>Loss of alternate source of Target CEA position in channel of origin.</p> <p>Loss of receive ports for alternate CEA position to CEAC 2.</p>	<p>CPP Trouble OM/MTP indication in affected channel, Channel Trouble annunciation in all four channels and Channel Trouble indication on OM/MTP in all 4 channels due to loss of 1 of 2 redundant sources of CEA position input</p> <p>Run 2 lamp out on affected CPP</p> <p>Diagnostics identify loss of SDL input to CPC.</p> <p>WDT in the affected CPP provide failure to CPC</p>	<p>CPPs 1 and 2 are redundant in each channel.</p> <p>CPP 2 in channels C and D is alternate source of CEAC 2 CEA position in all channels, and alternate source of Target CEA position.</p>	<p>None.</p> <p>CEAC2 in all channels normally receives CEA position from CPP1.</p> <p>Similarly, CPP 1 provides preferred source of target CEA position in the affected channel. These are unaffected by a failure of CPP 2.</p> <p>Loss of CPP 2 receive ports in channels C and D disables the alternate source of SDL input to CEAC 2.</p> <p>This has no effect on CEAC 2 since the preferred SDL input is directly to the CEAC processor receive port.</p>	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.

Table 7.2-7 (30 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-15	CEA Position Processor 2 in Channels C or D Processor and/ or communication section. (Continued)	b) ON; Erroneous CEA position transmitted, but processor remains functional.	Unrecognized hardware or software malfunction	Failure to provide proper alternate source of CEA position in CEAC 2 in all channels Improper alternate source of target CEA position in channel of origin	If problem is due to processor failure, this is detected by on line diagnostics and a CPP trouble/CPP WDT timeout.	CPPs 1 and 2 are redundant in each channel. CPP 2 in channels C and D is alternate source of CEAC 2 CEA position in all channels, and alternate source of Target CEA position.	None. CEAC2 in all channels normally receives CEA position from CPP1. Similarly, CPP1 provides preferred source of target CEA position in the affected channel. These are unaffected by a failure of CPP2. Loss of CPP 2 receive ports in channels C and D disables the alternate source of SDL input to CEAC 2. This has no effect on CEAC 2 since the preferred SDL input is directly to the CEAC processor receive port.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.

Table 7.2-7 (31 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-16	One CEAC to CPC High Speed Link in a CPC channel	Loss of one SDL	Mechanical failure, loss of fiber optic modem power, damage to link	<p>SDL diagnostics indicate SDL failure, Channel Trouble indication on OM/MTP, Trouble annunciation</p> <p>CPC uses last valid PF from inoperable CEAC versus current PF from operable CEAC.</p> <p>Target CEA position sent to CPC over remaining link</p>	<p>Channel trouble indicated on OM/MTP in affected channel(s)</p> <p>Diagnostics identify nature of failure.</p>	<p>Redundant CEAC to CPC SDL provides PFs and Target CEA position input.</p> <p>One channel has one inoperable CEAC.</p> <p>All others channels fully operable.</p>	<p>One channel has one inoperable CEAC.</p> <p>Other channels fully operable.</p> <p>RPS remains in 2-out-of-3 coincidence logic.</p>	Operation with one failed CEAC in one or more channels addressed by LCO 3.3.3.
2-17	Both CEAC to CPC High Speed Links in a CPC channel	Loss of both SDL	Mechanical failure, loss of fiber optic modem power, damage to link	<p>SDL diagnostics indicate SDL failure, Channel Trouble indication on OM/MTP, Trouble annunciation</p> <p>Both CEACs fail. CPC uses pre-assigned PF on loss of both CEACs.</p> <p>Likely channel trip if at high power levels</p> <p>If SDL failure also causes loss of target CEA position transmission, CPC Fail and DNBR/LPD channel trip occurs.</p>	<p>CPC Fail indicated on OM/MTP in affected channel(s)</p> <p>Diagnostics identify nature of failure</p> <p>Channel trip (DNBR/LPD trip/pre-trip/CWP) likely</p>	<p>On loss of both CEACs, CPC channel uses pre-assigned penalty.</p> <p>Trip likely at high power levels.</p> <p>Loss of Target CEA position input causes aux trip (DNBR/LPD)</p> <p>Three channel redundancy in PPS</p>	<p>One channel has two inoperable CEACs. Likely channel trip.</p> <p>RPS is converted to 1-out-of-2 coincidence logic.</p>	To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed.

Table 7.2-7 (32 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-18	Loss of all SDL within a single CPC channel	Off, no transmission	loss of fiber optic modem power	<p>Channel trouble indication on OM/MTP in receiving channels</p> <p>DNBR/LPD trip in failed channel due to loss of target CEA position</p> <p>CPC Fail indicated at OM/MTP</p> <p>Failure of one CEAC in other operable CPC channels</p>	<p>SDL include diagnostics to detect failures by receiving processor.</p> <p>Channel Trouble indicated on OM/MTP in receiving channel(s)</p> <p>One CEAC failed in other channels.</p> <p>Both CEACs failed in inoperable channel DNBR/LPD trips in failed channel.</p> <p>CPC Fail indication on OM/MTP</p> <p>Diagnostics in receiving processors identify nature of failure</p>	<p>Two CEACs per operable CPC channel.</p> <p>Other CEAC remains operable.</p> <p>CPC uses last valid PF from failed CEAC or current PF from operable CEAC, whichever is larger.</p> <p>One CPC channel in trip, three channel redundancy</p>	<p>One CEAC Failed in all operable CPC channels, and one CPC channel in trip (RPS in a 1-out-of-2 coincidence logic).</p> <p>Other CPC channels remain operable with one CEAC in each channel.</p>	<p>Operation with a single CEAC failure in one or more channels addressed in LCO .3.3.3.</p> <p>To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed.</p>

7.2-74

APR1400 DCD TIER 2

Table 7.2-7 (33 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
3	Analog Input Module (PPS BP Rack)	a) Failure of microprocessor common to all analog input channels	Component failure	Scan and processing of analog input channels stop Process measurements for analog bistables are tagged as bad quality by BP	AI diagnostic alarms are activated; comparisons of signals between BPs and between channels (performed by IPS) detect and alarm differences.	BP signal selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Failure of analog portion common to all input channels	Component failure	Digitized values for all the AI channels may not be representative of the process. It could result in the partial trip occurring early, late, at setpoint or not at all.	Comparisons of signals between BPs and between channels (performed by IPS) detect and alarm differences	Coincidence needs at least two safety channels to have the same process partial trip. An early partial trip does not result in coincidence. A late trip has no affect since coincidence already exists. BP selection logic in all the LCLs performs a logical OR of data from the redundant BPs in each of safety channels. This addresses the AI module input failure resulting in the BP not generating a partial trip.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

7.2-75

APR1400 DCD TIER 2

Table 7.2-7 (34 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
3	Analog Input Module (PPS BP Rack)	c) Single channel fails out of range high or low	Component failure	Channel value set to range limit; with bad quality	AI module diagnostic alarms are activated; comparisons of signals between BPs and between channels (performed by IPS) detect and alarm differences	Partial trip/actuation selection logic in all LCLs uses quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		d) Failure of BIOB interfaces	Component failure	BP notes lack of response from input module and flags all channels as BAD quality.	AI module diagnostic alarms are activated; comparisons of signals between BPs and between channels (performed by IPS) detect and alarm differences	BP signal selection logic in all the LCLs uses the quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		e) Single channel experience calibration shift or becomes noisy.	Component failure	Could result in the PM partial trip occurring early, late or not at all. If failure causes the analog value to go out range, high or low, see "Single channel out of range, high or low" failure above.	Comparisons of signals between BPs and between channels (performed by IPS) detect and alarm differences	Coincidence needs at least two safety channels to have the same process partial trip. An early partial trip does not result in coincidence. A late trip has no affect since coincidence already exists. BP signal selection logic in all the LCLs performs a logical OR of data from the redundant BPs in each of safety channels. This addresses the AI module input failure resulting in the BP not generating a partial trip.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

7.2-76

APR1400 DCD TIER 2

Table 7.2-7 (35 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
4	Digital Input Module (PPS BP Rack)	a) Entire module (common portion) fails.	Component failure	BP sets bad quality on all affected input signals based on detected failure of module to respond to I/O read. Digital inputs for function enable switch position, setpoint reset switch, operating bypass switch, and trip channel bypass switch from MTP switch panel are lost.	Detected I/O module failure results in BP activating a diagnostic alarm	CPCS trip inputs and ENFMS trouble (generates Lo DNBR and HI LPD trips) are provided by the digital input modules. BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Single channel fails ON (normal, un-tripped state).	Component failure	The affected channel cannot enter trip state.	Inability to trip is detected by Periodic test	BP signal selection logic in all the LCLs performs logical OR of the partial trip data from the redundant BPs of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		c) Single channel fails OFF (tripped state).	Component failure	BP generates partial trip for failed single channel. Coincidence occurs on next safety channel becoming tripped for this bistable.	ITP detects discrepancy between BP processors and alarms.	LCL voting needs 2 safety channels to be tripped for coincidence. A manual partial bypass can be entered for the failed input channel.	No loss of safety function Coincidence changes from 2-out-of-3 logic to 1-out-of-2 logic. If manual partial bypass entered, coincidence changes from 1-out-of-2 logic to 2-out-of-3 logic.	N/A

7.2-77

APRI400 DCD TIER 2

Table 7.2-7 (36 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
5	Bistable Processor Module (PPS BP Rack)	a) Processing section fails to execute program instructions.	Component failure	Affected BP halts. No periodic updates transmitted to SDL and SDN from affected BP	Lack of BP processor updates detected by MTP/ITP via SDN Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs uses quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Application program memory failure	Component failure	Affected BP halts. No periodic updates transmitted to SDL and SDN from affected PM	CRC checks performed on memory. Lack of BP processor updates detected by MTP/ITP via SDN Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs uses quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		c) Processing section fails to scan input/output modules.	Component failure	BP inputs (process values, CPC trips, ENFMS permissives) not updated periodically. BP outputs (SOE points) are not updated periodically. Calculated bistable outputs are set to Bad quality.	Corrupted I/O bus cycles are detected. Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs uses quality data from the redundant BP in affected channel. SOE points are provided by redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (37 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
5	Bistable Processor Module (PPS BP Rack)	d) Processing section fails to read from communication section.	Component failure	No periodic updates received from SDL by affected BP Op Bypass and Variable Setpoint (VSP) reset request data from MCR-CPM and RSR-CPM via SDL are lost to the BP bistable logic. Lack of CS/PS handshaking causes affected processor to halt. No periodic updates transmitted to SDL and SDN from affected PM	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of BP processor updates detected by LCL via SDL Lack of BP processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		e) Processor section fails to write to communication section.	Component failure	No periodic updates transmitted to SDL from affected BP	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		f) Communication section fails to receive SDL.	Component failure	No periodic updates received from SDL by affected PM Op Bypass and VSP reset request data from MCR-CPM and RSR-CPM via SDL are lost to the BP bistable logic.	Lack of CPM processor updates detected by BP via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (38 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
5	Bistable Processor Module (PPS BP Rack) (Continued)	g) Communication section fails to transmit SDL.	Component failure	No periodic updates transmitted to SDL from affected PM	Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		h) General failure of communication section	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN No periodic updates received from SDL by affected PM Op Bypass and VSP reset request data from MCR-CPM and RSR-CPM via SDL are lost to the BP bistable logic.	PS detects lack of live signal handshaking and sets diagnostic alarm. Lack of BP processor updates detected by MTP/ITP via SDN Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		i) PM locks (permanently) the backplane input/output network (BIOB)	Component failure	Affected processor halts. All I/O functions are prevented including data exchange with SDN Communication Module.	Lack of BIOB activity detected by BP diagnostics Lack of BP processor updates detected by LCL via SDL Lack of BP processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (39 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
6	Fiber-optic SDL link to LCLs	Failure of fiber-optic modem	Component failure	BP periodic updates to one LCL via SDL do not get to the destination.	Lack of BP processor periodic updates detected by LCL SDL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
7	Fiber-optic SDL link from MCR-CPM or RSR-CPM	Failure of fiber-optic modem	Component failure	BP periodic updates of control switch status via SDL does not occur (only one location is active at a time) Loss of Operating Bypass and VSP Reset requests from SDL	Lack of CPM periodic updates is detected by BP via SDL Trouble alarm is actuated.	Coincidence logic requires at least two safety channels to have the same process partial trip. A partial trip due to inability to perform Operating Bypass or VSP Reset does not result in coincidence. MTP provides alternate capability to perform these functions.	No loss of safety function. Coincidence remains 2003 if no bistable partial trip occurs. If bistable partial trip occurs, coincidence changes to a 1-out-of-2 logic.	N/A
8	Failure of BP Process Station Backplane (PPS BP Rack)	Loss of power to one BP Station	Power Supply Wire termination failed.	LCL processors in four PPS safety channels connected to failed BP detect loss of periodic updates.	Lack of BP processor periodic updates detected by LCL SDL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (40 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
9	SDN Communication Module (PPS BP Rack)	a) Shared memory failure	Component failure	BP halts. No PM periodic updates to all LCLs via SDL and on SDN network	Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Back Plane failure	Component failure	BP halts. No PM periodic updates to all LCLs via SDL and on SDN network	Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		c) SDN interface failure	Component failure	BP halts. No PM periodic updates to all LCLs via SDL and on SDN network	Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		d) Microprocessor failure	Component failure	BP halts. No PM periodic updates to all LCLs via SDL and on SDN network	Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCL Trouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
				Data storm. Spurious data is sent to the receiving processors	Trip alarm is actuated.	Three-channel redundancy	Coincidence remains as 1-out-of-2 logic.	N/A

7.2-82

APR1400 DCD TIER 2

Table 7.2-7 (41 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
10	LCL processor performing RT function (PPS LCL Rack)	a) Processing section fails to execute program instructions.	Component failure	Affected LCL halts and the WDT contact opens. No periodic updates transmitted to SDN from affected PM No periodic updates received from SDL by affected PM	Lack of LCL processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Open WDT contact only affects one-half of the affected safety channel RT initiation circuit.	Open WDT contact trips one-half of the safety channel RT initiation circuit.	N/A
		b) Application program memory failure	Component failure	Affected LCL halts and the WDT contact opens. No periodic updates transmitted to SDN from affected PM No periodic updates received from SDL by affected PM	CRC checks performed on memory Lack of LCL processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Open WDT contact only affects one-half of the affected safety channel RT initiation circuit.	Open WDT contact trips one-half of the safety channel RT initiation circuit.	N/A
		c) Processing section fails to scan input/output modules.	Component failure	LCL outputs (reactor trips) not updated periodically Digital Output module sets outputs to default de-energized state.	Corrupted I/O bus cycles detected Trouble alarm is actuated.	Digital Output only affects one-half of the affected safety channel RT initiation circuit.	Digital Output trips one-half of the safety channel RT initiation circuit.	N/A

Table 7.2-7 (42 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
10	LCL processor performing RT function (PPS LCL Rack) (Continued)	d) Processing section fails to read from communication section.	Component failure	No periodic updates received from SDL by affected PM. Lack of CS/PS handshaking causes affected processor to halt and the WDT contact opens. No periodic updates transmitted to SDN from affected PM	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of LCL processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Open WDT contact only affects one-half of the affected safety channel RT initiation circuit.	Open WDT contact trips one-half of the safety channel RT initiation circuit.	N/A
		e) Processing section fails to write to communication section.	Component failure	SDL transmits are not provided by this processor.	CS detects lack of live signal handshaking and sets diagnostic alarm.	N/A	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		f) Communication section fails to receive SDL.	Component failure	No periodic updates received from SDL by affected PM	Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in ESF LCL and both RT LCLs of affected LCL process station use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		g) Communication section fails to transmit SDL.	Component failure	SDL transmits are not provided by this processor.	N/A	N/A	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (43 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
10	LCL processor performing RT function (PPS LCL Rack) (Continued)	h) General failure of communication section	Component failure	Affected processor halts and the WDT contact opens. No periodic updates transmitted to SDN from affected PM No periodic updates received from SDL by affected PM	PS detects lack of live signal handshaking and sets diagnostic alarm. Lack of LCL processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	Partial trip/actuation selection logic in ESF LCL and second RT LCL of affected LCL process station use quality data from the redundant BP in affected channel. Open WDT contact only affects one-half of the affected safety channel RT initiation circuit.	No loss of safety function Coincidence remains as 2-out-of-3 logic. Open WDT contact trips one-half of the safety channel RT initiation circuit.	N/A
		i) PM locks (permanently) the BIOB.	Component failure	Affected processor halts and the WDT contact opens. RT initiation circuit associated with affected LCL station causes 1/2 leg trip. All I/O functions are prevented including data exchange with SDN Communication Module.	Lack of BIOB activity detected by PM diagnostics Lack of LCL processor updates detected by MTP/ITP via SDN Trouble alarm is actuated.	System level reactor trip provided by other three safety channels. Redundant LCL station available to provide RT function for affected channel.	No loss of safety function. Coincidence remains as 2-out-of-3 logic.	N/A
		j) WDT relay coil shorts when energized. WDT relay NO contact opens with coil energized.	Component failure Mechanical failure	RT initiation circuit associated with affected LCL station causes 1/2 leg trip due to WDT NO contact opening.	Trouble alarm is actuated.	System level reactor trip provided by other three safety channels. Redundant LCL station available to provide RT function for affected channel.	No loss of safety function. Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (44 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
10	LCL processor performing RT function (PPS LCL Rack) (Continued)	k) WDT relay NO contact does not open when coil required to de-energize.	Mechanical failure	WDT NO contact, one of three contacts in series forming one of the two half-leg trips of the RT initiation circuit associated with affected LCL station does not contribute to a 1/2 leg trip due to WDT NO contact not opening.	Trouble alarm is actuated.	System level reactor trip provided by other three safety channels. Redundant LCL station available to provide RT function for affected channel.	No loss of safety function. Coincidence remains as 2-out-of-3 logic.	N/A
11	LCL Processor Module performing ESF actuation function (PPS LCL Rack)	a) Processing section fails to execute program instructions.	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM Partial actuation data to one ESFCCS GC is lost. No periodic updates received from SDL by affected PM	Lack of LCL processor updates detected by MTP/ITP via SDN Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Application program memory failure	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM Partial actuation data to one ESF-CCS GC is lost No periodic updates received from SDL by affected PM	CRC checks performed on memory Lack of LCL processor updates detected by MTP/ITP via SDN Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (45 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
11	LCL Processor Module performing ESF actuation function (PPS LCL Rack) (Continued)	c) Processing section fails to scan input/output modules.	Component failure	LCL outputs not updated periodically.	Corrupted I/O bus cycles detected Trouble alarm is actuated.	N/A	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		d) Processing section fails to read from communication section.	Component failure	No periodic updates received from SDL by affected PM Lack of CS/PS handshaking causes affected processor to halt No periodic updates transmitted to SDL and SDN from affected PM Partial actuation data to one ESF-CCS GC is lost	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of LCL processor updates detected by MTP/ITP via SDN Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		e) Processing section fails to write to communication section.	Component failure	No periodic updates transmitted to SDL from affected PM Partial actuation data to one ESF-CCS GC is lost.	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	No loss of safety function occurs Coincidence remains as 2-out-of-3 logic.	

7.2-87

APRI400 DCD TIER 2

Table 7.2-7 (46 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
11	LCL Processor Module performing ESF actuation function (PPS LCL Rack) (Continued)	f) Communicati on section fails to receive SDL.	Component failure	No periodic updates received from SDL by affected PM Partial trip/actuation data from two BPs (each from a separate channel) via SDL are lost to the LCL voting logic.	Lack of BP processor updates detected by LCL via SDL Trouble alarm is actuated.	Partial trip/actuation selection logic in ESF LCL and both RT LCLs of affected LCL process station use quality data from the redundant BP in affected channel.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		g) Communicati on section fails to transmit SDL.	Component failure	No periodic updates transmitted to SDL from affected PM Partial actuation data to one ESF-CCS GC is lost.	Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	No loss of safety function occurs Coincidence remains as 2-out-of-3 logic.	N/A
		h) General failure of communicati on section	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM Partial actuation data to one ESF-CCS GC is lost. No periodic updates received from SDL by affected PM	PS detects lack of live signal handshaking and sets diagnostic alarm. Lack of LCL processor updates detected by MTP/ITP via SDN Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	No loss of safety function occurs Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (47 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
11	LCL Processor Module performing ESF actuation function (PPS LCL Rack) (Continued)	i) PM locks (permanently) the BIOB.	Component failure	Affected processor halts. All I/O functions are prevented including data exchange with SDN Communication Module.	Lack of BIOB activity detected by PM diagnostics Lack of LCL processor updates detected by MTP/ITP via SDN Lack of LCL processor updates detected by ESF-CCS GC via SDL Trouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
12	SDN Communication Module (PPS LCL Rack)	a) Shared memory failure	Component failure	All affected LCL station processors halts and the WDT times out. All I/O functions are prevented, as is data exchange with SDN Communication Module. Affected LCL station causes half leg trip in the RT initiation circuit.	Diagnostic alarms actuated upon failure of normal I/O functions Lack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCS Lack of LCL station periodic updates on SDN network detected by MTP/ITP Trouble alarm is actuated.	Other safety channel cabinet RT initiation circuit half leg available to provide the safety channel RT function. ESFAS initiations for the safety channel with the affected LCL station will be received from the redundant LCL process station ESF PM.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (48 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
12	SDN Communication Module (PPS LCL Rack) (Continued)	b) BIOB ASIC failure	Component failure	<p>All affected LCL station processors halt and the WDT times out.</p> <p>All I/O functions are prevented, as is data exchange with SDN Communication Module.</p> <p>Affected LCL station causes half leg trip in the RT initiation circuit.</p>	<p>Diagnostic alarms actuated upon failure of normal I/O functions</p> <p>Lack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCS</p> <p>Lack of LCL station periodic updates on SDN network detected by MTP/ITP</p> <p>Trouble alarm is actuated.</p>	<p>Other safety channel cabinet RT initiation circuit half leg available to provide the safety channel RT function.</p> <p>ESFAS initiations for the safety channel with the affected LCL station will be received from the redundant LCL process station ESF PM.</p>	<p>No loss of safety function</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A
		c) SDN interface ASIC failure	Component failure	<p>All affected LCL station processors halt and the WDT times out.</p> <p>All I/O functions are prevented, as is data exchange with SDN Communication Module.</p> <p>Affected LCL station causes half leg trip in the RT initiation circuit.</p>	<p>Diagnostic alarms actuated upon failure of normal I/O functions</p> <p>Lack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCS.</p> <p>Lack of LCL processor periodic updates on SDN network detected by MTP/ITP</p> <p>Trouble alarm is actuated.</p>	<p>Other safety channel cabinet RT initiation circuit half leg available to provide the safety channel RT function.</p> <p>ESFAS initiations for the safety channel with the affected LCL station will be received from the redundant LCL process station ESF PM.</p>	<p>No loss of safety function</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A

Table 7.2-7 (49 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
12	SDN Communication Module (PPS LCL Rack) (Continued)	d) Microprocessor failure	Component failure	<p>All affected LCL station processors halt and the WDT times out.</p> <p>ESFAS initiation signals to GC is not updated via SDL for affected LCL process station.</p> <p>Affected LCL station causes half leg trip in the RT initiation circuit.</p>	<p>Diagnostic alarms actuated upon failure of normal I/O functions</p> <p>Lack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCS.</p> <p>Lack of LCL processor periodic updates on SDN network is detected by MTP/ITP.</p> <p>Trouble alarm is actuated.</p>	<p>Other safety channel cabinet RT initiation circuit half leg available to provide the safety channel RT function.</p> <p>ESFAS initiations for the safety channel with the affected LCL station will be received from the redundant LCL process station ESF PM.</p>	<p>No loss of safety function</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A

Table 7.2-7 (50 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
13	DO Relay Output Module	a) Channel (UV) contact does not open on command.	Component failure	Contact resistance remains near zero.	DO relay contacts are tested during surveillance test.	Reactor Trip via UV interposing relay provided through other 3 RT LCL processors and corresponding 3 DO Relay Output Modules.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		b) Channel (UV) contact spuriously opens.	Component failure	Causes loss of 1 of 2 voltages to UV interposing relay coil.	ITP detects change in voltage on the UV circuit; actuates diagnostic alarm.	UV interposing relay remains energized through RT initiation circuit leg in opposite cabinet.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A
		c) Common portion (BIOB) fails	Component failure	Upon lack of communication with PM the DO outputs are set to their default (de-energized) state. Affected LCL station causes half leg trip in the RT initiation circuit.	ITP detects difference in voltage on the UV half leg circuits; actuates diagnostic alarm.	The UV relay coils remains energized through RT initiation circuit leg in opposite cabinet.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (51 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
14	Fiber-optic SDL link to GC Process Stations	Failure of fiber-optic modem	Component failure	<p>Only failed fiber optic modem does not transmit ESF initiations, from the connected LCL ESF PM, to one of the four GCs.</p> <p>Other three fiber optic modems transmit initiations to their connected GC.</p>	GC detects loss of periodic updates and activates a diagnostic alarm.	<p>Redundant GC process station receives valid communications from LCL ESF PM in redundant LCL station in opposite safety channel cabinet.</p> <p>GC front end processing of PPS ESF initiations is a logical OR, hence a loss of a single input does not result in a loss of function.</p>	<p>No loss of safety function</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A
15	Failure of LCL Process Station Backplane	Loss of power to one LCL station	Power supply wire termination failed	<p>Contacts open on digital output modules removing one leg of the two powering both interposing relay coils for RT initiation for the safety channel SDL.</p> <p>The communication for ESFAS initiation to GC is lost.</p>	Safety Channel ITP detects loss of LCL periodic updates on SDN network and alarm.	<p>The digital output modules in the redundant LCL station of the safety channel continue to provide the power to the interposing relay coils for RT initiation in the cabinet with the failed LCL station as well as its own cabinet.</p> <p>The LCL ESF processor in the redundant LCL station of the safety channel continues to provide ESFAS initiations to the other ESF-CCS group controller.</p>	<p>No loss of safety function</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A

Table 7.2-7 (52 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
16	UV Relay (One/safety channel)	a) Open or shorted coil	Component failure	Energized UV relay drops out opening current path for TCB UV coil in safety channel TCB opens.	UV relay function is verified during routine surveillance test. ITP provides TCB position and UV relay contact status signals to MTP for PPS screen display.	When four safety channel TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	No loss of safety function Coincidence remains as 2-out-of-3 logic. The Safety Channel TCB UV coil is commanded to open.	N/A
		b) High resistance trip contact	Component failure	RT contact on UV relay does not close when coil energized. TCB remains open.	ITP provides breaker position and UV relay contact status signals to MTP for PPS screen display.	When four safety channel TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	No loss of safety function Coincidence remains as 2-out-of-3 logic. The safety channel TCB UV coil is commanded to operate.	N/A
		c) Welded trip contact	Component failure	RT Contact on UV relay does not open when coil de-energized. TCB UV coil keeps TCB closed.	UV relay function is verified during routine surveillance test.	When four safety channel TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	No loss of safety function Coincidence remains as 2-out-of-3 logic.	N/A

Table 7.2-7 (53 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
17	ITP Processor Module	a) Functional processor section fails to execute program instructions.	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM PPS status data from affected ITP are lost to the QIAS-N.	Lack of ITP processor updates detected by MTP via SDN Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels	No effect on PPS safety function PPS status data processed by ITP for indication not updated for affected channel. PPS status data transmitted to QIAS-N not updated for affected channel.	N/A
		b) Application program memory failure (mirror RAM)	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM PPS status data from affected ITP are lost to the QIAS-N.	CRC checks performed on memory Lack of ITP processor updates detected by MTP via SDN Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels	No effect on PPS safety function PPS status data processed by ITP for indication not updated for affected channel. PPS status data transmitted to QIAS-N not updated for affected channel.	N/A

Table 7.2-7 (54 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
17	ITP Processor Module (Continued)	c) Processor section fails to scan I/O modules.	Component failure	ITP inputs (PPS status, ENFMS test requests) not updated periodically. ITP outputs (ENFMS test permissive, MTP Panel indications) not updated periodically.	Corrupted I/O bus cycles detected Trouble alarm is actuated.	ENFMS test capability provided by other channels.	No effect on PPS safety function PPS status data processed by ITP for indication not updated for affected channel.	N/A
		d) Processor section fails to read from communication section.	Component failure	No periodic updates received from SDL by affected PM Lack of CS/PS handshaking causes affected processor to halt No periodic updates transmitted to SDL and SDN from affected PM PPS status data from affected ITP are lost to the QIAS-N.	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of ITP processor updates detected by MTP via SDN Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function PPS status data processed by ITP for indication not updated for affected channel. PPS status data transmitted to QIAS-N not updated for affected channel.	N/A
		e) Processor section fails to write to communication section.	Component failure	No periodic updates transmitted to SDL from affected PM PPS status data from affected ITP are lost to the QIAS-N.	CS detects lack of live signal handshaking and sets diagnostic alarm. Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function	N/A

Table 7.2-7 (55 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
17	ITP Processor Module (Continued)	f) Communication section fails to receive SDL.	Component failure	No periodic updates received from SDL by affected PM	Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function	N/A
		g) Communication section fails to transmit SDL.	Component failure	No periodic updates transmitted to SDL from affected PM PPS status data from affected ITP are lost to the QIAS-N.	Lack of ITP processor updates detected by other ITPs via SDL Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function	N/A
		h) General failure of communication section.	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM PPS status data from affected ITP are lost to the QIAS-N.	Lack of ITP processor updates detected by MTP via SDN Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function. PPS status data processed by ITP for indication not updated for affected channel. PPS status data transmitted to QIAS-N not updated for affected channel.	N/A

Table 7.2-7 (56 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
17	ITP Processor Module (Continued)	i) PM locks (permanently) the BIOB.	Component failure	Affected processor halts. No periodic updates transmitted to SDL and SDN from affected PM PPS status data from affected ITP are lost to the QIAS-N. All I/O functions are prevented including data exchange with SDN Communication module.	Lack of ITP processor updates detected by MTP via SDN Lack of ITP processor updates detected by QIAS-N via SDL Trouble alarm is actuated.	ITPs operating in three other safety channels.	No effect on PPS safety function. PPS status data processed by ITP for indication not updated for affected channel. PPS status data transmitted to QIAS-N not updated for affected channel.	N/A
18	ITP Fiber Optic Modem	Transmitter fails	Component failure	PPS status data transmitted to QIAS-N is not updated due to failed FOM for affected channel.	Lack of ITP processor updates, due to failed FOM in affected channel, detected by QIAS-N	None in ITP	No effect on PPS safety function.	N/A
19	MTP PC Node Box	General failure	Component failure	MTP display becomes “frozen” and does not update or respond to operator inputs; Communication on SDN and Ethernet link to IPS stops; Unable to modify setpoint values in BP or CPCS	ITP process station monitors MTP health via SDN network; activates diagnostic alarm on loss of periodic data update.	Data from the other three safety channels are available to the non-safety system. Data through the OM safety display still available.	No effect on PPS safety function. Data from this channel is not available to the IPS.	N/A

Table 7.2-7 (57 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
20	MTP SDN Communication Module	General failure	Component failure	MTP display reacts normally, but data from channel is stale.	ITP process station Monitors MTP health via SDN network; activates diagnostic alarm on loss of data update	Data from the other three safety channels are available to the IPS. Data through the QIAS-N is available. Display still available; affected module is repaired before surveillance testing or software maintenance can take place.	No effect on PPS safety function. Data from this channel is not available to the IPS. Surveillance testing or software maintenance not available.	N/A
				Data storm. Spurious data is sent to the receiving processors.	Periodic test	Function enable keyswitch	No effect on PPS safety function.	N/A
21	MTP Ethernet Adapter	General failure	Component failure	Loss of communication to the IPS	ITP process station monitors MTP health via SDN network; activates diagnostic alarm on loss of periodic update	Data from the other three safety channels are available to the system IPS.	No effect on PPS safety function. Data from this channel is not available to the IPS.	N/A
22	MTP Flat Panel Display	a) Degraded display	Component failure	Loss of raster line; ghost image (burn-in); display flicker	Technician notices degraded display when attempting to use MTP.	May be possible to use display depending on extent of failure.	No effect on PPS safety function.	N/A
		b) Total failure	Component failure	Dark display	Technician notices lack of display when attempting to use MTP.	The safety channel operator's module PPS screens are available to the operator.	No effect on PPS safety function. Repair is performed before PPS safety channel surveillance testing or software maintenance is available.	N/A

Table 7.2-7 (58 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
23	MTP Keyboard	Erratic key stroke data	Component failure	Spurious keystrokes or one key does not respond	Technician notices erratic behavior when attempting to use keyboard.	Not applicable	No effect on PPS safety function. Keyboard is not required for any safety function.	N/A
24	PPS Vital Bus Inverter	Off	Circuit Breaker feed for PPS safety channel opens.	Loss of PPS safety channel PPS safety channel signals reactor trip breaker to open. SDLs to ESF-CCS group controllers do not update.	LCL stations in other three safety channels provide alarm loss of SDL updates from PPS safety channel without power. ITP in safety channel does not provide alarm.	Three PPS safety channels remain operable. A complete reactor trip requires two breakers to open. ESF-CCS group controllers take default action.	No effect on PPS safety function. Coincidence changes from 2-out-of-3 logic to 1-out-of-2 logic for RPS and coincidence changes from 2-out-of-3 logic to 2-out-of-2 logic for ESFAS.	N/A
25	PPS Input Circuit Breaker	a) Breaker is ON: does not trip on overload.	Internal mechanical failure	Device causing overload fails.	If a mechanical problem exists, it may manifest itself when attempting to turn the breaker OFF.	Other protective devices are provided for downstream loads.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic. No loss of DC circuit functionality.	N/A
		b) Breaker OFF: cannot be turned ON.	Internal mechanical failure	Loss of PPS safety channel cabinet Reactor trip leg in cabinet is open. PPS cabinet SDLs to ESF-CCS group controllers and SDN network do not update.	LCL stations in other three safety channels provide alarm loss of SDL updates from PPS safety channel cabinet without power.	Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates. Redundant PPS safety channel cabinet providing all signals necessary for safety functions.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (59 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
26	PPS Surge Suppressor	Open circuit (failure to provide surge suppression)	Device burned open	<p>Loss of PPS safety channel cabinet</p> <p>PPS safety channel has 1-out-of-2 legs for reactor trip open.</p> <p>PPS cabinet SDLs to ESF-CCS group controllers and SDN network do not update.</p>	LCL stations in other three safety channels provide alarm loss of SDL updates from PPS safety channel cabinet without power.	<p>Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates.</p> <p>Redundant PPS safety channel cabinet providing all signals necessary for safety functions.</p>	<p>No effect on PPS safety function.</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A
27	PPS EMI Filter	a) Open (OFF); internal failure; short circuit	Device shorts internally	<p>Loss of PPS safety channel cabinet</p> <p>PPS safety channel has 1-out-of-2 legs for reactor trip open.</p> <p>PPS cabinet SDLs to ESF-CCS group controllers and SDN network do not update.</p>	LCL stations in other three safety channels provide alarm loss of SDL updates from PPS safety channel cabinet without power.	<p>Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates.</p> <p>Redundant PPS safety channel cabinet providing all signals necessary for safety functions.</p>	<p>No effect on PPS safety function.</p> <p>Coincidence remains as 2-out-of-3 logic.</p>	N/A
		b) Input to output short	Internal failure	System may act spuriously in the presence of noise introduced via the vital network.	Periodic surveillance measurements manifest defective EMI filter.	AC input rating of PS not exceeded.	<p>No effect on PPS safety function.</p> <p>No effect on the DC circuit functionality.</p>	N/A

7.2-101

APR1400 DCD TIER 2

Table 7.2-7 (60 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
28	PPS Cabinet power supplies:	Overvoltage	Component failure	Overvoltage device detects and removes voltage to the connected load. Lose BP and LCL stations. Results in safety channel half-leg reactor trip.	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	Second cabinet containing redundant BP and LCL stations in the safety channel provide signals for safety functions.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic. Affected safety channel has a half-leg reactor trip.	N/A
29	PPS I/O power supplies:	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic.	N/A
30	PPS Power supply auctioneering circuit applicable to 24 VDC power supplies:	a) Open diode	Overload component failure	One supply is not available to power the downstream components in the affected cabinet.	Annunciation – one of the auctioneered power supplies is offline.	The companion power supply/diode combination supplies power to the components receiving power from the supply.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic. No loss of DC circuit functionality.	N/A
		b) Shorted diode	Overload component failure	The voltage applied to the components in the cabinet is the same as the voltage at the supply terminals.	Periodic test	Each power supply in the auctioneered pair is capable of providing power to all of the components.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic. No loss of DC circuit functionality.	N/A

APR1400 DCD TIER 2

7.2-102

Table 7.2-7 (61 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
31	PPS Power supply auctioneering circuit applicable to 24 VDC cabinet power supply:	Overvoltage	Over voltage protection device operates when voltage is in range.	Overvoltage device detects and removes voltage to the connected load. Lose BP and LCL stations Results in safety channel half-leg reactor trip	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	Second cabinet containing redundant BP and LCL stations in the safety channel provide signals for safety functions.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic. Affected safety channel has a half-leg reactor trip.	N/A
32	PPS Power supply auctioneering circuit applicable to 24 VDC I/O power supply:	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	No effect on PPS safety function. Coincidence remains as 2-out-of-3 logic.	N/A
33	MTP / ITP Cabinet Input Circuit Breaker	a) Breaker is ON does not trip on overload.	Internal mechanical failure	Device causing overload fails. No loss of DC circuit functionality	If a mechanical problem exists, it may manifest itself when attempting to turn the breaker OFF.	Other protective devices are provided for downstream loads.	No loss of safety function	N/A
		b) Breaker OFF: cannot be turned ON.	Internal mechanical failure	Redundant power feed is not affected. No loss of DC circuit functionality	If a mechanical problem exists, it may manifest itself when attempting to turn the breaker ON.	Functionality maintained within the channel due to redundant power feed.	No loss of safety function	N/A

Table 7.2-7 (62 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
34	MTP / ITP Cabinet Surge Suppressor	Open circuit (failure to provide surge suppression).	Device burned open	If voltage surges are present on the vital bus power, spurious operation may result. No loss of DC circuit functionality.	Periodic test and/or periodic replacement	Other protective devices are provided for downstream loads.	No loss of safety function	N/A
35	MTP / ITP Cabinet EMI Filter	a) Open (OFF); internal failure; short circuit.	Series component failure	Redundant power feed is not affected. No effect on the circuit functionality.	Annunciation – one of the auctioneered power supplies is offline.	Circuits are powered by the redundant auctioneered power supply.	No loss of safety function	N/A
		b) Input to output short	Internal failure	System may act spuriously in the presence of noise introduced via the vital bus. No effect on the DC circuit functionality.	Periodic surveillance measurements manifest defective EMI filter.	AC input rating of PS not exceeded.	No loss of safety function.	N/A
		c) Short between input terminals or short between output terminals.	Internal failure	Input circuit breaker trips. No effect on the circuit functionality.	Annunciation – one of the auctioneered power supplies is offline.	Redundant power feed is not affected.	No loss of safety function.	N/A
36	MTP / ITP Cabinet power supplies: 24 VDC	Overvoltage	Component failure	Overvoltage device detects and removes voltage to the connected load. Lose ITP station. No SDL or SDN activity.	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	ITP in other three safety channels operable.	No loss of safety function. Some PPS screens on MTP and OM not updated.	N/A

Table 7.2-7 (63 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
37	MTP / ITP Cabinet I/O power supplies: 24 VDC	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	No effect on PPS safety function.	N/A
38	MTP / ITP Cabinet Power supply auctioneering circuit applicable to all cabinet power supplies: 24 VDC	a) Open diode	Overload, component failure	One supply is not available to power the downstream components in the affected cabinet. No loss of DC circuit functionality.	Annunciation – one of the auctioneered power supplies is offline.	The companion power supply/diode combination supplies power to the components receiving power from the supply.	No loss of safety function	N/A
		b) Shorted diode	Overload, component failure	The voltage applied to the components in the cabinet are the same as the voltage at the supply terminals. No loss of DC circuit functionality.	Periodic test	Each power supply in the auctioneered pair is capable of providing power to all of the components.	No loss of safety function	N/A
39	MTP / ITP Cabinet Power supply auctioneering circuit applicable to 24 VDC Cabinet power supply	Overvoltage	Component failure	Overvoltage device detects and removes voltage to the connected load. Lose ITP station No SDL or SDN activity.	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	ITP in other three safety channels operable	No loss of safety function. Some PPS screens on MTP and OM not updated.	N/A
40	MTP / ITP Cabinet Power supply auctioneering circuit applicable to: 24 VDC I/O power supplies	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	No effect on PPS safety function	N/A

Table 7.2-7 (64 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
41	MTP / ITP Cabinet Primary AC Feed breaker for MTP	Breaker opens on overload.	Component failure	MTP AC transfer relay de-energizes and provides alternate Vital AC to MTP via relay contacts.	Indicator on relay module not illuminated.	Two Vital AC sources provided for powering MTP / ITP Cabinet.	No loss of safety function	N/A
42	MTP / ITP Cabinet Alternate AC Feed breaker for MTP	Breaker opens while powering the MTP.	Component failure	Alternate Vital AC lost to MTP. MTP is not available as it normally operates from primary Vital AC.	Stations on SDN detect loss of updates from MTP and generate an alarm.	MTPs operating in three other safety channels.	Lose MTP function with PPS in the safety channel.	N/A
43	MTP AC transfer relay	a) Relay coil opens.	Component failure	MTP AC transfer relay de-energizes and provides alternate Vital AC to MTP via relay contacts.	Indicator on relay module not illuminated.	Two Vital AC sources provided for powering MTP.	No loss of safety function.	N/A
		b) One relay contact position not in agreement with coil state.	Mechanical failure	The Neutrals of the Vital AC feeds are independent, so a failure in the relay contact, which switches the lines or neutrals, results in the loss of Vital AC to the MTP.	Stations on SDN detect loss of updates from MTP and generate an alarm.	Three other safety channels operating.	Lose MTP function with PPS in the safety channel.	N/A

Table 7.2-7 (65 of 65)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
44	Trip Circuit Breaker (TCB) of RTSG	1) Open	Loss of 125Vdc control power Unwanted energizing of UV coil Mechanical failure of TCB	The RTSG opens.	Alarm Indication on the MTP and OM in the MCR	The RTSGs in other channels are not affected.	The logic of RTSGs changes to 1-out-of-3.	
		2) Closed	Mechanical failure of TCB Failure of UV coil Short contact of TCB	The RTSG cannot be opened.	Periodic test	The RTSGs in other channels are not affected.	The logic of RTSGs changes to 2-out-of-3.	

(1) FMEA assumes that all trip parameters in one channel are already bypassed. The Inherent Compensating Provisions and effects are described based on this assumption.

APR1400 DCD TIER 2

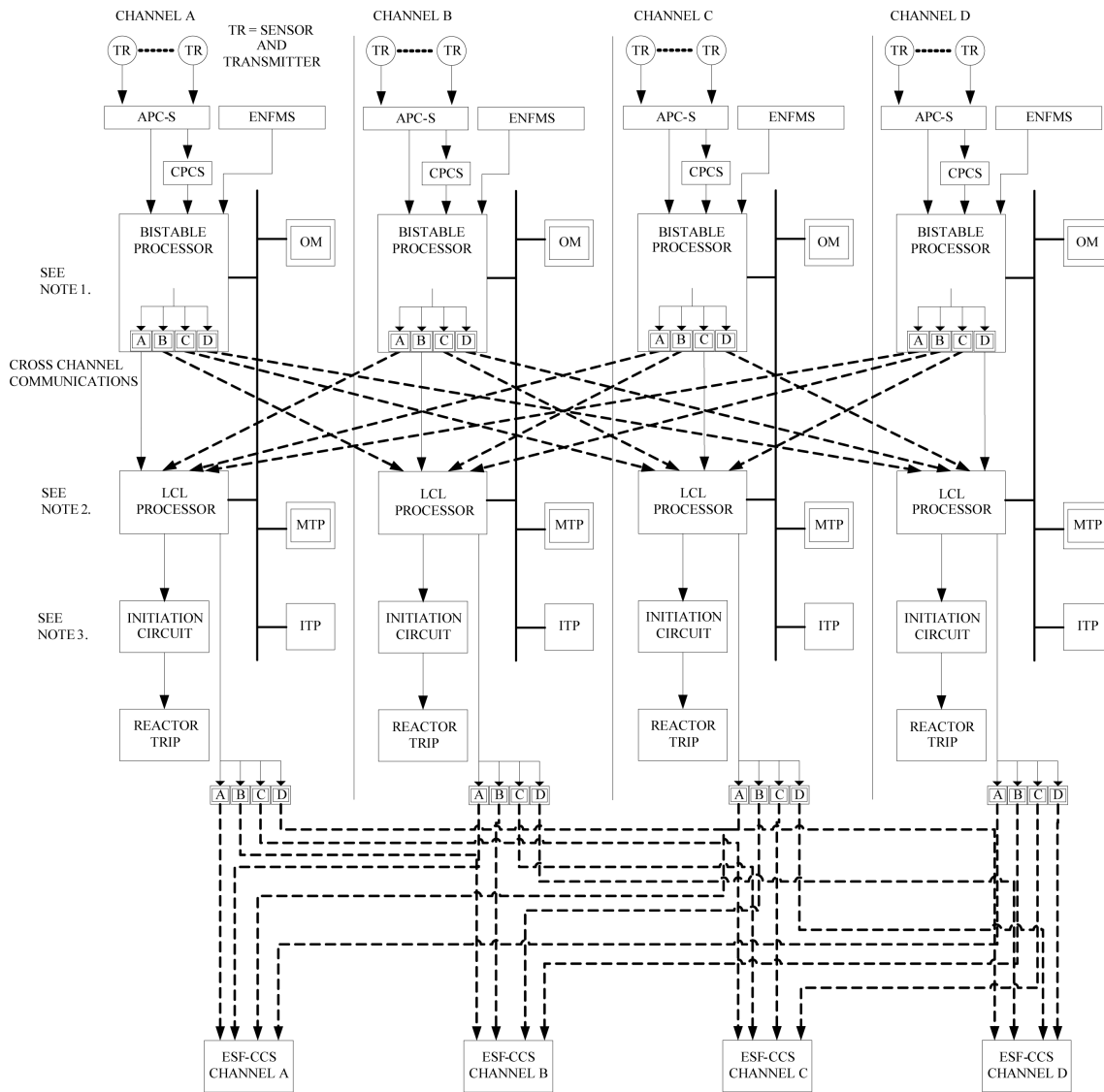


Figure 7.2-1 PPS Basic Block Diagram

APR1400 DCD TIER 2

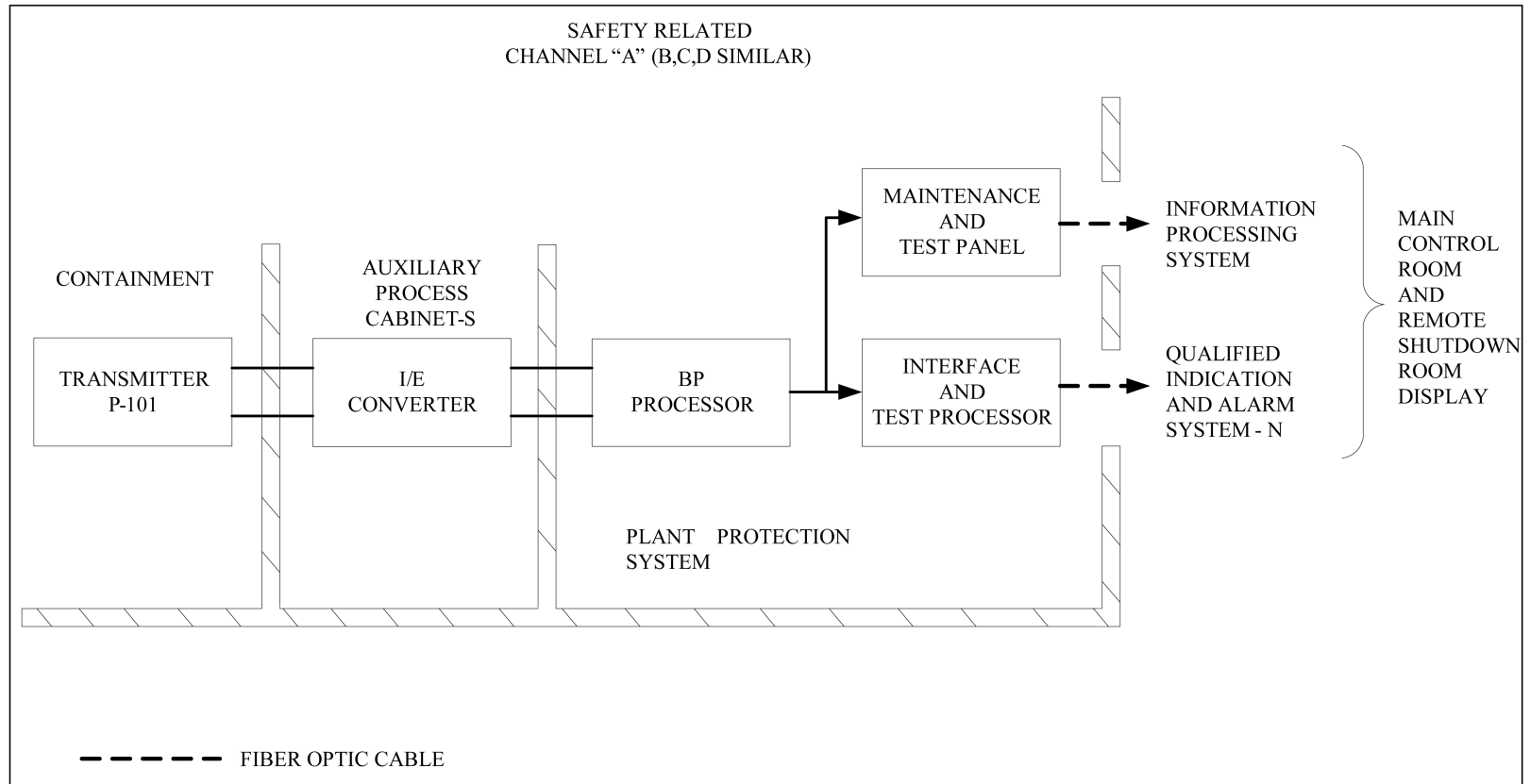


Figure 7.2-2 Typical PPS Measurement Channel Functional Diagram (Pressurizer Pressure Wide Range)

APR1400 DCD TIER 2

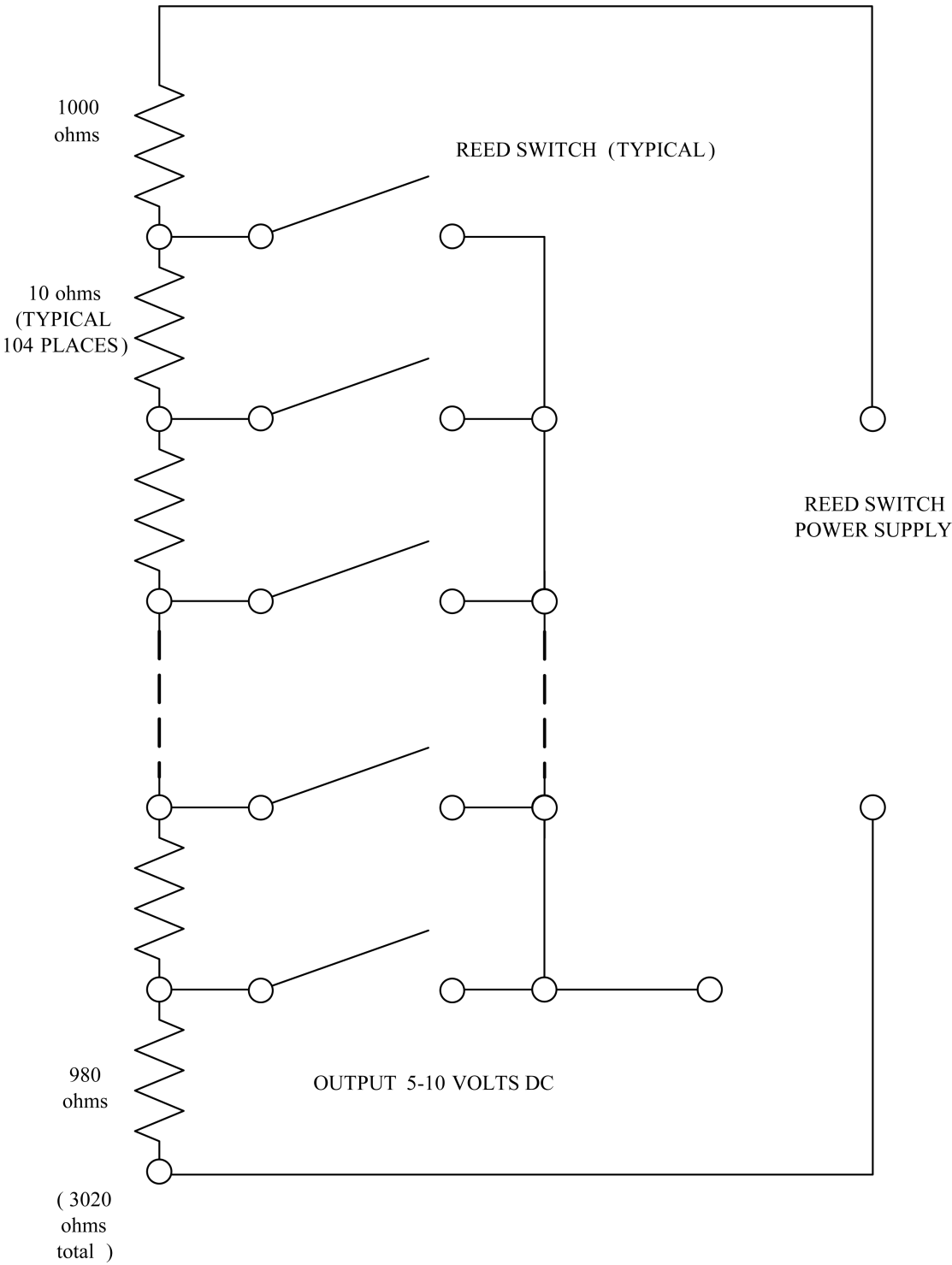


Figure 7.2-3 Reed Switch Position Transmitter Assembly Schematic

APR1400 DCD TIER 2

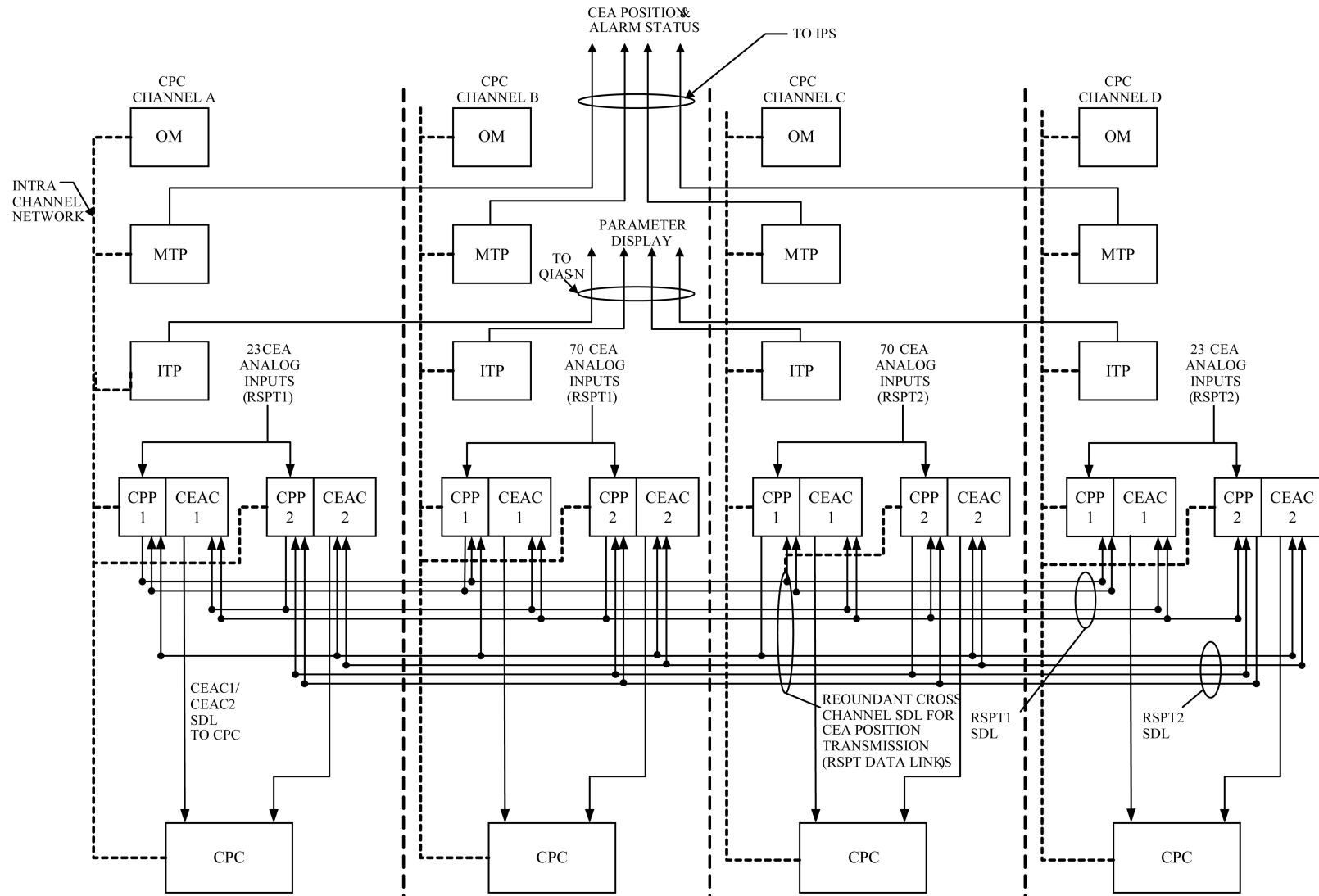


Figure 7.2-4 CEA Position Signal Flow for CPCS

APR1400 DCD TIER 2

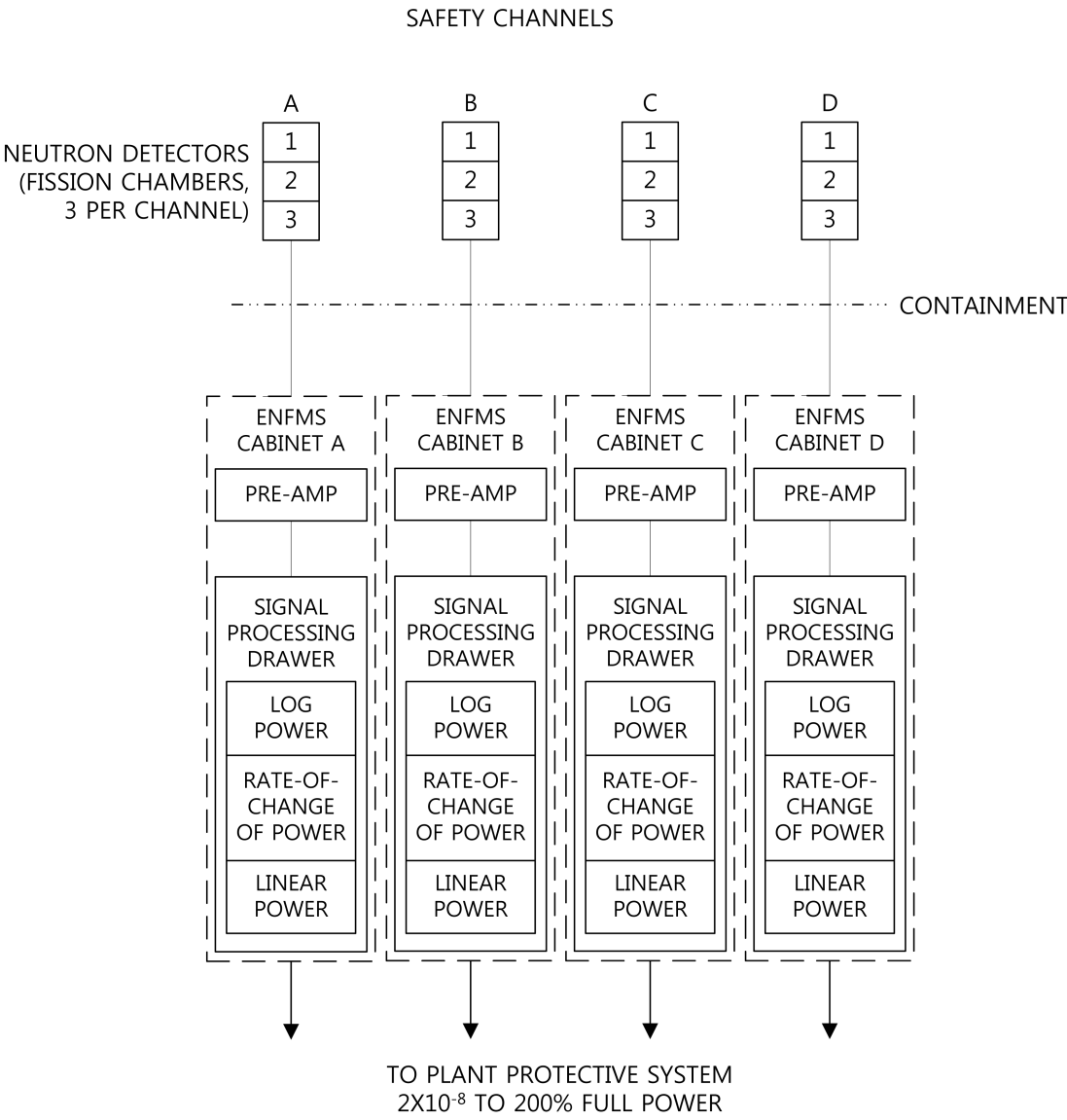


Figure 7.2-5 Ex-Core Neutron Monitoring System (Safety Channel)

APR1400 DCD TIER 2

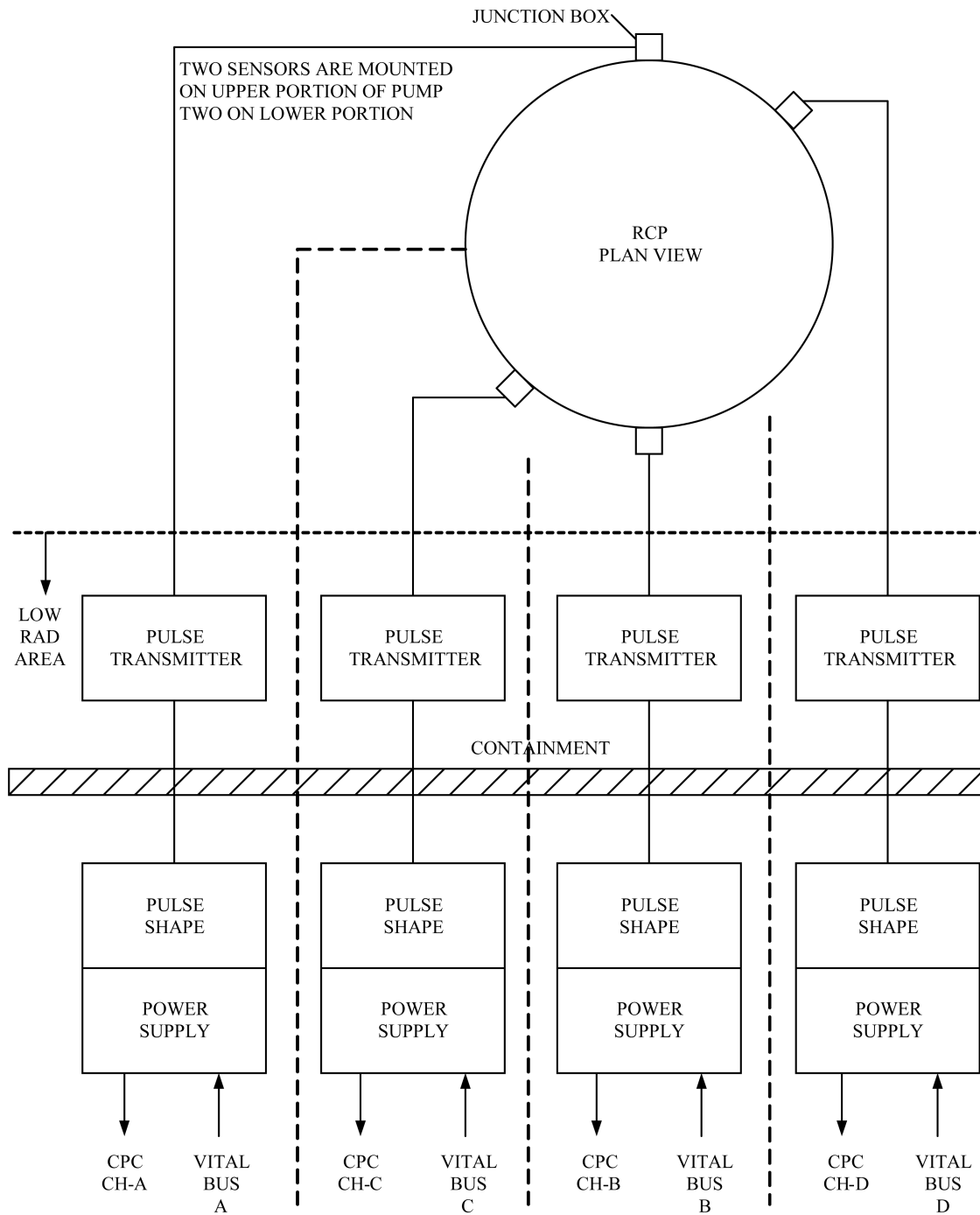


Figure 7.2-6 Reactor Coolant Pump Shaft Sensing System

APR1400 DCD TIER 2

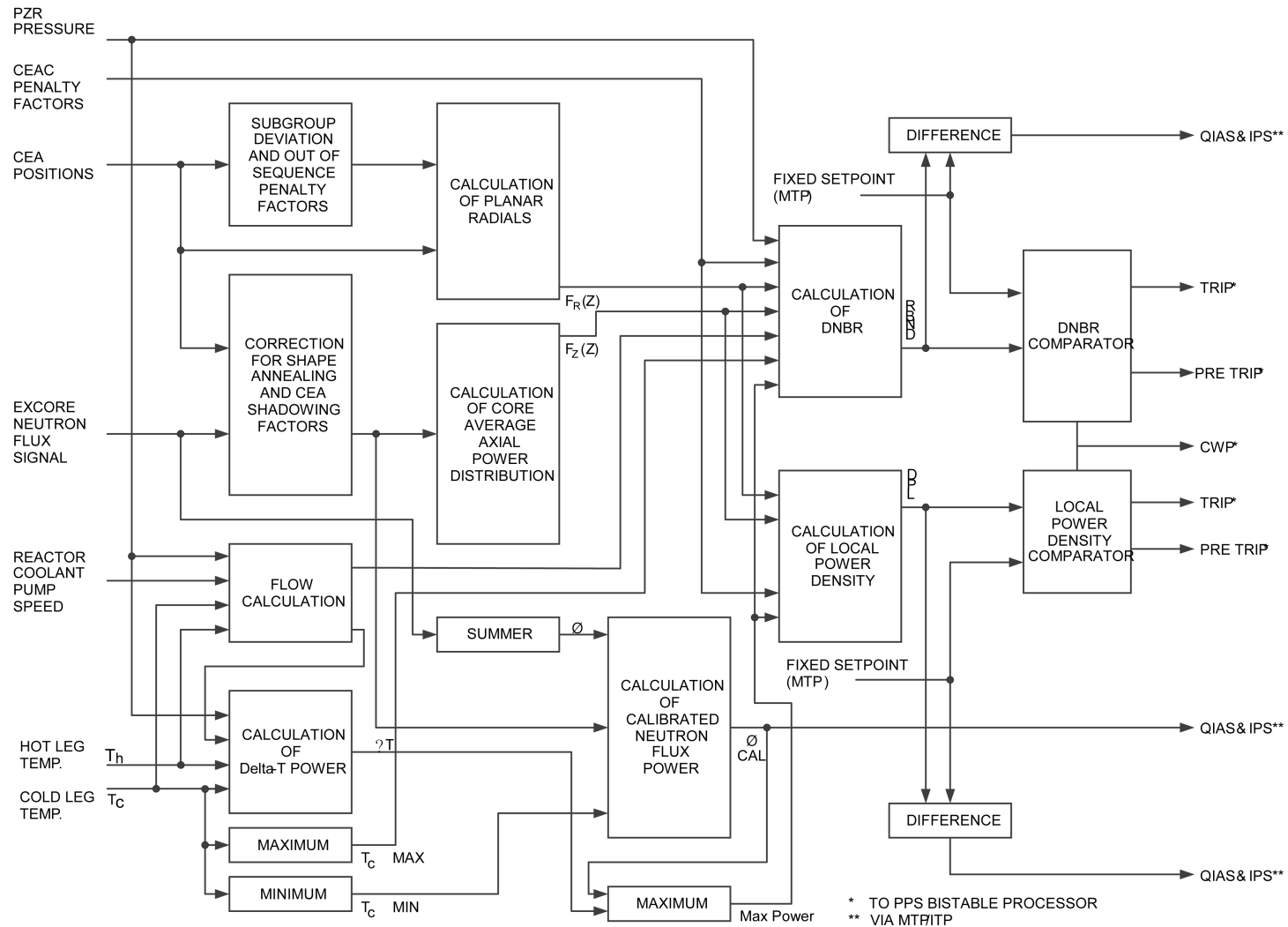


Figure 7.2-7 Core Protection Calculator System Functional Block Diagram

APR1400 DCD TIER 2

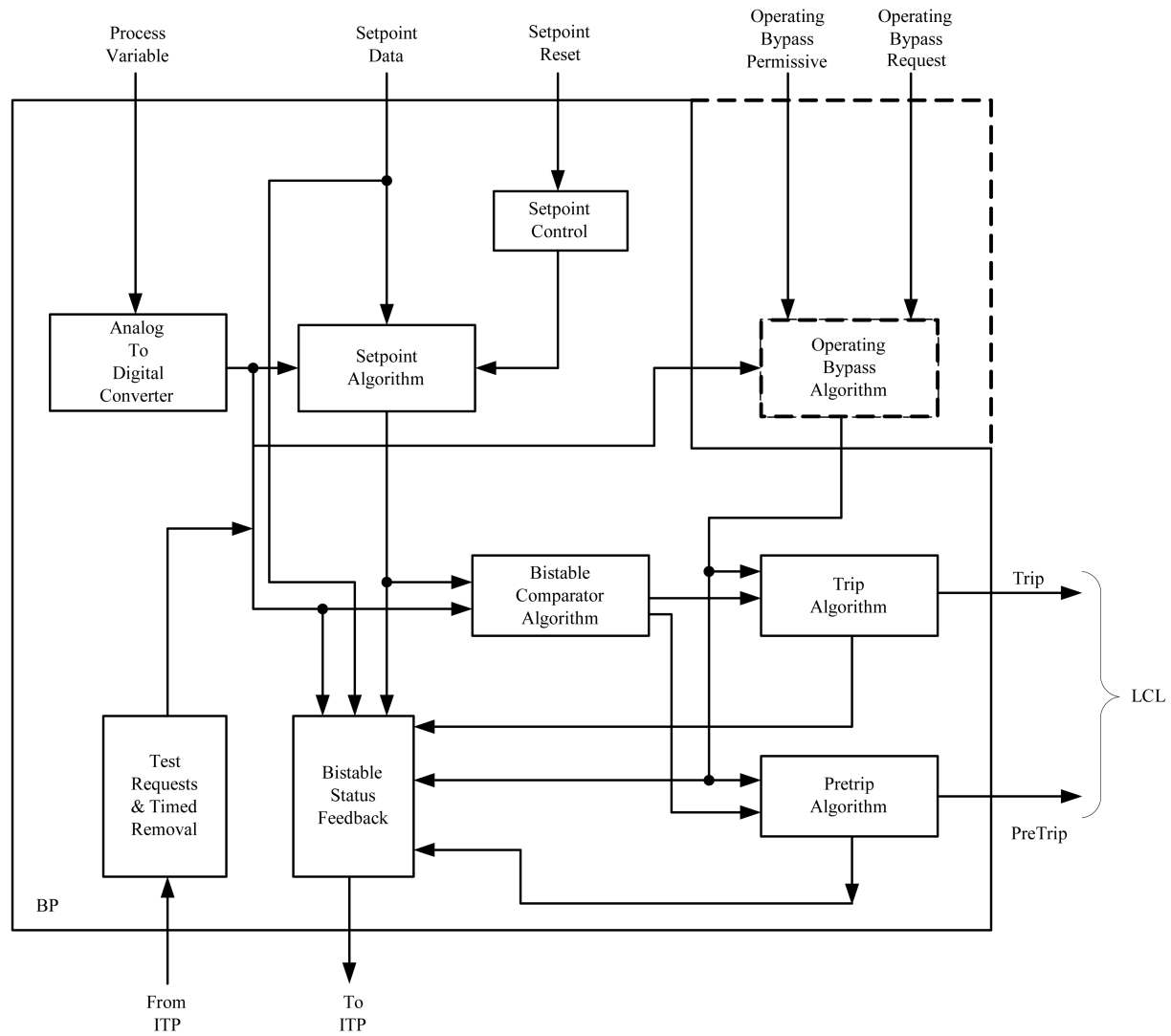


Figure 7.2-8 PPS Bistable Trip Logic Functional Block Diagram

APR1400 DCD TIER 2

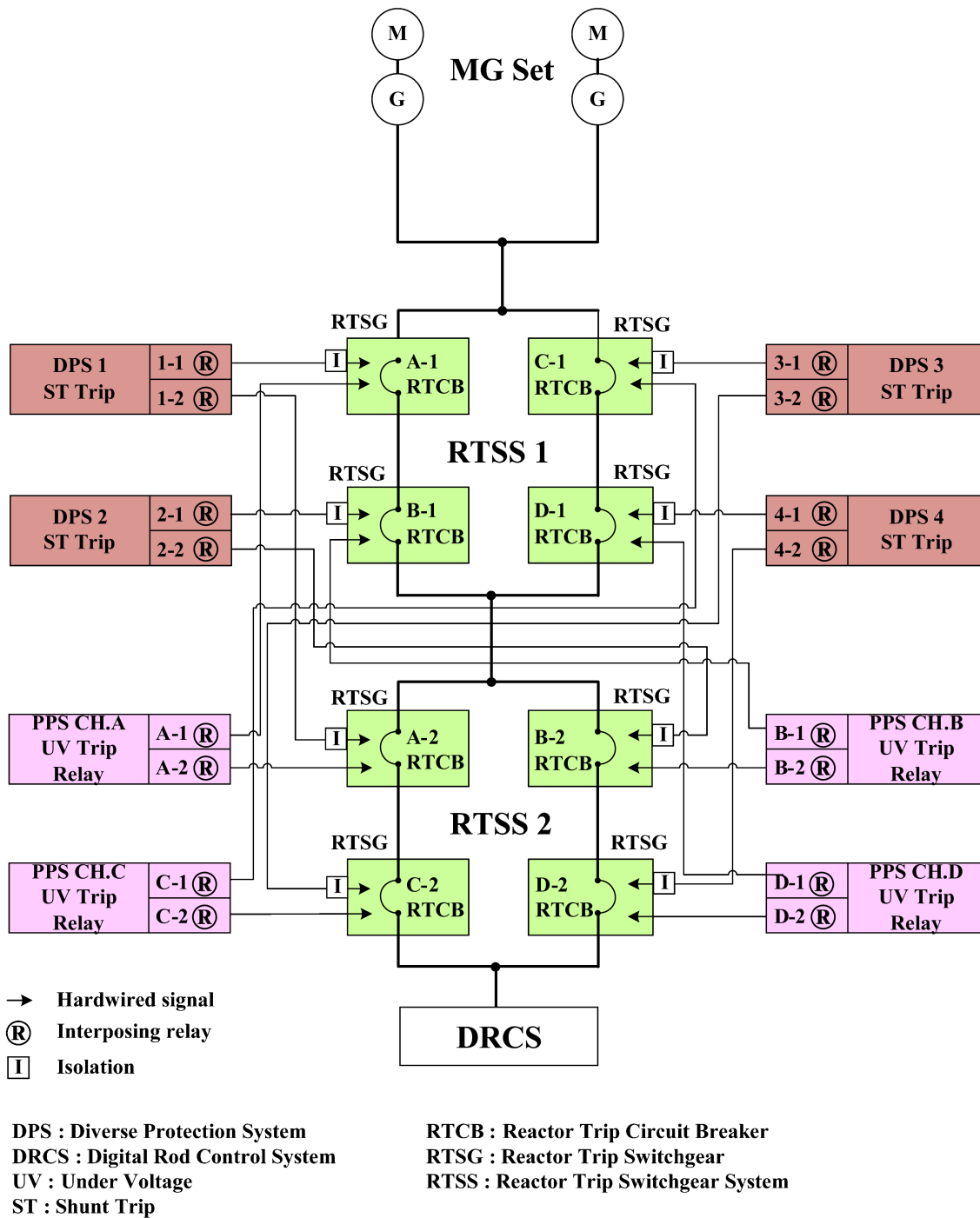


Figure 7.2-9 Reactor Trip Switchgear System Interface Diagram

APR1400 DCD TIER 2

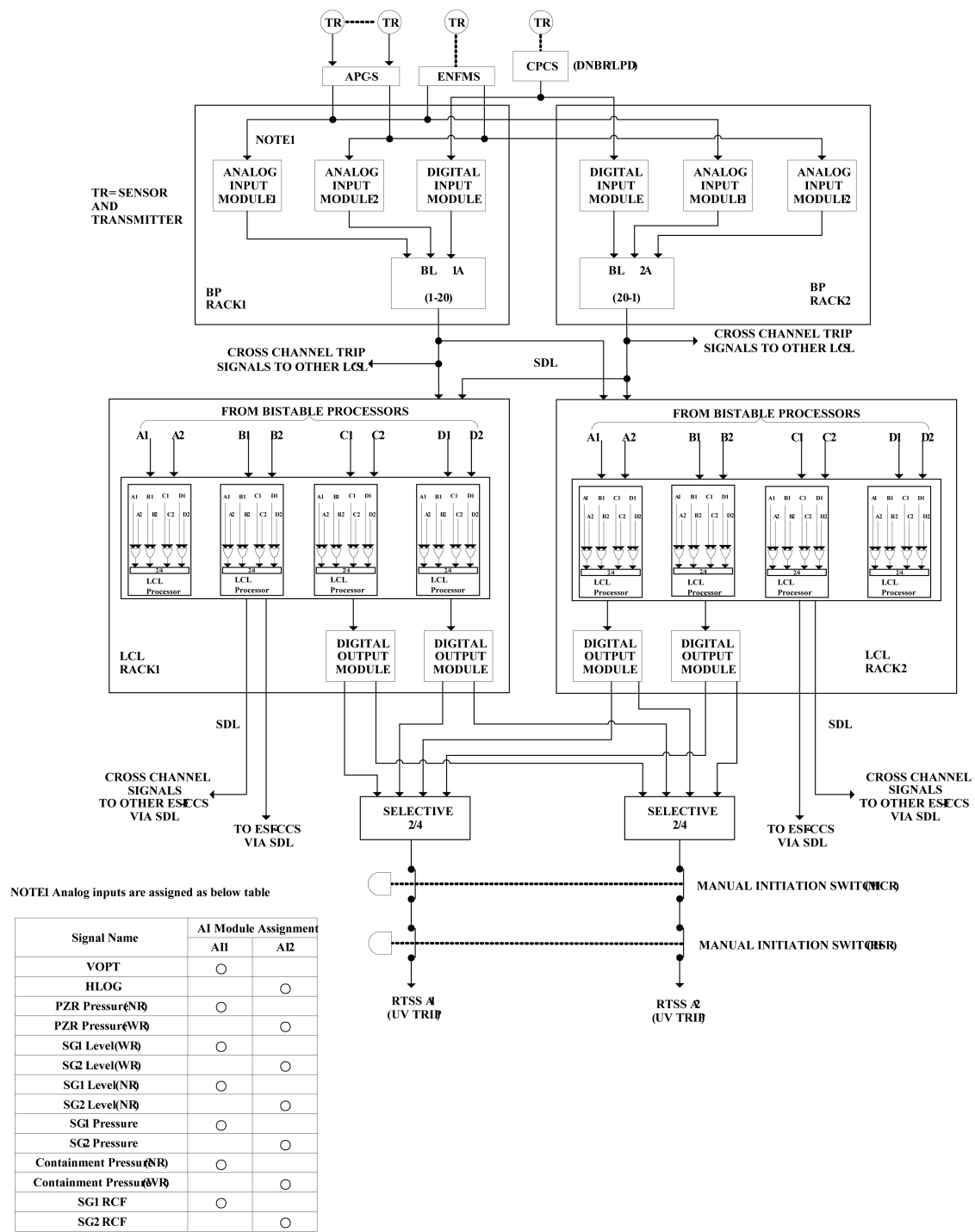


Figure 7.2-10 PPS Channel A Trip Path Diagram

APR1400 DCD TIER 2

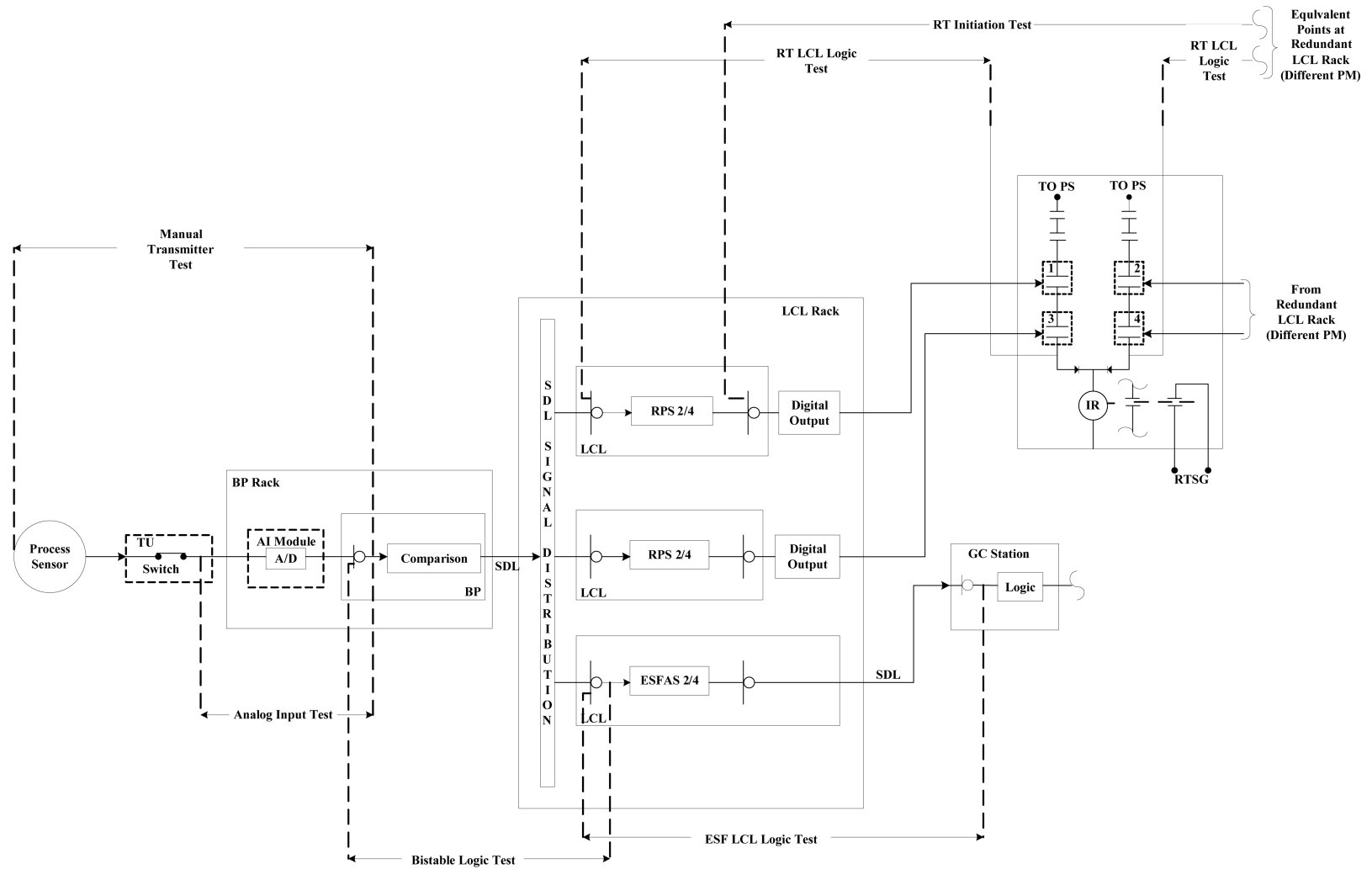


Figure 7.2-11 PPS Testing Overlap

APR1400 DCD TIER 2

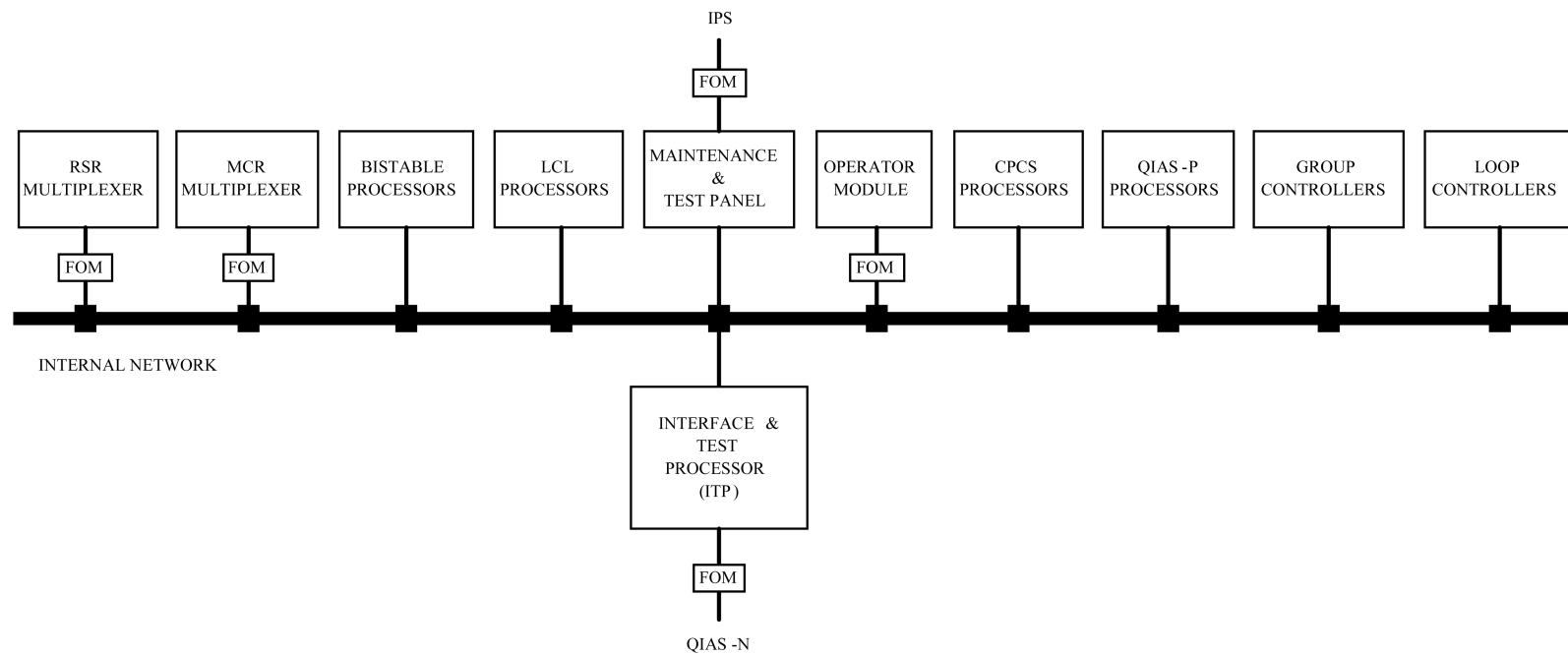


Figure 7.2-12 Interface and Test Processor Block Diagram

APR1400 DCD TIER 2

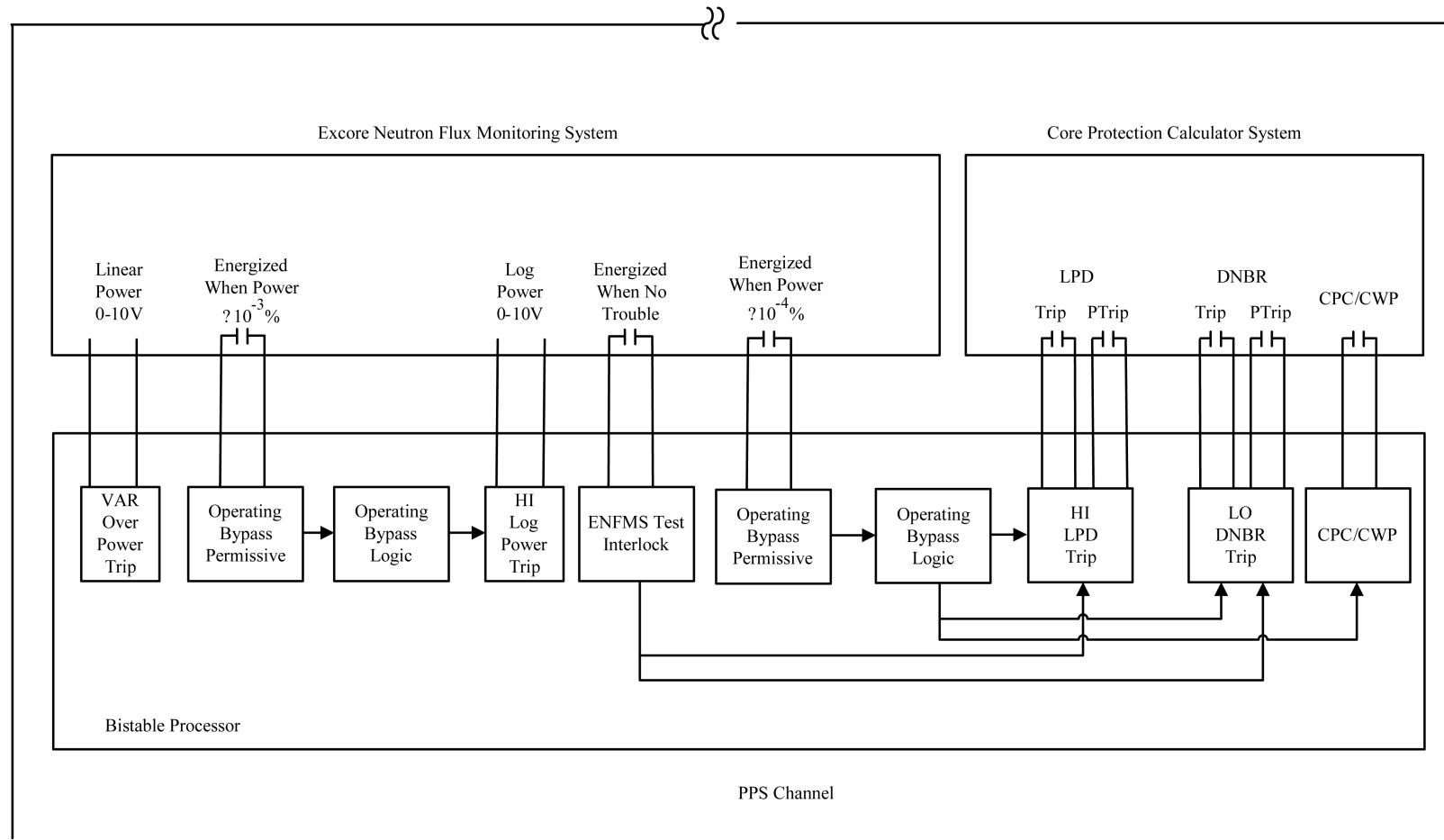


Figure 7.2-13 PPS Channel Contact Bistable Interface Diagram

APR1400 DCD TIER 2

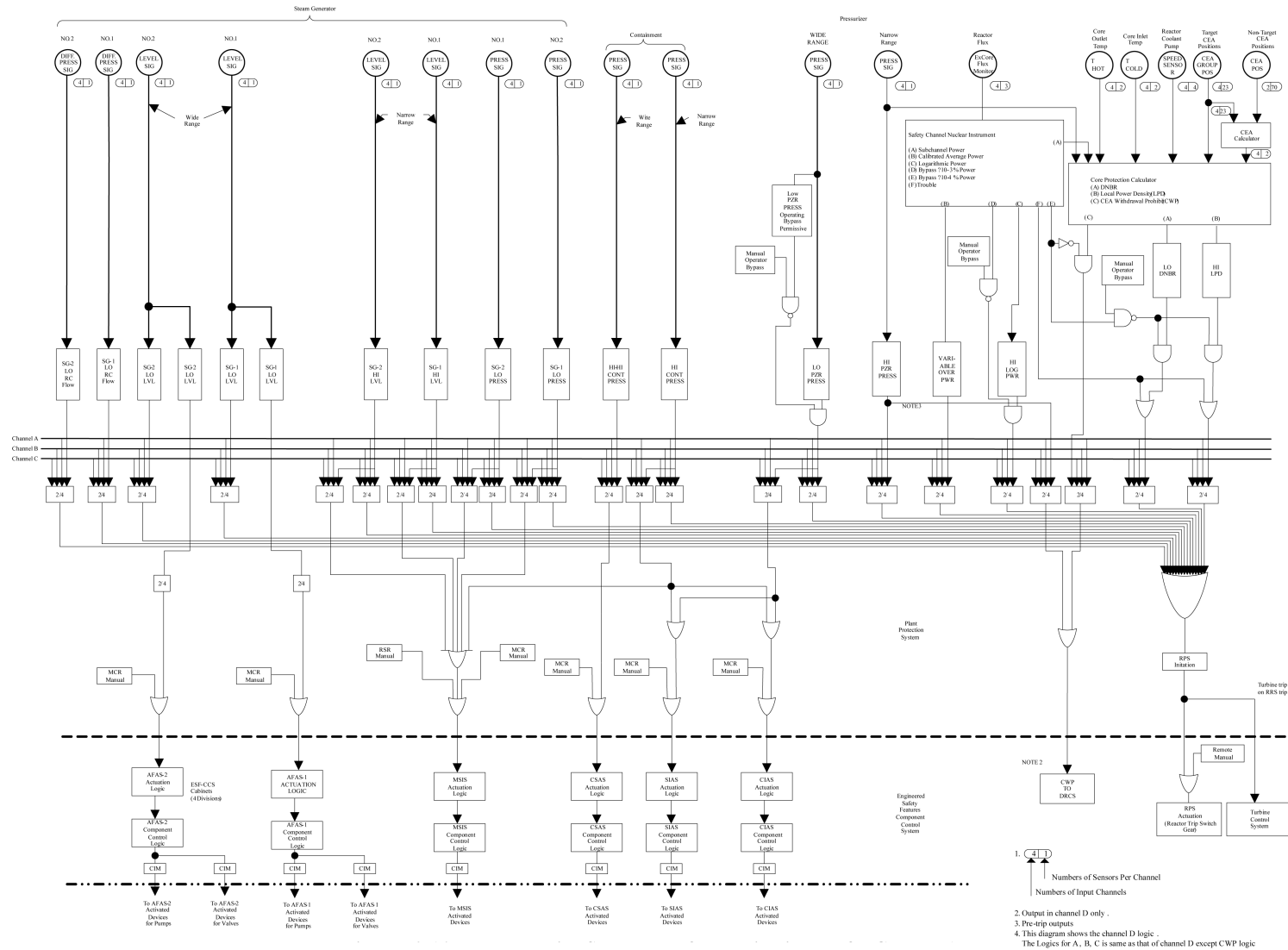


Figure 7.2-14 Plant Protection System Interface Logic Diagram for Channel A

APR1400 DCD TIER 2

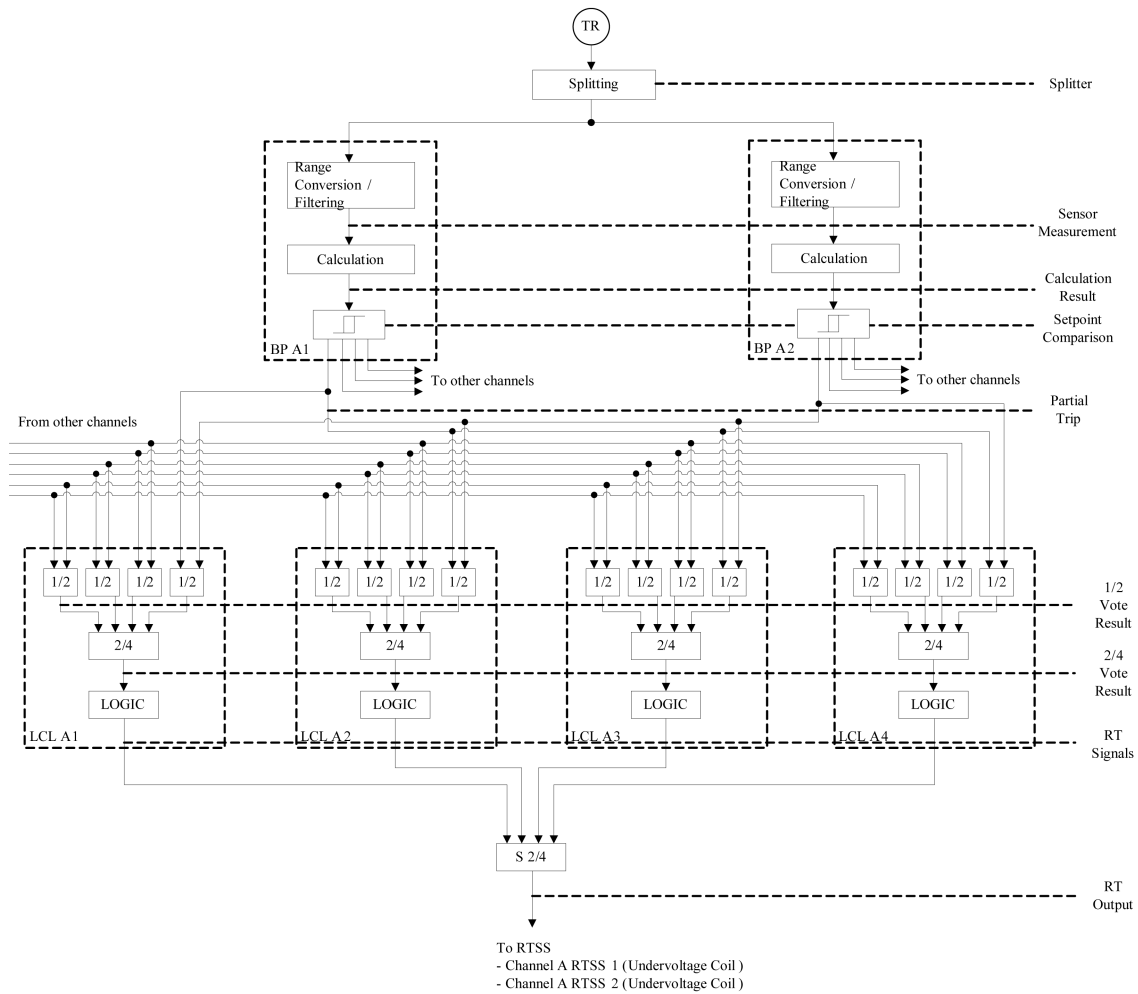
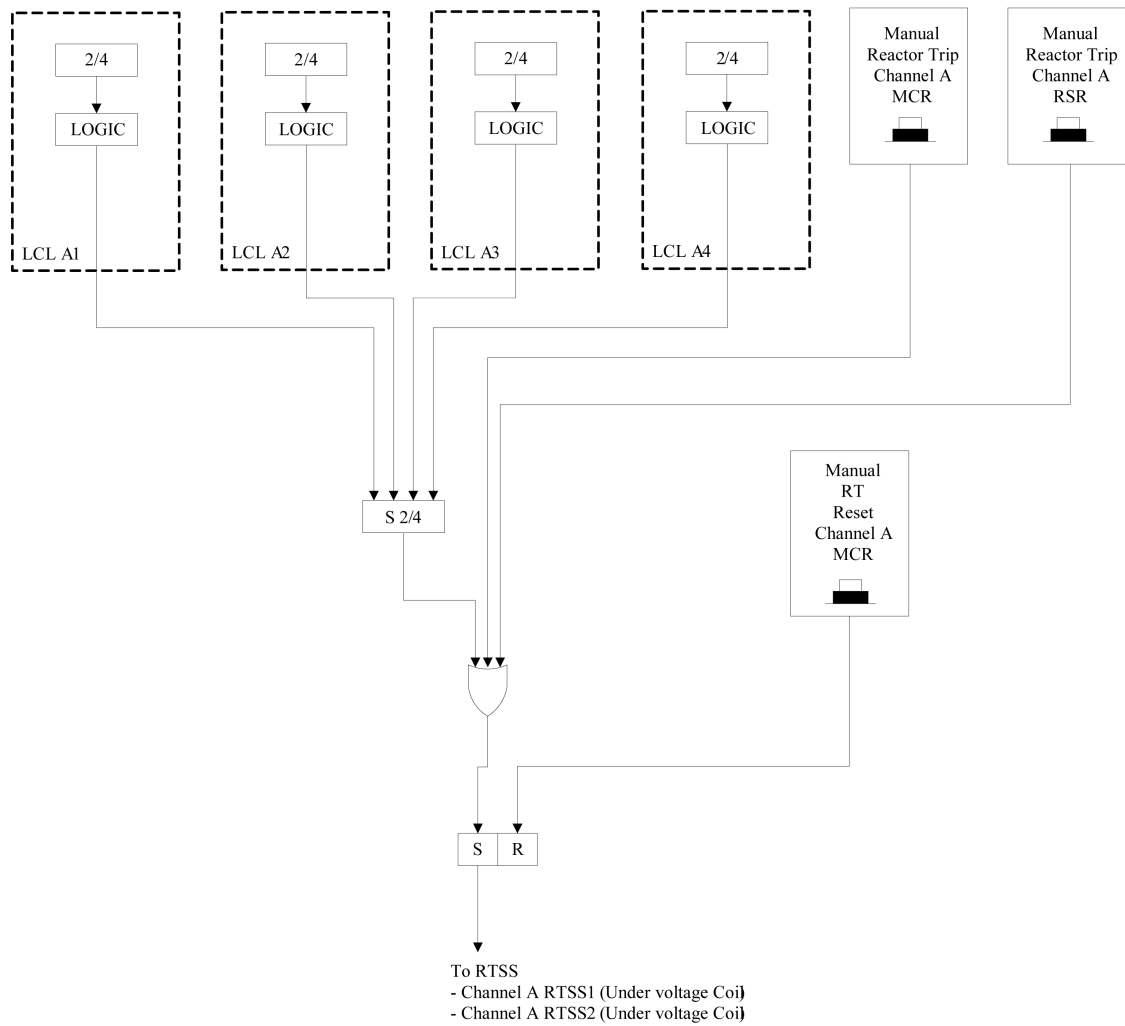


Figure 7.2-15 Reactor Trip Initiation Diagram

APR1400 DCD TIER 2



* Functional logics for channel B C and D are same as that of channel A. The manual reactor trip switches in the RSR are provided only in channel A and B

Figure 7.2-16 Manual Reactor Trip Initiation Diagram

APR1400 DCD TIER 2

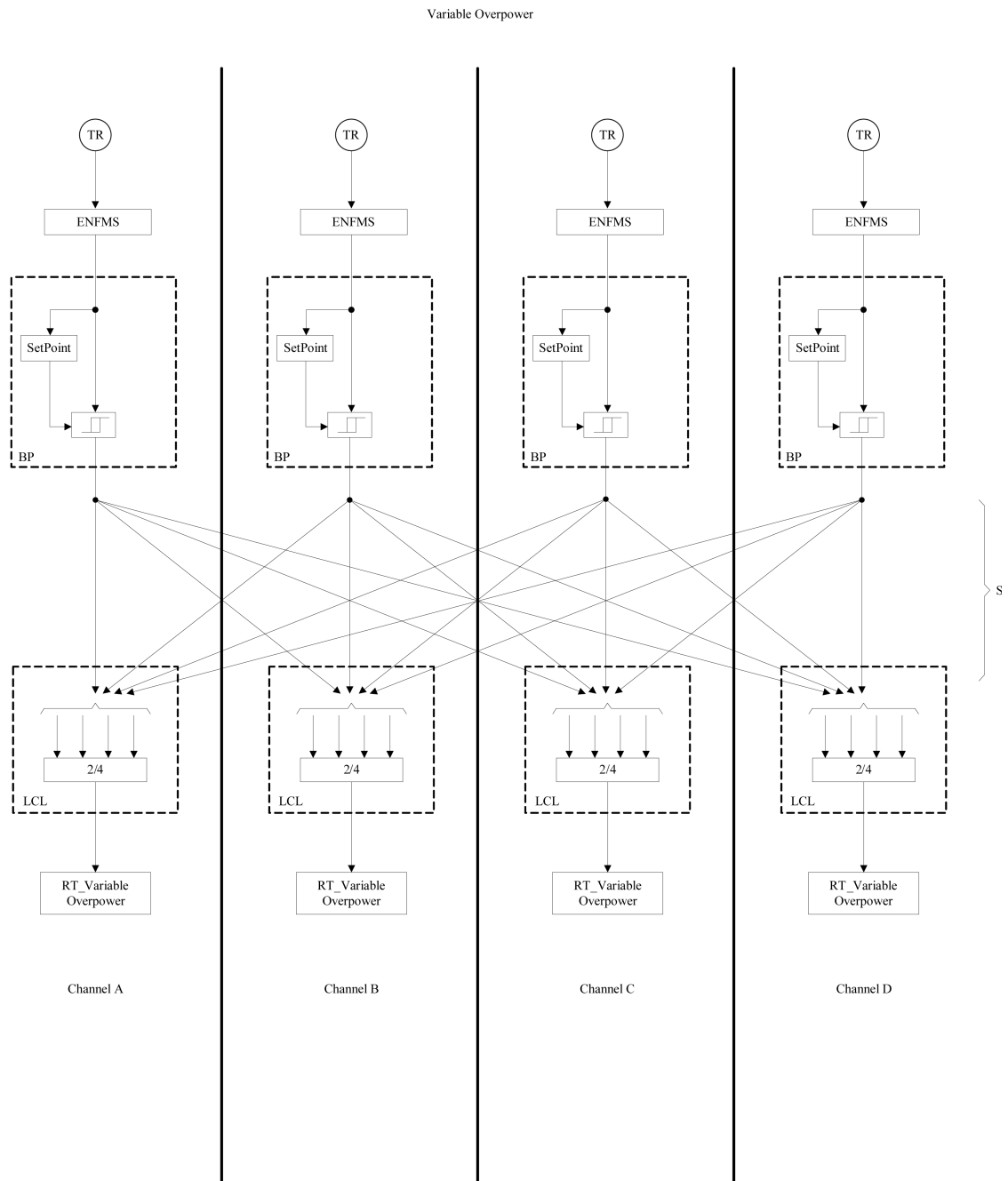


Figure 7.2-17 Functional Logic Diagram for Variable Overpower

APR1400 DCD TIER 2

High Logarithmic Power

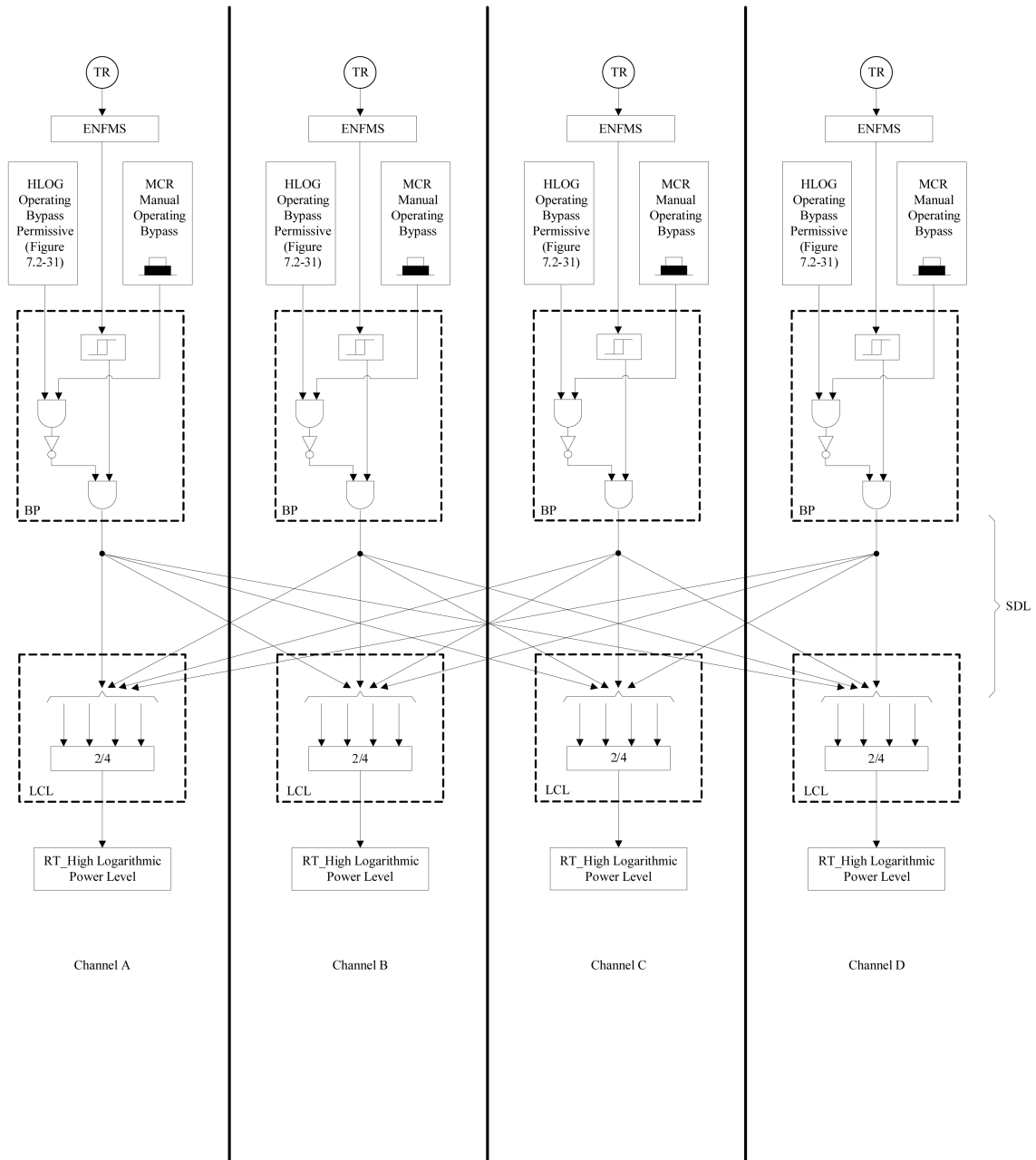


Figure 7.2-18 Functional Logic Diagram for High Logarithmic Power Level

APR1400 DCD TIER 2

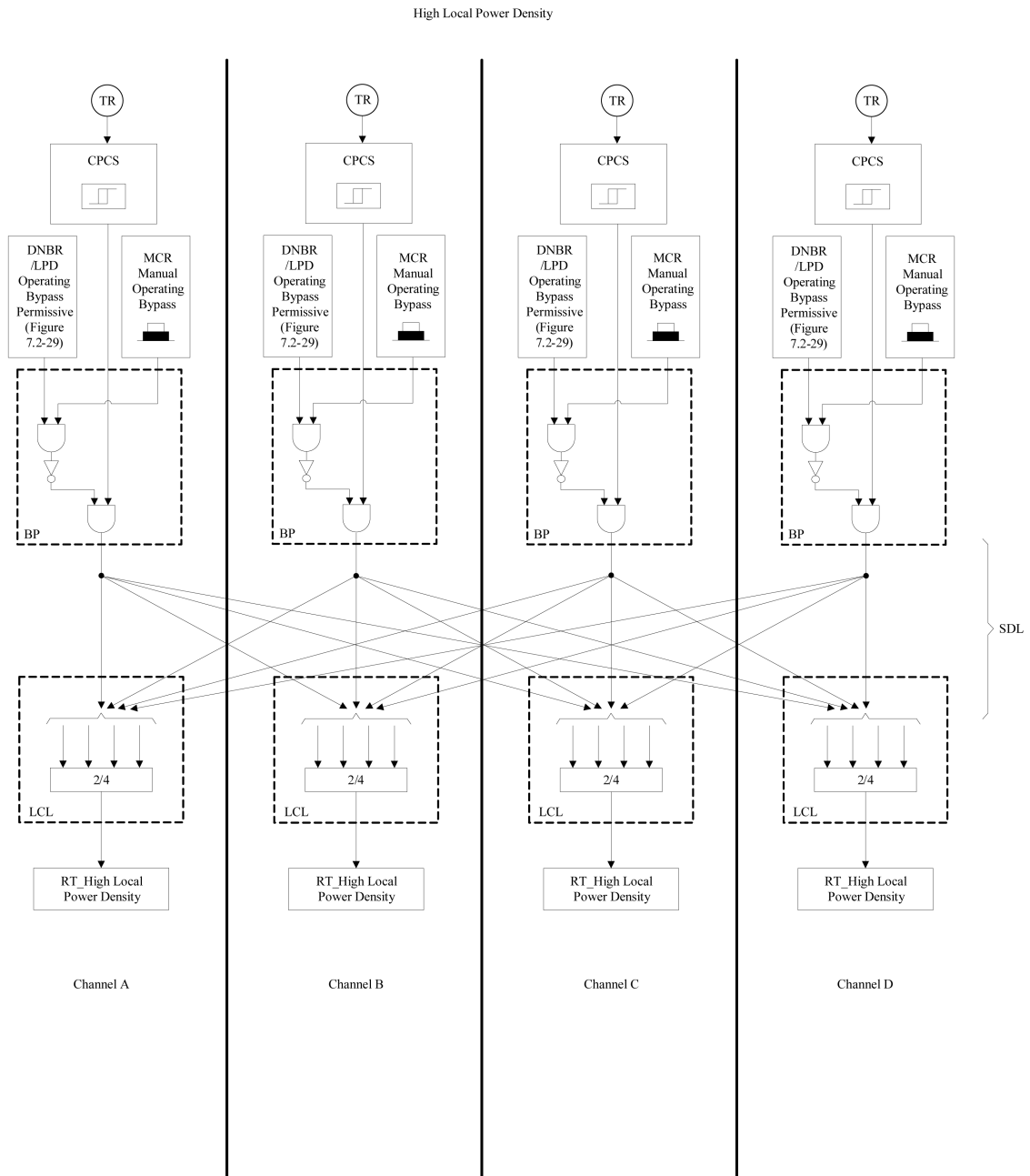


Figure 7.2-19 Functional Logic Diagram for High Local Power Density

APR1400 DCD TIER 2

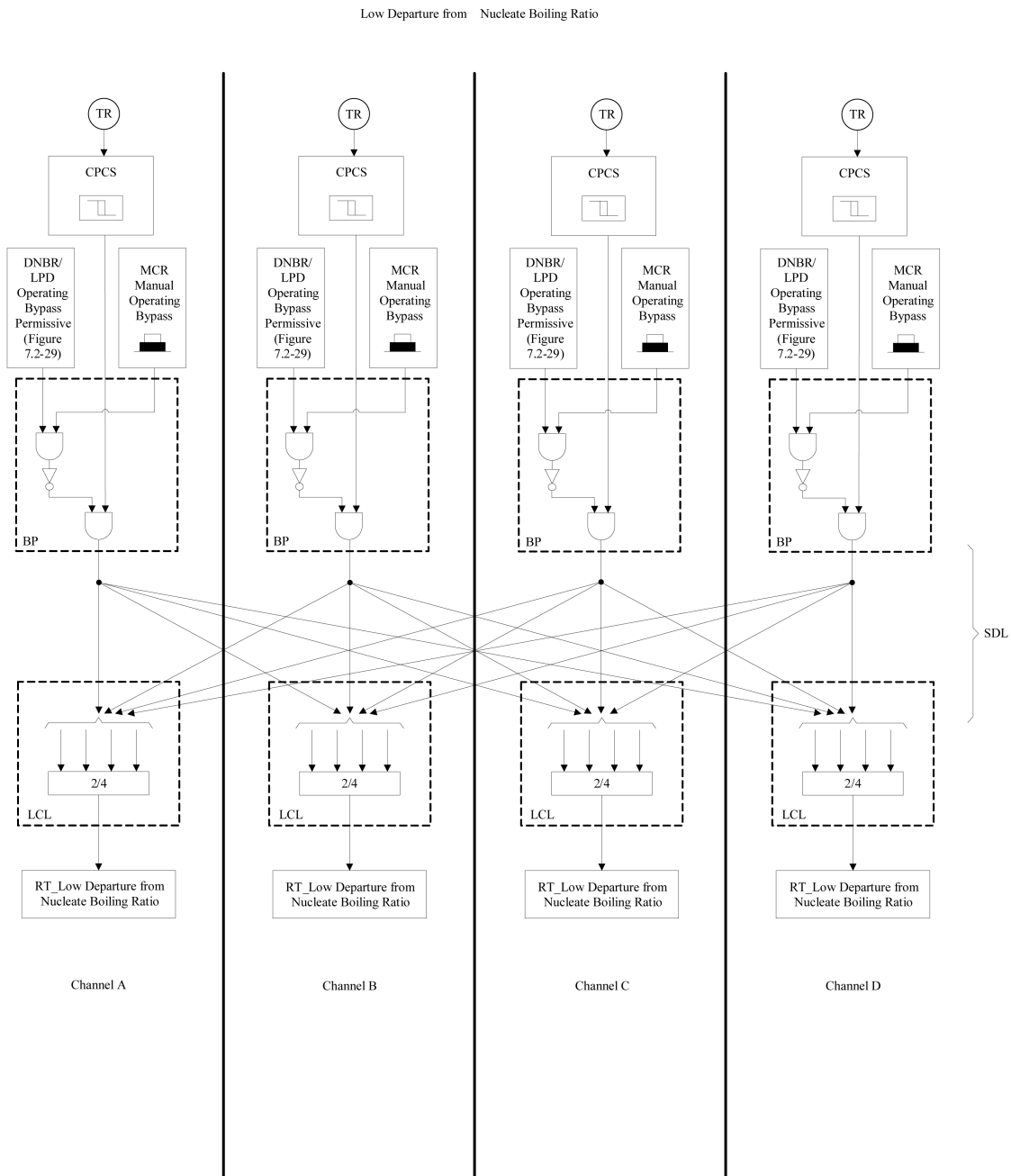


Figure 7.2-20 Functional Logic Diagram for Low Departure from Nucleate Boiling Ratio

APR1400 DCD TIER 2

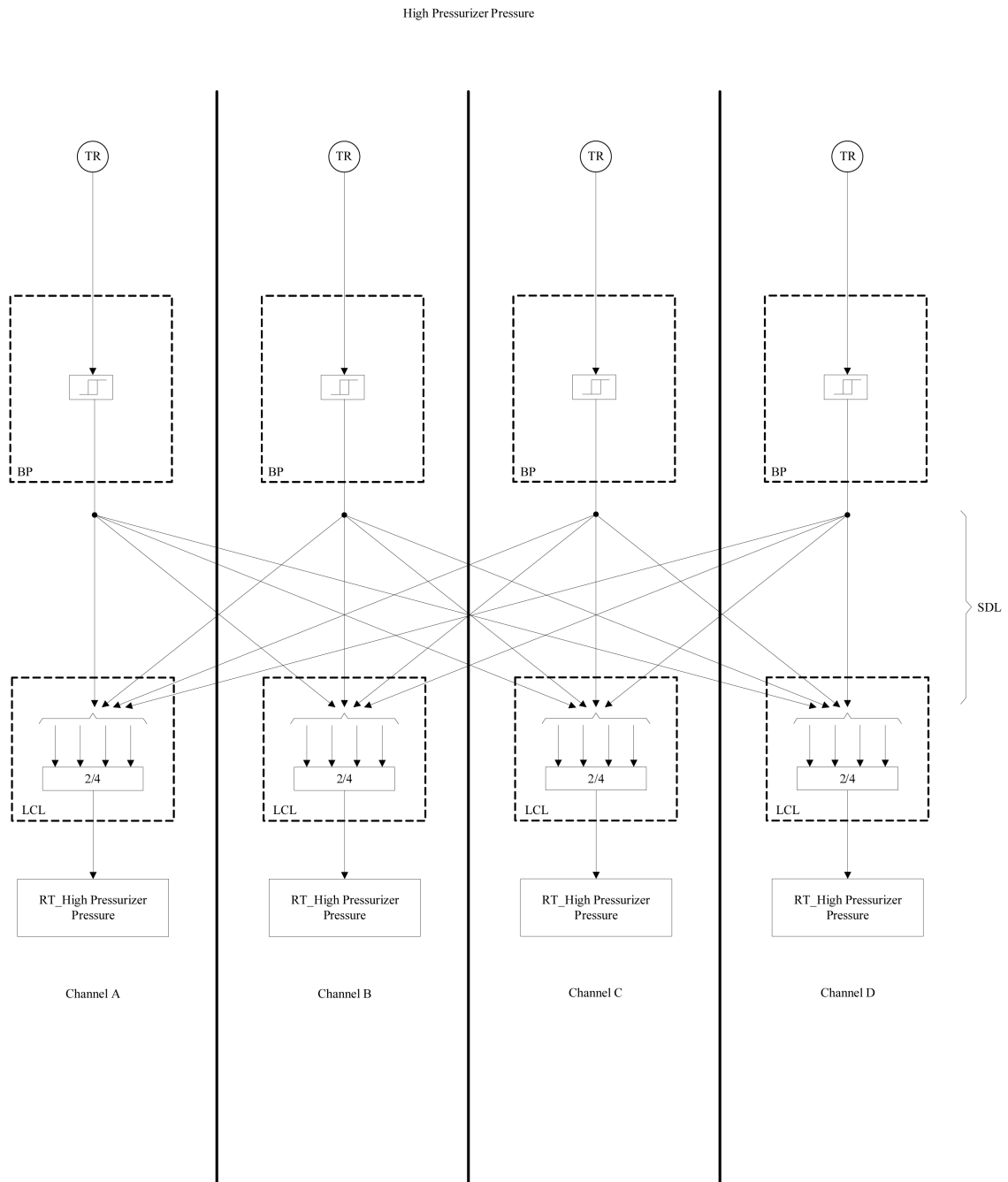


Figure 7.2-21 Functional Logic Diagram for High Pressurizer Pressure

APR1400 DCD TIER 2

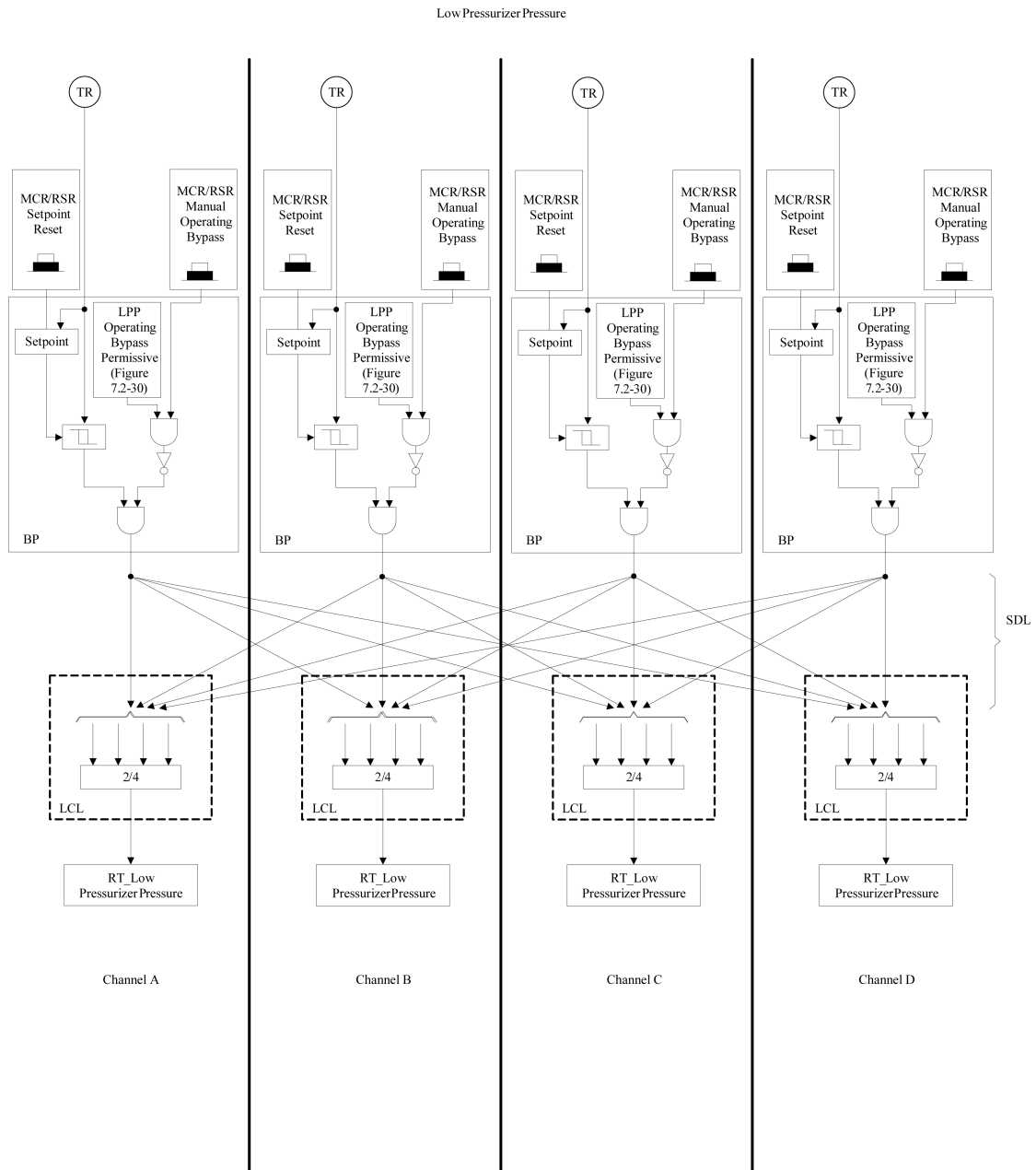
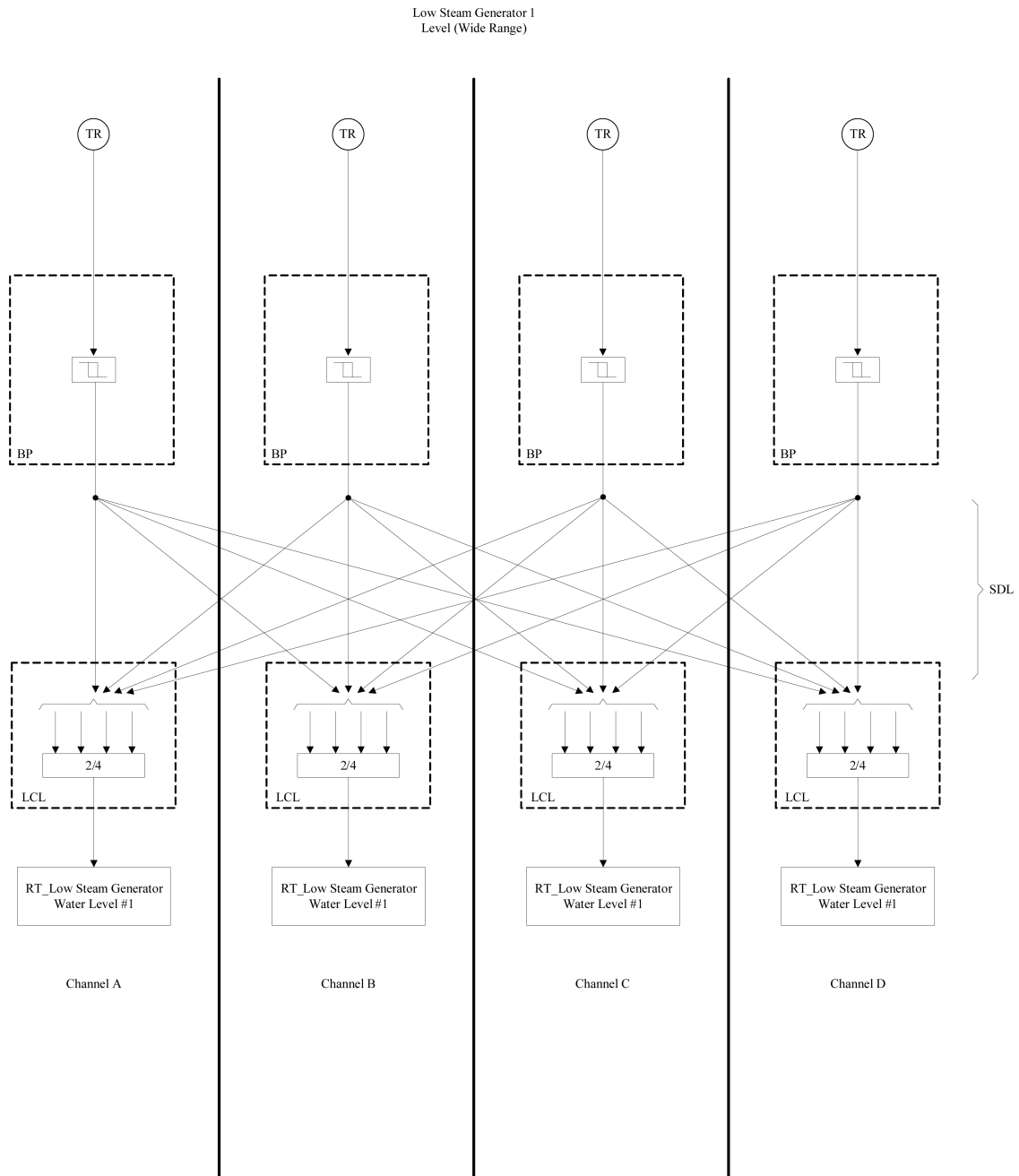


Figure 7.2-22 Functional Logic Diagram for Low Pressurizer Pressure

APR1400 DCD TIER 2

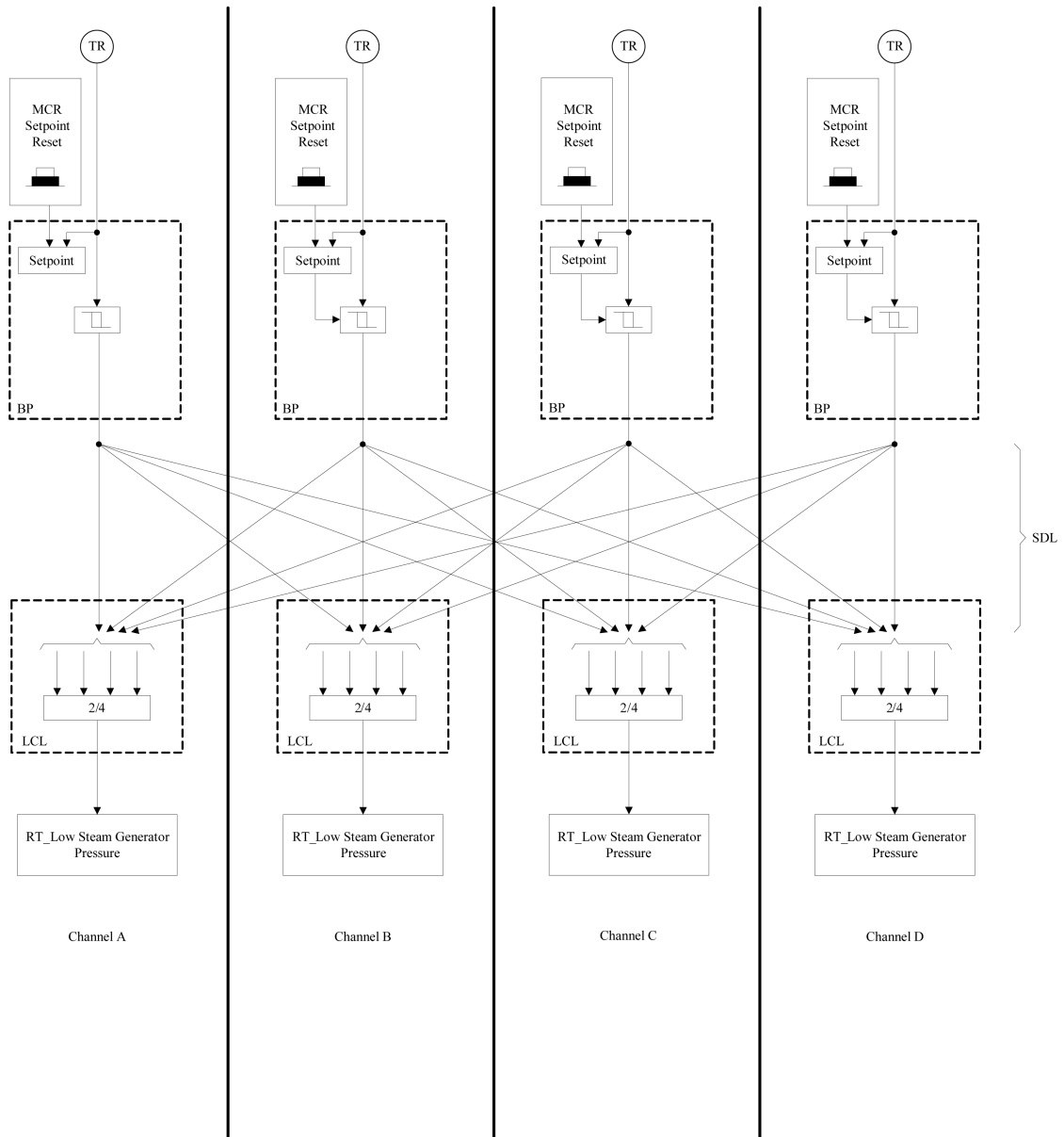


Note : Low Steam Generator #2 Water Level Logic is same as that of Low Steam Generator #1 Level

Figure 7.2-23 Functional Logic Diagram for Low Steam Generator Water Level

APR1400 DCD TIER 2

Low Steam Generator 1 Pressure



Note: Low Steam Generator #2 Pressure is same as that of Low Steam Generator #1 Pressure

Figure 7.2-24 Functional Logic Diagram for Low Steam Generator Pressure

APR1400 DCD TIER 2

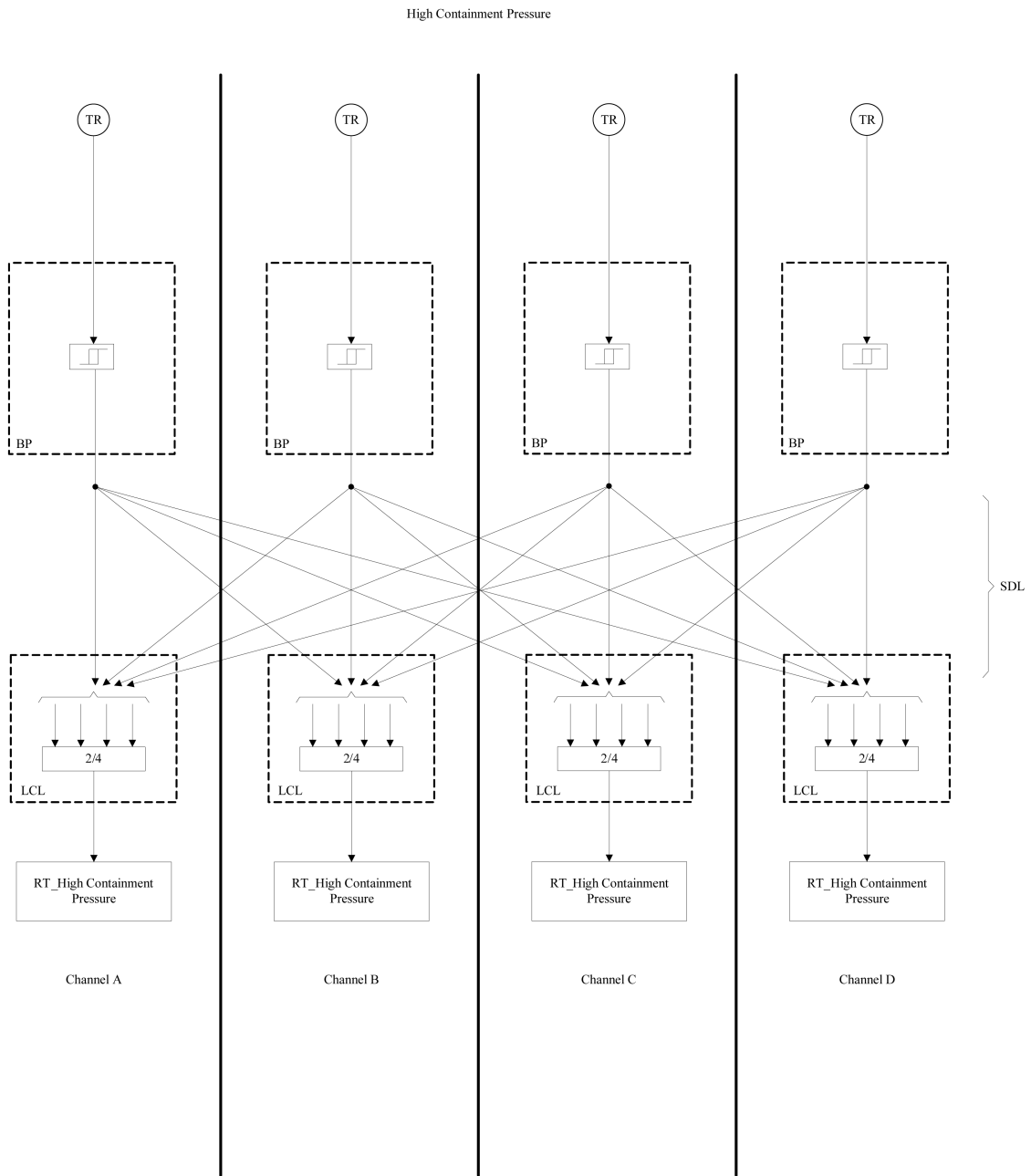
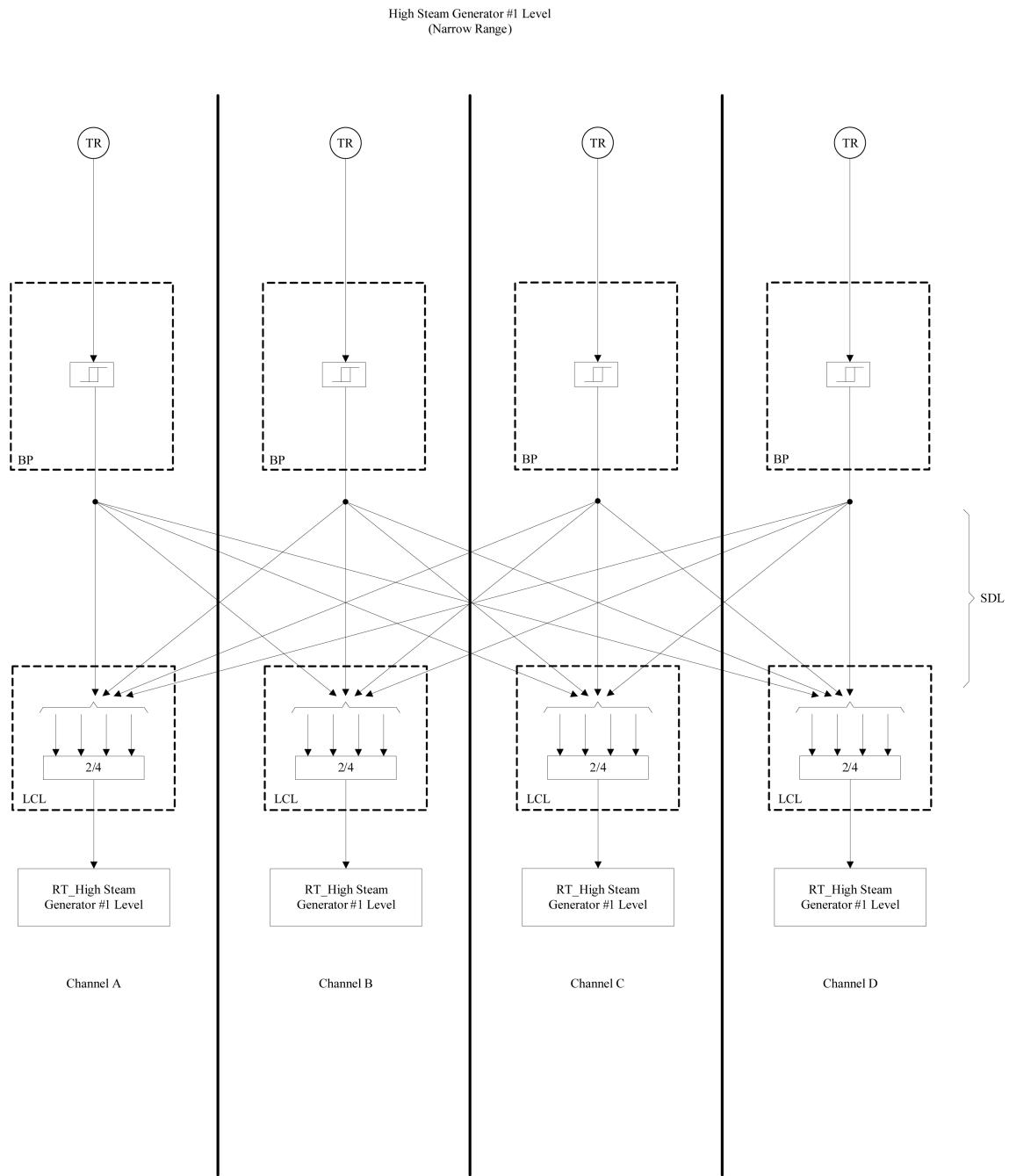


Figure 7.2-25 Functional Logic Diagram for High Containment Pressure

APR1400 DCD TIER 2

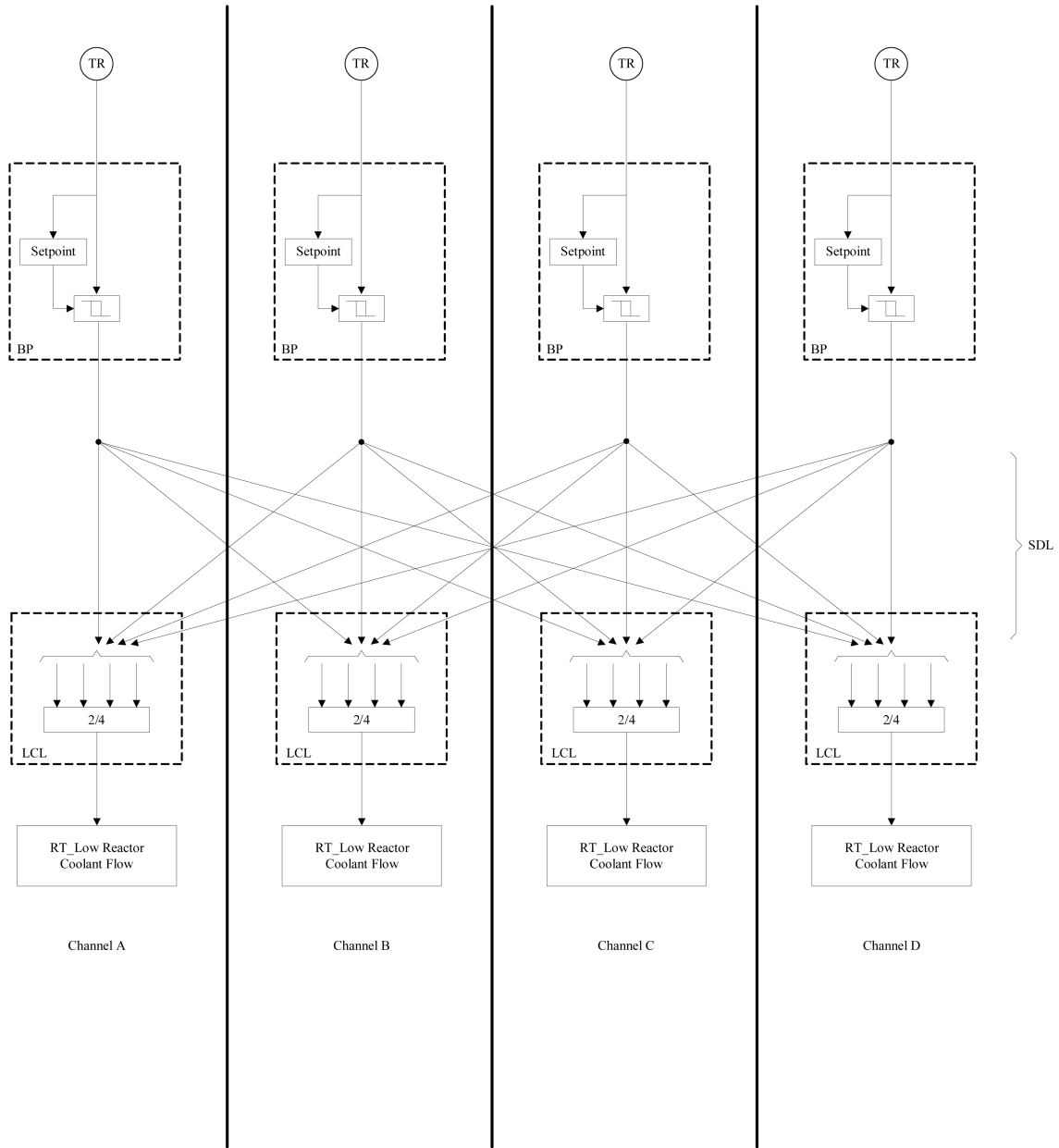


Note : High Steam Generator #2 Level Logic is same as that of High Steam Generator #1

Figure 7.2-26 Functional Logic Diagram for High Steam Generator Water Level

APR1400 DCD TIER 2

Low Reactor Coolant Flow #1



Note : Reactor Coolant Flow #2 Logic is same as that of Reactor Coolant Flow #1

Figure 7.2-27 Functional Logic Diagram for Low Reactor Coolant Flow

APR1400 DCD TIER 2

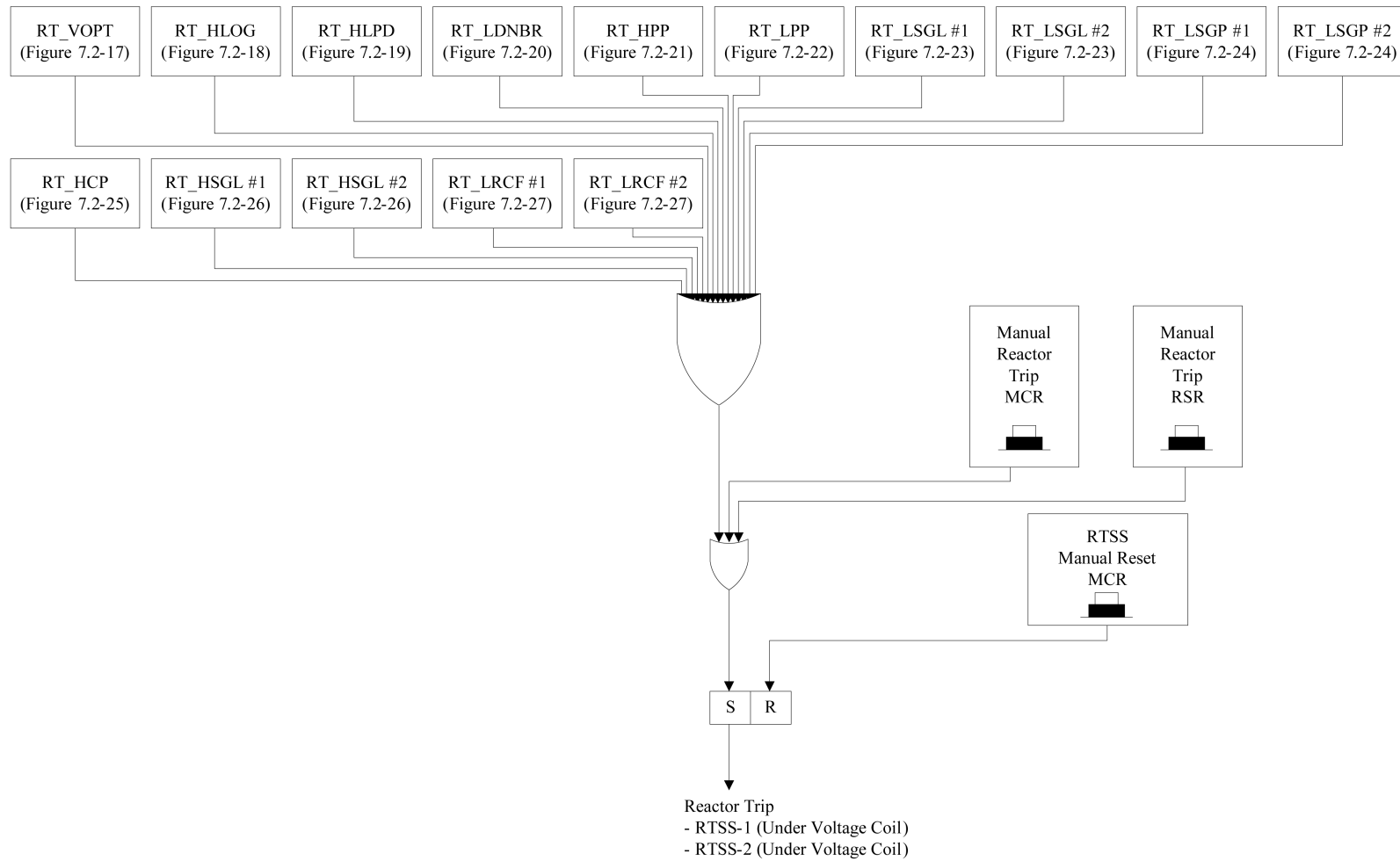


Figure 7.2-28 Functional Logic Diagram for Reactor Trip Signal Generation

APR1400 DCD TIER 2

Excore Neutron Flux Power

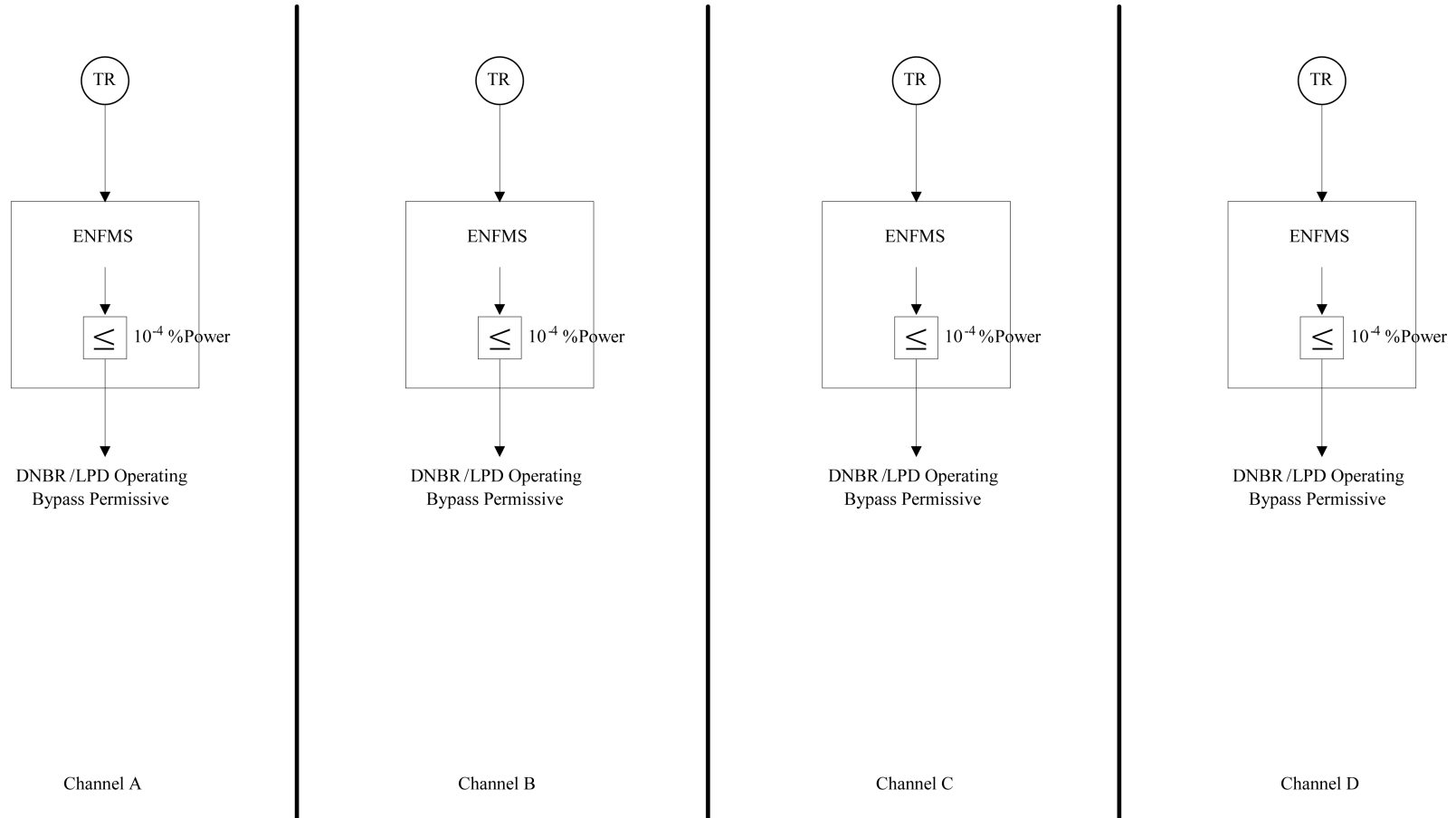


Figure 7.2-29 Functional Logic Diagram for DNBR LPD Operating Bypass Permissive

APR1400 DCD TIER 2

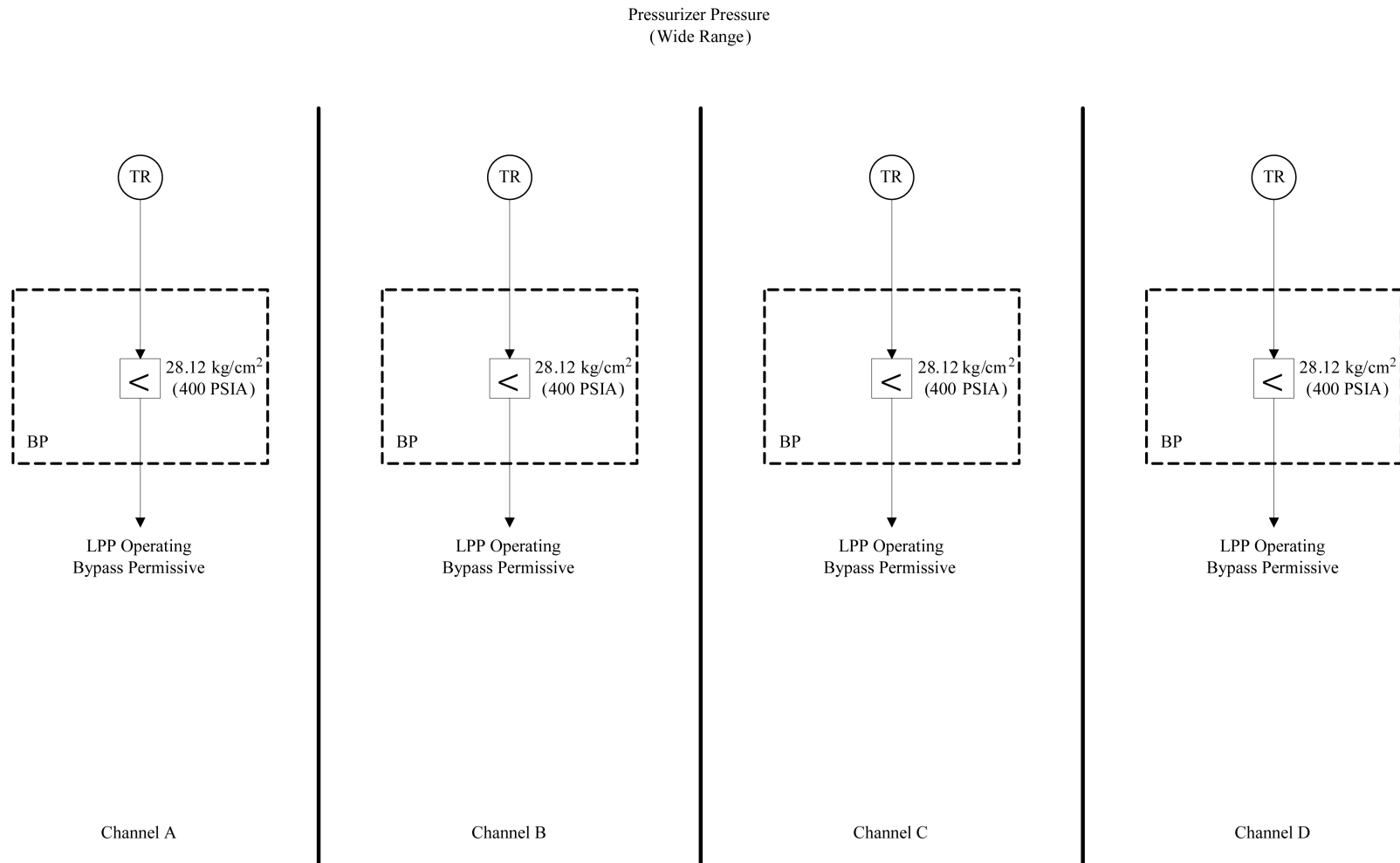


Figure 7.2-30 Functional Logic Diagram for Low Pressurizer Pressure Operating Bypass Permissive

APR1400 DCD TIER 2

Excore Neutron Flux Power

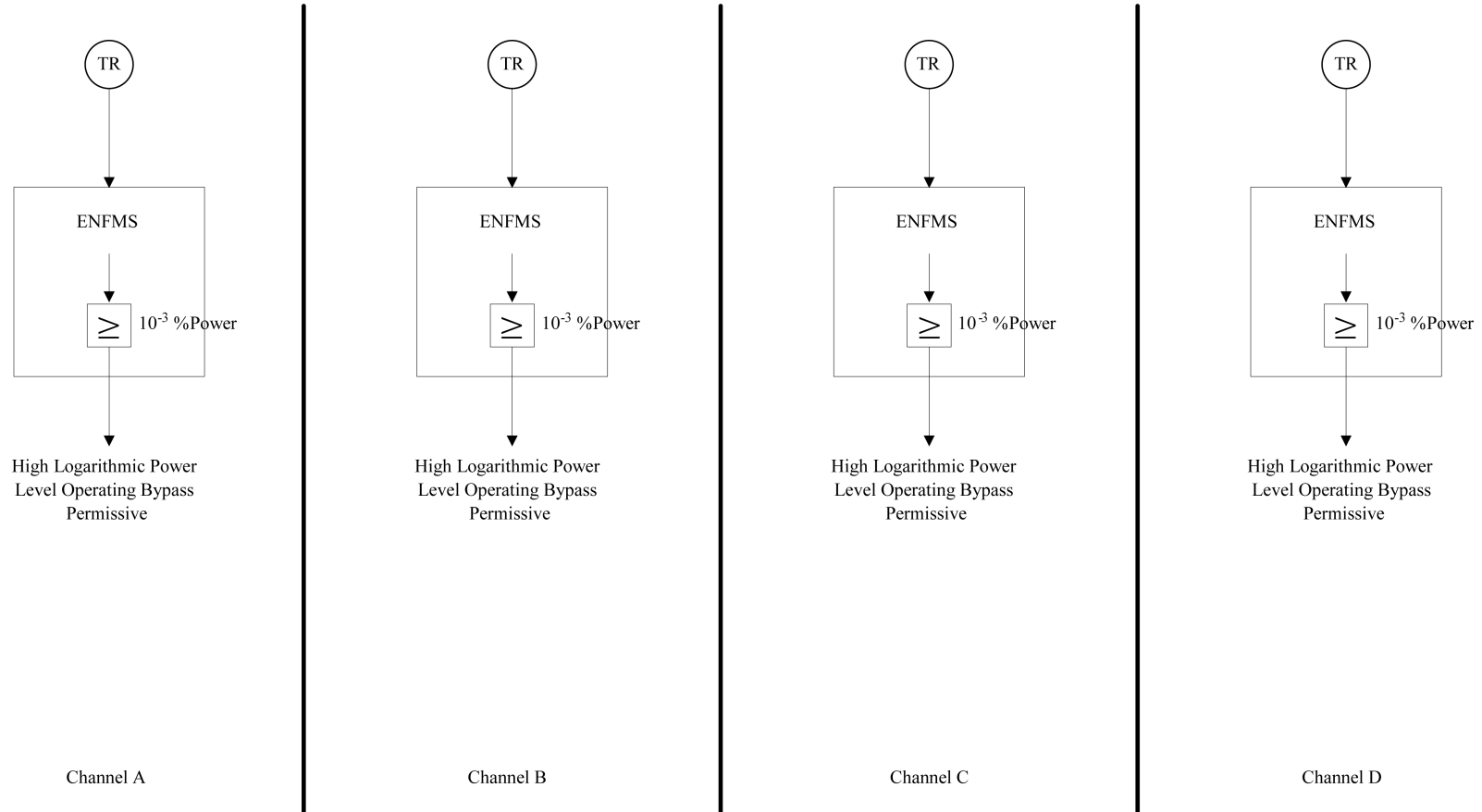


Figure 7.2-31 Functional Logic Diagram for High Logarithmic Power Level Operating Bypass Permissive

APR1400 DCD TIER 2

Excore Neutron Flux Power

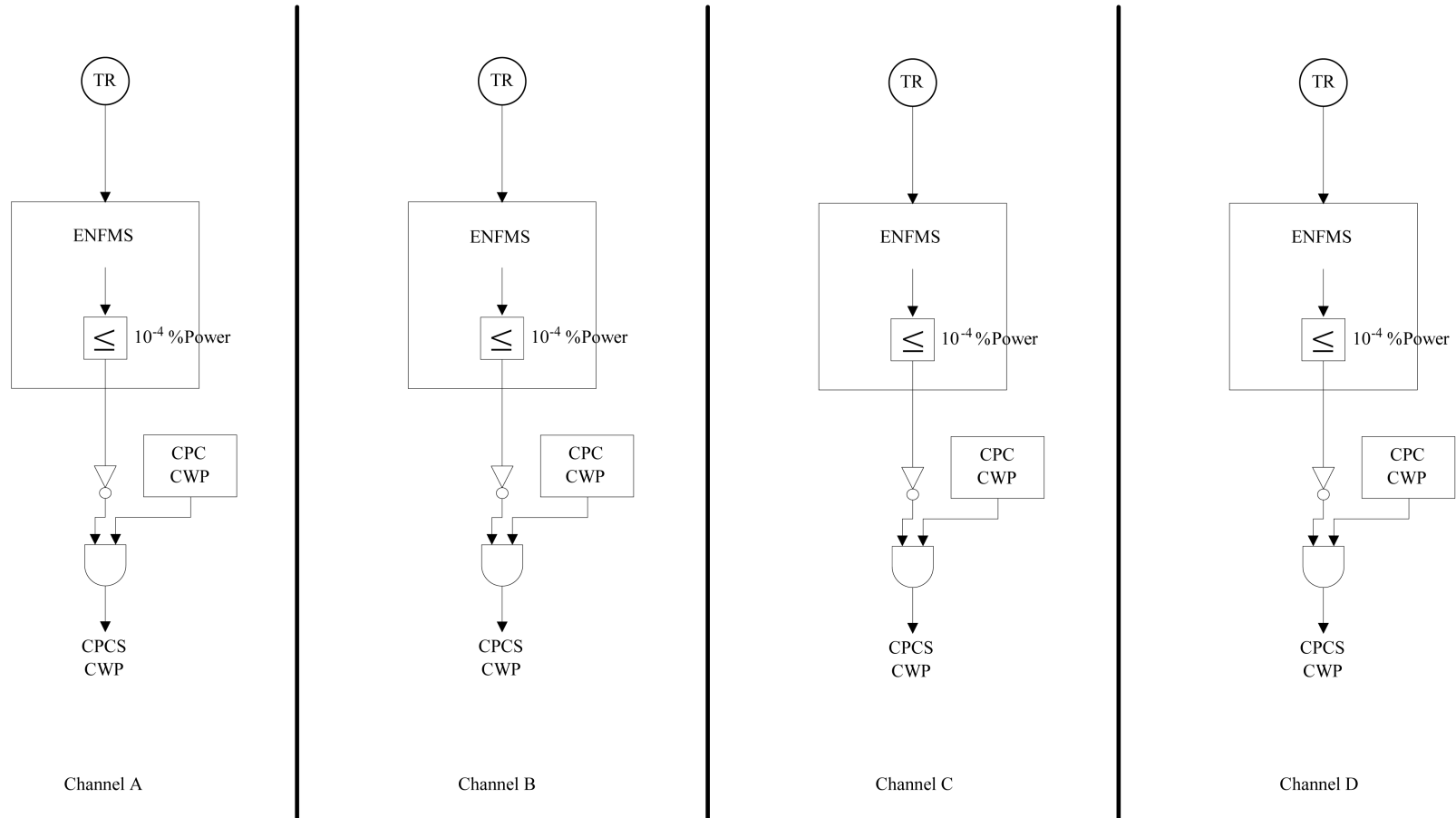


Figure 7.2-32 Functional Logic Diagram for CPC CWP Operating Bypass

7.3 Engineered Safety Features Systems

7.3.1 System Description

The engineered safety features (ESF) system consists of four channels of sensors, auxiliary process cabinet-safety (APC-S), the engineered safety features actuation system (ESFAS) portion of the plant protection system (PPS), and the engineered safety features-component control system (ESF-CCS). The safety instrumentation and controls of the ESF systems consist of the electrical and mechanical devices and circuitry from sensors to actuation device input terminals that are involved in generating signals that actuate the required ESF systems.

The ESFAS portion of the PPS includes the following functions: bistable trip logic, local coincidence logic, ESFAS initiation, and testing function.

The ESF-CCS receives ESFAS initiation signals from the PPS and the radiation monitoring system (RMS), or from the operator and generates ESFAS actuation signals to actuate the ESF system equipment. The control circuitry for the components provides the proper sequencing and operation of the ESF systems.

The ESF-CCS provides discrete and continuous control of the safety-related systems as well as automatic or manual actuation of the ESF systems components. ESF-CCS controls breaker/relay operated components (e.g., pumps, fans, heaters, motor-operated valves), solenoid operated components (e.g., pneumatic, electro-pneumatic, direct-operated valves), and control valves. The ESF-CCS also controls continuous control devices such as modulating valves. The ESFAS actuation and component control logics are located in the ESF-CCS cabinets.

Upon receipt of ESFAS initiation signals from the PPS and RMS, the ESF-CCS generates ESFAS actuation signals.

The simplified functional diagram and the block diagram of the ESF-CCS are shown in Figure 7.3-3A and Figure 7.3-3B respectively.

a. ESF-CCS configuration

APR1400 DCD TIER 2

The ESF-CCS consists of four channels of group controller (GC) cabinets and loop controller (LC) cabinets. The ESF-CCS interfaces with the maintenance and test panel (MTP), interface and test processor (ITP), and operator module (OM).

Each GC provides an ESFAS actuation signal to the LC and supports the component control. The ESF functions are assigned to GCs within each ESF-CCS channel. Each LC has component control logic and multiplexing function.

The MTP provides the indication for ESF-CCS status, ESFAS reset, and the human-system interfaces (HSIs) for maintenance, testing, and diagnostics. The MTP supports the interface with the IPS. The ITP has a data communication interface with the qualified indication and alarm system-non-safety (QIAS-N). The OM provides the indication of the ESFAS actuation, ESF-CCS status, and ESFAS reset.

*[The ESF-CCS is designed based on a programmable logic controller (PLC) platform. The ESF-CCS software is developed and tested in accordance with the Software Program Manual Technical Report (Reference 1).]**

b. ESF-CCS logic

The ESF-CCS provides system-level actuation logic for the ESF actuation, component control logic, test logic, and diesel loading sequencer logic.

Each ESF-CCS GC performs 2-out-of-4 logic using the ESFAS initiation signals from the four channel PPS.

The output of the 2-out-of-4 logic is transmitted to the component control logic in the LC. The component control logic is the component-level logic that processes manual on-off demand and interlock signals to control the process component. The component control logic performs prioritization of command signals. This logic also processes the status information of the component.

The ESF-CCS provides interface and signal fan out capability for the ESF actuation signals to the switchgear and motor control center via component control logic within the ESF-CCS. The logic produces digital output signals to control the component through the component interface module (CIM), which performs signal

APR1400 DCD TIER 2

prioritization. The CIM transmits signals to the final actuated device (e.g., switchgear, motor control center, solenoids).

The ESF-CCS provides master transfer switching to disable all main control room (MCR) controls and enable remote shutdown room (RSR) controls.

7.3.1.1 ESFAS Measurement Channels

The ESFAS measurement channels perform continuous monitoring of each selected plant variable and transmit analog signals to bistables.

A typical measurement channel is shown in Figure 7.2-2. It consists of a sensor/transmitter, current loop resistors, loop power supply, and fiber optic isolated outputs for the IPS and QIAS-N.

A measurement channel is physically separated and electrically isolated from other channels.

7.3.1.2 ESFAS Bistable and Coincidence Logic

The bistable processors (BPs) are in the PPS cabinet. The ESFAS bistable logic in the BP compares the analog signal from the sensors with predetermined fixed or variable setpoints. If the input signal exceeds the setpoint, the bistable logic produces trip signals that are transmitted to the coincidence logic.

For the nuclear steam supply system (NSSS) ESFAS, there are two redundant BP processors in each channel. The outputs of the two BP processors are designated as follows: A1 and A2 in channel A; B1 and B2 in channel B; C1 and C2 in channel C, and D1 and D2 in channel D, as shown in Figure 7.2-10.

The LCL consists of redundant 2-out-of-4 voting of 1-out-of-2 logic of the redundant BP processor outputs in each channel. For example in channel A, the logic is 2-out-of-4 of [(A1 or A2), (B1 or B2), (C1 or C2), (D1 or D2)].

The resulting signal in the LCL is transmitted to the ESF-CCS logic via serial data link (SDL).

APR1400 DCD TIER 2

7.3.1.3 Actuation Logic

The ESFAS consists of nuclear steam supply system (NSSS) ESFAS and balance of plant (BOP) ESFAS.

NSSS ESFAS signals are as follows:

- a. Safety injection actuation signal (SIAS)
- b. Containment spray actuation signal (CSAS)
- c. Containment isolation actuation signal (CIAS)
- d. Main steam isolation signal (MSIS)
- e. Auxiliary feedwater actuation signal (AFAS)

BOP ESFAS signals are as follows:

- a. Fuel handling area emergency ventilation actuation signal (FHEVAS)
- b. Containment purge isolation actuation signal (CPIAS)
- c. Control room emergency ventilation actuation signal (CREVAS)

The ESF-CCS serves as an interface between the ESFAS portion of PPS with the switchgear and motor control center, as shown Figure 7.3-3B.

Each ESF-CCS channel consists of redundant group controller logic (GC) and redundant logic control (LC). Each ESF-CCS channel receives ESFAS initiation signals from all four channels of the PPS and performs an automatic initiation of the affected ESF system(s) when coincidence logic conditions are satisfied. The 2-out-of-4 actuation logic is performed in the ESF GC 1 and 2 process logic, which independently receive ESFAS initiation signals from four PPS channels (Channels A, B, C, and D) and perform a 2-out-of-4 coincidence voting logic on the initiating signals. Valid ESF-CCS system-level initiation signals are latched and require a manual reset. Two redundant GCs (GC 1 and GC 2) are provided for improved GC availability within each ESF-CCS channel.

The 2-out-of-4 actuation logic in GC processors enhances the fault tolerance to maintain system-level availability and minimize the consequences of single failures. A failure of a

APR1400 DCD TIER 2

processor in the PPS or data communication between PPS and ESF-CCS is tolerated by the signal quality checking logic and the voting logic in GC.

The ESF-CCS GCs 1 and 2 provide initiation signals to the redundant LCs in the respective channel via SDLs. Each ESF LC receives the ESF initiation signals from both ESF-CCS GCs 1 and 2. Refer to Figure 7.3-3A for a simplified ESF-CCS control diagram.

All ESF actuation signals can be initiated using manual ESF system-level actuation switches on the safety console. In the actuation logic, each signal also sets a latch to provide reasonable assurance that the system-level signal is not automatically reset once it has been initiated, as shown in Figure 7.3-2. Each ESFAS, excluding the cycling portion of the AFAS, can be manually reset to restore the initiation logic to the non-actuated state from the OM or MTP when ESF actuation condition is cleared.

The BOP ESFAS consists of 1-out-of-2 logics taken twice, BOP manual ESF system-level actuation switches, channel bypasses, and indicating lights on the safety console.

ESFAS Function

The ESFAS consists of six NSSS ESFAS signals and three BOP ESFAS signals. Each ESFAS has manual actuation switches on the safety console and operator workstation in the MCR. MSIS also has manual actuation switches at the remote shutdown console.

- a. Safety injection actuation signal (SIAS)

Input

Low pressurizer pressure, high containment pressure, or manual ESF system-level actuation switches located on the MCR safety console (SC). The pressure signals are shared with the RPS.

Function

The SIAS actuates the components necessary to inject borated water into the RCS and actuates components for emergency cooling. An SIAS also actuates the containment spray pumps. An SIAS is also initiated by a loss of power to two PPS channels. The SIAS also actuates the emergency diesel generator (EDG).

APR1400 DCD TIER 2

The functional logic for SIAS is shown in Figure 7.3-1A.

b. Containment spray actuation signal (CSAS)

Input

High-high containment pressure signals or manual ESF system-level actuation switches located on the MCR SC.

Function

The CSAS actuates the containment spray system (CSS). CSAS is also initiated by a loss of power to two channels.

The functional logic for CSAS is shown in Figure 7.3-1B.

c. Containment isolation actuation signal (CIAS)

Input

Low pressurizer pressure, high containment pressure, or manual ESF system-level actuation switches located on the MCR SC.

Function

The CIAS actuates the isolation of lines penetrating the containment. CIAS is also initiated by a loss of power to two channels.

The functional logic for CIAS is shown in Figure 7.3-1B.

d. Main steam isolation signal (MSIS)

Input

Low pressure from each SG, high containment pressure, low level from each SG, or manual ESF system-level actuation switches located on the MCR SC.

Function

The MSIS is provided to actuate the isolation of each SG. MSIS is also initiated by a loss of power to two channels.

APR1400 DCD TIER 2

The functional logic for MSIS is shown in Figure 7.3-1D.

- e. Auxiliary feedwater actuation signal (AFAS-1, AFAS-2)

Input

Low level from each SG or manual ESF system-level actuation switches located on the MCR SC.

Function

The AFAS actuates auxiliary feed water on low water level of the SG(s). AFAS is also initiated by a loss of power to two channels.

Actuation function AFAS-1 pertains to SG 1, and AFAS-2 actuation function pertains to SG 2.

The functional logic for MSIS is shown in Figure 7.3-1C.

- f. Fuel handling area emergency ventilation actuation signal (FHEVAS)

Input

High radiation level sensed by spent fuel pool area radiation monitors or manual system-level actuation switches located on the MCR SC.

Function

The FHEVAS isolates the normal HVAC and actuates the emergency ventilation system.

The functional logic for FHEVAS is shown in Figure 7.3-1F.

- g. Containment purge isolation actuation signal (CPIAS)

Input

High radiation level sensed by containment upper and operating area radiation monitors or manual system-level actuation switches located on the MCR SC.

APR1400 DCD TIER 2

Function

The CPIAS isolates and closes the containment purge lines and stops the containment purge fans.

The functional logic for CPIAS is shown in Figure 7.3-1G.

- h. Control room emergency ventilation actuation signal (CREVAS)

Input

High radiation level sensed by MCR air intake airborne radiation monitors or manual system-level actuation switches located on the MCR SC.

Function

The CREVAS isolates the normal main control room ventilation system, starts the emergency ventilation system, and thereby maintains the positive pressure in the MCR envelope.

The functional logic for CREVAS is shown in Figure 7.3-1H.

7.3.1.4 Component Control Logic

All ESF component control logics are located in the ESF-CCS cabinets. Each redundant LC component control logic consists of a primary processor module and a standby processor module as shown in Figure 7.3-3B. The primary and standby processor modules exchange health status data with each other via an SDL. If PM1 experiences a hardware failure, its health status is sensed by PM2, which initiates a failover, and PM2 then becomes the “output active” processor module. If a failure is detected in GC-1 or GC-2, the output signal of the failed GC is assigned a bad data quality. The LC detects the bad data quality and uses the signals from the redundant GC to calculate the LC output. The LCs provide discrete ESF component-level actuation signals to the associated CIM.

The redundant LCs receive the following input signals:

- a. Diesel sequencer load shed signals
- b. Diesel sequencer load sequence signals

APR1400 DCD TIER 2

- c. ESF-CCS GC automatic output signals
- d. Dedicated manual system-level ESFAS function switches located on the MCR safety console
- e. Dedicated MI component-level switches located on the safety console
- f. Soft component-level controls from non-safety workstations on the operator console via the ESF-CCS soft control module (ESCM) and control channel gateway (CCG).

The LC priority logic performs a prioritization on the applicable input signals on a component-level basis. The output of the LC priority logic is then input to the priority logic in the CIM.

For each ESFAS function, there is an associated group of outputs to send component actuation demand to LC. Outputs from the ESF-CCS GC override the interlock in the component control logic in the ESF-CCS LC.

The features of the override logic for the component control are described in the Safety I&C System Technical Report (Reference 2).

The LC logic processes status of the component. The actuation logic is categorized by the following five types depending on the actuated equipment:

- a. Solenoid-operated valve control
- b. Reversing motor starter control
- c. Non-reversing motor starter control
- d. Medium voltage switchgear and load center control
- e. Electro-hydraulic motor damper control

ESF-CCS also provides continuous control and monitoring functions.

Solenoid-Operated Valves

- a. Two-state solenoid valve control

APR1400 DCD TIER 2

The ESF-CCS executes the control logic necessary to energize the solenoid as a function of the open/closed state to which the energized solenoid corresponds. In general, there is one solenoid for direct operation of the electro-hydraulic or electro-pneumatic valve types. Figure 7.3-6 is a typical control logic diagram (CLD) that shows the control design of a solenoid-operated valve. For valves that have multiple solenoids with various energize/de-energize sequencing requirements that apply to different operating or test modes, the generic control logic design and electrical interface design are modified appropriately.

The ESFAS actuation signal provides an input to the override logic to interlock in the functional control logic for override of each of these components.

The following signals are used in the control logic:

1) Position status

The control logic uses fully open (FO) and fully closed (FC) position signals. These signals come from limit switches mounted on the process control valve. The signals are used primarily for status indication and for interlocking with other components.

2) Control signal

The control logic uses the two-state output relay and the continuity monitoring circuit associated with the output. A digital output module in the loop controller provides the relay output interface to energize the solenoid.

The position signals, control output status, and continuity monitoring status are logically combined to provide a component status indication (OPEN/CLOSED), component operation status deviation indication (i.e., a component not in the required position), and component inoperable indication (i.e., loss of control power or circuit continuity).

The component inoperable signal is used to reset the component control logic following a loss of motive or control power, and is delayed momentarily to prevent the normal switching transients or momentary losses of power from unnecessarily resetting the component logic.

APR1400 DCD TIER 2

b. Modulating valves with solenoid operators

Modulating valves with solenoid operators are solenoid-operated valves that have electro-pneumatic modulators to allow continuous valve positioning. Figure 7.3-7 is a typical CLD depicting the generic control design of a modulating valve with a solenoid operator.

The following signals are used in the control logic:

1) Position status

The position status signal is used for status indication of the energized state of the solenoid. This signal is derived from limit switches mounted on the valve. Where this is not available, the signal is derived from a logic element that is representative of solenoid energization.

2) Analog position

The continuous valve position indication is provided for valves when it is required for operational tasks. An analog input is received from a position transducer on the valve and interfaced with an analog input module in the loop controller.

3) Control signal

The continuous process signal for positioning the modulating valve is provided to the electro-pneumatic or electro-hydraulic positioner from an interface with an analog output module in the loop controller.

The control design for modulating valves and other modulated components without discrete state operators are discussed in this subsection.

Reversing Motor Starter Control

This subsection describes the control logic for motor-operated valves (MOVs) that use reversing motor contactors. The ESF-CCS executes the control logic necessary to energize the open and close motor control contactors.

a. Interface signals

APR1400 DCD TIER 2

Interlocking of the open/closed motor control contactors, electrical fault and/or thermal overload protection, and interlocking with the limit and torque switches are wired external to the ESF-CCS control logic. These features are not shown in the CLDs. Figure 7.3-8 depicts a typical MOV functional interface design. The interface signals are as follows:

- 1) Position status

Position status signals are the same as those for solenoid valves. All MOVs have discrete state position indicators. Throttling MOVs also have a continuous position indication if required for operational tasks.

- 2) Control signal

The control logic uses the two-state output relay and the continuity monitoring circuit associated with each output. A digital output module in the loop controller provides the relay output to energize the motor control contactor.

- 3) Motor control contactor de-energized

The control logic uses one signal to determine when the opening coil or closing coil is de-energized. This signal is generated from a combination of opening and closing coil contacts that are wired together in the motor starter. The signal interfaces with a digital input (DI) module in the loop controller. This design allows the valve motor to stop by torque or limit switches without ESF-CCS intervention. The contactor de-energized signal results in the ESF-CCS opening its control contacts, thereby allowing the use of local controls.

The position signals, contactor de-energized signal, control output status, and continuity monitoring status are logically combined to provide the component status indication (OPEN/CLOSE), component operation status deviation indication (component not in the requested position), component inoperable indication (loss of control power or circuit continuity), and high torque conditions (torque switch open). The component inoperable signal prevents the resetting of the latches in the control logic and is used to provide an indication to the operator that the component is inoperable.

APR1400 DCD TIER 2

b. Throttling and full stroke designs

The ESF-CCS provides full stroke or throttling (or jogging) valve control. Full stroke valves are actuated by signals that are latched in the control circuit so that valve travel continues even if the initiating control signal is removed. All full stroke MOVs can be reversed in mid-travel by removal of the initiating control signal and application of a control signal for travel in the opposite direction. Figure 7.3-9 is a typical CLD depicting the generic design of a full stroke MOV.

Throttling MOVs stop traveling when the operator-initiated control signal is removed. As such, they can be positioned by the operator between 0 percent and 100 percent. Where throttling MOVs are also controlled by automatic ESFAS actuation signals, the control response to the ESFAS actuation signal is always full stroke. Figure 7.3-10 is a typical CLD depicting the generic design of a throttling motor-operated valve.

c. Thermal overload monitoring

The application of thermal overload protection devices in Class 1E motor-operated valve circuits is described in Subsection 8.3.1.2.2. Thermal overload protection devices are used for trip. The trip setpoint of the thermal overload protection devices are established to complete the safety action.

Non-reversing motor starter control

A typical CLD for the generic control design of a motor control is shown in Figure 7.3-11. The ESF-CCS provides the control logic necessary to energize the contactor. The designs for electrical fault and/or thermal overload protection in the electrical panel are wired external to the ESF-CCS. The interface signals are described as follows:

a. Position status

The control logic uses an auxiliary contact from the contactor for the status signal. The signal interfaces with a DI module in the loop controller.

b. Control signal

APR1400 DCD TIER 2

The control logic uses the state of the output relay and continuity monitoring circuit associated with the output. A digital output module in the loop controller provides the relay output signal to energize the contactor.

The position status signal, control signal, output status, and continuity monitoring are logically combined to provide contactor status indication (ON/OFF), contactor discrepancy indication (contactor not in requested position), and component inoperable (loss of control power or circuit continuity) status. The component inoperable signal prevents the resetting of the latches in the control logic and is used to provide an indication to the operator that the component is inoperable.

Medium Voltage Switchgear and Load Center Control

The circuit breakers are used to control most of the loads requiring voltage greater than 480 Vac. Figure 7.3-12 is a typical CLD depicting the generic control logic necessary to energize the breaker closing circuit and energize the breaker trip circuit.

Modulating components

A typical CLD showing the generic design of a modulating component is depicted in Figure 7.3-13A. These types of devices include electro-pneumatic and electro-hydraulic actuated components (valves) that require only analog signal inputs for continuous control (i.e., no discrete state controls from pilot solenoids).

The following signals are interfaced with the ESF-CCS from the component:

a. Status

Valve position

- 1) Full open (FO) and full closed (FC) position signals from the indicating limit switches interface with a DI module of the loop controller.
- 2) The analog valve position is used as required, based on the operational task requirement. The position signal generated from a position transducer interfaces with an analog input module of the loop controller.

b. Component inoperable

APR1400 DCD TIER 2

The component inoperable indication is provided from the component (circuit breaker or contactor) when a loss of control feedback signals and motive power signals occur.

Electro-hydraulic Motor Damper

The electro-hydraulic motor circuit is used for the single coil ac motor starter with the process damper position limit switches. The process damper opens when the hydraulic motor is started, and closes when the coil is de-energized.

In general, there is an ac motor starter for a direct-operating electro-hydraulic motor damper. Figure 7.3-13B shows a typical CLD that depicts the control design of an electro-hydraulic motor damper.

The following signals are used in the control logic:

a. Position status

The control logic uses FO and FC position signals. These signals are from the direct indicating limit switches on the dampers and are used primarily for status indication and interlocking with other components.

b. Control signal

The control logic uses a two state output relay and the continuity monitoring circuit associated with the output. A digital output module in the loop controller provides the relay output to energize the motor starter.

The position signals, control output status, and continuity monitoring status are logically combined to provide the component status indication (OPEN/CLOSED), the component operation status deviation indication (component not in the required position), and the component inoperable indication (loss of control power or circuit continuity).

The component inoperable signal is used to reset the component control logic following a loss of motive or control power, and is delayed momentarily to prevent normal switching transients or momentary losses of power from unnecessarily resetting the component logic.

7.3.1.5 Bypasses

a. Operating bypass

The low pressurizer pressure bypass as shown in Figure 7.3-1A, is provided to allow plant depressurization without initiating protective actions when not desired. The bypass can be initiated manually in each protective channel. However, the bypass cannot be initiated if pressurizer pressure is greater than that shown in Table 7.3-1. Once the bypass is initiated, it is automatically removed when pressurizer pressure increases above the value shown in Table 7.3-1.

b. Channel bypass

A trip channel bypass prevents a bistable trip. The bistable logic bypass converts the local coincidence logic to a 2-out-of-3 coincidence.

An individual trip channel bypass is possible on each MTP switch panel for each bistable trip. A trip channel bypass is used when removing a trip channel input from service for maintenance or testing. The trip channel bypass signal is distributed to the LCLs in the four redundant channels.

The process sensor (or transmitter) signal can be bypassed using the trip channel bypass.

An all-bypass function for all ESFAS variables is provided to bypass all parameters in one channel. The all-bypass switch is connected to local coincidence logic (LCL) DI module.

7.3.1.6 Interlocks

a. Trip channel bypass interlock

Bypassing the same parameter simultaneously in more than one channel is restricted by an administrative procedure. An all-bypass function for bypassing all parameters in the channel is interlocked in the LCL algorithm to prevent simultaneous bypass of more than one channel. The all-bypass interlock is implemented based on analog circuit through a hard-wired cable between LCLs in

APR1400 DCD TIER 2

all channels. The purpose of the all-bypass function is to support testing and maintenance of BP whereas the trip channel bypass is used against sensor failure.

b. Manual test interlock

The manual test function is performed when the function enable key switch is activated.

7.3.1.7 Redundancy

There are four independent channels for each parameter from the process sensors to the initiation logics in the PPS for the NSSS ESFAS.

There are two independent channels for each parameter from the process sensors to the actuation logics in the GC for BOP ESFAS.

Each ESF-CCS channel actuates the ESF components assigned in that channel.

The ESF system meets the single failure criterion and can be tested during operation.

The ESFAS coincidence logic in the LCL is changed to 2-out-of-3 logic when a channel is removed for testing or maintenance without affecting system availability.

7.3.1.8 EDG Loading Sequencer

Because of the large power requirements imposed on the EDGs by equipment that is connected, there is a need to sequentially load the equipment.

The diesel generators are used in the design as a source of backup electrical power to provide reasonable assurance of the availability of plant safety systems when the preferred power is lost. Further defense-in-depth is provided by the alternate ac power source, which can be aligned to feed power to either of the safety buses in the event of failure of either the diesel generators or the preferred power source.

The plant equipment is arranged into several load groups. Each load group is connected to the emergency diesel generator (EDG) one at a time by the ESF-CCS EDG loading sequencer to avoid simultaneous loading of large loads, which could overload the EDG. The equipment is energized in a predetermined time interval to minimize the overall plant disturbance.

APR1400 DCD TIER 2

The loading sequencer is implemented in each ESF-CCS channel.

To minimize the EDG size and eliminate unnecessary equipment cycling but maintain plant safety, the ESF-CCS loading sequencer design provides reasonable assurance of loading one group at a time but has the capability to vary the loading sequence in response to changing plant conditions (e.g., initiation of ESF systems).

The loading sequencer is also used when fast transfer of offsite power is made to prevent a large voltage dip on the bus when multiple large Class 1E pump motors are started in response to either manual commands or ESF actuation signals.

The loading sequencer is designed to respond to the occurrence of a plant accident prior to, concurrent with, or any time after the initial loss of offsite power (LOOP). The ESF equipment required in the event of a design basis event (DBE) is energized within a predetermined time interval after the accident has occurred to maintain the plant within its design limits. The equipment that is required depends on the type of accident. Several load groups of equipment are used if multiple ESF systems are required to mitigate the accident.

The control logic diagram for the ESF-CCS EDG loading sequencer is shown in Figure 7.3-4.

a. Sequencer initiation logic

The four redundant undervoltage relays detect the loop condition on each of two 4.16 kV buses in each Class 1E power division. An undervoltage condition occurs when any two of four relays detect an undervoltage condition. Upon occurrence of an undervoltage condition, the logic that monitors that bus initiates an automatic start of the associated EDG, initiates load shed (trip) signals to large loads in that power division, and sets all sequencer outputs to latch. The EDG loading sequencer monitors the position of the breakers, which receive load shed signals and, upon receiving an indication that all of the breakers are open, generates a permissive to allow load sequencing to proceed. When the diesel generator is ready to accept the first load group, the EDG circuit breaker close signal is transmitted to connect the EDG to the plant bus.

An EDG auto start signal is also transmitted to the diesel generator upon occurrence of an SIAS, AFAS, and CSAS. If a bus undervoltage condition is not present, the signal is not sent, and the EDG circuit breaker is not closed. The

APR1400 DCD TIER 2

equipment loading sequence then begins loading the components onto the 4.16 kV Class 1E bus, which is powered from the preferred power source.

b. EDG loading sequencer logic

The basis of the EDG loading sequencer logic is an eight-step counter. Steps are added as necessary to provide the sequencing control of other equipment. When the EDG has attained a necessary operating condition (e.g., speed, voltage, frequency), the EDG circuit breaker is closed, and the counter advances, one step at a time, with a constant time base interval between each step.

Each EDG is automatically started and runs on receipt of an SIAS, AFAS, or CSAS from the ESF-CCS or LOOP signal from 4.16 kV Class 1E buses. Receipt of an SIAS or a LOOP signal at the 4.16 kV Class 1E buses automatically initiates the sequence. Following the LOOP signal, when the emergency diesel generator reaches rated voltage and frequency, the EDG circuit breaker closes, and the sequencer generates the proper signal to connect the ESF equipment to the Class 1E buses in the programmed time sequence. All ESF equipment is connected to the Class 1E buses within a predetermined time period after the EDG start signal upon a LOOP alone or a LOOP concurrent with SIAS, AFAS, or CSAS.

The EDG loading sequencer provides the following features:

- 1) Because all load groups are always energized one at a time, the EDG size can be minimized.
- 2) Accident loads are always energized in the sequence step immediately following the accident occurrence to achieve the best availability possible for the accident equipment.
- 3) Equipment is load shed one time only. Once a Class 1E Division load group is energized, that group is unaffected by the occurrence of an accident.
- 4) The EDG loading sequencer testing features, defined in Subsection 7.3.2.5, allow complete system check-out while the plant remains online.

APR1400 DCD TIER 2

- 5) When offsite power is lost at some time after the diesel generators are up to rated voltage and speed and after the required ESF equipment is running ESF actuations, the response time assumed in Chapter 15 safety analyses are met.

In the event that offsite power is unavailable and the diesel generators are not yet up to rated voltage and speed at the time that an ESFAS is generated, there can be a delay of up to 20 seconds before the EDG output breakers close and power is supplied to the ESF buses. After the generators are connected to the ESF buses, the ESF loads that are appropriate in a particular ESFAS group are automatically sequenced on. Refer to Section 8.3 and Table 8.3.1-1.

7.3.1.9 Actuated Systems

The ESF systems are maintained in a standby mode during normal operations. Actuating signals, generated by the ESFAS, provide reasonable assurance that the ESF systems actuate the required protective actions within the response time identified in the safety analyses. Table 7.3-2 presents the DBE that require ESF system actuation for mitigation. Table 7.3-3 presents the monitored variables required for each ESF system actuation. The variables and their ranges are shown in Table 7.3-6.

a. Containment isolation system

Subsection 6.2.4 contains a description of the containment isolation system (CIS). The actuation system is composed of redundant channels A and B. The instrumentation and controls of the two trains are physically and electrically separate and independent so that the loss of one train will not impair the safety function.

The CIS instrumentation and controls are designed for operation during all phases of plant operation. However, the system is removed from service prior to containment leak checking at refueling period intervals in order to prevent undesired system actuation. The removal from service is accomplished in accordance with the procedures prepared by the site operator.

The CIS is automatically actuated by a CIAS.

Remotely operated (automatic or manual) containment isolation valves (CIVs) are provided with control and indication capability in the MCR. Additionally, a

APR1400 DCD TIER 2

closed position signal of each valve inputs into the IPS and QIAS for critical function monitoring, which detects unisolated containment penetrations by monitoring valve status required to close on a CIAS.

The process information is provided in the MCR, which the operator uses to determine when to isolate the fluid systems.

All systems that provide a path from the containment to the environment (e.g., containment purge and vent systems) have their CIVs closed on a CIAS signal.

b. Containment spray system

Subsection 6.5.2 contains a description of the CSS. The CSS is actuated by a CSAS. The containment spray pumps are also actuated by an SIAS. When used in the containment spray configuration, the shutdown cooling pumps are actuated by an SIAS or CSAS.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of each train are physically and electrically separate and independent. Each train has 100 percent capacity. Therefore, the CSS can sustain the loss of an entire train and still provide its required protective action and safety function. The CSS instrumentation and controls are designed to operate under all plant conditions.

The CSAS is removed from service prior to the containment leak test at refueling period in order to prevent undesired system actuation. The removal from service is accomplished in accordance with procedures prepared by the site operator.

The ESF-CCS design accommodates realignment of a spray pump for use as a shutdown cooling pump and vice versa.

c. Main steam isolation system

Section 10.3 contains a description of the main steam isolation system. Subsection 10.4.7 contains a description of the main feedwater isolation system. Subsection 10.4.8 contains for a description of the blowdown isolation system.

The actuation system is composed of redundant trains A and B. The instrumentation and controls of the valves in train A are physically and electrically

APR1400 DCD TIER 2

separate and independent of the instrumentation and controls of the valves in train B. The separation and independence are such that a failure of one train does not impair the protective action and safety function.

The main steam isolation valves (MSIVs), MSIV bypass valves, main feedwater isolation valves (MFIVs), and the isolation valves for the blowdown lines are actuated by an MSIS.

These valves effectively isolate the SGs from the rest of the main steam and feed water system.

A variable SG pressure setpoint is implemented to allow controlled pressure reductions, such as shutdown depressurization, without initiating a MSIS. The pressure setpoint tracks the pressure until it reaches its normal setpoint value.

d. Safety injection system

Refer to Section 6.3 for a description of the SIS. The safety injection system (SIS) is actuated by an SIAS. The actuation system is composed of redundant channels A, B, C, and D. The I&Cs of each train are independent. The SIS can sustain the loss of an entire train and still provide its required protective action because each train is a 100 percent capacity system. The SIS I&Cs are designed to operate under all plant conditions.

The low pressurizer pressure setpoint can be decreased to avoid inadvertent operation during startup and shutdown. As pressurizer pressure increases, the setpoint follows up to its normal value. The SIAS is removed from service during containment leak checking at refueling period to prevent undesired system operation. The removal from service is accomplished in accordance with procedures prepared by the site operator.

e. Auxiliary feedwater system

The auxiliary feedwater system (AFWS) is actuated by an AFAS-1 for SG 1 and an AFAS-2 for SG 2. The AFWS is also actuated by the DPS.

Both motor-driven and turbine-driven auxiliary feedwater pumps aligned to the affected SG(s) are started simultaneously, and the auxiliary feedwater modulating

APR1400 DCD TIER 2

valves to the SG are automatically placed in the modulation mode. When an AFAS signal is actuated, the auxiliary feedwater modulation valves are in a modulation mode and opened/closed depending on SG level.

f. Fuel handling area HVAC system

Two radioactivity detectors in the spent fuel pool area provide radioactivity signals that produce signals for generation of a FHEVAS. The fuel handling area emergency ventilation system automatically starts following a receipt of an FHEVAS.

The logic for the FHEVAS is shown in Figure 7.3-1F.

g. Containment purge system

Four independent radioactivity monitors (e.g., two for monitoring the containment operating area and two for monitoring the containment upper operating area) provide, upon detection of high radiation levels, signals to the bistable logic, which produces redundant CPIAS.

The logic for the CPIAS is shown in Figure 7.3-1G.

h. Control room HVAC system

The process radiation system detects high radiation signals from the two outside supply air intakes in each train and takes the following actions:

- 1) Generates an alarm signal on high radiation levels in the affected supply air intake for the MCR
- 2) Automatically closes the normal path of makeup air supply to the control room HVAC system and routes air to the appropriate emergency makeup air cleaning units

The logic for the control room emergency ventilation actuation signal is shown in Figure 7.3-1H.

On detection of combustion products in the control room by the smoke detection system, an alarm is annunciated in the MCR. The I&C system for the HVAC

APR1400 DCD TIER 2

system complies with ANS 59.2 (Reference 3), and the instrumentation for emergency makeup air cleaning units is designed in conformance with NRC RG 1.52 (Reference 4).

7.3.1.10 Vital Instrument Power Supply

The vital instrument power supply is described in Chapter 8.

7.3.1.11 Component Interface Module and Interface Logic

The CIM provides the function of priority logic, feedback signal processing, and coil monitoring for safety critical component control. The priority logic is implemented by the non-software-based CIM. Based on its non-software design, the CIM is not considered in the potential of software common-cause failure (CCF). The CIM receives component control signals from the ESF-CCS, diverse manual ESF actuation (DMA) switches, and DPS and prioritizes the output signal to the plant component according to the predefined priority.

7.3.2 Design-Basis Information

The design bases of the ESF systems are addressed in Chapter 6. The ESFAS is designed to provide initiating signals for ESF components that require automatic actuation following the design basis events shown in Table 7.3-2.

System compliance with the 10 CFR 50 Appendix A, GDC is described in the Safety I&C System Technical Report, and cross references to information are provided in Table 7.1-1.

7.3.2.1 Single Failure Criterion

The ESFAS is designed so that any single failure within the system does not prevent proper protective action at the system level. No single failure defeats more than one channel. The system performs its protection function in the presence of any single failure and spurious system action that cause or may be caused by a design basis event.

Each ESF-CCS cabinet contains the actuation logic for only one channel, and a failure in one cabinet cannot affect the circuit or actuated equipment of the other channels.

APR1400 DCD TIER 2

The single failure of the initiation logic for the NSSS ESFAS in the PPS cabinet has no effect because 2-out-of-4 actuation logic is implemented in GC. The single failure of the actuation logic will cause the failure only of a component, group of components, or at worst an entire division. Actuation of the remaining channels is sufficient for the protective action.

The purpose of the BOP ESFAS is to automatically actuate valves and dampers of HVAC systems for ventilation of the fuel handling area, operation of containment purge system, and operation of the MCR HVAC system. If the BOP ESFAS signals are produced by spurious actuation of the BOP ESFAS system, which has 1-out-of-2 logic taken twice, the supply and return air fan in air control unit are actuated. The actuating ESFAS signals do not adversely affect plant safety or reactor trip.

Because the BOP ESFAS design is based on 1-out-of-2 taken twice, even if one channel is placed in bypass for testing and would occur simultaneously for both the radiation release accident and the single failure to another channel, the 1-out-of-1 logic of another channel can be actuated. The single failure criterion is met by changing the logic from 1-out-of-2 to 1-out-of-1 in the maintenance bypass.

In addition, the purpose of the bypass mode of the BOP ESFAS is to test a measurement channel. For BOP ESFAS design, double sets of two channels (A and B) are provided for measurement channels. Even if one measurement channel is placed in test mode, the other measurement channel of same channel is available.

7.3.2.2 Quality of Components and Modules

All ESFAS functions are implemented using Class 1E components.

7.3.2.3 Independence

The locations of the sensors for the ESFAS and the points at which the sensing lines are connected to the process loop have been selected to provide physical separation of the channels within the system, thereby precluding a situation in which a single event could remove or negate a protective action and safety function.

The cabling routing and sensing lines from sensors comply with NRC RG 1.75 (Reference 5) and NRC RG 1.151 (Reference 6). Cables for each channel are physically separated. The I&C cables are routed separately from the power cables.

APR1400 DCD TIER 2

The initiation logics are located in four PPS cabinets, and the actuation devices are controlled from four ESF-CCS cabinets. The geographical separation and electrical isolation between these cabinets reduces the possibility of a common-cause failure.

The outputs of each channel are isolated from each other. The loss of one channel does not cause loss of the system function.

7.3.2.4 Defense-in-Depth and Diversity

The defense-in-depth and diversity features within the ESF-CCS are implemented by the CIM. The output commands from the ESF-CCS, DPS, and/or DMA switch are inputted to the CIM, and the CIM prioritizes the command signals according to the priority logic as described in the CIM Technical Report (Reference 7).

According to BTP 7-19 and SECY 93-087 II.Q, Position 4, occurrence of both software CCF of PPS and ESF-CCS, and LOOP is evaluated.

Under the LOOP condition, the EDG is started to supply into the safety buses. However, if a disabled condition is initiated by software CCF of PPS/ESF-CCS, necessary power buses are supplied by the AAC DG through manual action.

The EDG start/stop function can be carried by the manual operation of the local switches for the applicable breakers. Load shedding and load sequencing can be carried by the manual operation of the local switches for the applicable load.

The ESFAS provides the echelon of defense, as described in Diversity and Defense-in-Depth Technical Report (Reference 8).

7.3.2.5 System Testing and Inoperable Surveillance

The ESFAS integrity is confirmed through periodic testing during power operation or shutdown. The tests cover the trip actions from sensor input to actuation device. The system test does not interfere with the protective function. The tests comply with the criteria of IEEE Std. 338 (Reference 9), which are endorsed by NRC RG 1.118 (Reference 10) and NRC RG 1.22 (Reference 11). The test intervals are specified in Chapter 16, Technical Specifications.

APR1400 DCD TIER 2

The test equipment consists of channelized MTP, ITP, and the associated interface circuits. Test results are verified at the MTP.

Bypasses and inoperable status of the safety system is displayed at the MTP and OM in accordance with NRC RG 1.47 (Reference 12).

Status information including input variable value, setpoint, trip, pre-trip, initiation, trip channel bypass, and operating bypass is displayed at MTP, OM and IPS.

ESFAS manual testing consists of the following:

a. Sensor check

During power operation, measurement channels for the ESFAS are checked by comparing process input values between channels in the IPS.

b. Bistable test

The manual bistable logic test is initiated to verify bistable logic functions from the MTP.

c. LCL test

The LCL test is initiated manually from the MTP. Trip path of 2-out-of-4 coincidence logic is tested for all input combination.

Testing of the BOP ESFAS logic is accomplished using the test features within the RMS.

d. Initiation logic test

The testing for the initiation “OR” logic is initiated from the MTP. Each ESFAS initiation logic function is tested individually.

APR1400 DCD TIER 2

e. Actuation logic test

Actuation logic testing is performed manually. Trip path of 2-out-of-4 coincidence logic is tested for all input combination.

f. Selective group test

For each ESF function, there is an associated group of outputs. Each group of outputs is divided into subgroups. Outputs within a subgroup are tested concurrently and are selectively arranged so that concurrent actuation does not adversely affect plant operations.

ESF-CCS selective group test is performed manually in the MTP. The testing is conducted one group at a time to prevent the complete undesired actuation of an ESF system during testing.

g. Response time test

Response time from the sensor to the actuation device is tested during shutdown to verify that the response times assumed in the Chapter 15 safety analysis are less than or equal to the actual time response.

h. EDG loading sequencer test

The EDG loading sequencer incorporates design features, shown in Figure 7.3-4, which allow complete online testing. During normal operation, all output control signals are disabled, allowing all logic functions to be tested without disturbing plant equipment. The outputs are enabled automatically when a valid initiation logic input signal is received. In this manner, testing can be conducted without impeding required sequencer operation.

7.3.2.6 Use of Digital Systems

All ESFAS functions rely on digital systems.

7.3.2.7 Setpoint Determination

The ESFAS nominal trip setpoints are determined based on the analysis setpoints in the Chapter 15 safety analysis.

APR1400 DCD TIER 2

When determining uncertainties, the worst environment considering ESF actuation is assumed for each different event. *[The methodology for calculating uncertainty is provided in Uncertainty Methodology and Application for Instrumentation Technical Report (Reference 13).]**

*[The methodology for combining uncertainty in a channel and determining the final actuation setpoint is provided in the Setpoint Methodology for Plant Protection System Technical Report (Reference 14).]**

The setpoint methodology follows the methodology in ISA-S67.04 (Reference 15) as endorsed by NRC RG 1.105 (Reference 16).

The response time of the instrumentation channel is a signal propagation time from the process sensor to the final actuation device. The response time for the ESF meets the amount of time assumed in Chapter 15. The ESFAS instrumentation response times assumed in the safety analysis in Chapter 15 are shown in Table 7.3-7.

7.3.2.8 Equipment Qualification

The ESF system is designed and tested in accordance with the requirements of IEEE Std. 323 (Reference 17) for environmental qualification and IEEE Std. 344 (Reference 18) for seismic qualification.

The ESF system is designed and tested to minimize both the emission and susceptibility of EMI and RFI in compliance with NRC RG 1.180 (Reference 19).

The ESF system is designed and tested to have immunity to electrostatic discharge and surge in accordance with IEC 61000-4-2 (Reference 20) and IEC 61000-4-5 (Reference 21), respectively.

7.3.2.9 System Drawings

The typical measurement channel functional diagram and functional logics are shown in Figures 7.2-2, 7.3-1A through 7.3-1H and 7.3-2.

7.3.3 Analysis

7.3.3.1 Failure Modes and Effects Analysis

The failure modes and effects analysis (FMEA) follows the methods of IEEE Std. 352 (Reference 22) referred from IEEE Std. 603 (Reference 23), IEEE Std. 7-4.3.2 (Reference 24), and IEEE Std. 379 (Reference 25).

The FMEA assumes that one bistable trip channel is bypassed for maintenance.

The FMEA results demonstrate that:

- a. Any single failure does not prevent a system-level ESFAS function due to four-channel redundancy
- b. Any single failure is detected by diagnostic or periodic test

The FMEA for ESFAS function from sensor to LCL is included in Table 7.2-7. Table 7.3-8 describes the FMEA for the ESF-CCS.

7.3.3.2 Conformance to IEEE Std. 603

Compliance with IEEE Std. 603 is addressed in the Safety I&C System Technical Report.

7.3.3.3 Conformance to IEEE Std. 7-4.3.2

Compliance with IEEE Std. 7-4.3.2 is addressed in the Safety I&C System Technical Report.

7.3.3.4 Analysis for Additional Postulated Failure

The analysis for additional postulated failures is as follows:

- a. Loss of cooling water to vital equipment: The APR1400 has four channels of safety-related cooling water, corresponding to the four channels of safety-related ESF equipment. These four channels are controlled by the ESF-CCS. Therefore, loss of a single channel of cooling water does not prevent accomplishing the safety function.

APR1400 DCD TIER 2

- b. Loss of plant instrument air: There is no reliance on plant instrument air for any safety functions.
- c. Loss of power source: All the subsystems in the safety system are provided 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 can result in a transient condition. A transient condition is considered in the safety analysis described in Chapter 15.

7.3.3.5 Periodic Testing Method

Compliance with the ESFAS to NRC RG 1.22 and IEEE Std. 338 is addressed in Table 7.1-1. Test intervals and their bases are included in Chapter 16, Technical Specifications.

The ESFAS is periodically tested to verify its operability. A channel is completely tested without causing a system actuation and affecting system operability and availability. Testing is overlapped to provide reasonable assurance that the entire channel is tested.

The response time test is performed during refueling outage.

7.3.4 Combined License Information

No COL information is required with regard to Section 7.3.

7.3.5 References

1. [APR1400-Z-J-NR-13003-P, “Software Program Manual Technical Report,” September 2013.]*
2. APR1400-Z-J-EC-13001-P, “Safety I&C System Technical Report,” September 2013.
3. ANSI/ANS 59.2-1985, “Safety Criteria for HVAC Systems Located Outside Primary Containment,” 1985.
4. NRC RG 1.52, Rev. 4, “Design, Inspection, and Testing Criteria for Air Filtration and Adsorption Units of Post-Accident Engineered-Safety-Feature Atmosphere Cleanup Systems in Light-Water-Cooled Nuclear Power Plants,” 2012.

APR1400 DCD TIER 2

5. NRC RG 1.75, Rev. 3, "Criteria for Independence of Electrical Safety Systems," 2005.
6. NRC RG 1.151, Rev.1, "Instrument Sensing Lines," 2010.
7. APR1400-E-J-NR-13001-P, "Component Interface Module," September 2013.
8. APR1400-Z-J-EC-13002-P, "Diversity and Defense-in-Depth Technical Report," September 2013.
9. IEEE Std. 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems."
10. NRC RG 1.118, Rev. 1, "Periodic Testing of Electric Power and Protection Systems," 2010.
11. NRC RG 1.22, "Periodic Testing of Protection System Actuation Functions," 1972.
12. NRC RG 1.47, Rev. 1, "Bypassed and Inoperable Status indication for Nuclear Power Plant Safety Systems," 2010.
13. *[APR1400-Z-J-NR-13004-NP, "Uncertainty Methodology and Application for Instrumentation Technical Report," April 2013.]**
14. *[APR1400-Z-J-NR-13005-P, "Setpoint Methodology for Plant Protection System Technical Report," April 2013.]**
15. ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation."
16. NRC RG 1.105, Rev. 3, "Setpoints for Safety-Related Instrumentation," 1999.
17. IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
18. IEEE Std. 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"
19. NRC RG 1.180, Rev.1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control," 2003.

APR1400 DCD TIER 2

20. IEC 61000-4-2, “Electromagnetic Compatibility – Testing and Measurement Techniques – Electrostatic Discharge Immunity Test.”
21. IEC 61000-4-5, “Electromagnetic Compatibility-Testing and Measurement Techniques – Surge Immunity Test.”
22. IEEE Std. 352-1987, “Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.”
23. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”
24. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
25. IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

APR1400 DCD TIER 2

Table 7.3-1

ESFAS Operating Bypass Permissive

Title	Operating Bypass Function	Operating Bypass Permissive	Removed By
Pressurizer pressure operating bypass permissive	Disables low pressurizer pressure of SIAS/CIAS by manual operation of the bypass switch ⁽¹⁾	Manual switch (one per channel), if pressure ≤ 28.12 kg/cm ² A (400 psia)	Automatic, if pressurizer pressure ≥ 35.15 kg/cm ² A (500 psia)

(1) SIAS/CIAS actuation due to high containment pressure is unaffected.

Table 7.3-2

Design Basis Events Requiring ESF System Action

Event	Containment Isolation	Containment Spray	Main Steam Isolation	Safety Injection	Auxiliary Feedwater	Control Room Emergency Ventilation	Fuel Handling Area Emergency Ventilation	Containment Purge Isolation
LOCA – Large Break	×	×		×		×		×
LOCA – Small Break ⁽¹⁾	×	×		×	×	×		×
Steam line break (inside containment)	×	×	×	×	×	×		×
Steam line break (outside containment)			×	×	×	×		
Feedwater line break	×	×	×		×			×
Steam generator tube rupture	×		×	×	×	×		
Fuel handling accident (inside containment)								×
Fuel handling accident (inside auxiliary building)							×	

(1) Includes CEA ejection and pressurizer safety valve opening

APR1400 DCD TIER 2

Table 7.3-3

Monitored Variables for ESFAS Signals

Monitored Variable	CIAS	CSAS	MSIS	SIAS	AFAS	CREVAS	FHEVAS	CPIAS
Pressurizer pressure	Low			Low		Low		
Containment pressure	High	High-High	High	High		High		
Steam generator pressure			Low					
Steam generator water level			High		Low			
Containment operating area radiation level								High
Spent fuel pool area radiation level							High	
Control room air intake radiation level						High		

APR1400 DCD TIER 2

Table 7.3-4

ESFAS Sensors

Monitored Variable	Sensor Type	Number of Sensors	Location
Pressurizer pressure	Pressure transducer (wide range)	4 ⁽¹⁾	Pressurizer
Containment pressure (Hi-Hi)	Pressure transducer (wide range)	4	Outside containment
Containment pressure (Hi)	Pressure transducer (narrow range)	4 ⁽¹⁾	Outside containment
Steam generator pressure	Pressure transducer	4/steam generator ⁽¹⁾	Steam generator
Steam generator level	Differential pressure transducer (wide and narrow range)	8/steam generator ⁽¹⁾	Steam generator
Containment upper operation area radiation level	Ion chamber	2	Inside containment
Containment operation area radiation level	Ion chamber	2	Inside containment
Spent fuel pool area radiation level	Ion chamber	2	Fuel handling area
Control room air intake radiation level	Scintillation	4	Control room air intake duct

(1) Shared with the reactor protection system

APR1400 DCD TIER 2

Table 7.3-5A

NSSS ESFAS Setpoints and Margins to Actuation

Actuation Signal	Nominal Full Power	Normal Operation Range	Nominal Actuation Setpoint	Margin to Actuation
SIAS and CIAS				
Low pressurizer pressure	158.19 kg/cm ² A (2,250 psia)	152.9 to 163.46 kg/cm ² A (2,175 to 2,325 psia)	127.26 kg/cm ² A (1810 psia ⁽¹⁾)	30.93 kg/cm ² A (440 psia)
High containment pressure	0 kg/cm ² (0 psig)	−0.02 to +0.02 kg/cm ² (−0.3 to +0.3 psig)	0.13 kg/cm ² (1.9 psig)	0.13 kg/cm ² (1.9 psig)
CSAS				
High-high containment pressure	0 kg/cm ² (0 psig)	−0.02 to +0.02 kg/cm ² (−0.3 to +0.3 psig)	1.4 kg/cm ² (20.03 psig)	1.4 kg/cm ² (20.03 psig)
MSIS				
Low steam generator pressure	70.31 kg/cm ² A (1,000 psia)	70.31 to 77.34 kg/cm ² A (1,000 to 1,100 psia)	60.11 kg/cm ² A (855 psia ⁽¹⁾)	10.2 kg/cm ² A (145 psia)
High containment pressure	0 kg/cm ² (0 psig)	−0.02 to +0.02 kg/cm ² (−0.3 to +0.3 psig)	0.13 kg/cm ² (1.9 psig)	0.13 kg/cm ² (1.9 psig)
High steam generator level	59.1 % NR	0 to 95 % NR	90 % NR	30.9 %
AFAS (PPS)				
Low steam generator level	76.8 % WR	40.7 to 97.2 % WR	25% WR	51.8%
AFAS (DPS)				
Low steam generator level	76.8 % WR	40.7 to 97.2 % WR	22.4 % WR	54.4 %
SIAS (DPS)				
Low pressurizer pressure	158.19 kg/cm ² A (2,250 psia)	152.9-163.46 kg/cm ² A (2,175-2,325 psia)	114.60 kg/cm ² A (1,630 psia ⁽¹⁾)	43.59 kg/cm ² A (620 psia)

(1) Setpoint can be manually decreased as pressure is reduced and is automatically increased as pressure is increased.

APR1400 DCD TIER 2

Table 7.3-5B

BOP ESFAS Setpoints and Margin to Actuation

Actuation Signal	Nominal Full Power	Normal Operation Range	Nominal Actuation Setpoint	Margin to Actuation
CPIAS				
Containment upper operating area radiation level	1 mSv/hr	14 mSv/hr	28 mSv/hr	14 mSv/hr
Containment operating area radiation level (during fuel handling operation)	0.02 mSv/hr	0.5 mSv/hr	2.5 mSv/hr	2.0 mSv/hr
FHEVAS				
Spent fuel pool area radiation level	0.02 mSv/hr	0.025 mSv/hr	0.25 mSv/hr	0.23 mSv/hr
CREVAS				
Control room air intake radiation level	Negligible	0.052 Bq/cc	0.52 Bq/cc	0.51 Bq/cc

APR1400 DCD TIER 2

Table 7.3-6

ESFAS Variable Ranges

Monitored Variable	Minimum	Nominal Full Power	Maximum
Pressurizer pressure (narrow range)	0 kg/cm ² A (0 psia)	158.19 kg/cm ² A (2,250 psia)	210.92 kg/cm ² A (3,000 psia)
Containment pressure	−0.35 kg/cm ² (−5 psig)	0 kg/cm ² A (0 psia)	4.22 kg/cm ² A (60 psig)
Steam generator pressure	1.05 kg/cm ² A (15 psia)	70.31 kg/cm ² A (1,000 psia)	105.46 kg/cm ² A (1,500 psia)
Steam generator level (wide range)	0 %	76.8 %	100 %
Steam generator level (narrow range)	0 %	59.1 %	100 %
Containment upper operation area radiation level	10 mSv/hr	—	10 ⁸ mSv/hr
Containment operation area radiation level	10 ^{−3} mSv/hr	—	10 ² mSv/hr
Spent fuel pool area radiation level	10 ^{−3} mSv/hr	—	10 ² mSv/hr
MCR intake duct radiation level	3.7 × 10 ^{−2} Bq/cc	—	3.7 × 10 ³ Bq/cc

APR1400 DCD TIER 2

Table 7.3-7 (1 of 3)

ESF Response Time

Initiating Signal and Function	Total Response Time in Seconds ⁽¹⁾
1. Manual	
a. SIAS	Not applicable
b. CSAS	Not applicable
c. CIAS	Not applicable
d. MSIS	Not applicable
e. AFAS	Not applicable
f. CREVAS	Not applicable
g. FHEVAS	Not applicable
h. CPIAS	Not applicable

APR1400 DCD TIER 2

Table 7.3-7 (2 of 3)

Initiating Signal and Function	Total Response Time in Seconds ⁽¹⁾
2. Pressurizer pressure – Low	
a. Safety injection	≤ 40
b. Containment isolation	
1) CIAS actuated low volume purge valves	≤ 5
2) Other CIAS actuated valves	$\leq 83.5^{(2)} / 62.0^{(3)}$
3. Containment Pressure – High	
a. Safety injection	≤ 40
b. Containment isolation	
1) CIAS actuated low volume purge valves	≤ 5
2) Other CIAS actuated valves	$\leq 83.5^{(2)} / 62.0^{(3)}$
c. Main steam isolation	
1) MSIS actuated MSIVs	≤ 6.35
2) MSIS actuated MFIVs	≤ 11.35
4. Containment pressure – High-High	
a. Containment spray pump	$\leq 50.4^{(4), (6)} / 28.5^{(5), (6)}$
b. Containment isolation valves closed on CSAS	$\leq 73.5^{(2)} / 52.0^{(3)}$
5. Steam generator pressure – Low	
a. Main steam isolation	
1) MSIS actuated MSIVs	≤ 6.35
2) MSIS actuated MFIVs	≤ 11.35
6. Steam generator level – Low	
a. Auxiliary feedwater pump (motor driven)	$\leq 61.45^{(4)}$
b. Auxiliary feedwater pump (turbine driven)	≤ 61.45
7. Steam generator level – High	
a. Main steam isolation	
1) MSIS actuated MSIVs	≤ 6.35
2) MSIS actuated MFIVs	≤ 11.35

APR1400 DCD TIER 2

Table 7.3-7 (3 of 3)

Initiating Signal and Function	Total Response Time in Seconds ⁽¹⁾
8. CREVAS	
Control room air intake radiation – High	
a. CREVAS actuated isolation dampers	$< 8.4^{(7), (8)}$
b. Emergency makeup ACU fan	$< 5.0^{(7), (8), (9)}$
9. FHEVAS	
Fuel handling area spent fuel pool area radiation – High	
a. FHEVAS actuated isolation dampers	$< 8.2^{(7), (8), (9)}$
b. Emergency makeup ACU fan	$< 5.0^{(7), (8)}$
c. Normal ACU fan	Not applicable
10. CPIAS	
Containment upper operating area/operating area radiation – High	
a. CPIAS actuated isolation valves	$< 9.9^{(7), (8)}$
b. High – Volume purge fan	Not Applicable
11. 4.16 kV Emergency bus undervoltage (degraded voltage) loss of power 90 % system voltage	$< 5 \text{ min}^{(7)}$
12. 4.16 kV Emergency bus undervoltage (loss of voltage) loss of power	$< 2^{(7)}$

- (1) PPS cabinet delays are included.
- (2) A loss of offsite power. EDG starting delay is included. Response time includes movement of valves and attainment of pump or blower discharge pressure.
- (3) Offsite power is available. EDG starting delay is not included. Response time includes movement of valves and attainment of pump or blower discharge pressure.
- (4) Same as No. 2. In addition, delays of load-sequencing are included.
- (5) Same as No. 3. In addition, delays of load-sequencing are included.
- (6) Spray line fill time is not included.
- (7) EDG starting delay is not included.
- (8) The response time of the radiation detectors is not included. The response time of the radiation signal portion of the channel is measured from the detector output or from the input of the first electronic component in channel to closure of dampers/valves or start fans.
- (9) Fan motor run-up time is not included since the building volume is too large to make a substantial change to pressure compared to the isolation function.

Table 7.3-8 (1 of 13)

Engineered Safety Feature – Component Control System Failure Modes and Effects Analysis

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
1)	ESF-CCS MCR CPM	a) Off	<p>Loss of internal CPM power supply or electronics failures within CPM</p> <p>Open circuit wiring to switches and status indication</p> <p>Loss of CPM data communications</p>	Loss of status indication and control of components assigned to CPM in the safety console	CPM health status is monitored by GC, LC and is annunciated automatically via communication data link to QIAS-N and IPS. Periodic test and maintenance are performed.	<p>CPMs in other channels are not affected.</p> <p>Operator can take control of affected components using ESCM in MCR.</p>	Automatic or manual ESF actuation not affected.	Components remain in last demanded state of operation (Fail-as-is).
		b) On	<p>Electronics failures within CPM</p> <p>Short circuit wiring to switches and status indication</p> <p>Erroneous data transmitted to either start or stop components.</p>	Erroneous status indication and control of components assigned to CPM in the Safety console.	Erroneous status indication or change in component operating status observed by operator.	<p>ESF-CCS redundant channels B, C, and D remain available.</p> <p>CPM in other channel not affected.</p>	<p>Affected ESF components may be actuated or stopped/ closed.</p> <p>Possible actuation of Division A component assigned to CPM in this group: SIS, SDS, and CSS.</p>	<p>Same as 1). Plant power production process may be perturbed.</p> <p>Spurious actuation of SIS division A bounded by DBE</p> <p>Erroneous actuation of ESF-CCS a SDS valves is acceptable since redundant SDS valves are assigned to different ESF-CCS channels to prevent spurious depressurization</p> <p>Erroneous actuation of ESF-CCS CSS components is acceptable, since the spray pump and a valve in series are assigned to different ESF-CCS channels to prevent spurious containment spray</p>

Table 7.3-8 (2 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2)	ESF-CCS Control Channel Gateway (channel A typical)	a) Off	Loss of internal power supply in CCG, failures (hardware or software) within CPU or data communications links that halt execution	Loss of status indication and control of components on the ESCM	CCG health status is monitored by LC, GCs and MTP and automatically annunciation via communication data links to QIAS-N and IPS.	Minimum inventory control and indications remain available CCGs in other channels are not affected	None, PPS automatic ESFAS remains available. Component remains in last demanded state of operation (Fail-as is).	Automatic or manual ESF actuation via PPS not affected.
		b) On	Failures (hardware or software) or data communications Errors within gateway that cause loss of halts execution.	Erroneous status indication and control of components related with gateway	Annunciating automatic via health status of communication data links to QIAS-N and IPS. Erroneous status indication or change in component operating status observed by operator.	ESF-CCS redundant Channels B, C, and D gateways remain available. Operator retains component control and status information by Minimum Inventory, IPS, and QIAS-N.	Automatic or manual ESF actuation via PPS not affected.	An ESF component may be actuated or stopped/closed. Possible actuation of a component.

7.3-45

APR1400 DCD TIER 2

Table 7.3-8 (3 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
3)	ESF-CCS ITP (channel A typical)	a) Off	<p>Loss of internal power supply</p> <p>Electronics failures</p> <p>Open or short circuit output wiring.</p>	Loss of data communication to other safety channel and QIAS-N.	<p>Annunciated automatic by self-health monitoring of ESF-CCS intra channel data communications via channel master to IPS and QIAS-N.</p> <p>Periodic maintenance and test</p>	<p>Operation or malfunction of ITP does not prevent PPS safety functions from being accomplished.</p> <p>ITP of Redundant IPS Channels B, C, and D not affected.</p> <p>ITP test feedback can be monitored from its local MTP.</p>	Loss of test feedback via channel A ITP.	Automatic testing of own PPS channels continued.
		b) On	Hardware or software failures cause erroneous data transmittal.	<p>Other channel A ITP test results do not agree with expected results.</p> <p>channel A OM is inoperable.</p>	IPS and QIAS-N alarm	Same as 4a).	Possible transfer of ESF-CCS A controls to RSR.	Same as 4 a).

7.3-46

APR1400 DCD TIER 2

Table 7.3-8 (4 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
4)	ESCM in MCR	a) Off Static display no response	<p>Loss of power supply to the ESCM FPD,</p> <p>Loss of fiber optic SDN</p> <p>Electronic or software failures within the ESCM FPD.</p>	<p>Passive loss of indications on the ESCM.</p> <p>ESF-CCS LC keeps the ESCM data static (same as prior to failure).</p>	<p>Loss of ESF-CCS status indication on the ESCM. Annunciating automatic by ESF-CCS CCG self-diagnostics via IPS and QIAS-N.</p> <p>Periodic maintenance and manual test.</p> <p>Loss of heartbeat rotation on the ESCM FPD.</p>	<p>Other channel ESCMs are available.</p> <p>MCR minimum inventory on the safety console controls via MCR CPM available.</p> <p>Manual ESFAS initiation via PPS remains available.</p>	<p>None, PPS automatic ESFAS remains available.</p> <p>Component remains in last demanded state of operation (Fail-as is).</p>	Inability to monitor dedicated channel of ESF-CCS status or take control of components in division when a CPM in the same channel is also out of service.
		b) On, dynamic, spurious random displays and controls	<p>Electronics or software failures within the ESCM</p> <p>Erroneous data transmitted over fiber optic data link.</p>	<p>Active indications on the ESCM erroneous or abnormal.</p> <p>Possible erroneous control signals to component within only same channel.</p>	<p>Erroneous status indication or component operating status change observed by operator. Possible annunciating automatic by CCG. Self-diagnostics via IPS and QIAS-N.</p> <p>Periodic maintenance and manual test.</p>	Same as 4a).	Number of redundant ESCM channels available reduced to one. Same as 2b).	Same as 2 b) and 4 a).

7.3-47

APR1400 DCD TIER 2

Table 7.3-8 (5 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
5)	Information FPD	a) Off, Static displays in information FPD are no response	<p>Loss of power supply to information FPD.</p> <p>Electronic or software failures within information FPD.</p> <p>Loss of data link between information FPD and IPS.</p>	<p>Passive loss of indications on information display.</p> <p>Loss of communication with the ESCM FPD.</p> <p>Inability to select components for control.</p>	<p>Loss of status indication on information display.</p> <p>Annunciating automatic by IPS self-diagnostics via IPS and QIAS-N. Periodic maintenance and manual test.</p> <p>Loss of heartbeat rotation on information FPD display.</p>	<p>MCR minimum inventory switches remains available.</p> <p>ESCM is operable without interface with IFPD</p>	No effect on ESF-CCS during normal operation.	Inability to monitor safety component status on IFPD and LDP.
		b) On, dynamic, spurious random displays	<p>Electronics or software failures within information FPD.</p> <p>Erroneous component ID data transmitted over fiber optic data link from information FPD to ESCM FPD.</p>	<p>Active indications on information FPD erroneous or abnormal. Possible erroneous component ID signals to ESCM FPD.</p>	<p>Erroneous status indication or component operating status change observed by operator.</p> <p>Possible annunciating automatic by IPS and ESCM FPD self-diagnostics via IPS and QIAS-N.</p> <p>Periodic maintenance and manual test.</p>	<p>Redundant information FPD and ESCM FPD remain available.</p> <p>Same as 5, a)</p>	No effect on ESF-CCS during normal operation.	Same as 5 a).

Table 7.3-8 (6 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
6)	MCR/RSR master transfer switch	a) Off	Loss of power supply to fiber optic switch, fiber optic switch fails closed, severed fiber optic cable.	Passive failure Inability to transfer channel A ESF-CCS controls to RSR using this switch	Periodic test and maintenance.	ESF-CCS redundant Channel B, C, and D transfer remain available. The other switch and switch at maintenance and test panel remains available.	None, PPS automatic ESFAS remains available. Component remains in last demanded state of operation (Fail-as is).	Automatic or manual ESF actuation via PPS not affected.
		b) On	Fiber optic switch fails open.	Transfer of channel A ESF-CCS to RSR occurs controls inoperable from MCR.	Annunciation automatic from IPS and QIAS-N.	Bumpless transfer occurs, controls remain in last demanded state. Automatic ESFAS control actions remain available.	Channel A ESF-CCS and PPS controls Transferring are not available to RSR.	Transfer of control back to MCR achieved from ESF-CCS maintenance and test panels.
7)	Soft control in RSR	a) Off, static display or no response	Same as 4 a).	Same as 2 a), if control is transferred to RSR.	Same as 4 a).	Other channel ESCMs are available. Manual ESFAS initiation via PPS remains available.	None, PPS automatic ESFAS remain available Component remains in last demanded state of operation (Fail-as is)	Under transferring control to RSR, loss of control and status indication of components in one division through ESCM of same channel.
		b) On, dynamic, spurious, random displays or controls	Same as 4 b).	Same as 4 b), Under transferring control to RSR.	Same as 4 b).	Same as 4 a).	No effect on ESF-CCS during normal operation. Under transferring control to RSR, same as 4 b)	Under transferring control to RSR, same as 4 b).

Table 7.3-8 (7 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
8)	ESF-CCS Maintenance and Test Panel Module (channel A typical)	a) Off, static display or no response	Loss of power supply, loss of data link or Electronics hardware or software failure within MTP module.	Passive Loss of local indications on MTP module. Same as prior to failure during test condition. Impaired maintenance and test capability. Loss of data communication to IFPD	Loss of status indication, maintenance, and test functions locally at ESF-CCS. Possible annunciation automatic by CCG self-diagnostics via IPS and QIAS-N Periodic maintenance and test Loss of indication for information of channel A on IFPD	Ability to use either MCR or RSR ESF-CCS soft control and CPM for component status and control, dependent upon which was last selected for control. Redundant channel MTP unaffected.	No effect on ESF-CCS during normal operation.	Automatic ESFAS actuation by PPS not affected. Inability to use MTP to transfer control from MCR to RSR or vice versa in one channel.
		b) On, spurious, random displays or controls	Electronics hardware or software failures within module or erroneous data transmittal.	Active erroneous or abnormal indications on module. Possible erroneous control signals to components within division. Possible transfer of control from MCR to RSR in one channel.	Erroneous status indication or component operating status change observed by operator. Possible annunciating automatic by CCG. Self-diagnostics via IPS and QIAS-N. Periodic maintenance and manual test. Annunciations of control transfer to RSR via IPS and QIAS-N during test.	Same as 4a) and 4b).	Possible inability to transfer control from MCR to RSR or vice versa in one channel. Same as 3b).	Plant power production process may be perturbed. Same as 3b).

Table 7.3-8 (8 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
9)	ESF-CCS Channel A Group Controller (typical)	a) Off	Loss of vital bus power to all ESF-CCS channel A GC	<p>Loss of data communications to or from PPS</p> <p>Soft controls located in MCR and RSR become disabled</p> <p>PPS interface/test system annunciates PPS/ESF interface test failure</p>	<p>Loss of component status and ESCM indication in MCR and RSR</p> <p>Annunciating automatic from QIAS-N and IPS due to health status data communications</p>	ESF-CCS redundant Channels B, C, and D remain available.	<p>ESF-CCS "A" outputs revert to fail-safe condition corresponding to the electrical failure mode of the final actuation device for the Division A actuated equipment (MOVs, motors, breakers fail-as-is; solenoids fail to their fail-safe state).</p> <p>Other three ESF divisions are available</p>	Loss of data to QIAS-N and IPS for parameters and component status from this channel.
		b) Off	Loss of processor internal power supply, failures (hardware or software) within CPU, or data communications links, which halt execution.	Fail-over to standby Group Control occurs.	Annunciated automatic via ITP and MTP communication data links from standby processor to QIAS-N and IPS.	Standby processor assumes control	None.	

Table 7.3-8 (9 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
9)	ESF-CCS Channel A Group Controller (typical) (cont.)	c) On	Failures (hardware or software) within processor that cause loss of failover and halts execution.	Inability to control or change operating state of components assigned to this processor from ESCM in MCR. Component status indication and displays remain static at IPS and QIAS-N.	Annunciated automatic via IPS and QIAS-N due to integrated test processor detection of ESF-CCS interface test failure. Periodic maintenance and test. Loss of component control responses detected by operator.	ESF-CCS redundant Channels B, C, and D remain available. Operator retains component control from minimum inventory switches on the safety console via loop controllers.	Loss of PPS automatic and PPS remote manual initiation of components controlled by this processor.	Processor components remain in last demanded state of operation unless control action taken by operator or ESCM.
		d) On	Electronics or software failure within controller, or erroneous data transmitted, cause false ESF initiation signals.	Possible erroneous control signals to Loop Controllers associated with this Group Controller.	Same as 1 b).	Same as 1 b)	Same as 1b).	Same as 1b). A faulty Group Controller(s) may cause MSIS, CIS, or AFWS division A component actuation, dependent upon the functional group assignment, which is designed to minimize impact on plant systems. Based on the safety analysis, this spurious actuation results in acceptable consequences.

Table 7.3-8 (10 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
10)	SDL interfaces between ESF-CCS and PPS	a) Off	Loss of power supply or electronics failure in SDL transmitter or receiver; severing of fiber optic cable(s) in one redundant PPS channel.	Loss of PPS signals sensed as initiation trip signal into ESF-CCS processor 2-out-of-4 coincidence logic.	Annunciated automatic via IPS and QIAS-N due to PPS integrated test processor detection of ESF-CCS interface test failure. Periodic manual ESF-CCS testing.	Same as 10 a). Within ESF-CCS channel, redundant fiber optic receivers internal power supplies.	This channel of ESF-CCS actuation logic becomes 2-out-of-3 coincidence.	Manual actuation available from MCR.
		b) On	Electronics failure causes fiber optic transmitter or receiver to stay on from one redundant PPS channel.	PPS ESF initiation signals not sensed by ESF-CCS selective 2-out-of-4 coincidence logic.	Annunciated automatic via IPS and QIAS-N due to two-channel trip condition.	Same as 10 b).	This channel of ESF-CCS actuation logic becomes 2-out-of-3 coincidence.	Same as 10 a).
11)	ESF-CCS Loop Controller	a) Off	<p>Loss of vital bus power to all ESF-CCS channel A LC.</p> <p>Loss of loop controller power supply, electronics failure within controller, CPM, or data communication network causes outputs to assume default state.</p>	<p>Components assigned to Loop Controller revert to fail-safe state.</p> <p>Process instrumentation or component status inputs to affected ESF-CCS group controller not refreshed for affected ESF system.</p>	<p>Periodic maintenance and testing.</p> <p>Loss of component controls response detected by operator.</p> <p>Annunciating automatic from IPS and QIAS-N due to health status data communications.</p>	ESF-CCS redundant Channels B, C, and D remain available.	<p>Affected ESF-CCS outputs go to fail safe condition corresponding to the electrical failure mode (state) of the final actuation device for the actuated equipment (MOVs, motors, breakers Fail-as-is and solenoids fail to their fail-safe state).</p> <p>Other three ESF divisions are available.</p>	Loss of control and status indication of affected ESF system in one division.

Table 7.3-8 (11 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
11)	ESF-CCS Loop Controller (cont.)	b) On	Failure in electronics, Controllers, CPM, or data communications causes CPM outputs to assume their actuated state.	Components assigned to the Loop Controller may receive erroneous control signals.	Erroneous status indication or change in component operating status observed by operator. Periodic maintenance and testing.	ESF-CCS redundant Channels B, C, and D remain unaffected. Components are assigned to Loop Controllers based on ESF system functional groups to limit impact on plant systems.	ESF system components assigned to this Loop Controller actuated or stopped/closed. Other three ESF divisions are available.	Plant power production process may be perturbed. A faulty Loop Controller may cause SIS, CSS, MSIS, CIS or AFWS division A component actuation or stop/close dependent upon the functional group assignments, which are designed to minimize impact to plant systems. Based on the safety analysis, these spurious actuation or failures result in acceptable consequences.
12)	ESF-CCS SDN Communication Networks	a) Off	Open, short, ground, or application of 480 V AC to one network in SDN data communications errors occur.	Possible damage to communications module. Group Controllers, Loop Controllers, CCG Safety soft controls, MTP, and ITP self-diagnostics detect loss of data communications; these components supported by the redundant network and annunciation of the failure are via IPS and QIAS-N.	Annunciating automatic by associated ESF-CCS GC self-diagnostics via IPS and QIAS-N. Periodic maintenance and test	Redundant SDN communications network available.	None	

Table 7.3-8 (12 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
12)	ESF-CCS SDN Communication Networks (cont.)	b) On	Open, short, ground or application of 480 V AC to both networks in SDN data communications errors occur.	<p>Loss of SDN communications between G C, LC, MTP, ITP, DPS, CPCS, QIAS-P Network to PPS, CPM at RSR, and [[Gateway to ESCM]][1], Master Transfer Switches, IPS and QIAS-N.</p> <p>Loss of data transmittal to IPS, QIAS-N via MTP.</p> <p>Loss of status indication and control of component on the ESCM.</p>	<p>Periodic maintenance and testing.</p> <p>MTP and ITP self-diagnostics detects loss of communication and automatically annunciates via IPS and QIAS-N.</p>	<p>Automatic and manual ESFAS from PPS, and manual control of Loop Controls via MI switch via CPM at safety console continue to function.</p>	<p>Loss of some interlocking signals between Group Controllers within same ESF-CCS channel.</p> <p>Loss of feedback for PPS automatic testing.</p>	Loss of capability to transfer control from MCR to RSR for those channels.
13)	ESF-CCS Intersystem communications data link to IPS. (channel A typical)	a) Off	Open, short, ground, or application of 480 V AC to one network in SDN data communications errors occur.	Possible damage to data communication module (Ethernet card). QIAS-N & MTP annunciates loss of data link.	<p>Annunciated by IPS and MTP</p> <p>Periodic maintenance and testing.</p>	Redundant Gateway data link remains available.	<p>None</p> <p>Fiber optic cable prevents faults originating in IPS from affecting ESF-CCS</p>	Data sent to QIAS-N not affected.

Table 7.3-8 (13 of 13)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
14)	ESF-CCS Intersystem Communications Data Link to QIAS-N (channel A typical)	a) Off	Open, short, ground, or application of 480 V AC to one network in SDN data communications errors occur.	Possible damage to data communications module. QIAS-N & MTP annunciates loss of data link.	Annunciated automatic by QIAS-N self-health diagnostics of data link. Periodic maintenance and testing.	Redundant Gateway data link remains available.	None Fiber optic cable prevents faults originating in QIAS-N from affecting ESF-CCS	Data sent to IPS not affected.
		b) Off	Open, short, ground, or application of 480 V AC to both networks in SDN data communications errors occur.	Possible damage to data communication module	Same as 16 a).	Fiber optic cables prevent faults originating in QIAS-N from affecting Gateways.	None	Same as 14 a).
15)	CI Communication Interface Module Processor	Fails Off	Component failure	Module failure is detected by the processors in the rack	Trouble annunciation	CI module and global memory	None	

- (1) No effect on the control system. The control system signal validation logic avoids undesirable control actions due to failed signal inputs.

APR1400 DCD TIER 2

Low Pressurizer Pressure

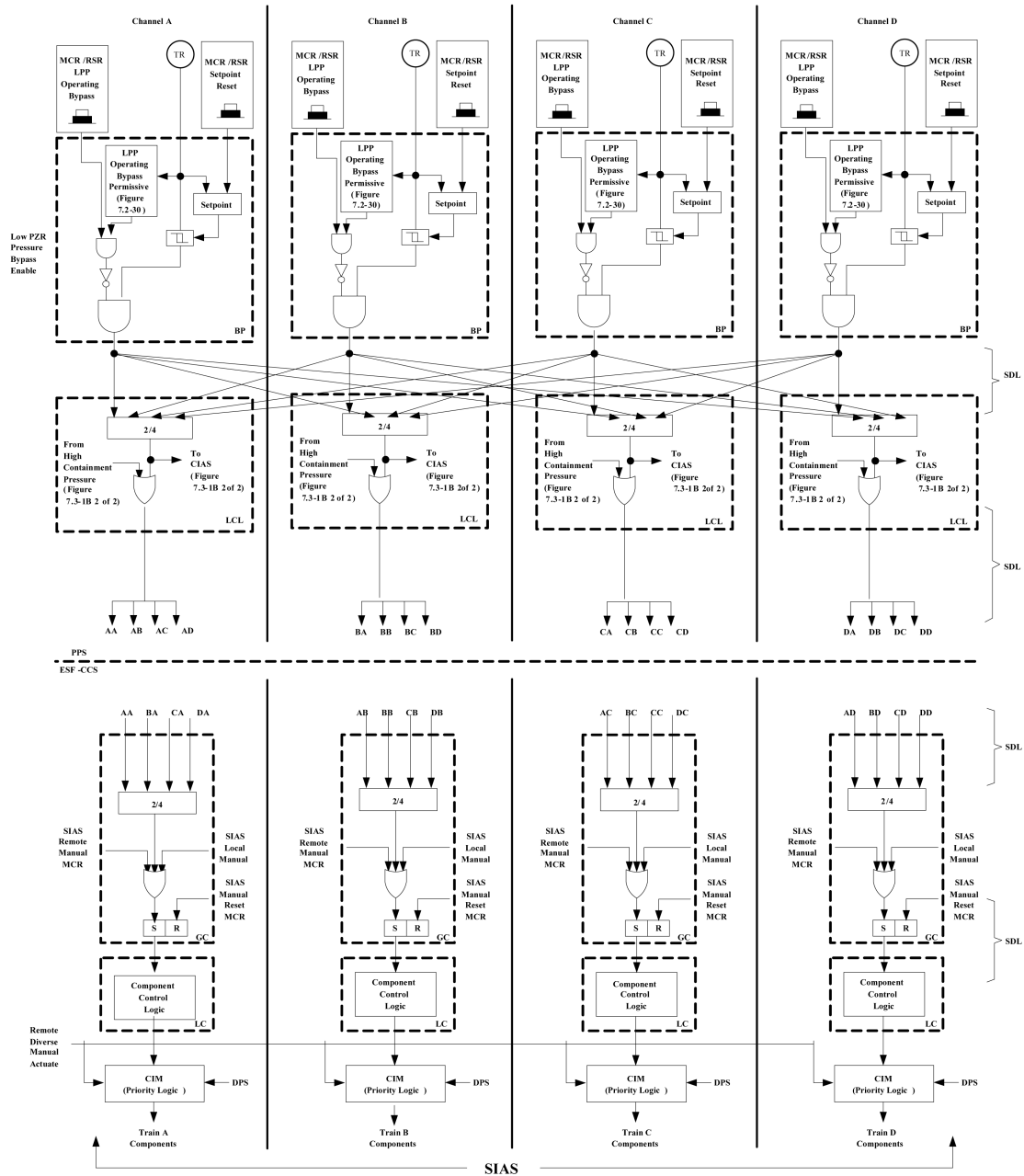


Figure 7.3-1A ESFAS Functional Logic (SIAS)

APR1400 DCD TIER 2

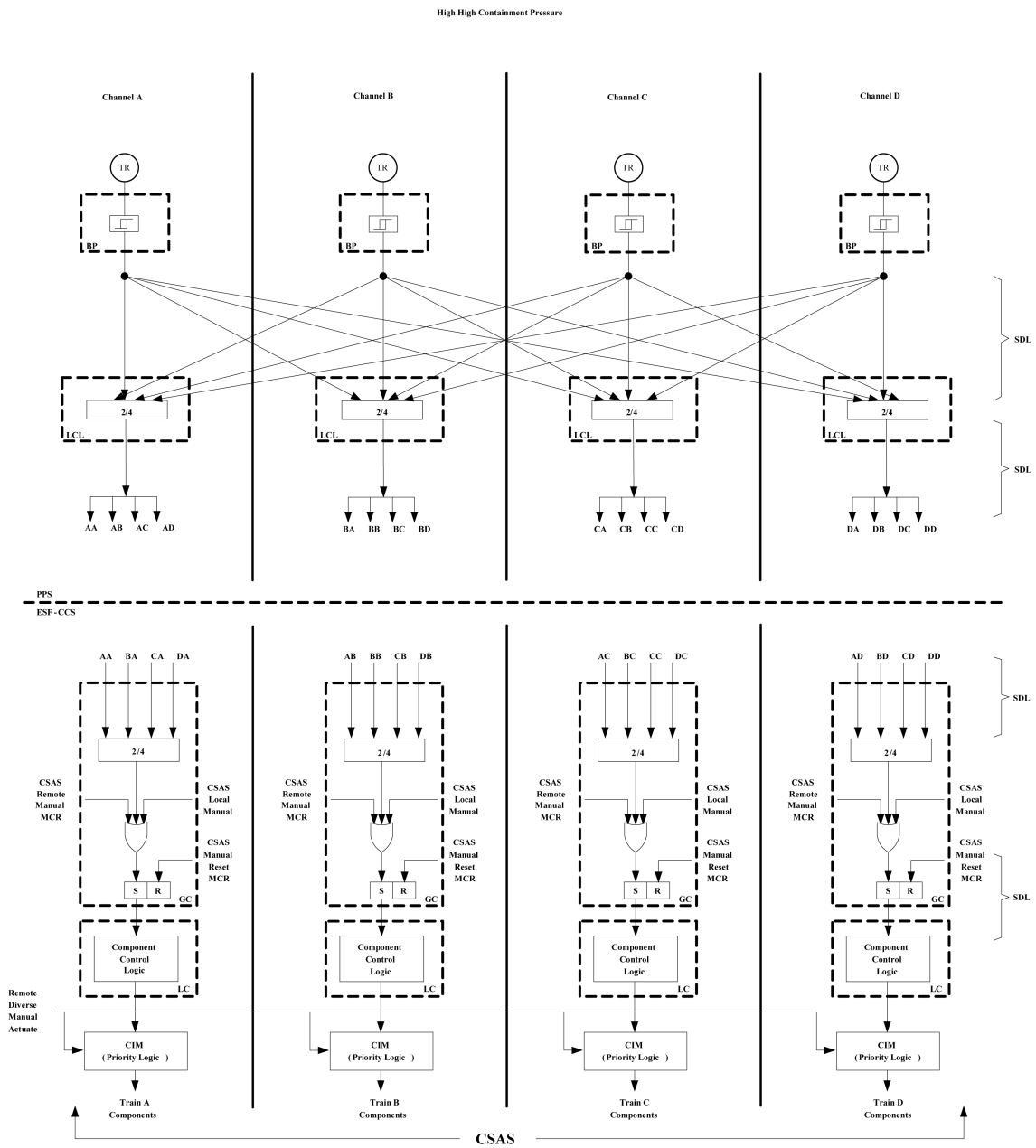


Figure 7.3-1B ESFAS Functional Logic (CSAS, CIAS) (1 of 2)

APR1400 DCD TIER 2

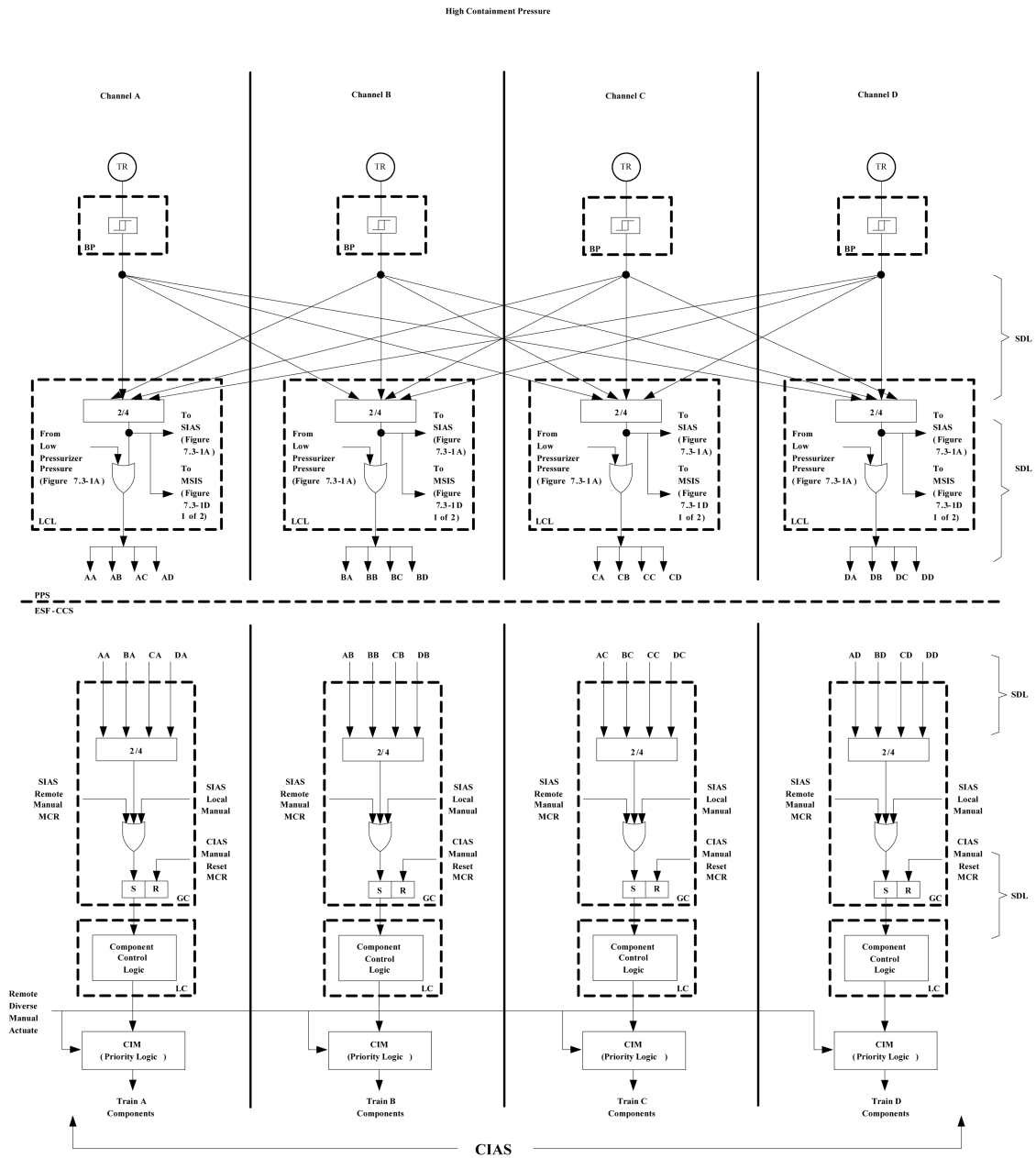


Figure 7.3-1B ESFAS Functional Logic (CSAS, CIAS) (2 of 2)

APR1400 DCD TIER 2

Low Stream Generator - 1 Level

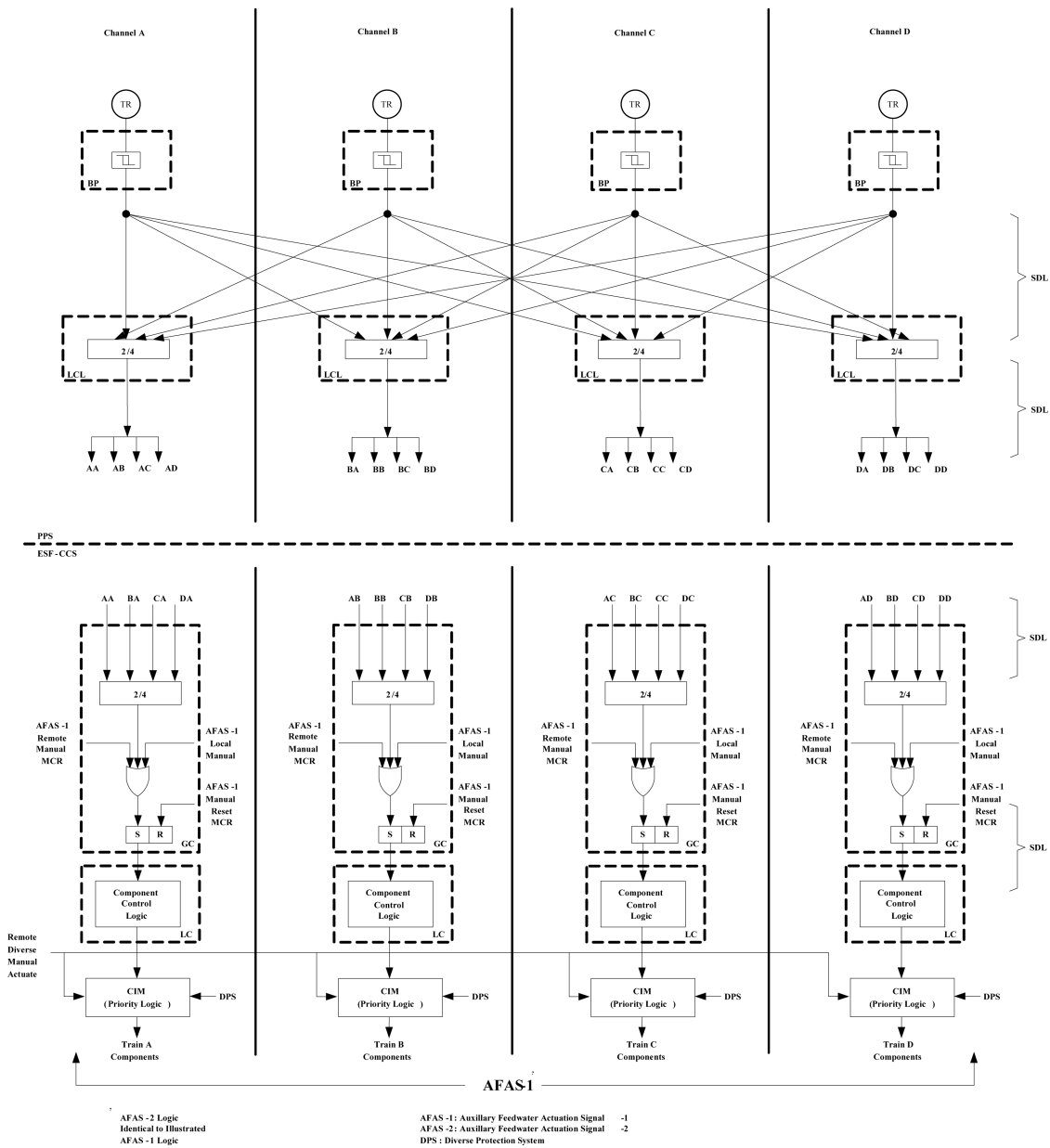


Figure 7.3-1C ESFAS Functional Logic (AFAS-1, AFAS-2)

APR1400 DCD TIER 2

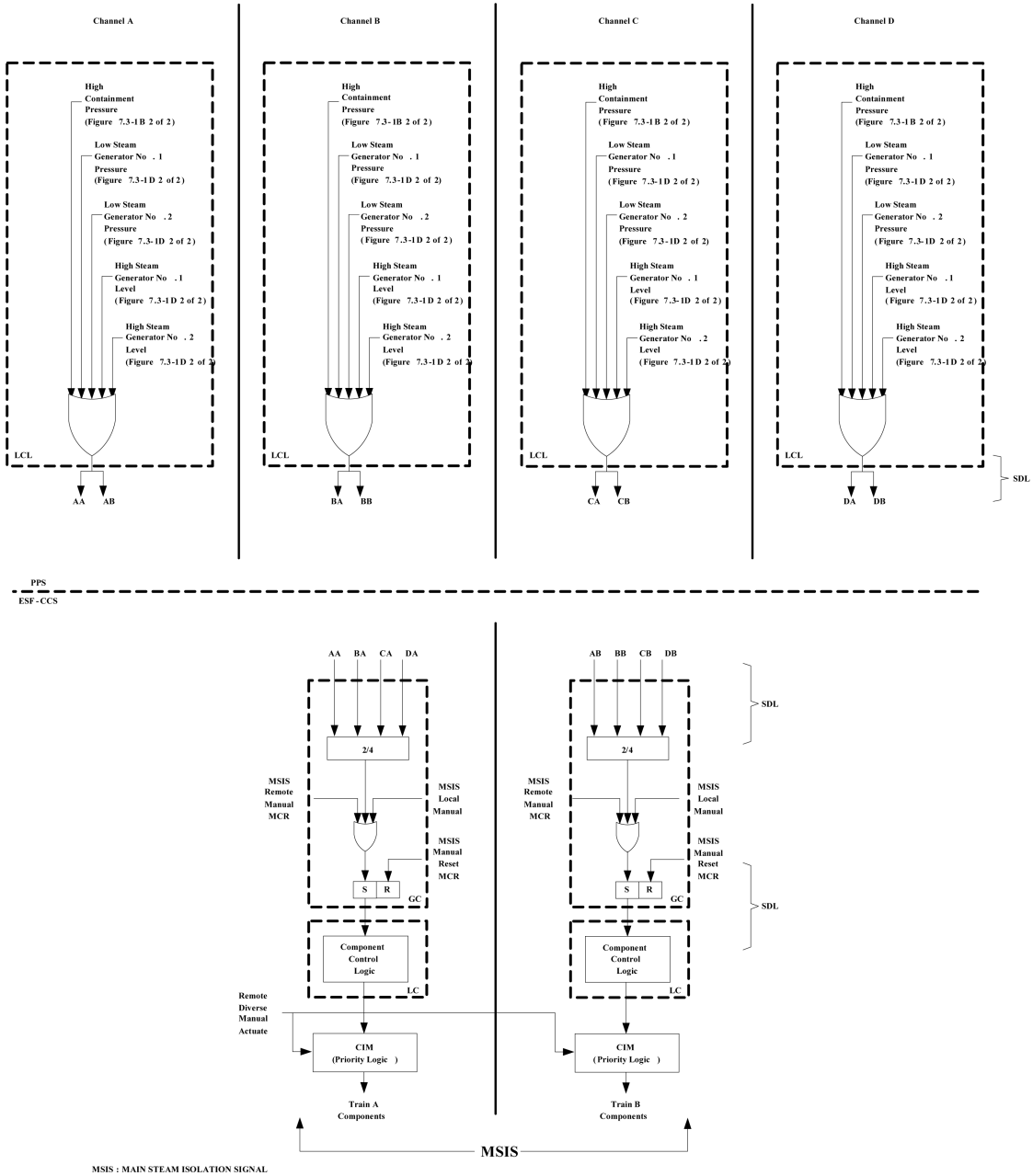


Figure 7.3-1D ESFAS Functional Logic (MSIS) (1 of 2)

APR1400 DCD TIER 2

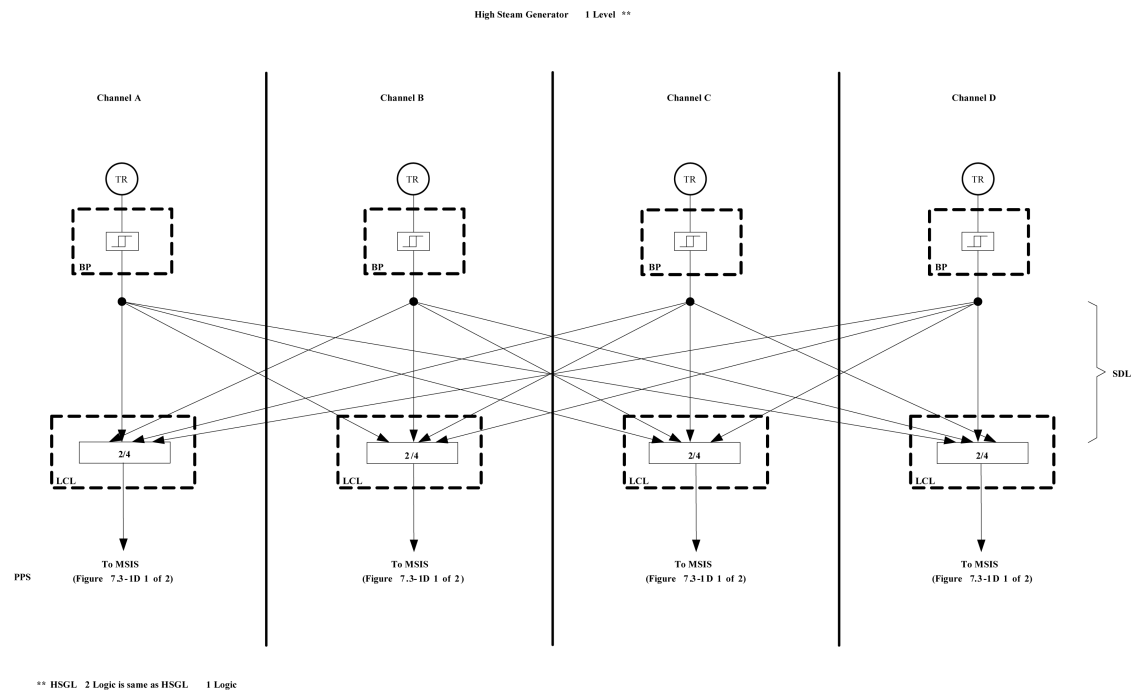
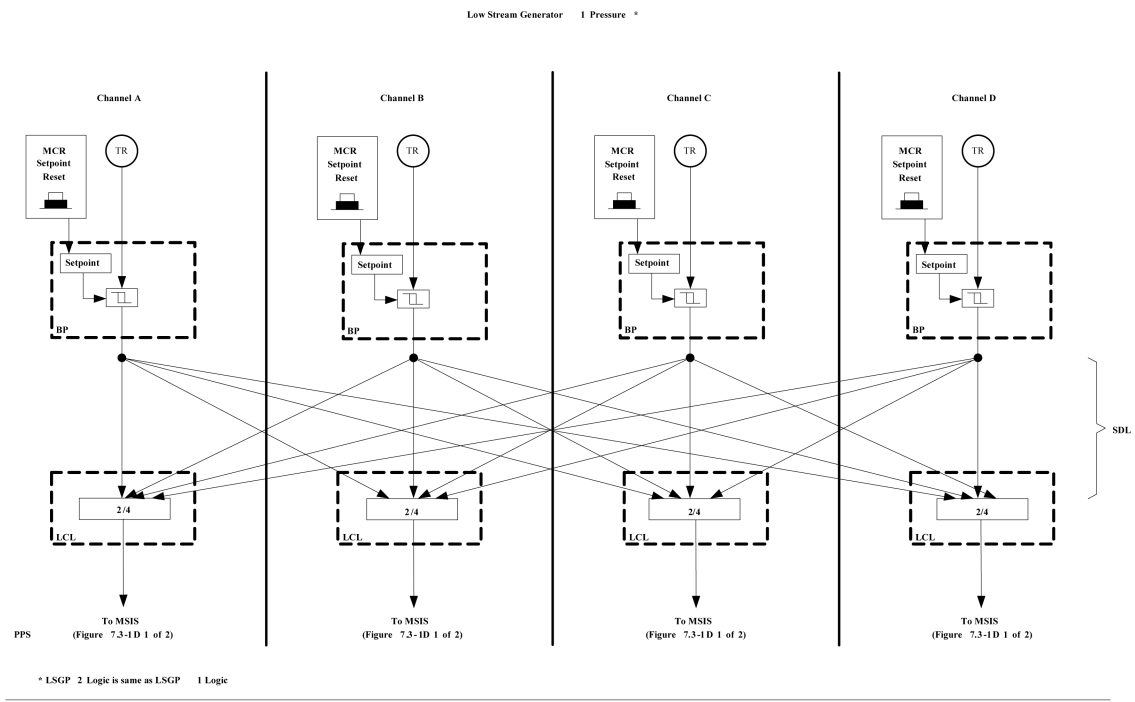


Figure 7.3-ID ESFAS Functional Logic (MSIS) (2 of 2)

APR1400 DCD TIER 2

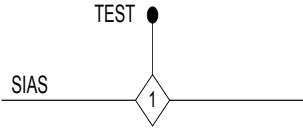
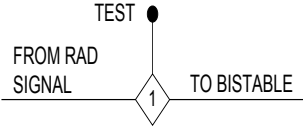
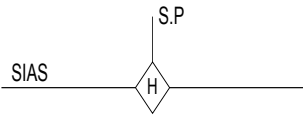
<u>FUNCTION</u>	<u>SYMBOL</u>	<u>DEFINITION</u>
TEST FEATURE FOR NSSS ESFAS		A TEST SIGNAL CAN BE MANUALLY INSERTED INTO THE ESFAS ACTUATION CIRCUIT AT THE ESF-CCS CABINET FOR THE NSSS ESFAS AND AT THE RADIATION MONITORING SYSTEM CABINET FOR THE BOP ESFAS. THE NUMBER WITHIN THE DIAMOND INDICATES THE TYPE OF TEST OPERATION DESCRIBED BELOW : TYPE 1 : GO-TEST GO-TEST OPERATION OF EQUIPMENT THAT CAN BE PLACED IN THE ESF ACTUATION MODE DURING NORMAL PLANT POWER OPERATION AND VERIFIED BY OBSERVATION FROM MAIN CONTROL ROOM. NO SPECIAL SYSTEM PREPARATION AND ALIGNMENT IS NECESSARY. TYPE 2 : GO-TEST WITH SYSTEM ALIGNMENT. GO-TEST OPERATION SAME AS TYPE 1 ABOVE BUT SPECIAL SYSTEM PREPARATION AND ALIGNMENT IS NECESSARY BEFORE THE END DEVICE CAN BE ACTUATED. THE REQUIRED SYSTEM PREPARATION AND/OR ALIGNMENT WILL BE DEFINED IN APPROPRIATE OPERATING PROCEDURES.
TEST FEATURE FOR BOP ESFAS		TYPE 3 : NO GO-TEST TEST OPERATION OF THE EQUIPMENT CANNOT BE PERFORMED DURING NORMAL PLANT OPERATION. SINCE TEST ACTUATION CAN CAUSE PLANT UPSET AND/OR EQUIPMENT DAMAGE DURING THE NORMAL PLANT OPERATION. TEST SHOULD BE PERFORMED DURING THE PLANT SHUTDOWN ONLY. N : NO TEST IS REQUIRED.
BISTABLE		DIGITAL OUTPUT EXISTS ONLY WHEN ANALOG INPUT IS HIGHER (H) OR LOWER (L) THAN THE SET POINT INDICATED.

Figure 7.3-1E ESFAS Functional Logic (General Legend)

APR1400 DCD TIER 2

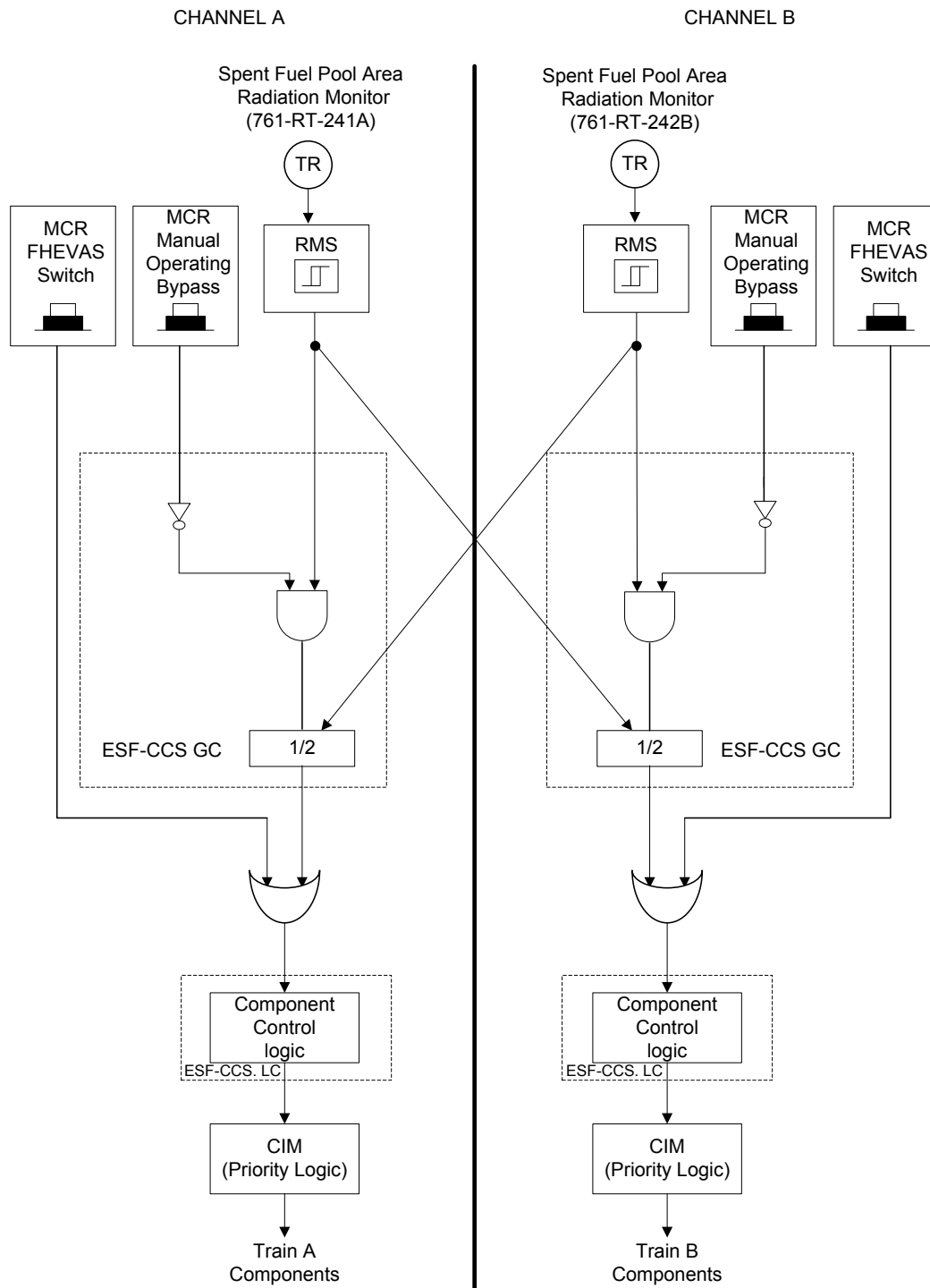


Figure 7.3-1F ESF Functional Logic (FHEVAS)

APR1400 DCD TIER 2

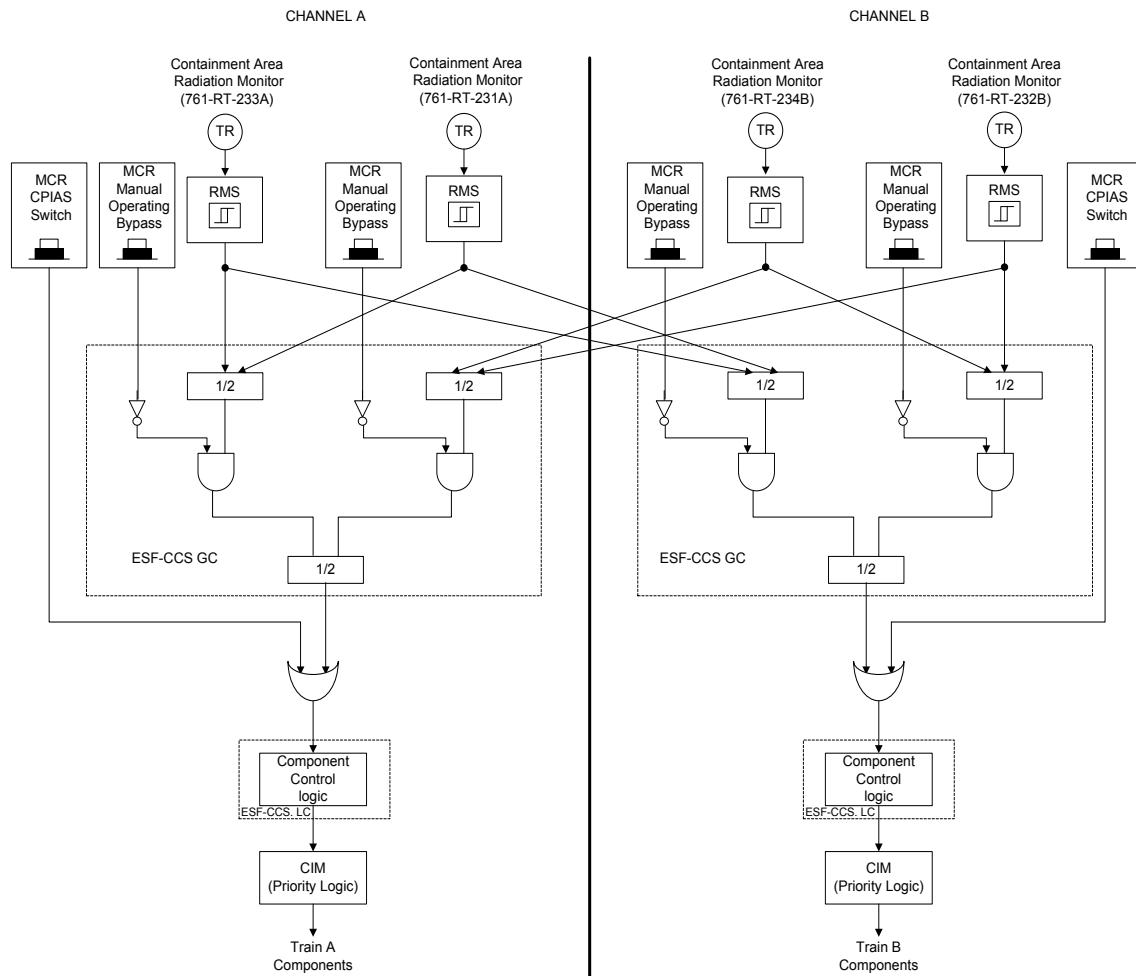


Figure 7.3-1G ESF Functional Logic (CPIAS)

APR1400 DCD TIER 2

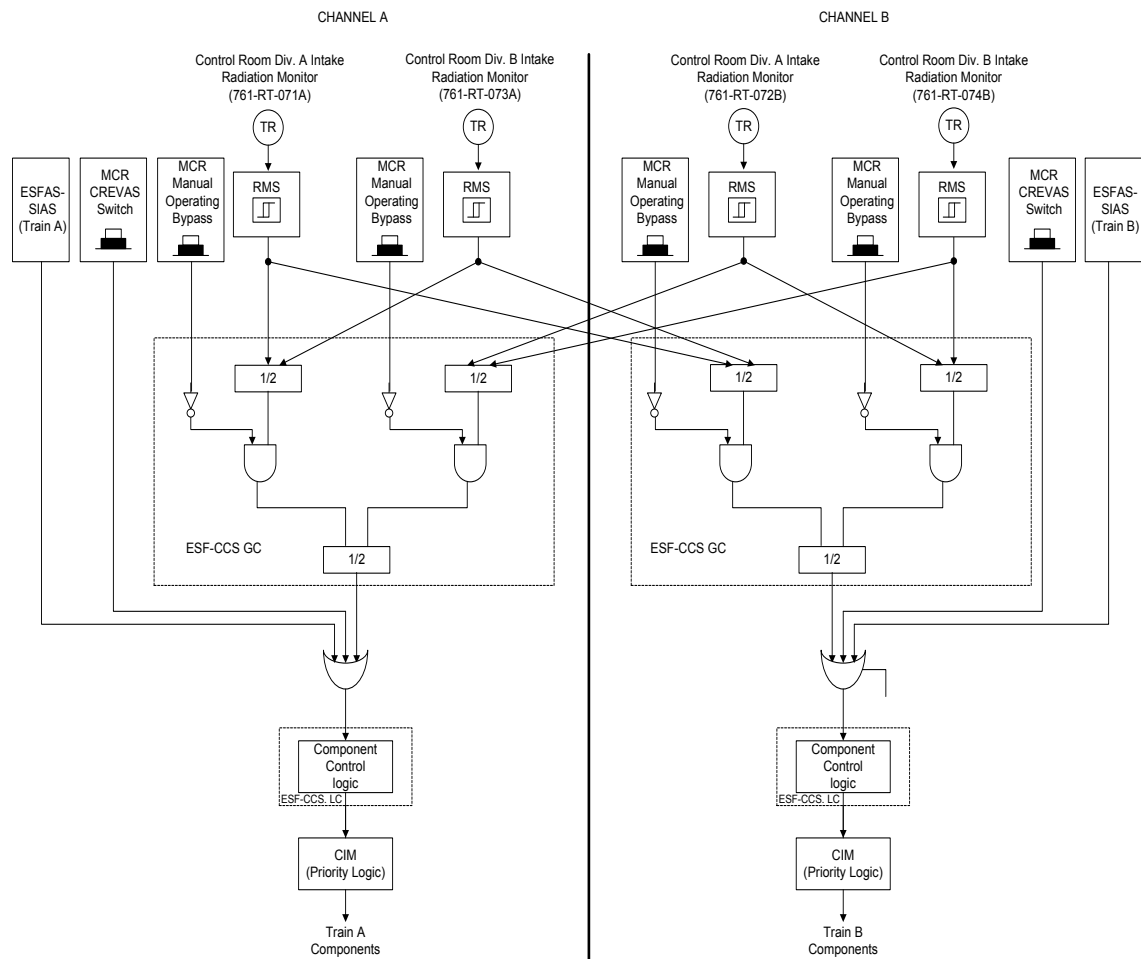


Figure 7.3-1H ESF Functional Logic (CREVAS)

APR1400 DCD TIER 2

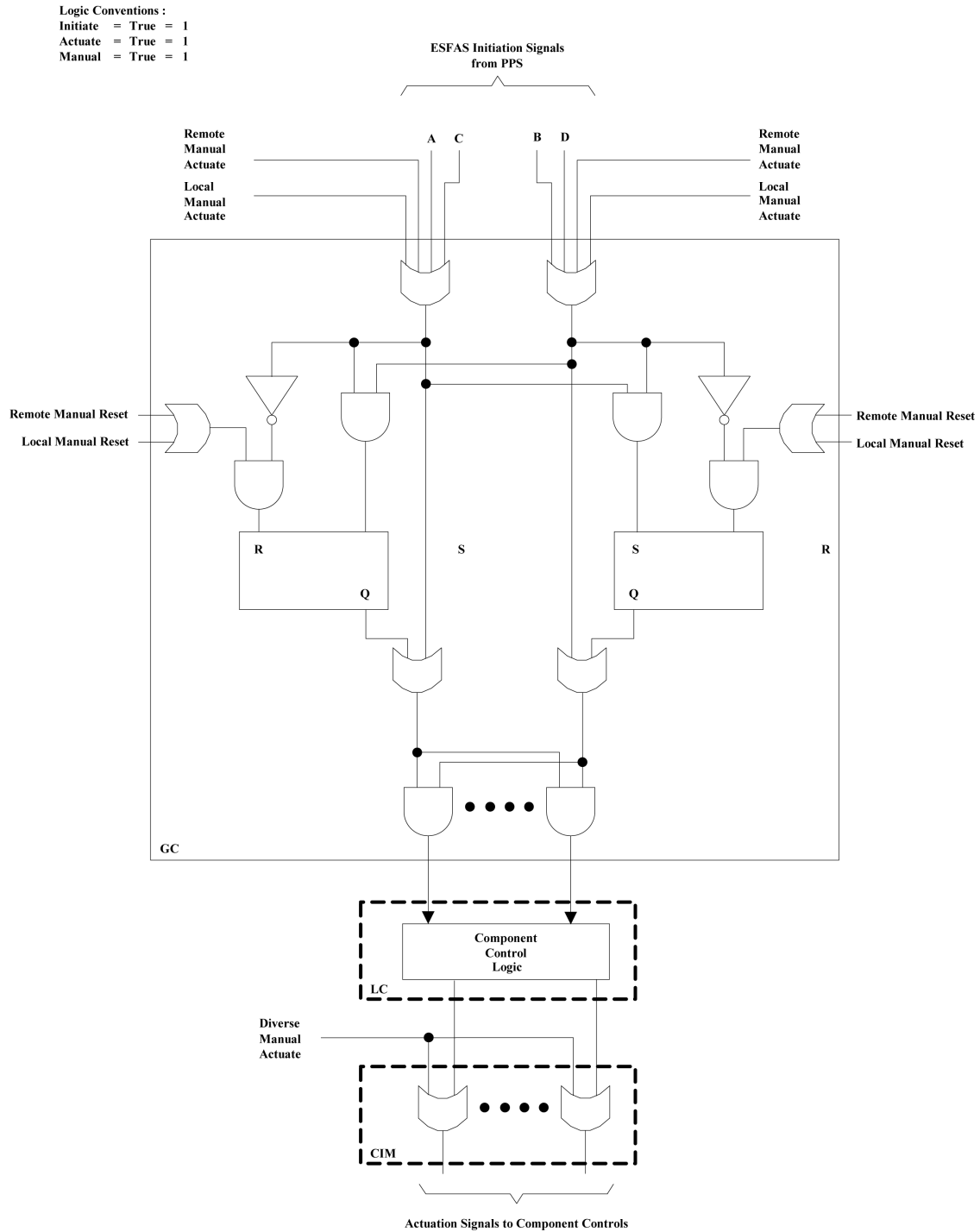


Figure 7.3-2 ESF-CCS Simplified Logic Diagram for Typical 2 out of 4 Actuation

APR1400 DCD TIER 2

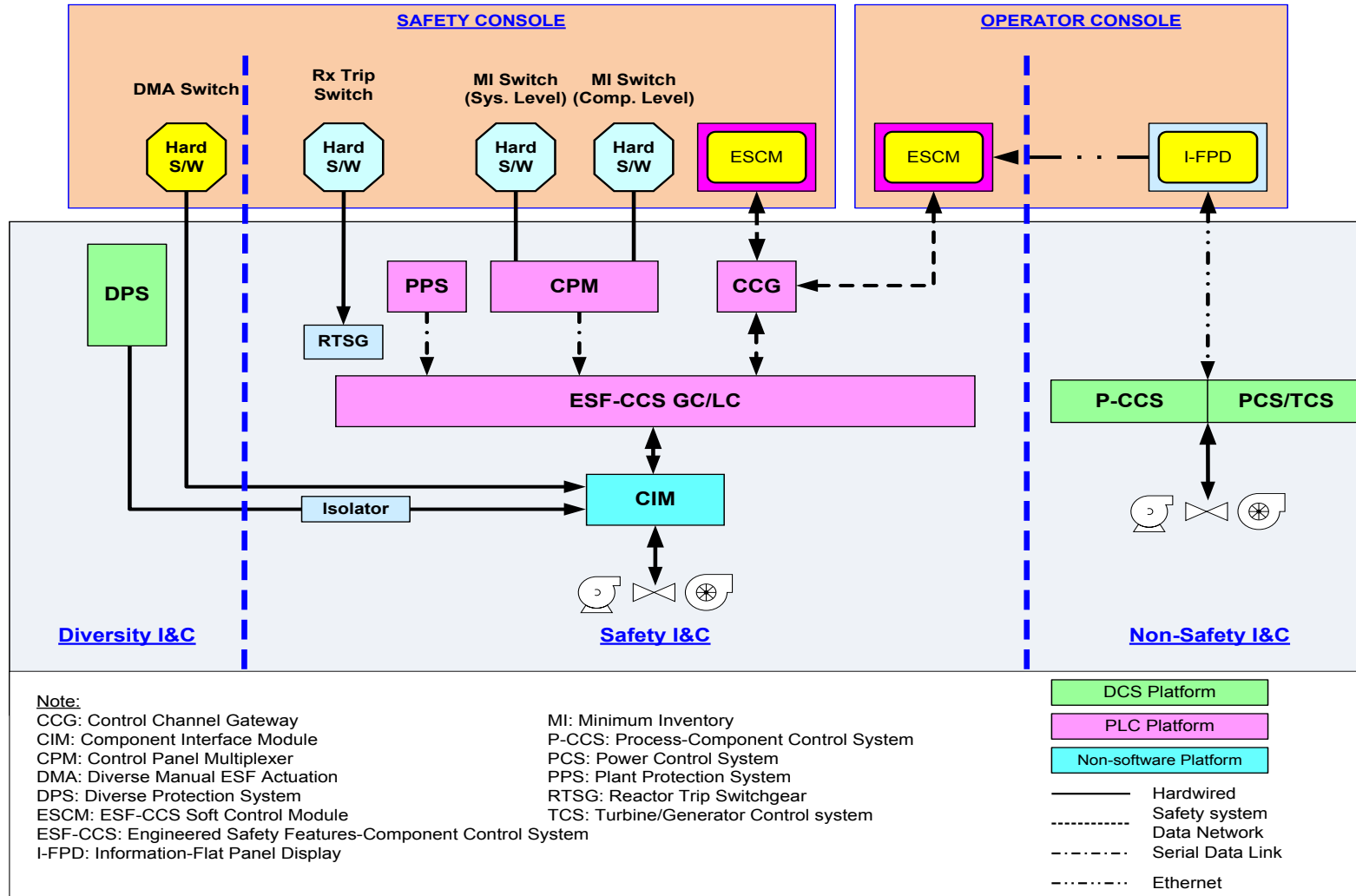


Figure 7.3-3A Simplified Functional Diagram of Engineered Safety Features Component Control System (ESF-CCS)

APR1400 DCD TIER 2

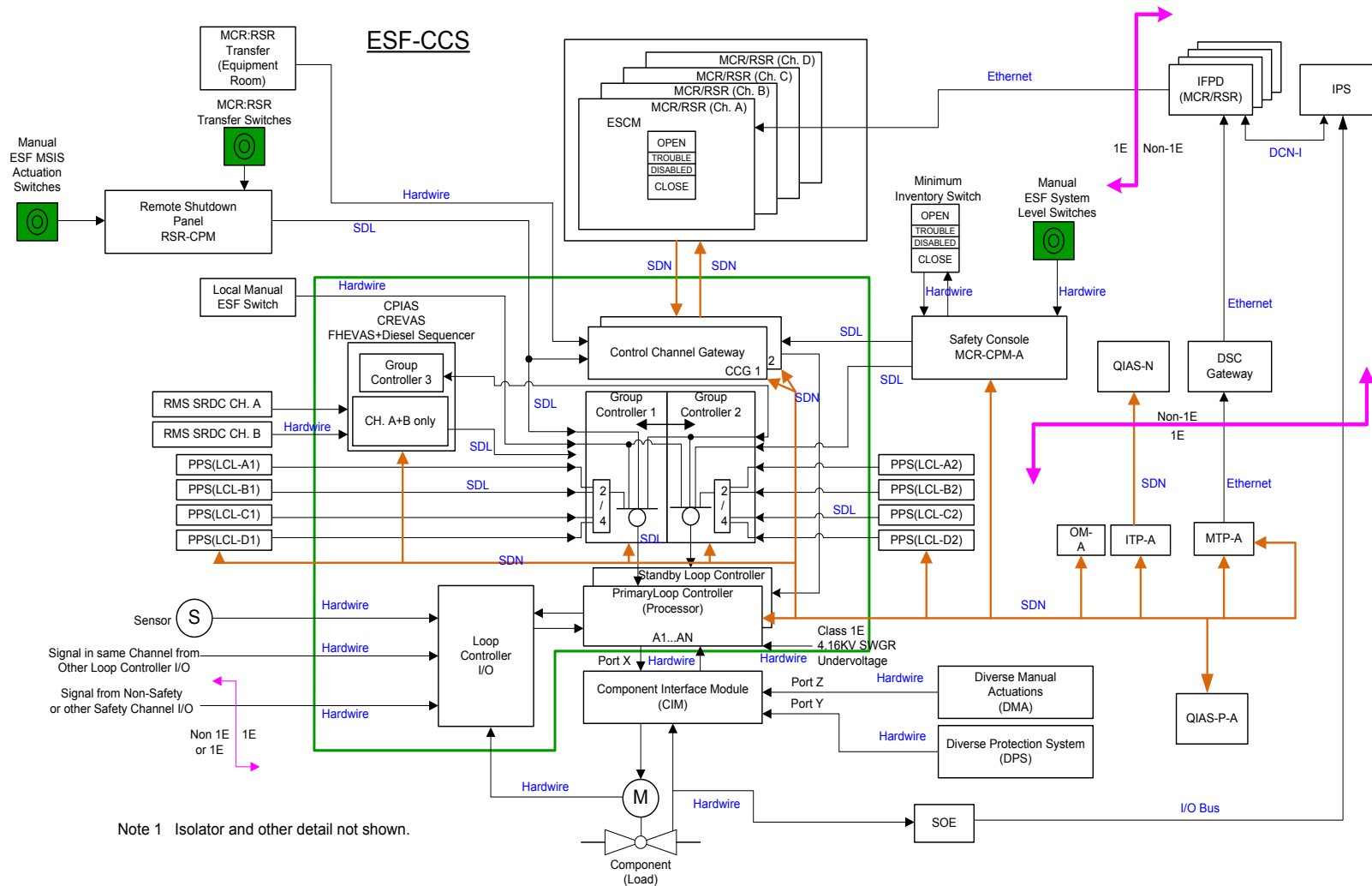


Figure 7.3-3B ESF-CCS Block Diagram

APR1400 DCD TIER 2

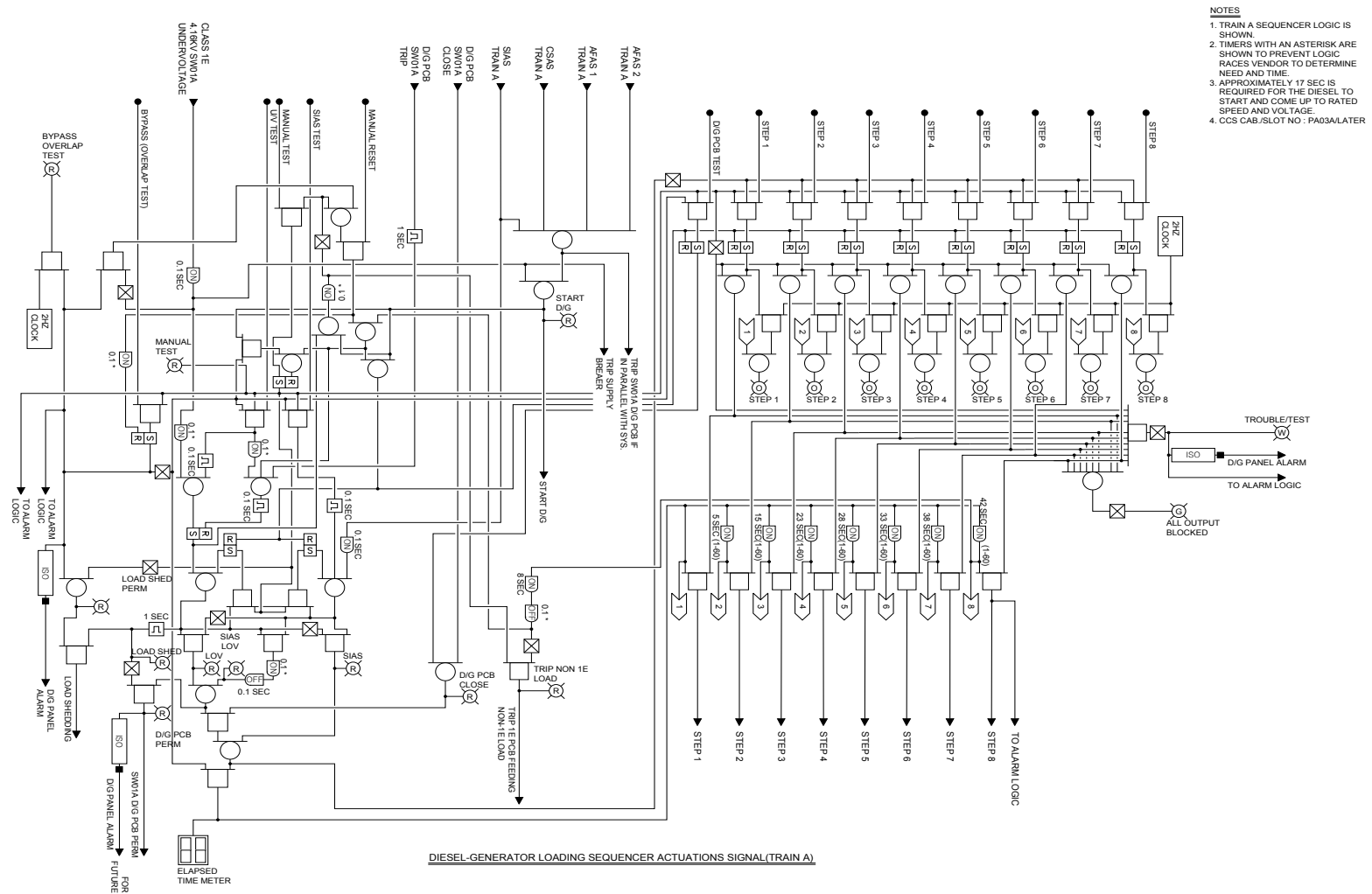


Figure 7.3-4 Loading Sequencer – Control Logic Diagram (1 of 4)

APR1400 DCD TIER 2

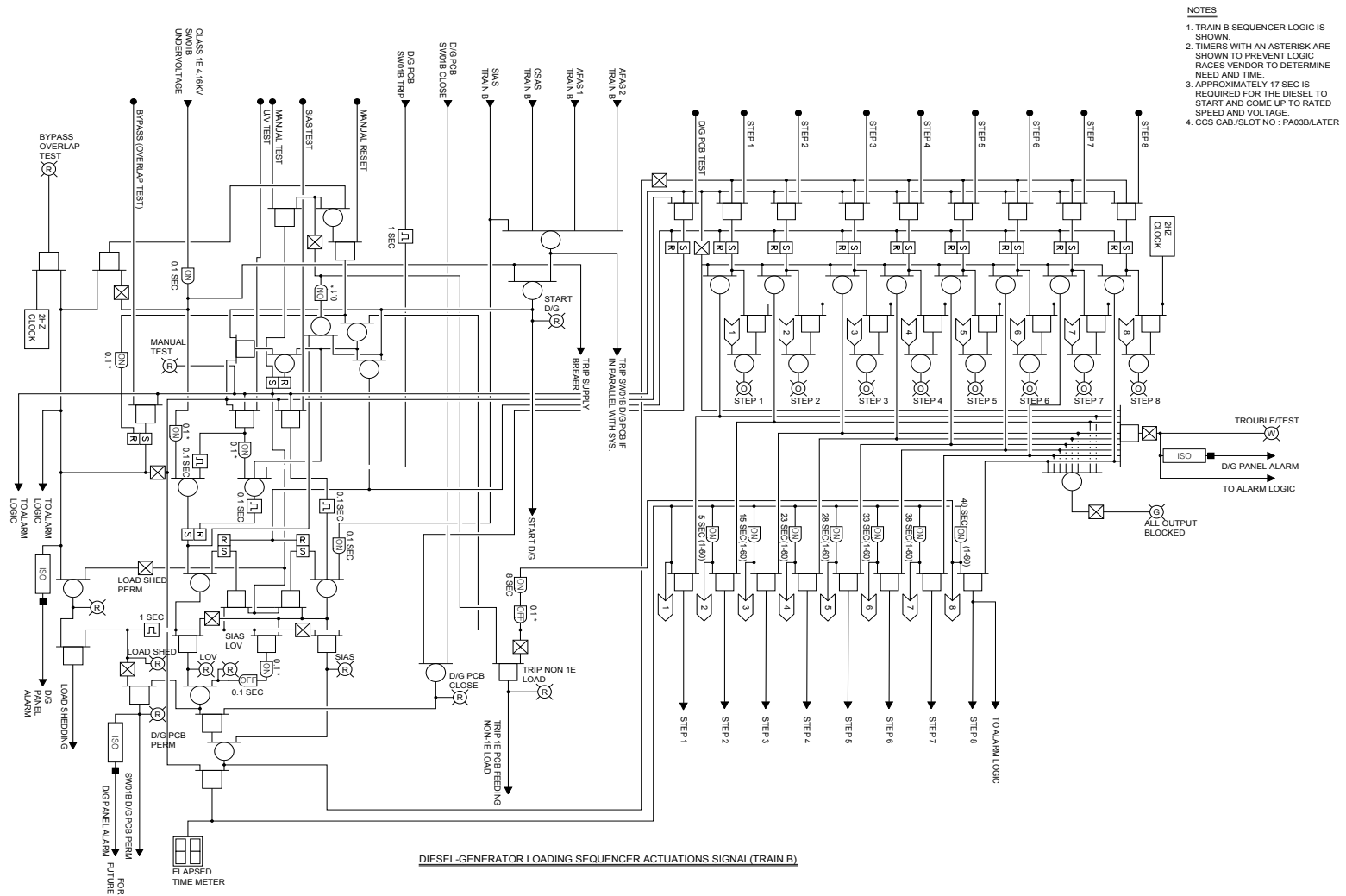


Figure 7.3-4 Loading Sequencer – Control Logic Diagram (2 of 4)

APR1400 DCD TIER 2

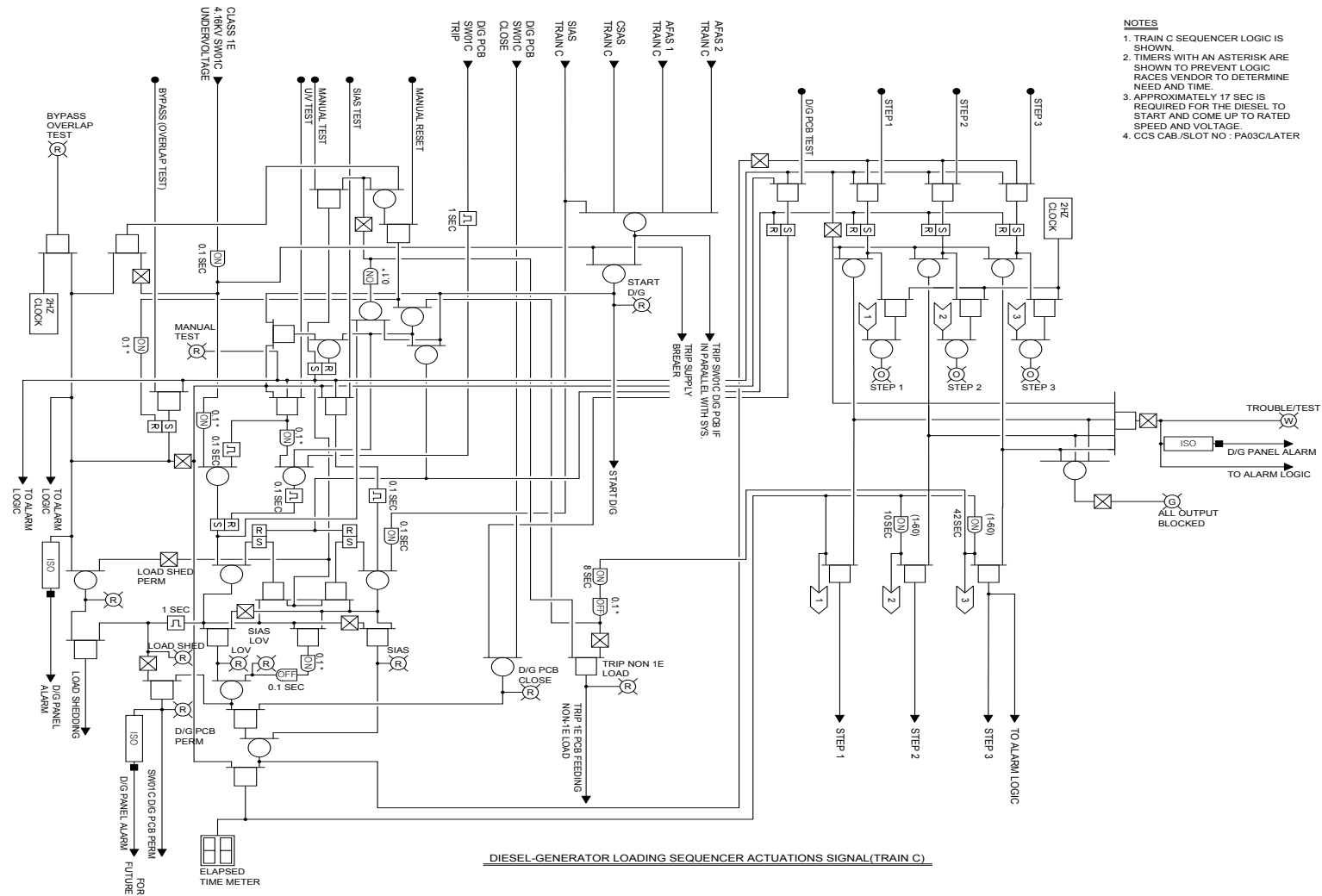


Figure 7.3-4 Loading Sequencer – Control Logic Diagram (3 of 4)

APR1400 DCD TIER 2

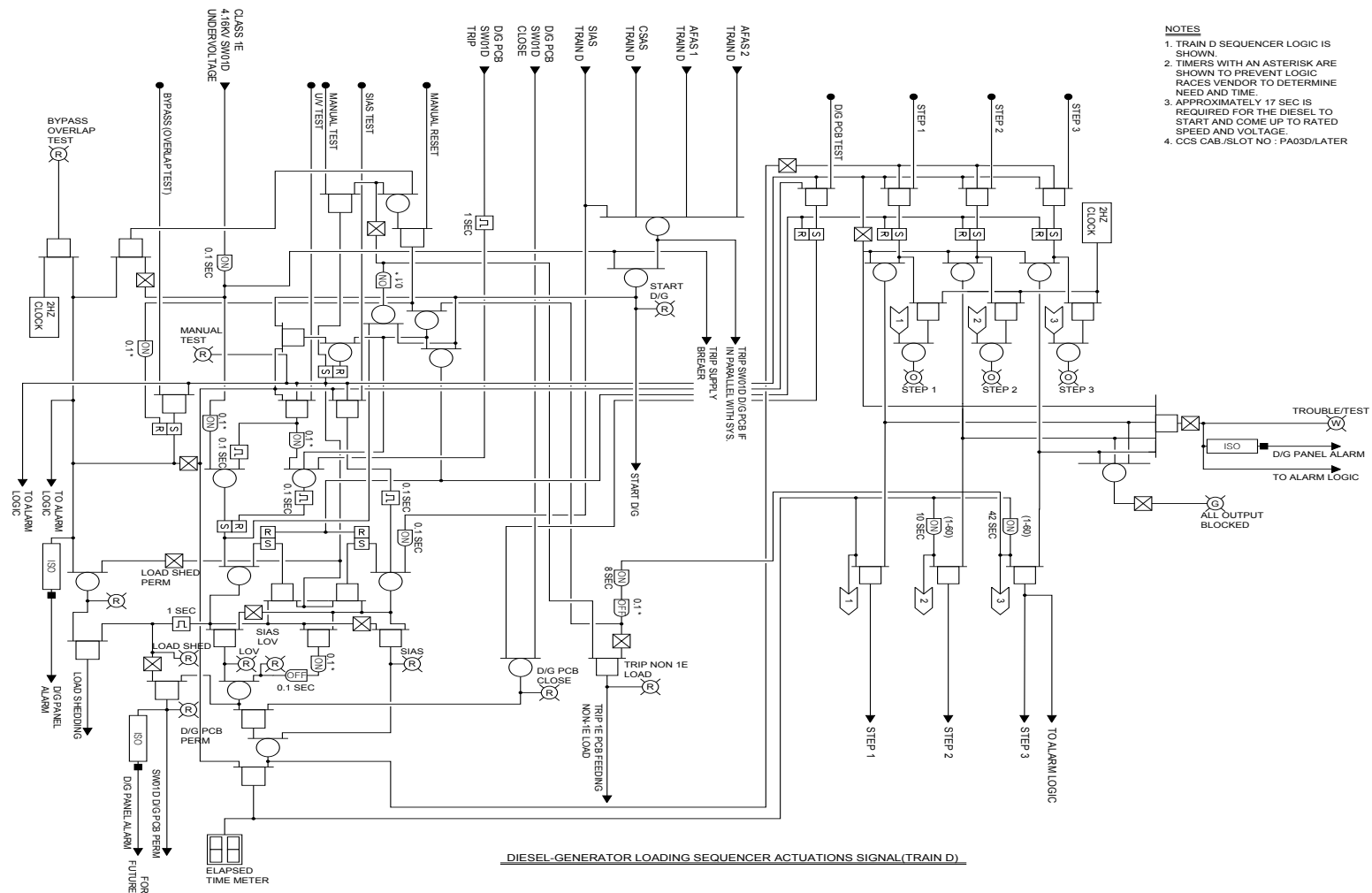


Figure 7.3-4 Loading Sequencer – Control Logic Diagram (4 of 4)

APR1400 DCD TIER 2

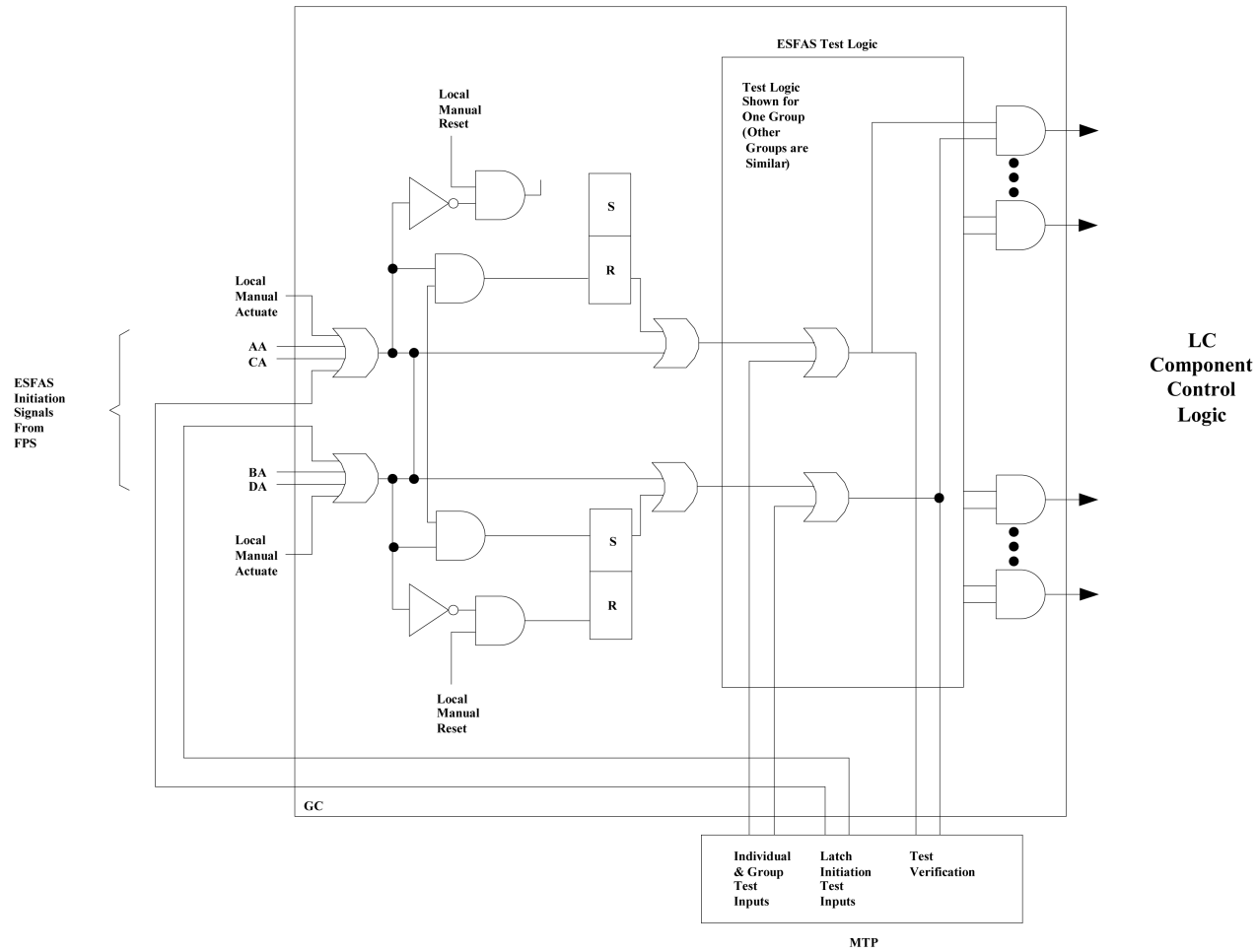


Figure 7.3-5 ESF-CCS Simplified Test Logic Diagram

APR1400 DCD TIER 2

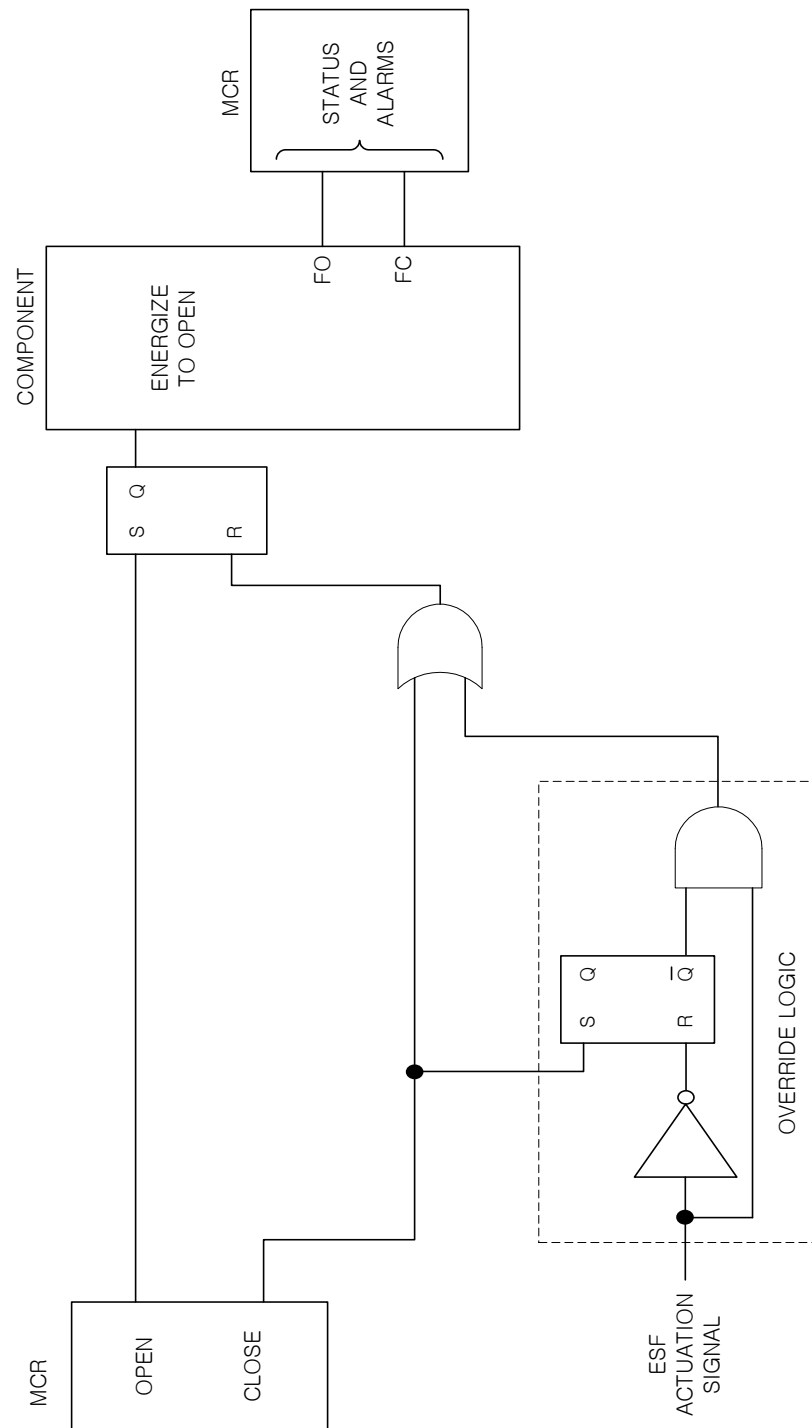


Figure 7.3-6 Typical CLD for a Solenoid Operated Valve

APR1400 DCD TIER 2

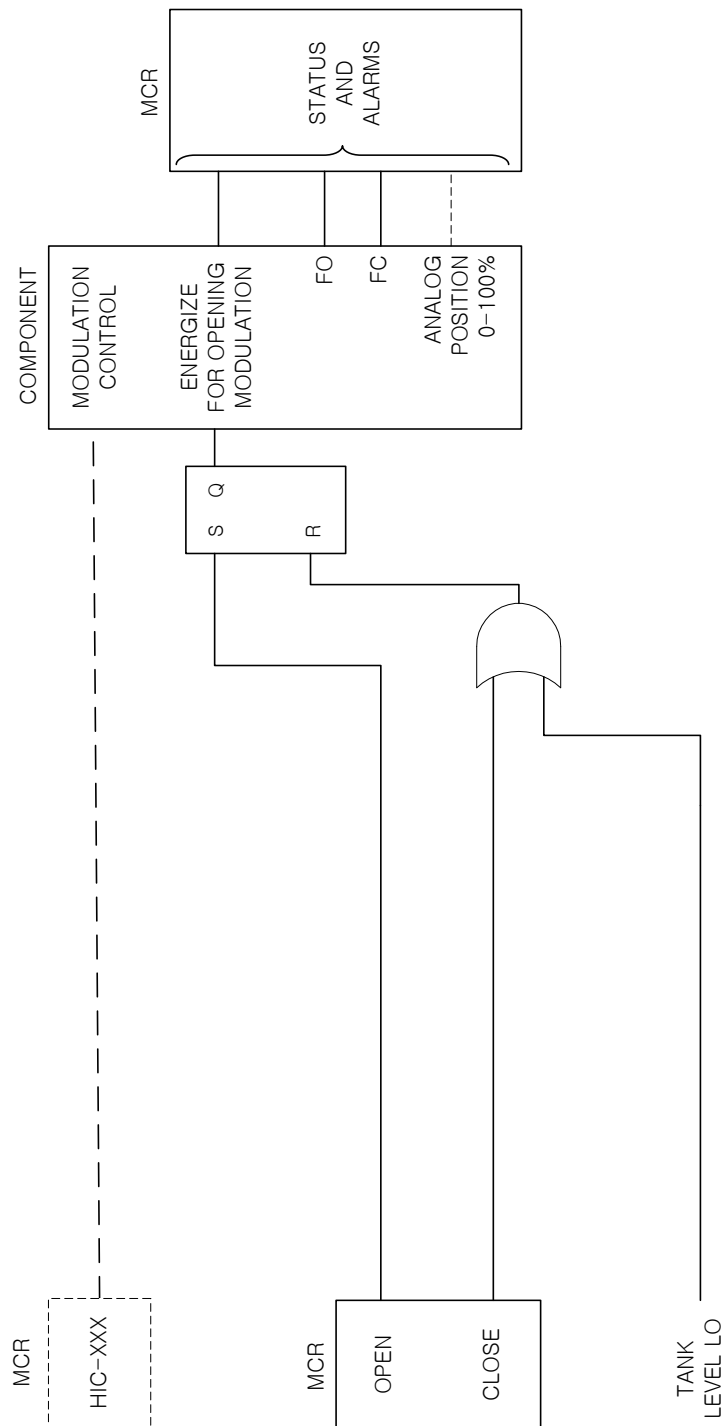


Figure 7.3-7 Typical CLD for a Modulating Valve with Solenoid Operator

APR1400 DCD TIER 2

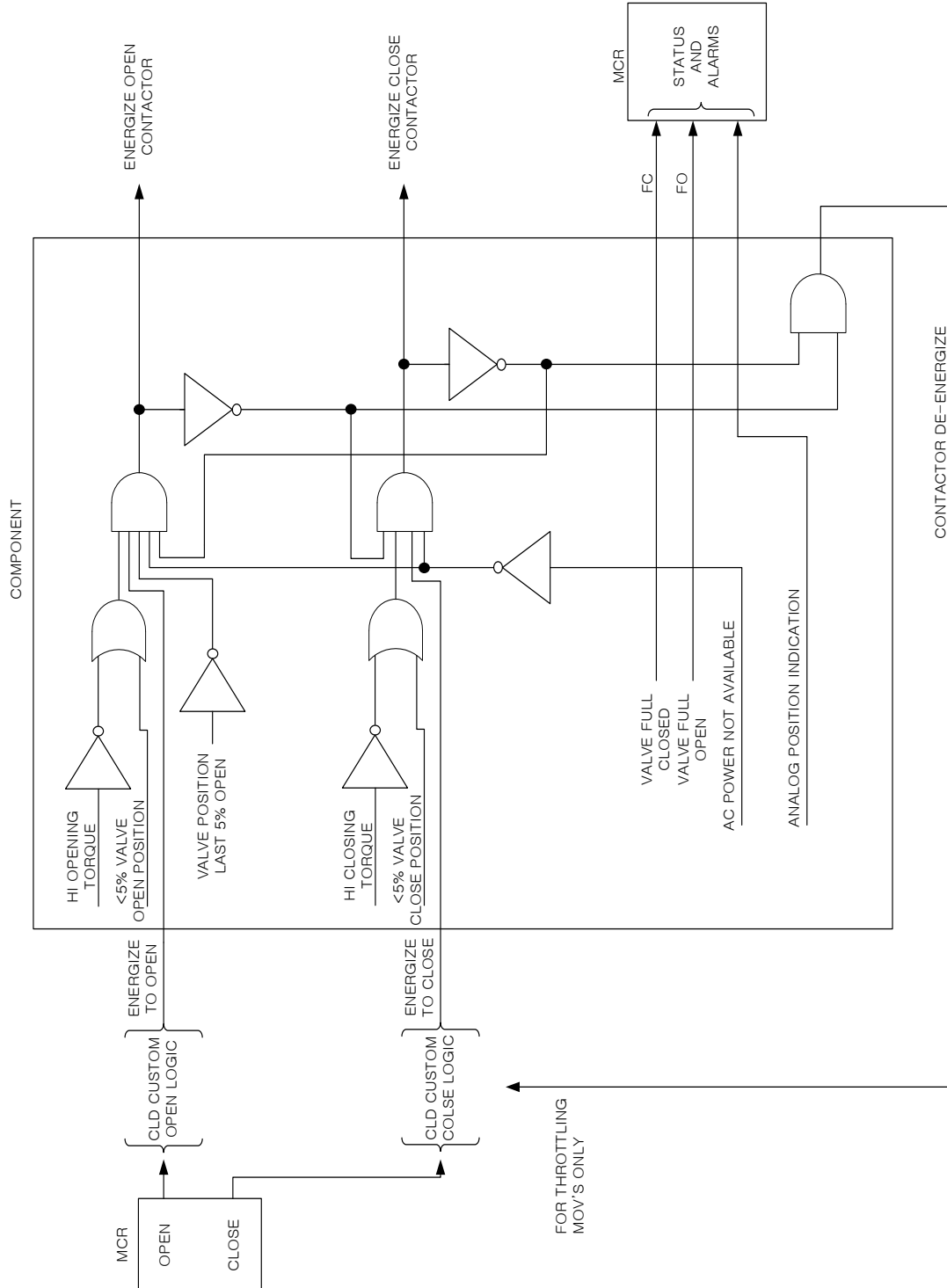


Figure 7.3-8 Typical Motor Operated Valve Functional Interface Design

APR1400 DCD TIER 2

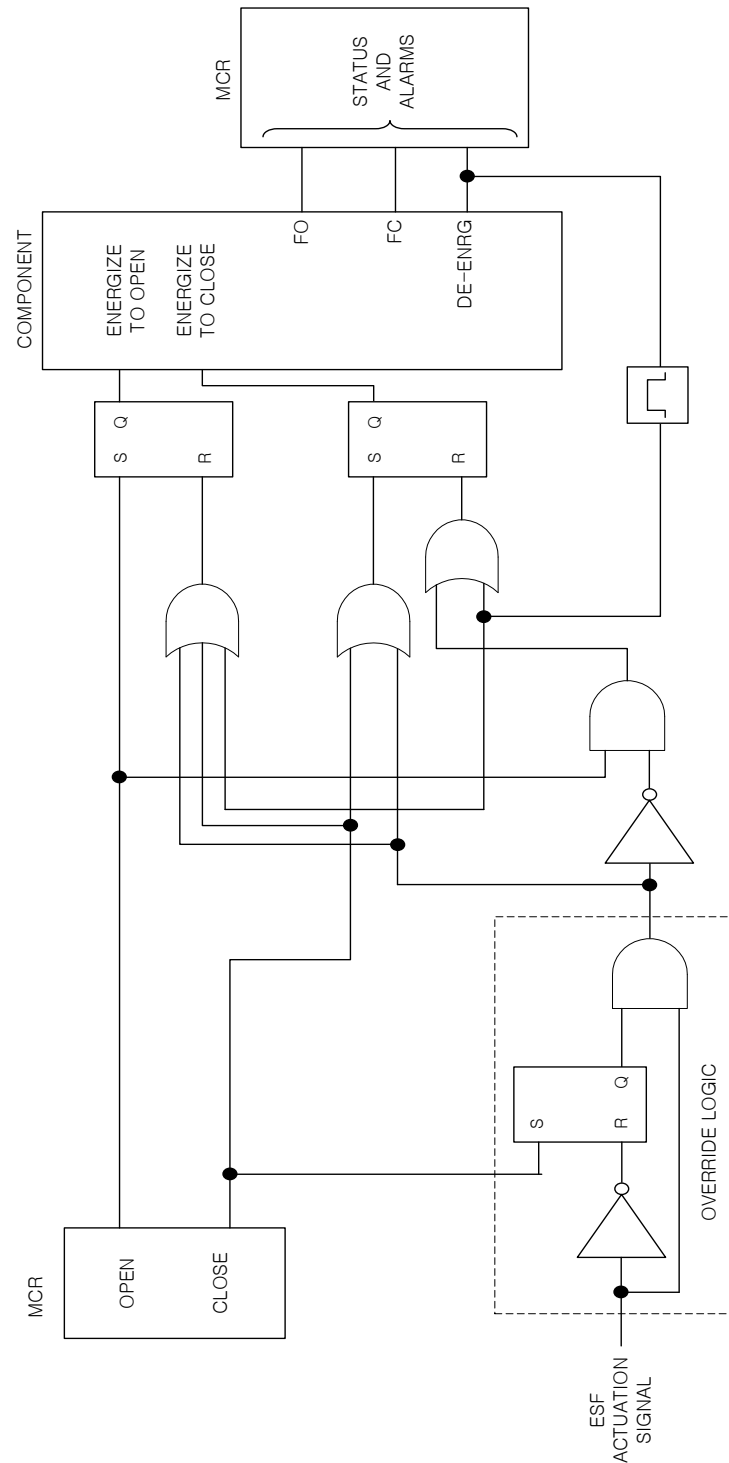


Figure 7.3-9 Typical CLD for a Full Stroke Motor Operated Valve

APR1400 DCD TIER 2

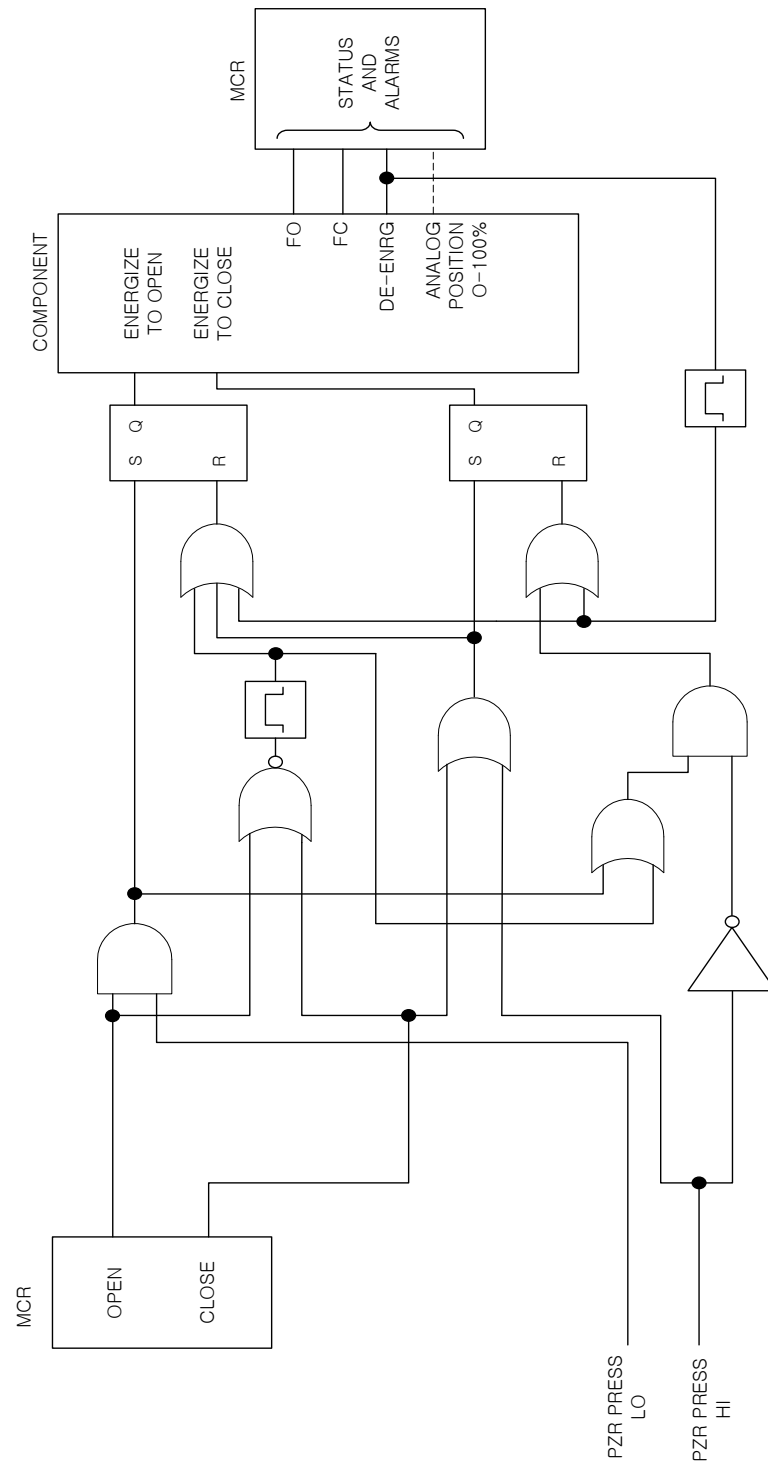


Figure 7.3-10 Typical CLD for a Throttling Motor Operated Valve

APR1400 DCD TIER 2

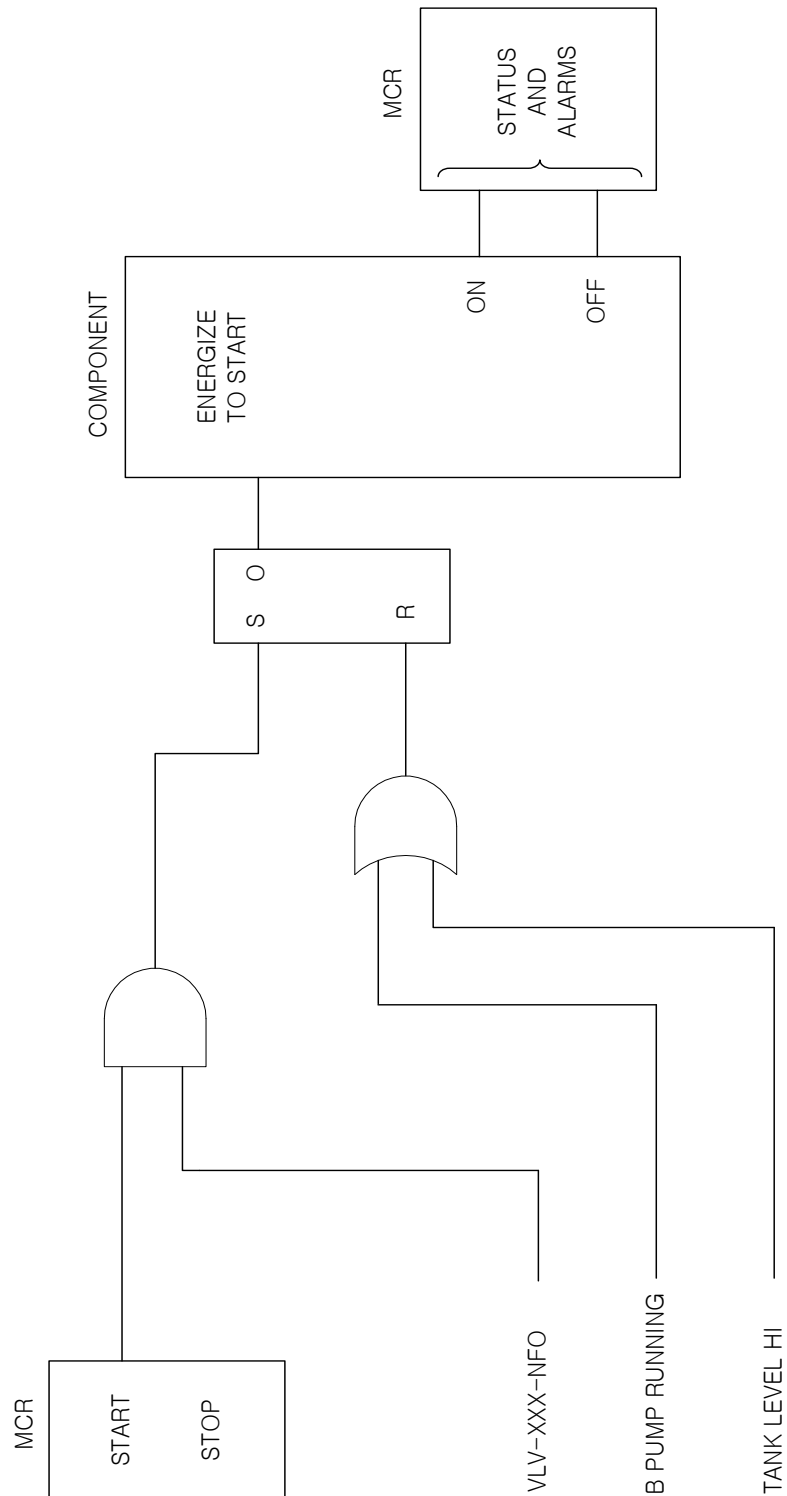


Figure 7.3-11 Typical CLD for a Non-reversing Motor Starter Operated Component

APR1400 DCD TIER 2

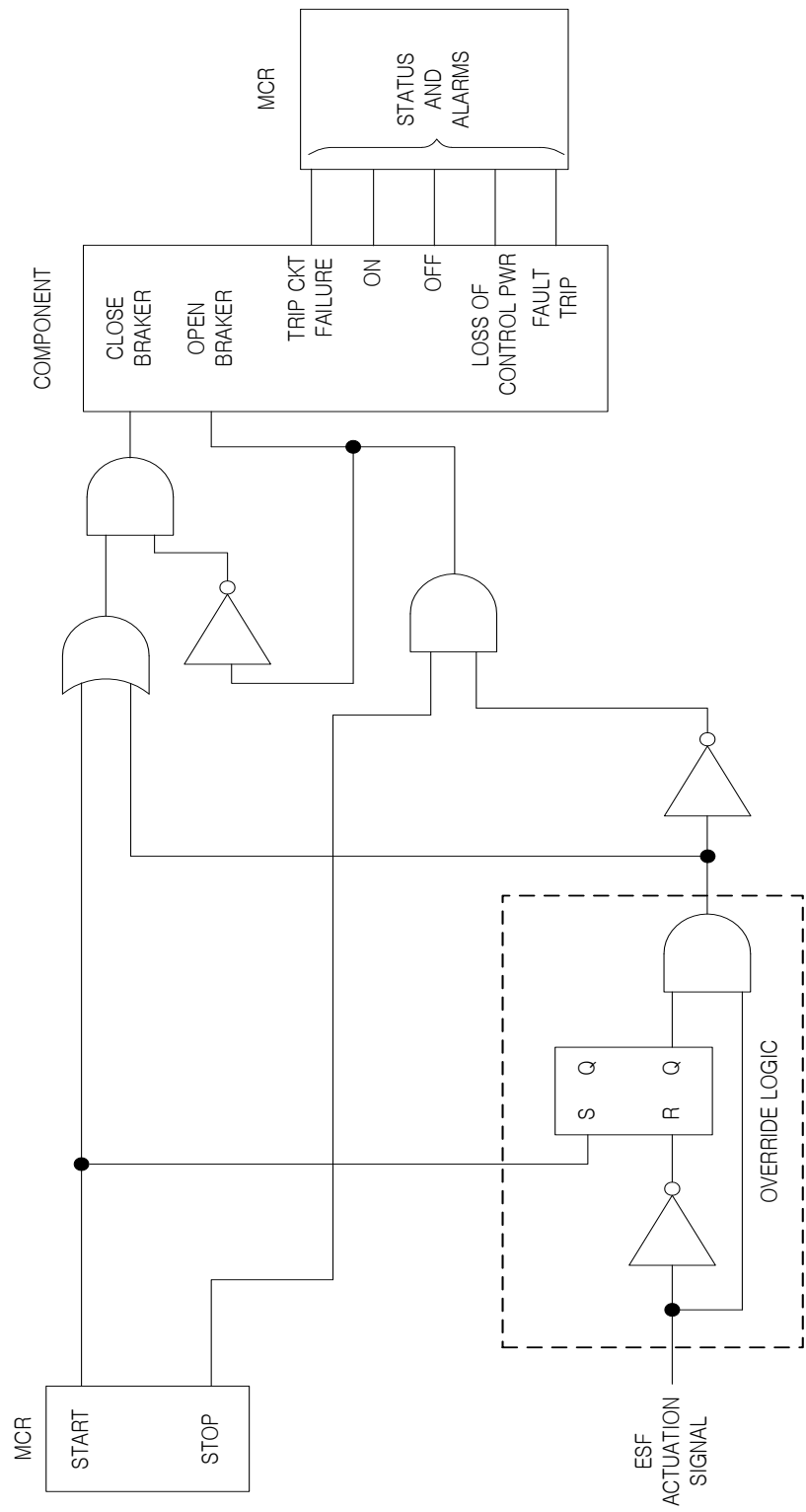


Figure 7.3-12 Typical CLD for a Circuit Breaker Operated Component

APR1400 DCD TIER 2

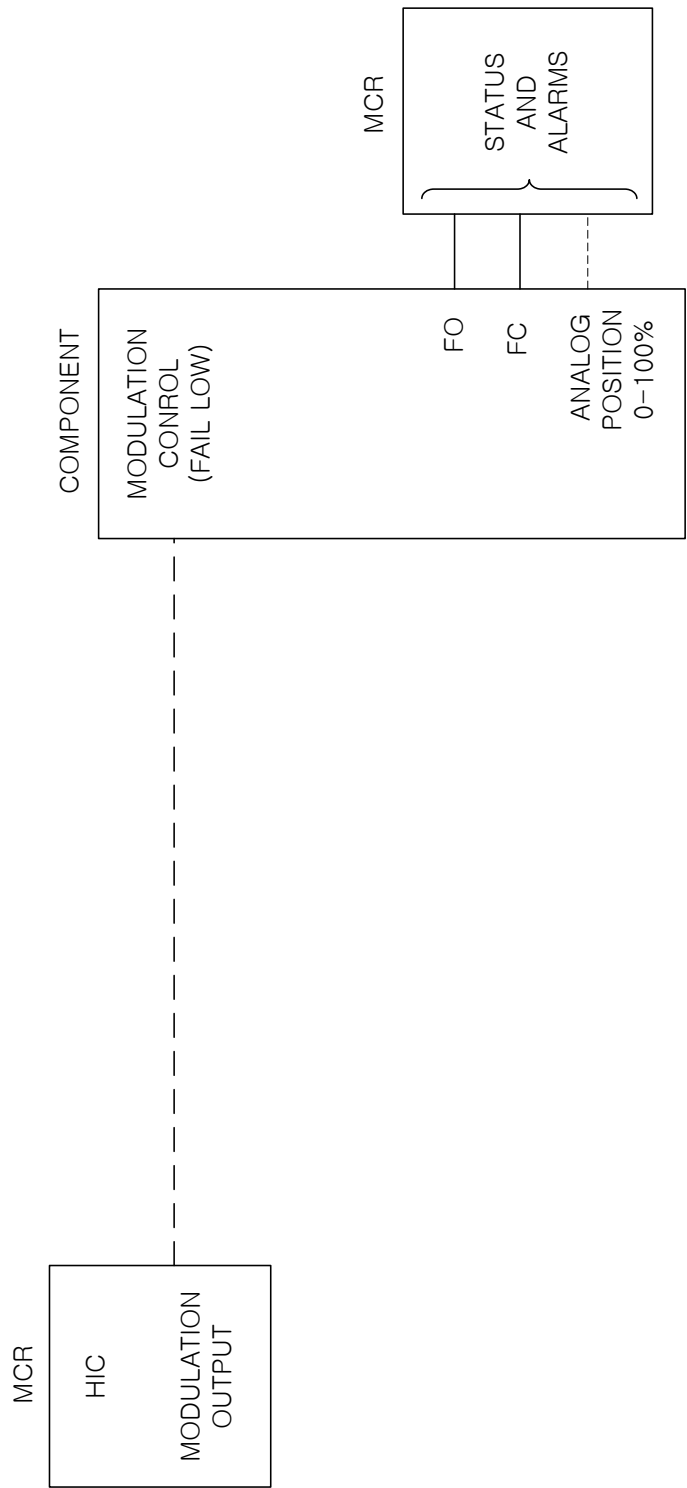


Figure 7.3-13A Typical CLD for a Modulating Component

APR1400 DCD TIER 2

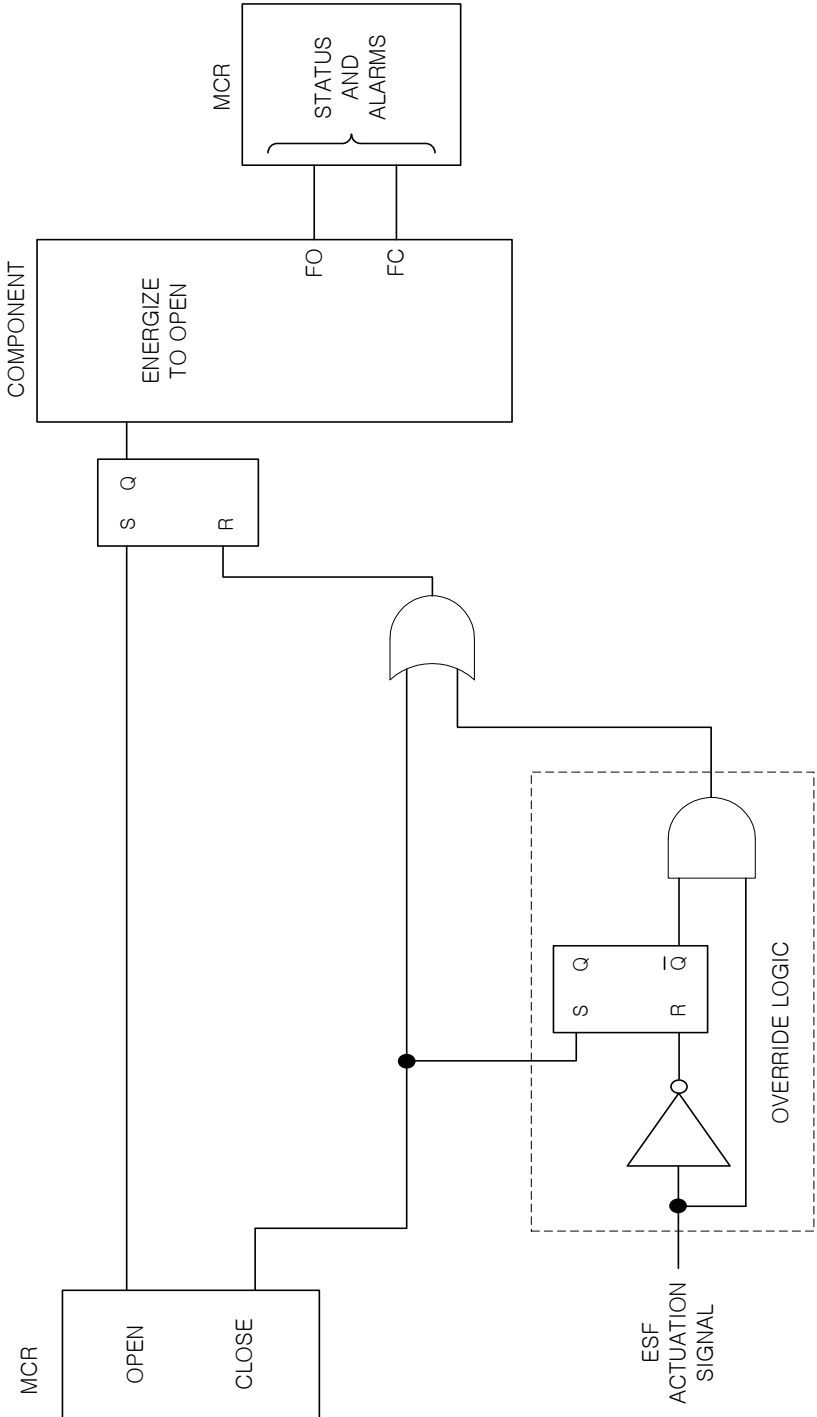


Figure 7.3-13B Typical CLD for a Electro Hydraulic Motor Damper

7.4 Systems Required for Safe Shutdown

This section describes the instrumentation and controls that are required to place and maintain the reactor in a safe shutdown condition. These systems are used in many cases during normal plant operations and, as such, cannot be exclusively identified as the safe shutdown function.

A description of these systems, together with the applicable codes, criteria and guidelines, is provided in other sections. In addition, the alignment of shutdown functions associated with the engineered safety features (ESFs) that are invoked under postulated limiting fault conditions is addressed in Chapter 6 and Section 7.3.

The instrumentation and control (I&C) functions required to maintain the reactor in a safe shutdown condition are described in this section. They represent the minimum number of functions required under non-accident conditions. These functions permit necessary operations that:

- a. Prevent the reactor from achieving criticality in violation of the Technical Specifications
- b. Provide an adequate heat sink such that design and safety limits are not exceeded

7.4.1 Description

The following systems are required to achieve and maintain a safe shutdown of the reactor:

- a. Auxiliary feedwater system (AFWS)
- b. Main steam system (MSS) – atmospheric dump
- c. Shutdown cooling system (SCS)
- d. Safety injection system (SIS)
- e. Safety depressurization and vent system (SDVS)
- f. Reactor coolant gas vent system (RCGVS)

APR1400 DCD TIER 2

The following auxiliary support systems are also required to achieve a safe shutdown of the reactor:

- a. Essential service water system (ESWS)
- b. Component cooling water system (CCWS)
- c. Class 1E emergency diesel generator system (EDG)
- d. Emergency diesel engine fuel storage and transfer system
- e. Class 1E power system
- f. Heating, ventilation, and air conditioning (HVAC) systems

7.4.1.1 System Description

The instrumentation, information displays, and controls of the auxiliary support system for safe shutdown are provided in the MCR and are described in their respective system description sections. Information systems important to safety that are necessary to achieve safe shutdown are described in Section 7.5.

- a. Auxiliary feedwater system

The safe shutdown features of these systems are described in Subsection 10.4.9. The instrumentation and controls for the AFWS are described in Subsection 7.3.1.

- b. Main steam system – atmospheric dump

The main steam atmospheric dump valves (MSADVs) are described in Subsection 10.3.2.2.4. The valves are located outside the containment upstream of the main steam isolation valves (MSIVs).

The valves are used to remove decay heat from the SG in the event that the main condenser is unavailable for certain reasons including loss of ac power. Under such a condition, the decay heat is removed by venting steam to the atmosphere. In this way, the RCS can either be maintained at hot standby conditions or cooled down.

APR1400 DCD TIER 2

The MSADV control circuits are designed so that no single failure prevents the operation of at least one valve on each SG.

c. Shutdown cooling system

The shutdown cooling system (SCS) is described in Subsection 5.4.7. The SCS instrumentation and control necessary to achieve and maintain cold shutdown are described below. The piping is shown in Figure 5.4.7-3.

The SCS is designed to be manually initiated upon the attainment of the required RCS conditions. The process instrumentation for MCR indication and status information are provided to enable the operator to determine system status, evaluate system performance, and detect malfunctions in the MCR. The control capability and valve position indication in the MCR are provided for the isolation valves and the heat exchanger inlet, outlet, and bypass valves. Indication is provided for low SCS pump discharge pressure and temperature, heat exchanger outlet temperature, and shutdown cooling system flow and pressure. SCS pump operating status is also indicated in the MCR.

The SCS has overpressure protection interlocks as described in Section 7.6. The system sequencing is provided by the operating procedures available to the site operator for the manually controlled equipment. There are no bypasses in the SCS instrumentation that would jeopardize the protection afforded by the interlocks.

The SCS trains A and B have independent Class 1E power sources for their actuated equipment (e.g., pumps, valves). The SCS isolation valve interlocks are implemented via the ESF-CCS using a redundant channel configuration such that a single failure will not cause loss of shutdown cooling nor spuriously actuate it.

d. Safety injection system (SIS)

Boron addition via the SIS may be used for the hot and cold shutdown processes. The SIS instrumentation and controls that are utilized to achieve cold shutdown are described below.

The SIS logic and piping are provided in Section 7.3 and Figure 6.3.2-1.

APR1400 DCD TIER 2

Initiating circuits and logic

To aid in achieving cold shutdown, the required SIS component actuation steps are as follows:

- 1) Coordinated control of the SI pumps and SI pump discharge valves to adjust and maintain the correct pressurizer water level.
- 2) Periodic sampling and adjustment of the boron concentration to compensate for the temperature decrease and other variables until shutdown concentration is reached.

The pressurizer level is automatically controlled during normal operation by the PLCS as described in Subsection 7.7.1.1. The operation of the SIS for RCS inventory control is further described in Subsection 6.3.2. Boric acid is injected to provide reasonable assurance that sufficient shutdown margin is maintained as the RCS is cooled down. The process instrumentation for indication and status information is provided to enable the operator to evaluate system performance and to control system operation manually at the operator consoles in the MCR.

Interlocks, sequencing, and bypasses

The interlocks, sequence of operation, and bypasses of the SIS are described in Subsection 6.3.1.

Redundancy and diversity

The SIS uses multiple signals as described in Section 6.3.

Supporting systems

The components of the system are powered from two separate Class 1E electrical divisions. Additional SIS supporting systems are described in Subsection 6.3.1.

- e. Manual actuation of pressurizer POSRVs

The manual actuation of pressurizer POSRVs is described in Subsection 5.4.14.2. A manual actuation of pressurizer POSRVs can be used for rapid depressurization for bleed-and-feed operations in the event of a total loss of feedwater.

APR1400 DCD TIER 2

f. Reactor coolant gas vent system

The RCGV function of SDVS can be used to provide a means of remotely venting non-condensable gases from the reactor vessel closure head and the pressurizer steam space during post-accident conditions and to provide a means of remotely removing steam from the pressurizer steam space and/or the reactor vessel for the RCS pressure control purposes in the event that pressurizer main spray and auxiliary spray are unavailable.

g. Essential service water system

The instrumentation and controls for ESWS system are described in Subsection 9.2.1.

h. Component cooling water system

The instrumentation and controls for CCWS system are described in Subsection 9.2.2.

i. Class 1E emergency diesel generator system

Four independent, 100 percent capacity emergency diesel generators (EDGs) (one per channel) provide a dependable onsite power source. Four EDGs are capable of starting and supplying the essential loads necessary to shut the plant down safely and reliably. The EDGs maintain the plant in a safe shutdown condition under a loss of offsite power (LOOP). Loading sequencers are provided to sequentially load essential components onto the 4.16 kV class 1E buses and are part of the ESF-CCS described in Section 7.3.

The EDGs start automatically by an undervoltage signal (LOOP detected on the associated 4.16 kV ESF bus), AFAS, SIAS, or CSAS.

Subsection 8.3.1 describes the non-Class 1E alternate alternating current (AAC) gas turbine generator (GTG) standby power supply. The emergency diesel engine starting system (EDESS) is described in Subsection 9.5.6. Additional information on EDG supporting auxiliaries is provided in Subsections 9.5.4, 9.5.5, 9.5.7, and 9.5.8.

APR1400 DCD TIER 2

- j. Emergency diesel engine fuel oil storage and transfer system

The instrumentation and controls for this system are described in Subsection 9.5.4.

- k. Class 1E power system

This system is described in Section 8.3.

- l. Emergency shutdown from outside the main control room

In the unlikely event that the MCR becomes uninhabitable, sufficient indications and controls are provided outside the MCR according to GDC 19 to:

- 1) Achieve hot standby of the reactor
- 2) Maintain the unit in a safe condition during hot shutdown
- 3) Achieve cold shutdown of the reactor through the use of operating procedures

For safe shutdown in the remote shutdown room (RSR), controls and indications are available through the soft controls and displays on the information FPD on the remote shutdown console (RSC). The shutdown overview display panel (SODP) at the RSC provides the information that the operator requires for assessing the plant status. Displays and controls on the RSC are the same type as those on the consoles of the MCR. The layout of the RSR is shown in Figure 7.4-4.

Postulated conditions or events that make the MCR uninhabitable are considered in the control room arrangement design. It is assumed that these circumstances are the result of the destruction of equipment due to a fire inside the MCR.

The MCR operator consoles and the RSC are in separate locations and at different elevations, have separate ventilation systems and multiple communication systems, and have lighted access routes between them. More information on the communication systems between the RSR and other emergency response facilities is provided in Subsection 9.5.2. The lighting systems are described in Subsection 9.5.3. The design includes the capability for the signal isolation and disabling of all main control, and the transfer of controls required to achieve hot standby to the RSC. Therefore, no single credible event that would require the evacuation of the MCR (or fire damage in the MCR) would make the RSC inoperable.

APR1400 DCD TIER 2

Transfer switches are located in the maintenance and test panel (MTP) in the I&C equipment rooms and RSR. One transfer switch is provided for each channel of the ESF-CCS and each channel of the P-CCS, respectively. Interface diagrams of the transfer switches are provided in Figures 7.4-1 and 7.4-2.

When the transfer switches are switched to the mode of RSR, all signals from the MCR are disabled and signals from the RSR are enabled. This includes signals from ESCMs and signals interfaced via the control panel multiplexers (CPMs).

The transfer initiated by these switches provides reasonable assurance that the switches cannot transfer the control back to the MCR operator consoles. The transfer of control back to the MCR operator consoles can be performed using the MTPs provided for each channel of the ESF-CCS and P-CCS in the I&C equipment rooms.

The MTPs also provide a backup means for performing the transfer of control from the MCR to the RSR. Each MTP has hardwired transfer switches, as shown in Figure 7.4-3.

The RSR is keylocked and under administrative control. In addition, the status of a control transfer is indicated at both the MCR operator consoles and the RSC. The system provides an alarm for each channel to the operator that the transfer logic has transferred the controls to the RSC. The component controls within each channel also report the component group transfer status to the information processing system (IPS). The transfer status is also indicated on the transfer switches by an indication light or on the displays without control and monitoring functions because of the transfer.

Furthermore, use of fiber-optic cables for the transfer switches maintains isolation between the ESF-CCS channels and between the P-CCS channels. No direct electrical connection exists between the switches and the ESF-CCS, the P-CCS, or the consoles.

The transfer switch implementation for one channel of the ESF-CCS is shown in Figure 7.4-1. Input to the transfer logic for channel A is provided from two locations: at the RSC and the MTP channel A. The logic transfers the operator interface for ESF components controlled by ESF-CCS channel A. The interfaces for manual initiation of reactor trip and main steam isolation signal (MSIS) are not

APR1400 DCD TIER 2

transferred because it can be performed from either the MCR or the RSR at any time.

The transfer switch implementation for one channel of the P-CCS is shown in Figure 7.4-2.

The HFE design approach for the RSR is described in Chapter 18.

Hot standby

If the MCR becomes uninhabitable, sufficient indications and controls are provided in the RSR to achieve and maintain hot standby of the reactor. The following are the assumptions for the evacuation of the MCR:

- 1) The operator trips the reactor prior to the evacuation of the MCR.
- 2) No adverse consequences other than an MCR fire and MCR evacuation occur (i.e., events proceed as if following a reactor trip).

Table 7.4-1 lists the indications and controls provided in the RSR that are necessary to achieve and maintain hot standby.

Hot shutdown and cold shutdown

Hot shutdown and cold shutdown can be achieved at the RSC by using the direct controls on the equipment listed in Tables 7.4-1 and 7.4-2.

The MCR has at least two independent exits that can be used if the MCR is evacuated. The RSR is accessible to operators from either exit.

m. Heating, ventilation, and air conditioning system

The heating, ventilation, and air conditioning (HVAC) systems maintain the ambient temperature of the systems and components that are necessary for safe shutdown. Additional information is provided in Section 9.4.

APR1400 DCD TIER 2

7.4.2 Design-Basis Information

Safe shutdown design, including the design of the RSR, is based on the following applicable codes and standards:

- a. 10 CFR 50.34(f)(2)(xx), “Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves”
- b. 10 CFR 50.55a(a)(1), “Quality Standards”
- c. 10 CFR 50.55a(h), “Protection Systems and Safety Systems”
- d. 10 CFR 50, Appendix A, GDC 1, “Quality Standards and Records”
- e. 10 CFR 50, Appendix A GDC 2, “Design Bases for Protection against Natural Phenomena”
- f. 10 CFR 50, Appendix A GDC 4, “Environmental and Missile Design Bases”
- g. 10 CFR 50, Appendix A GDC 13, “Instrumentation and Control”
- h. 10 CFR 50, Appendix A GDC 19, “Control Room”
- i. 10 CFR 50, Appendix A GDC 24, “Separation of Protection and Control Systems”
- j. 10 CFR 50, Appendix A GDC 34, “Residual Heat Removal”
- k. 10 CFR 50, Appendix A GDC 35, “Emergency Core Cooling”
- l. 10 CFR 50, Appendix A GDC 38, “Containment Heat Removal”
- m. NRC RG 1.189, “Fire Protection for Operating Nuclear Power Plants” (Reference 1)

7.4.2.1 Single Failure Criterion

The instrumentation and controls required for safe shutdown are designed and arranged so that no single failure can prevent a safe shutdown. The single failures that are considered include electrical faults and physical events resulting in mechanical damage. Each system is composed of redundant trains, including I&C, that are physically separated.

APR1400 DCD TIER 2

7.4.2.2 Quality of Components and Modules

The instrumentation and controls used for the safe shutdown systems are designed in accordance with the QA program described in Chapter 17.

7.4.2.3 Independence

The safe shutdown instrumentation and control independence is achieved by electrical and physical separation. The independence precludes a single event causing multiple channel failures.

7.4.2.4 Periodic Testing

The instrumentation and control components required for safe shutdown that are not normally in operation are capable of being tested periodically. The components include instrumentation and controls for the SCS, SIS, and the rapid depressurization function of SDVS. All automatic and manual actuation devices are capable of being tested to verify their operability. Transfer switches are also tested periodically. Periodic testing is further described in Section 13.5 and the Technical Specifications (Chapter 16).

7.4.2.5 Use of Digital Systems

The RPS and ESFAS functions rely on digital systems with the exception of the manual RT and ESFAS actuation switches in the MCR and RSR.

7.4.2.6 System Drawings

The logic diagrams for the operations of the SCS are shown in Figures 7.6-1A, 7.6-1B, and 7.6-1C.

7.4.3 Analysis

7.4.3.1 Conformance with IEEE Std. 603 and IEEE Std. 7-4.3.2

Compliance with IEEE Std. 603 (Reference 2) and IEEE Std. 7-4.3.2 (Reference 3) is described in the Safety I&C System Topical Report (Reference 4).

APR1400 DCD TIER 2

7.4.3.2 Conformance with General Design Criterion 19

Compliance with GDC 19 is addressed in Subsection 3.1.15. Remote instrumentation enables hot standby to be achieved if the MCR is not habitable. Hot standby, as used here, means the reactor is subcritical at normal operating pressure and temperature. The reactor can be brought to cold shutdown outside the MCR by use of appropriate procedures, the RSC controls, and local controls.

7.4.3.3 Consideration of Selected Plant Contingencies

7.4.3.3.1 Loss of Instrument Air System

None of the essential control or monitoring instrumentation relies solely on instrument air. Where necessary, safety-related accumulator tanks are provided or the failure mode of pneumatic devices upon loss of air is designed to fail in the safe position. Therefore, loss of instrument air does not degrade the instrumentation and control associated with systems required for plant shutdown.

7.4.3.3.2 Loss of Cooling Water to Vital Equipment

Loss of cooling water to vital equipment does not affect the capability of the safe shutdown function because the safety-related component cooling water system has two separate divisions of cooling water systems. Therefore, the loss of single division does not hinder the safe shutdown function.

7.4.3.3.3 Plant Load Rejection, Turbine Trip, and Loss of Offsite Power

In the event of a LOOP associated with plant load rejection or turbine trip, the power for safe shutdown is provided by the EDGs. The EDGs provide power for operation of pumps and valves; the batteries or EDGs via the battery chargers provide power for operation of instrumentation and control systems required to actuate and control essential components.

7.4.3.3.4 Restrictive Setpoints

There are no restrictive setpoints for the APR1400.

7.4.4 References

1. NRC RG 1.189-2007, "Fire Protection for Operating Nuclear Power Plants."

APR1400 DCD TIER 2

2. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”
3. IEEE Std. 7-4.3.2-2003, “IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
4. APR1400-Z-J-EC-13001-P, “Safety I&C System Technical Report,” September 2013.

APR1400 DCD TIER 2

Table 7.4-1 (1 of 4)

Remote Shutdown Console Instrumentation
and Controls for Hot Shutdown

No.	Function
1	Neutron Logarithmic Power
2	Hot/Cold Leg Temperature
3	Pressurizer Pressure
4	Pressurizer Level
5	Pressurizer RCGV Valve Steam Generator No. 1 Pressure
6	Steam Generator No. 1 Level
7	Steam Generator No. 2 Pressure
8	Steam Generator No. 2 Level
9	CVCS Charging Flow ⁽¹⁾
10	CVCS Charging Pressure ⁽¹⁾
11	Boric Acid Storage Tank Level ⁽¹⁾
12	In-containment Refueling Water Storage Tank (IRWST) Level
13	AFW Motor-Driven Pump 1 Discharge Pressure
14	AFW Motor-Driven Pump 2 Discharge Pressure
15	AFW Turbine-Driven Pump 1 Discharge Pressure
16	AFW Turbine-Driven Pump 2 Discharge Pressure
17	AFW Motor-Driven Pump 1 Suction Pressure and Low Pressure Alarm
18	AFW Motor-Driven Pump 2 Suction Pressure and Low Pressure Alarm
19	AFW Turbine-Driven Pump 1 Suction Pressure and Low Pressure Alarm
20	AFW Turbine-Driven Pump 2 Suction Pressure and Low Pressure Alarm
21	AFW Turbine-Driven Pump Turbine 1 Inlet Pressure
22	AFW Turbine-Driven Pump Turbine 2 Inlet Pressure
23	AFW Motor-Driven Pump 1 Flow
24	AFW Motor-Driven Pump 2 Flow
25	AFW Turbine-Driven Pump 1 Flow
26	AFW Turbine-Driven Pump 2 Flow

APR1400 DCD TIER 2

Table 7.4-1 (2 of 4)

No.	Function
27	AFW Motor-Driven Pump 1 Recirculation Flow
28	AFW Motor-Driven Pump 2 Recirculation Flow
29	AFW Turbine-Driven Pump 1 Recirculation Flow
30	AFW Turbine-Driven Pump 2 Recirculation Flow
31	AFW Storage Tank 1 Level and Low Alarm
32	AFW Storage Tank 2 Level and Low Alarm
33	AFW Steam-Driven Pump 1 Turbine Speed
34	AFW Steam-Driven Pump 2 Turbine Speed
35	AFW Turbine Trip and Throttle (Stop) Valves 1 & 2 Open Position and Close Position Alarm
36	SIS Pump Discharge Pressure P-308, P-309
37	SIT Wide Range Pressure P-311D, P-321B, P-331C, P-341A
38	Shutdown Cooling Inlet/Outlet Temperature (Loop1) T-300A, T-301A
39	Shutdown Cooling Inlet/Outlet Temperature (Loop2) T-303B, T-304B
40	Shutdown Cooling Pump Flow F-302A, F-305B
41	Safety Injection Pump Flow F-321B, F-341A
Balance of Plant Instrumentation	
42	Essential Component Coolant Pump and Service Water Pump Status Indication ⁽²⁾
43	Emergency Diesel Generator Status Indication
Nuclear Steam Supply System Control ⁽³⁾	
44	Reactor Coolant Pump Trip Pushbuttons
45	Pressurizer Backup Heater Groups 1 and 2 Controls
46	Atmospheric Steam Dump Valve and Atmospheric Dump Block Valves
47	Pressurizer Auxiliary Spray Valve ⁽⁴⁾
48	Pressurizer RCGV Valves RC-410, RC-411, RC-412, RC-413
49	Charging Pump ⁽⁴⁾
50	Letdown Isolation Valve ⁽⁴⁾
51	Reactor Coolant Pump Seal Bleed off Valve
52	MSIS Actuation Switches

APR1400 DCD TIER 2

Table 7.4-1 (3 of 4)

No.	Function
53	Manual Reactor Trip Switches
54	AFW Motor Driven Pump 1
55	AFW Motor Driven Pump 2
56	AFW Turbine Driven Pump 1
57	AFW Turbine Driven Pump 2
58	AFW Steam Generator Isolation Valves AF-100, AF-101, AF-102, AF-103
59	AFW Flow Control Valves AF-104, AF-105, AF-106, AF-107
60	AFW Steam Supply Bypass Valves AF-112, AF-113
61	AFW Steam Supply Isolation Valves AF-108, AF-109
62	AFW Turbine Trip and Throttle (Stop) Valves 1 & 2 Trip/Reset
63	AFW Turbine 1 & 2 Speed
64	Shutdown Cooling System Warmup Line Isolation Valve SI-690, SI-691
65	Shutdown Cooling System Suction Line Isolation Valve SI-651, SI-652, SI-653, SI-654, SI-655, SI-656
66	In-Containment Refueling Water Storage Tank (IRWST) Isolation Valve SI-304, SI-305
67	Shutdown Cooling System Test Return Line Isolation Valve (Throttle) SI-314, SI-315
68	Shutdown Cooling System Test Return Line Isolation Valve SI-688, SI-693
69	Containment Spray Pump/Shutdown Cooling Pump Suction Cross-Connection Valve SI-340, SI-342
70	IRWST Return Line Isolation Valve SI-300, SI-301
71	Shutdown Cooling Heat Exchanger Bypass Flow Control Valve SI-312, SI-313
72	Shutdown Cooling Heat Exchanger Isolation and Throttle Valve SI-310, SI-311
73	Safety Injection Low-Flow Control Bypass Valve SI-602, SI-603
74	Safety Injection Tank Atmospheric Vent Valve SI-605, SI-606, SI-607, SI-608, SI-613, SI-623, SI-633, SI-643
75	Safety Injection Tank Isolation Valve SI-614, SI-624, SI-634, SI-644
76	Shutdown Cooling System Direct Injection Isolation Valve SI-600, SI-601
77	Safety Injection Line Isolation Valve SI-626, SI-646

APR1400 DCD TIER 2

Table 7.4-1 (4 of 4)

No.	Function
78	Safety Injection Pump/Shutdown Cooling Pump Suction Cross-Connection Valve SI-344, SI-346
79	Safety Injection Pump SIP #1, SIP #2
80	Shutdown Cooling Pump SCP #1, SCP#2
81	Essential Component Coolant Pump and Service Water Pump Status Indication ⁽²⁾

- (1) These are not required to achieve or maintain hot standby, but are provided for operation status information as a convenience feature.
- (2) Ultimate heat sink indication and controls include a set required to support the operation of RSC components needed for hot standby.
- (3) Status indication for essential equipment (e.g., valve position, pump on/off status) is provided on the RSC.
- (4) These are not required to achieve or maintain Hot Standby, but are provided for operation status information as a convenience feature.

APR1400 DCD TIER 2

Table 7.4-2

Remote Shutdown Controlled Functions for Cold Shutdown

Instrumentation	
No.	Function
1	Pressurizer Pressure Variable Setpoints
2	Steam Generator Pressure Variable Setpoints
3	Shutdown Cooling System Suction Line Isolation Valve Interlock Status
4	Safety Injection Tank (SIT) Pressure
5	SCS Pump Flow
6	SCS Heat Exchanger/Bypass Inlet and Outlet Temperatures
Controls	
7	Steam Generator Pressure Setpoint Reset
8	Pressurizer Low-Pressure Setpoint Reset and Operating Bypass
9	SI Pumps
10	SIT Vent Valves
11	SIT Isolation Valves
12	Shutdown Cooling Header Valves
13	Shutdown Cooling Heat Exchanger Flow Control Valves
14	Shutdown Cooling Warm-up Bypass Valves
15	Shutdown Cooling Suction Line Valves
16	Shutdown Cooling Heat Exchanger Bypass Flow Control Valves

APR1400 DCD TIER 2

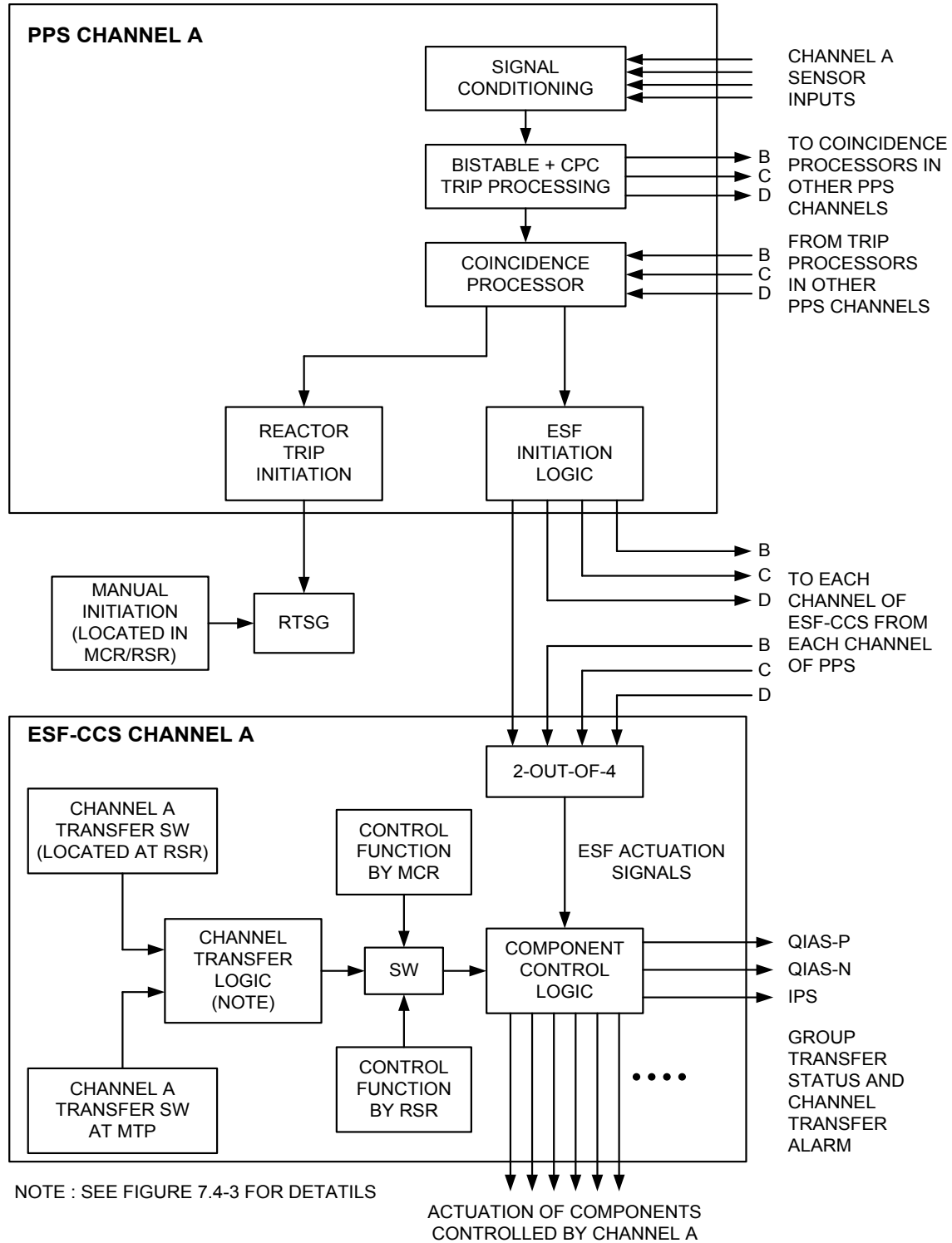


Figure 7.4-1 Interface Diagram for Division A Transfer Switches

APR1400 DCD TIER 2

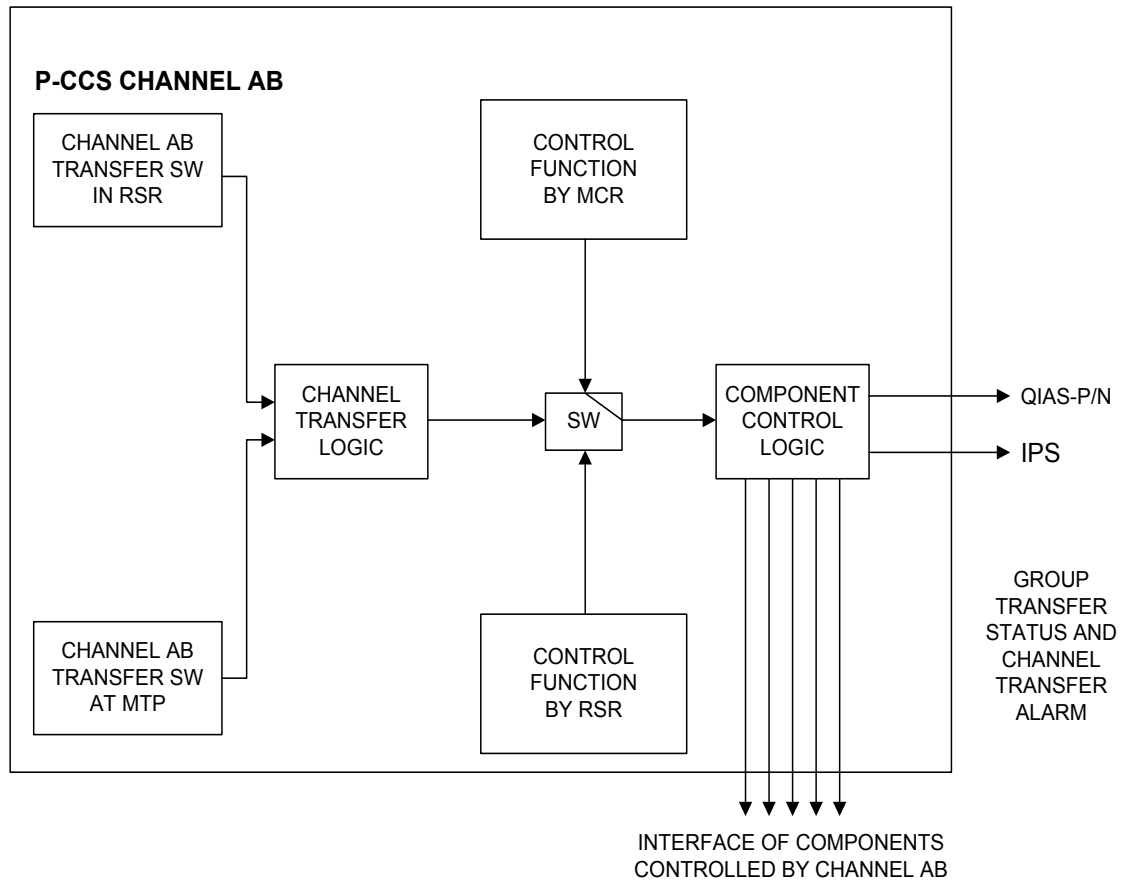


Figure 7.4-2 Interface Diagram for Division AB Transfer Switches

APR1400 DCD TIER 2

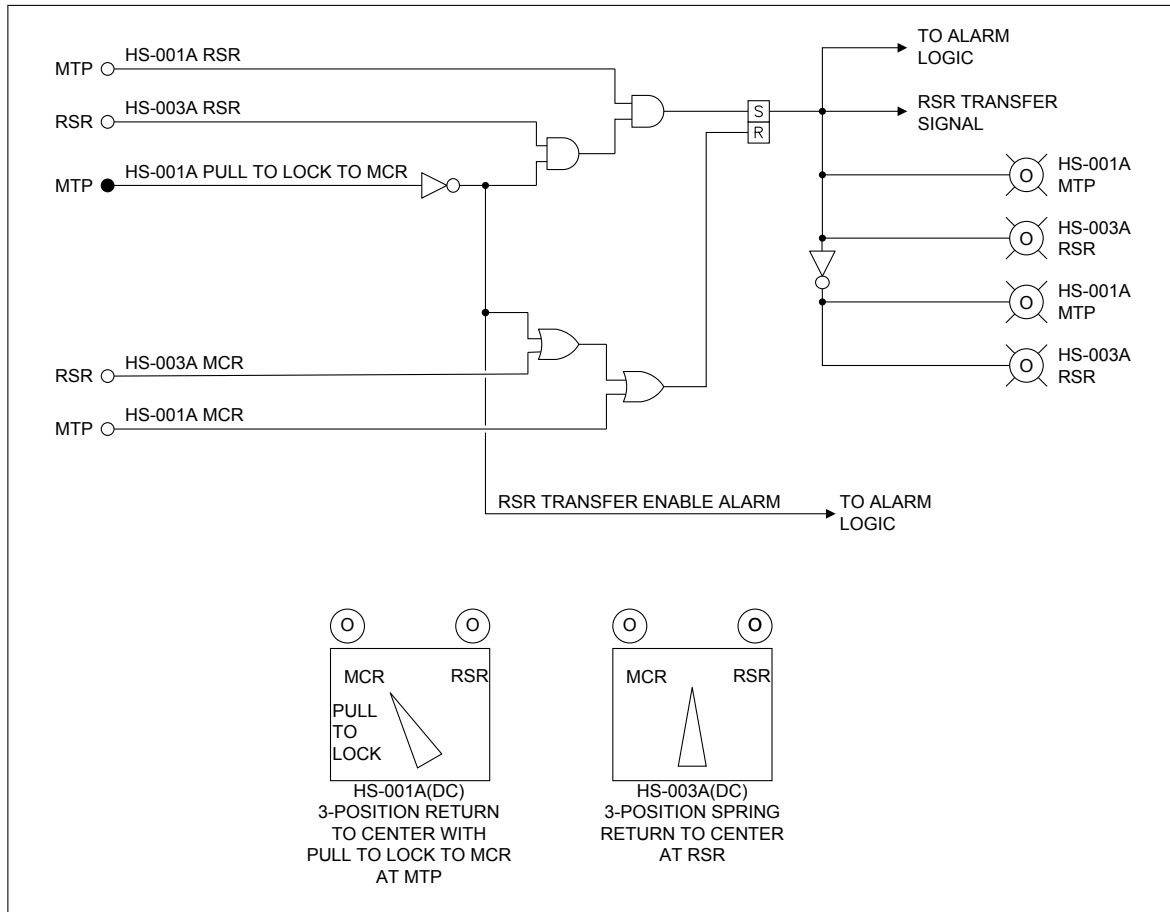


Figure 7.4-3 Channel Transfer Logic

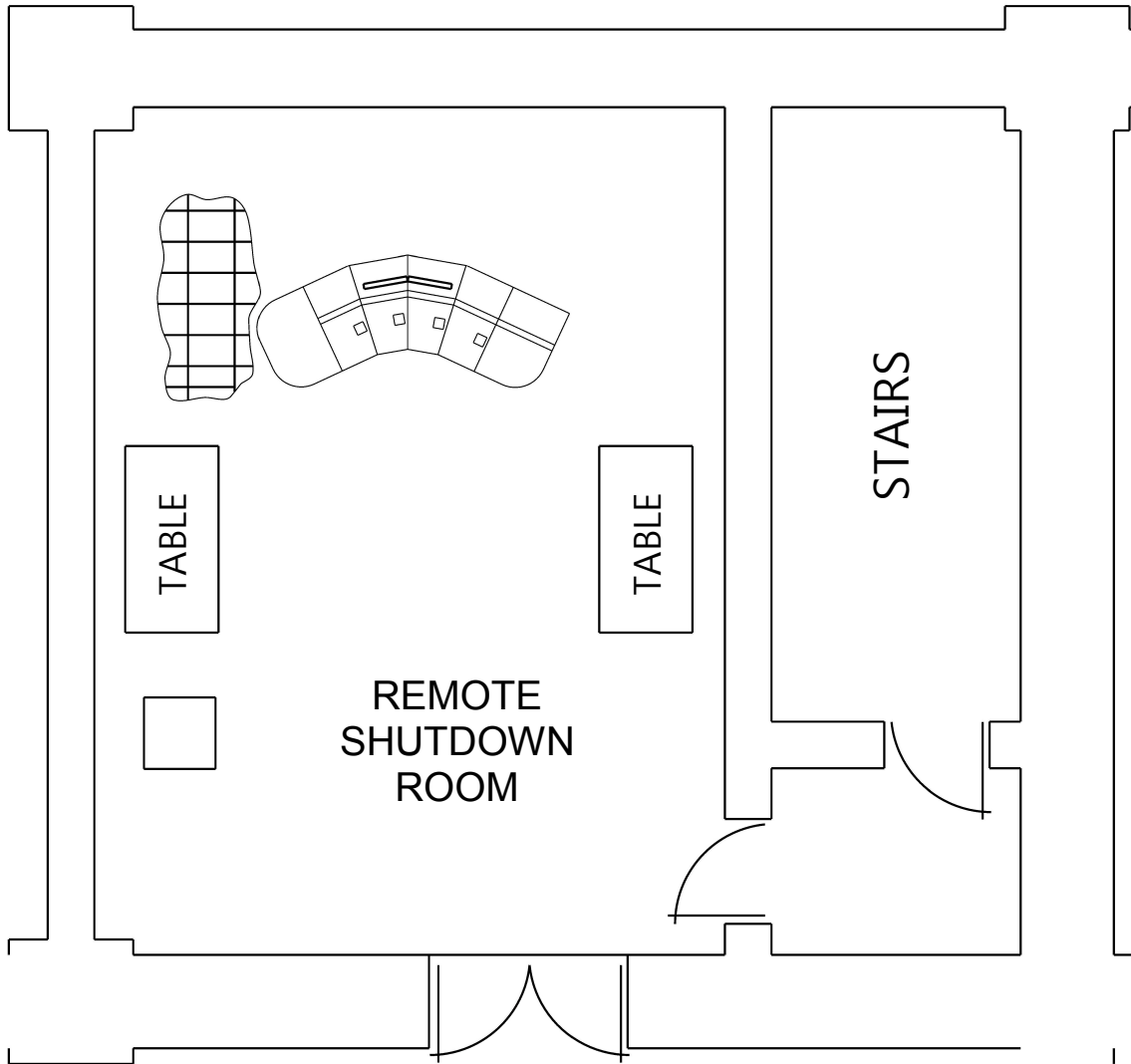


Figure 7.4-4 Layout of Remote Shutdown Room

APR1400 DCD TIER 2

7.5 Information Systems Important to Safety

7.5.1 System Description

This section describes instrumentation and control (I&C) systems that provide information to the plant operators for: (1) assessing plant conditions and safety system performance, (2) making decisions related to plant responses to abnormal events, and (3) taking preplanned manual operator actions related to accident mitigation. Information systems important to safety also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of anticipated operating occurrences (AOOs) and postulated accidents (PAs).

This section describes the following information systems important to safety:

- a. Accident monitoring instrumentation (AMI)
- b. Inadequate core cooling (ICC) monitoring instrumentations
- c. Bypassed and inoperable status indication (BISI)
- d. Alarm system
- e. Safety parameter display system (SPDS)
- f. Information systems associated with the emergency response facilities (ERF) and emergency response data system (ERDS)

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

- a. Main control room (MCR)
- b. Remote shutdown room (RSR)
- c. Technical support center (TSC)
- d. Emergency operation facility (EOF)

APR1400 DCD TIER 2

7.5.1.1 Accident Monitoring Instrumentation

AMI listed in Table 7.5-1 is provided to allow the operator to assess the state of the plant following design basis events by monitoring instruments, equipment, or systems that provide automatic action.

The AMI is designed to accommodate NRC Regulatory Guide (RG) 1.97 (Reference 1) as depicted in Figure 7.5-1 as follows:

- a. The qualified indication and alarm system - P (QIAS-P) is dedicated to continuously monitor and display NRC RG 1.97 Type A, B, and C variables. These displays are located on the MCR safety console.
- b. The qualified indication and alarm system - non-safety (QIAS-N) is designed to support continuous plant operation if the information processing system (IPS) becomes unavailable. The function of the QIAS-N also includes displaying NRC RG 1.97 Type A, B, C, and selected sets of Type D and E variables. These displays are located on the MCR safety console and remote shutdown console.
- c. The IPS provides displays for all NRC RG 1.97 variables. The IPS also has a historical data storage, retrieval, and trending capability.

The COL applicant is to provide a description of the site-specific AMI variables such as wind speed, and atmosphere stability temperature difference (COL 7.5(1)).

Qualified Indication and Alarm System – P

The QIAS-P provides the continuous display of NRC RG 1.97 Type A, B and C variables. The QIAS-P fulfills the requirements in NUREG-0737 Item II.F.2(Reference 2) and NRC RG 1.97. To address these requirements, the ICC monitoring and display of the QIAS-P performs following functions:

- a. Core exit thermocouple (CET) temperature signal processing and display
- b. Primary coolant saturation margin calculation and display
- c. Heated junction thermocouple (HJTC) signal processing, display, and HJTC heater power control

APR1400 DCD TIER 2

The QIAS-P also provides an unambiguous indication and advanced warning of the approach to recovery from inadequate core cooling.

The QIAS-P has channelized cabinets for channel A and B. The QIAS-P cabinets for each channel are geographically distributed into channelized I&C equipment rooms to meet the requirements of IEEE Std. 603(Reference 3).

The QIAS-P receives Type A, B, and C variables from the plant protection system (PPS), engineered safety features - component control system (ESF-CCS) via a serial data link (SDL) and auxiliary process cabinet - safety (APC-S) and process instrumentation via a hard-wired connection.

The QIAS-P processes the Type A, B, and C variables for accident monitoring.

The QIAS-P calculates a representative CET temperature from the CETs.

The QIAS-P calculates reactor coolant saturation margins based on the CET temperatures, the hot and cold leg temperatures, the HJTC temperature measurements from the reactor vessel head region and pressurizer pressure.

The QIAS-P also calculates the reactor vessel water level based on the HJTC signals.

The QIAS-P in each channel (A or B) drives one display, which is mounted on a safety console located in the MCR.

The QIAS-P displays Type A, B, and C variables, and provides backup displays for the ICC variables. Type A variables are displayed as conventional indicators on the safety console. The primary displays for ICC variables are implemented in the safety parameter display and evaluation system + (SPADES+) within the IPS.

The QIAS-P display provides to the operator following information:

- a. Type A, B, and C variables
- b. ICC variables

The QIAS-P controls the power for HJTC heaters. The heater power control devices are located in the QIAS-P cabinet. Heater control for the HJTC is manually switched from the

APR1400 DCD TIER 2

QIAS-P channel A only to the diverse indication system (DIS) via DIS switch on safety console.

The QIAS-P generates status information for all input parameters received by hard-wired connection from sensors or from the APC-S and alarms that are the result of the QIAS-P calculations. The QIAS-P transmits the alarms to the IPS and QIAS-N for alarm processing.

Qualified Indication and Alarm System – Non-safety

The QIAS-N monitors the safety parameters and key operating parameters to be used by the operators during both normal operation and accidents. The QIAS-N is designed to provide displays and audible and visual alarms that use signal validation, automatic ranging, alarm filtering, alarm prioritization, and other features.

The QIAS-N consists of the following equipment:

- a. QIAS-N redundant servers
- b. QIAS-N flat panel displays (FPDs)
- c. Mini-large display panel (LDP)
- d. Shutdown overview display panel (SODP)

The QIAS-N receives analog and digital signals from both safety and non-safety systems, analyzes the data, and presents the information to the operator via the FPDs and the mini-LDPs located in the safety console, and the SODP in the RSR. The system interfaces with the IPS to integrate alarm and process status information.

Each QIAS-N server uses redundant networks and processors such that the fail-over to the backup processor is accomplished without interrupting the information being displayed, as shown in Figure 7.5-2. The isolation devices are used to provide the isolation between the redundant safety systems and the QIAS-N.

The QIAS-N is designed to be physically separated from the QIAS-P and is physically separated and electrically isolated from the IPS so that a single failure of QIAS-N does not cause a loss of more than one of the three display methods (QIAS-P, QIAS-N, or IPS).

APR1400 DCD TIER 2

The QIAS-N is seismically qualified for physical and functional integrity to enhance information availability.

Information Processing System (IPS)

The IPS displays all NRC RG 1.97 variables of AMI on the information FPD of the consoles in the MCR and RSR and provides permanent historical recordings of AMI variables. All information displayed and recorded within the IPS is provided and available upon the operator's demand. Operators are able to use the AMI indications on the information FPDs and the LDP without referencing the QIAS-P and QIAS-N displays at the safety console. The IPS also includes a historical data storage, retrieval, and trending capability. The IPS design includes data links to the on-site TSC and to the EOF to provide the capability for monitoring plant conditions at these locations. The IPS is described in Subsection 7.7.1.4.

7.5.1.2 Inadequate Core Cooling Monitoring Instrumentation

The ICC monitoring instrumentations are designed in accordance with NUREG-0737, Item II.F.2.

The signals from the resistance temperature detectors (RTDs), unheated thermocouples in the HJTC system, CET temperature, and pressure sensors are used to calculate the loss of subcooling, occurrence of saturation, and achievement of a subcooled condition following core recovery.

The reactor vessel level monitors provide information to the operator on the decreasing liquid inventory in the reactor vessel (RV) regions above the fuel alignment plate (FAP), as well as the increasing RV liquid inventory above the FAP following core recovery from the ICC.

The CETs monitor the increasing RCS temperatures associated with the ICC and the decreasing RCS temperature associated with recovery from the ICC.

SPADES+ is designed to meet the criteria for SPDS set forth in NUREG-0696 (Reference 4) and NUREG-0737, Supplement 1 (Reference 5). The SPADES+ displays ICC variables as a primary display. The QIAS-P provides a backup display of the ICC variables as a backup.

a. Primary ICC displays

APR1400 DCD TIER 2

The ICC variables are incorporated into the SPADES+ and alarm logic of the IPS. The SPADES+ is a computer applications program of the IPS, and provides a primary display of ICC information.

The critical safety functions are monitored by a set of algorithms that process the measured plant variables to determine the plant safety status relative to safety function control. If any of the critical functions are violated (by exceeding logic setpoints), a critical function alarm is initiated. The calculated ICC outputs are incorporated into the core heat removal critical function alarm logic.

The SPADES+ of the IPS has an ICC summary page as part of the core heat removal control critical function, and more detailed display pages for each of the ICC variables.

The summary page includes the following information:

- 1) RCS/upper head saturation margin – the lower value of either the RCS saturation margin or upper head saturation margin
- 2) Reactor vessel level above the core
- 3) Representative core exit temperature

b. Backup ICC displays

The QIAS-P provides Class 1E backup displays for ICC variables, and is seismically and environmentally qualified. The displays of ICC variables are dedicated and integrated ICC variables in accordance with the Style Guide (Reference 6).

The QIAS-P displays are designed as follows:

- 1) To provide display for ICC variables
- 2) To give indications in the event that the primary display becomes inoperable
- 3) To provide confirmatory indication to the primary display

The following information is available on the QIAS-P display pages:

APR1400 DCD TIER 2

- 1) RCS/Upper head saturation margin
- 2) Reactor vessel level above the core
- 3) Representative core exit temperature

7.5.1.3 Bypassed and Inoperable Status Indication

System level automatic bypass indication is provided based on the guidance of NRC RG 1.47 (Reference 7). Compliance for NRC RG 1.47 is described as follows.

- a. Flags are provided to indicate, at the system level, the bypass or deliberate inoperability of a protection system. The system-level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.
- b. The auxiliary and support systems provide automatic flag activation to indicate, on a system level, the bypassed or deliberately induced inoperability of an auxiliary or support system that effectively bypasses or renders a protection system inoperable and the systems actuated or controlled by a protection system.
- c. Flags are provided in the control room, at the system level, for each bypassed or deliberately induced inoperable status in a protection system.
- d. The operator is able to activate each system-level bypass indicator manually in the control room.

Bypasses and inoperable status conditions are classified into the following groups:

- a. Operating bypasses
- b. Trip channel bypasses
- c. ESF components inoperable

There are no system-level bypasses for the RPS or ESFAS.

APR1400 DCD TIER 2

Operating Bypasses

Operating bypasses are provided to permit orderly startup and shutdown of the plant and to allow low power testing. The operating bypass for the RPS is described in Subsection 7.2.1.6, and the operating bypass for ESFAS is described in Subsection 7.3.1.5.

Operating bypasses include the RPS/ESFAS pressurizer pressure bypass, the high log power bypass, and the core protection calculator (CPC) DNBR/LPD trip bypass.

Trip Channel Bypasses

Trip channel bypasses are used to individually bypass channel trip inputs to the protection system logic for maintenance or testing. The trip logic is converted from a 2-out-of-4 to a 2-out-of-3 logic for the parameters being bypassed, while maintaining a coincidence of two for actuation. The trip channel bypass for the RPS is described in Subsection 7.2.1.6, and the trip channel bypass for ESFAS is described in Subsection 7.3.1.5.

Bypassed or Inoperable Condition Important to Plant Safety

The bypassed or inoperable condition of ESF components is communicated to the IPS, which indicates a system-level bypassed or inoperable condition. The IPS also provides status information at the component level. The operator has the ability to manually activate each RPS and ESF system-level bypass indication in the MCR. Inoperable indication is shown on the IPS displays and LDP.

The system-level alarms are actuated when a component actuated by a protection system is bypassed or deliberately rendered inoperable.

The system-level status indication of BISI is provided for the protection systems and auxiliary or supporting systems, which are required for safe operation of the plant and are listed as follows:

- a. Safety injection system
- b. Shutdown cooling system
- c. Chemical and volume control system

APR1400 DCD TIER 2

- d. Containment spray system
- e. Containment isolation system
- f. Essential service water system
- g. Essential chilled water system
- h. Auxiliary feedwater system
- i. Component cooling water system
- j. Auxiliary power system
- k. Emergency diesel generator system
- l. Emergency diesel generator area HVAC system
- m. Control room HVAC system
- n. Electrical and I&C equipment areas HVAC system
- o. Fuel handling area HVAC system
- p. Auxiliary building controlled area HVAC system
- q. Reactor containment building purge system

7.5.1.4 Alarm System

The alarm system alerts the operators by means of visual and audible signals of abnormal conditions that require operator action.

The alarm system is designed to perform the following functions:

- a. Alerting the operators to off-normal conditions that require the operator to take action
- b. Guiding the operators to the appropriate response

APR1400 DCD TIER 2

- c. Assisting the operators in determining and maintaining an awareness of the state of the plant and its systems or functions

Reliability

The alarm system is reliable based on following features:

- The alarm system is implemented in both the IPS and QIAS-N. Alarms that are used for all operating modes including normal, AOOs, and PAs, are provided in redundant operator workstation consoles by the IPS. The IPS has redundant alarm servers. An important alarm list is shown on the QIAS-N displays on the safety console.
- The IPS is configured by diverse hardware and software from the QIAS-N.
- The IPS performs online diagnostics for continuous self-health monitoring. The QIAS-N also includes automatic online diagnostics.
- The QIAS-N hardware is seismically and environmentally qualified. The QIAS-N is implemented as important-to-availability software.

Use of Digital Systems

All alarm functions are implemented by digital systems.

Independence

The IPS is isolated from the QIAS-N by qualified isolation devices. The QIAS-N is powered from Class 1E, and the IPS is powered from non-Class 1E. The communication independence between the IPS and the QIAS-N is described in Section 7.9.

7.5.1.5 Safety Parameter Display System

The SPADES+ provides the information for monitoring the critical safety parameters. Descriptions of SPADES+ are provided in Subsection 7.7.1.4.

7.5.1.6 Information Systems Associated with the ERF and ERDS

The emergency response facility (ERF) includes the control room, technical support center (TSC), operational support center (OSC), and near-site emergency operations facility (EOF). In addition, the ERF includes the SPDS and emergency response data system (ERDS). Information systems associated with the ERF provide important safety information to support emergency response decision making. The ERDS transmits reactor process variables and radiological data as well as site meteorological data of the plant to the NRC in accordance with NUREG-0696.

The TSC, OSC, EOF, and ERDS, which are associated with emergency planning, are described in Section 13.3.

The COL applicant is to provide a description of site-specific EOF (COL 7.5(2)).

7.5.2 Design Basis Information

7.5.2.1 Accident Monitoring Instrumentation

The AMI design complies with NRC RG 1.97, which endorses IEEE Std. 497 (Reference 8). IEEE Std. 497 is used to select and categorize AMI variables and establish design and performance requirements.

a. Design criteria

Single failure

The QIAS-P consists of two channels that are electrically and physically isolated from each other so AMI information is still displayed if any single failure within the system occurs. The QIAS-P is also independent and separate from the QIAS-N and IPS. The QIAS-N is classified as a non-safety system and a single failure criterion is not applied.

Common cause failure

To avoid complete AMI information loss caused by common cause failure, the QIAS-P and the QIAS-N are implemented using a PLC-based platform while the IPS is implemented using a distributed control system (DCS) based platform.

APR1400 DCD TIER 2

Independence and separation

Redundant AMI channels for the QIAS-P are electrically independent of and physically separated from each other. The QIAS-N is classified as a non-safety system and independence and separation criteria are not applied.

Isolation

The QIAS-P is isolated from the QIAS-N and the IPS. Isolation device meets the requirements of IEEE Std. 384 (Reference 9).

Information ambiguity

To resolve the information ambiguity, additional variables are provided as listed in Table 7.5-1

Power supply

The QIAS-P is powered from Class 1E, battery and emergency diesel generator (EDG) backed, vital instrument power bus A and B. The QIAS-N is classified as non-safety system, but is powered from Class 1E, battery and EDG backed, vital instrument power bus D. The IPS is powered from non-Class 1E, battery backed, vital instrument power.

Calibration, testability, and access control

Calibration and testing are performed after the related systems are offline.

Redundant design features provide reasonable assurance of the continuous display of AMI variables during calibration or test. Periodic tests are performed in accordance with NRC RG 1.118 (Reference 10). Access to any sensor or module for calibration or testing is administratively controlled.

The display systems are designed to allow control of access to constants, alarm setpoints, calibration, and test points. Isolation devices are located outside the containment so the devices can be accessed for maintenance during accident conditions.

Direct measurement

APR1400 DCD TIER 2

The QIAS-P provides direct measurement of desired variables.

b. Qualification criteria

The QIAS-P and QIAS-N are seismically and environmentally qualified.

c. Display and recording

Type A and B variables are continuously displayed on the dedicated QIAS-P. Type C variables are displayed upon demand on the QIAS-P. Type A variables are displayed on conventional indicators on the MCR safety console. Type A, B, C, and selected Type D and E variables are also displayed on the QIAS-N. Type A, B, C, D, and E variables are displayed on the IPS.

Recording is provided for at least one channel of Type A, B, and C variables. Recording on the IPS is also provided for Type E variables. Recording on the IPS is provided for at least 30 minutes pre-event and 12 hours post-event.

d. Display identification

Type A, B, and C variables have a salient designation to indicate that they are intended for use under accident conditions.

e. Performance Criteria

Range

The range of AMI described in Table 7.5-1 is established to provide reasonable assurance that it covers AOOs and PAs. Separate, narrow-range instrumentation is provided where the required range of monitoring instrumentation results in a loss of sensitivity during normal operating conditions.

The QIAS-P, QIAS-N, and IPS also allow access to individual channels for each range.

The IPS and the QIAS-N attempt to validate data using narrow range sensors. If successful, narrow range scale and demarcation are displayed. If the parameter is out of the narrow range, wide range sensors are used for the display with wide range scale and demarcation.

APR1400 DCD TIER 2

Accuracy

The required accuracy of AMI is established based on the assigned function.

Response Time

AMI is designed to provide real time and timely information. AMI signals are transmitted from sensors to QIAS-P, QIAS-N, and IPS. The response time between detection and indication is approximately one to three seconds. The update frequency is less than one second.

Required Instrumentation Duration

The post event operating time for each variable is defined as follows:

- The post event operating time for Type A, D, and E variables is the duration required by licensing basis documentation (LBD).
- The post event operating time for Type B variables is the duration associate with the longest-duration design event.
- The post-event operating time for Type C variables is 100 days for instrument channels monitoring the fission product barriers.

7.5.2.2 Inadequate Core Cooling Monitoring

The ICC monitoring is designed in accordance with 10 CFR 50.34(f)(2)(xviii) (Reference 11) and NUREG-0737, Item II.F.2.

7.5.2.3 Bypassed and Inoperable Status Indication

The BISI is designed in accordance with 10 CFR 50.34(f)(2)(v) (Reference 12) and NRC RG 1.47.

7.5.2.4 Alarm System

The alarm system is designed in accordance with the Staff Requirements Memorandum (SRM) SECY-93-087, Item II.T (Reference 13).

APR1400 DCD TIER 2

7.5.2.5 Safety Parameter Display System

The SPDS is designed in accordance with 10 CFR 50.34 (f)(2)(iv) (Reference 14), regarding the SPDS console, and NUREG-0737 Supplement 1.

7.5.2.6 Information Systems Associated with the ERF and ERDS

The ERF is designed to include EOF that provides sufficient information near site in accordance with 10 CFR 50.34 (f)(2)(xxv) (Reference 15).

7.5.3 Analysis

Compliance to IEEE Std. 603 and IEEE Std. 7-4.3.2 (Reference 16) is described in the Safety I&C System Technical Report (Reference 17).

The safety analysis shows that the APR1400 remains safe although required manual safety functions are delayed 30 minutes after a PAs occurs. Manual safety functions mitigate accident conditions as defined in the safety analysis. Manual safety functions are credited to maintaining the plant in a safe condition in post-accident conditions. The QIAS-P, QIAS-N, and IPS provide the operator with plant status information during AOOs, PAs, and post-accident conditions.

During and after plant accident conditions the QIAS-N and QIAS-P provide all information required for achieving plant safe shutdown and performing emergency operating procedure (EOP) even though the IPS is unavailable.

To satisfy this design feature, the QIAS-N and QIAS-P are seismically and environmentally qualified.

7.5.4 Combined License Information

COL 7.5(1) The COL applicant is to provide a description of the site-specific AMI variables such as wind speed, and atmosphere stability temperature difference.

COL 7.5(2) The COL applicant is to provide a description of the site-specific EOF.

APR1400 DCD TIER 2

7.5.5 References

1. NRC RG 1.97, Rev. 4, "Criteria for accident monitoring instrumentation for nuclear power plants."
2. NUREG-0737, Item II.F.2, U.S. Nuclear Regulatory Commission, "Clarification of TMI Action Plan Requirements."
3. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
4. NUREG-0696, "Functional Criteria for Emergency Response Facilities," 1981.
5. NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements" 1983.
6. APR1400-E-J-T(NR)-12005-P, "Style Guide," September 2013.
7. NRC RG 1.47, Rev. 1, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," 2010
8. IEEE Std. 497-2002, "Accident monitoring instrumentation for nuclear power generating stations."
9. IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits."
10. NRC RG 1.118, Rev. 3, "Periodic Testing of Electric Power and Protection Systems."
11. 10 CFR 50.34(f)(2)(xviii), "Instrumentation for Detection of Inadequate Core Cooling," [II.F.2].
12. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3].
13. SRM on SECY-93-087, Item II.T, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advance Light-Water Reactor (ALWR) Designs."
14. 10 CFR 50.34(f)(2)(iv), "Safety Parameter Display Console," [I.D.2].
15. 10 CFR 50.34 (f)(2)(xxv),"Additional TMI-related Requirements," [III.A.1.2].

APR1400 DCD TIER 2

16. IEEE Std. 7-4.3.2-2003, “IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”
17. APR1400-Z-J-EC-13001-P, “Safety I&C System Technical Report,” September 2013.

APR1400 DCD TIER 2

Table 7.5-1 (1 of 5)

Accident Monitoring Instrumentation Variables

Variable	Range	Monitored Function or System	Channel Number	Type	Ambiguity (Channel)
Pressurizer Pressure (Wide Range)	0 to 210.9 kg/cm ² a (0 to 3000 psia)	Pressurizer	2	A, B	C,D (PPS OM)
Pressurizer Level	0 to 100 % (0 to 562.15 in)	Pressurizer	2	A, B	C,D (PPS OM)
Reactor Coolant Hot Leg Temperature (Wide Range)	0 to 400°C (32 to 752 °F)	RCS	4	A, B	2 Hot Leg signals per Channel (QIAS-P)
Reactor Coolant Cold Leg Temperature (Wide Range)	0 to 400°C (32 to 752 °F)	RCS	4	A, B	2 Cold Leg signals per Channel (QIAS-P)
Steam Generator Pressure	0 to 105 kg/cm ² A (0 to 1494 psia)	Steam Generator	2/SG	A, B	C,D (PPS OM)
Steam Generator Level (Wide Range)	0 to 100 % (0 to 1117.6cm (0 to 440 in) tap span)	Steam Generator	2/SG	A, B	C,D (PPS OM)
Core Exit Temperature	0 to 1260 °C (32 to 2300 °F)	Inadequate Core Cooling	2	B, C	Validation (QIAS-P)
Degrees of Subcooling	RCS Temp Saturation Margin: -399 to 358.3 °C Upper Head (or CET) Temp Saturation Margin: -260 to 368.3 °C RCS (or Upper Head or CET) Press Saturation Margin: -225.5 to 210.9 kg/cm ²	Inadequate Core Cooling	2	B	C,D (PPS OM)
Reactor Vessel Coolant Level	0 to 100 %	RCS	2	B	Validation (QIAS-P)
RCS Pressure (Wide Range)	0 to 281.23 kg/cm ² (0 to 4000 psig)	RCS	2	B, C	C,D (PPS OM)
IRWST Level	0 to 100 %	IRWST	4	B	C,D (ESCM)

APR1400 DCD TIER 2

Table 7.5-1 (2 of 5)

Variable	Range	Monitored Function or System	Channel Number	Type	Ambiguity (Channel)
IRWST Temperature	10 to 177 °C (50 to 350 °F)	IRWST	4	B	C,D (ESCM)
Holdup Volume Tank Level	0 to 100 %	IRWST	5	B	C,D (ESCM)
Containment Level	0 to 100 %	Containment Monitoring System	2	B	C,D (ESCM)
Containment Pressure (Wide Range)	-400 to 5600 cmH ₂ O (-5.7 to 79.5 psig)	Maintaining Containment Integrity	2	B	C,D (PPS OM)
Reactor Cavity Level	0 to 100%	Maintaining Containment Integrity	4	B	C,D (ESCM)
Containment Isolation Valve Position	N/A	Maintaining Containment Integrity	1 pair/ valve	B, D	N/A
Logarithmic Reactor Power	1×10^{-6} to 2×10^{-8} 100 % power	Reactor Power	2	B	C,D (PPS OM)
Control Rod Position	0 to 381 cm (0 to 150 in)	Reactivity Control	1/rod	B	C,D (CPCS OM)
Containment Pressure (Extended Wide Range)	-500 to 14,500 cmH ₂ O (-7.1 to 206.2 psig)	Fission product release	2	C	PPS Containment pressure A,B,C,D (PPS OM)
Containment Operating Area Radiation	10^{-3} to 10^2 mSv/hr	Monitoring fueling handling accident	2	C	C,D (ESCM)
Spent Fuel Pool radiation	10^{-3} to 10^2 mSv/hr	Monitoring fueling handling accident	2	C	C,D (ESCM)
Containment Upper Operating Area Radiation	10 to 10^8 mSv/hr	Monitoring LOCA	2	C	C,D (ESCM)
Containment Area Radiation	3.7×10^{-5} to 3.7×10^1 Bq/cc (P, I) 3.7×10^{-2} to 3.7×10^5 Bq/cc (G)	RCS leak detection	2	C	C,D (ESCM)

APR1400 DCD TIER 2

Table 7.5-1 (3 of 5)

Variable	Range	Monitored Function or System	Channel Number	Type	Ambiguity (Channel)
POSRV Position	N/A	Verifying status of a safety system	1/valve	D	N/A
CS Flow	0 to 28,400 lpm (0 to 7,500 gpm)	Monitoring CS Operation	2	D	N/A
Containment Atmosphere Temperature	4.44 to 204.44 °C (40 to 400 °F)	Monitoring accomplishment of cooling	13	D	N/A
SI Hot Leg Injection Flow Rate	0 to 5678.12 lpm (0 to 1500 gpm)	Monitoring the operating status for a safety system	2	D	N/A
Wide Range Safety Injection Tank Level	0 to 100 % (402 inch full scale)	Monitoring the operating status for a safety system	4	D	N/A
Wide Range Safety Injection Tank Pressure	0 to 53kg/cm ² (0 to 750 psig)	Monitoring the operating status for a safety system	4	D	N/A
Emergency Ventilation Damper Position	N/A	Prevention of radiation effluent release	1 pair/ damper	D	N/A
DC Bus Voltage	0 to 150 Vdc	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
Emergency Diesel Generator Voltage	0 to 5,250 Vac	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
Emergency Diesel Generator Current	0 to 2000 Amps	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
4.16-kV Switchgear Voltage	0 to 5,250 Vac	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
4.16-kV Switchgear Current	0 to 2,000 Amps	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A

APR1400 DCD TIER 2

Table 7.5-1 (4 of 5)

Variable	Range	Monitored Function or System	Channel Number	Type	Ambiguity (Channel)
480-V L/C Voltage	0 to 600 Vac	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
480-V L/C Current	0 to 3,000 Amps	Electrical Power supplies for safety system and safe shutdown system	4	D	N/A
CCW Temperature	0 to 100 °C (32 to 212 °F)	Monitoring CCWS Operation	1/division	D	N/A
CCW Flow	0 to 110% design flow	Monitoring CCWS Operation	1/pump	D	N/A
ESW Temperature	0 to 50 °C (32 to 122 °F)	Monitoring ESW Operation	1/division	D	N/A
ESW Flow	0 to 120% design flow	Monitoring ESW Operation	1/pump	D	N/A
Charging Line Flow	0 to 749.43 lpm (0 to 198 gpm)	Monitoring the status of boric acid flow to RCS	1	D	N/A
Charging Line Pressure	0 to 220 kg/cm ² (0 to 3,129 psig)	Monitoring the status of boric acid flow to RCS	1	D	N/A
Shutdown Cooling Heat Exchange Outlet Temperature	0 to 200°C (40 to 392°F)	Monitor the operating status for a safety system	2	D	N/A
SC Pump Flow Rate	0 to 25,000 lpm (0 to 6604 gpm)	Monitor the operating status for a safety system	2	D	N/A
SIT Isolation Valve	N/A	Monitor the operating status for a safety system	4	D	N/A
SIP DVI Flow Rate	0 to 5678 lpm (0 to 1,500 gpm)	Monitor the operating status for a safety system	4	D	N/A
Backup Heater Status	N/A	Monitor the operating status for a safety system	N/A	D	N/A
RCP Motor Current	0 to 700 A	Verifying status of RCS flow and core cooling	4	D	N/A
Containment Purge Effluent	3.7×10^{-2} to 3.7×10^9 Bq/cc	Monitoring Gaseous Effluent in Containment Building	1	E	N/A
Auxiliary Building Controlled Area HVAC Effluent	3.7×10^{-2} to 3.7×10^7 Bq/cc	Monitoring Gaseous Effluent of controlled area in AUX. Building	2	E	N/A

APR1400 DCD TIER 2

Table 7.5-1 (5 of 5)

Variable	Range	Monitored Function or System	Channel Number	Type	Ambiguity (Channel)
Compound Building HVAC Effluent	3.7×10^{-2} to 3.7×10^3 Bq/cc	Monitoring Gaseous Effluent in Compound Building	1	E	N/A
Liquid Radwaste System Radiation	3.7×10^{-2} to 3.7×10^3 Bq/cc	Monitoring Liquid Radwaste System radiation	2	E	N/A
Condenser Vacuum Vent Effluent Radiation	3.7×10^{-2} to 3.7×10^3 Bq/cc	Monitoring SG tube leakage	1	E	N/A
MCR and TSC Area Radiation	10^{-3} to 10^2 mSv/hr	Monitoring Area Radiation level	1	E	N/A
Primary Sampling Room Area Radiation	10^{-3} to 10^2 mSv/hr	Monitoring Area Radiation level	1	E	N/A
Chemistry Lab. Area Radiation	10^{-3} to 10^2 mSv/hr	Monitoring Area Radiation level	1	E	N/A
Wind Direction	0 to 360°	Release Assessment	1	E	N/A
Wind Speed	0 to 50 mph	Release Assessment	1	E	N/A
Atmosphere Stability Temperature Difference	-22.78 to -7.78°C (-9 to +18°F) Delta-T	Release Assessment	2	E	N/A
Main Steam Line Radiation	10^{-3} to 10^2 mSv/hr	Monitoring leakage of Steam Generator	4	E	N/A

APR1400 DCD TIER 2

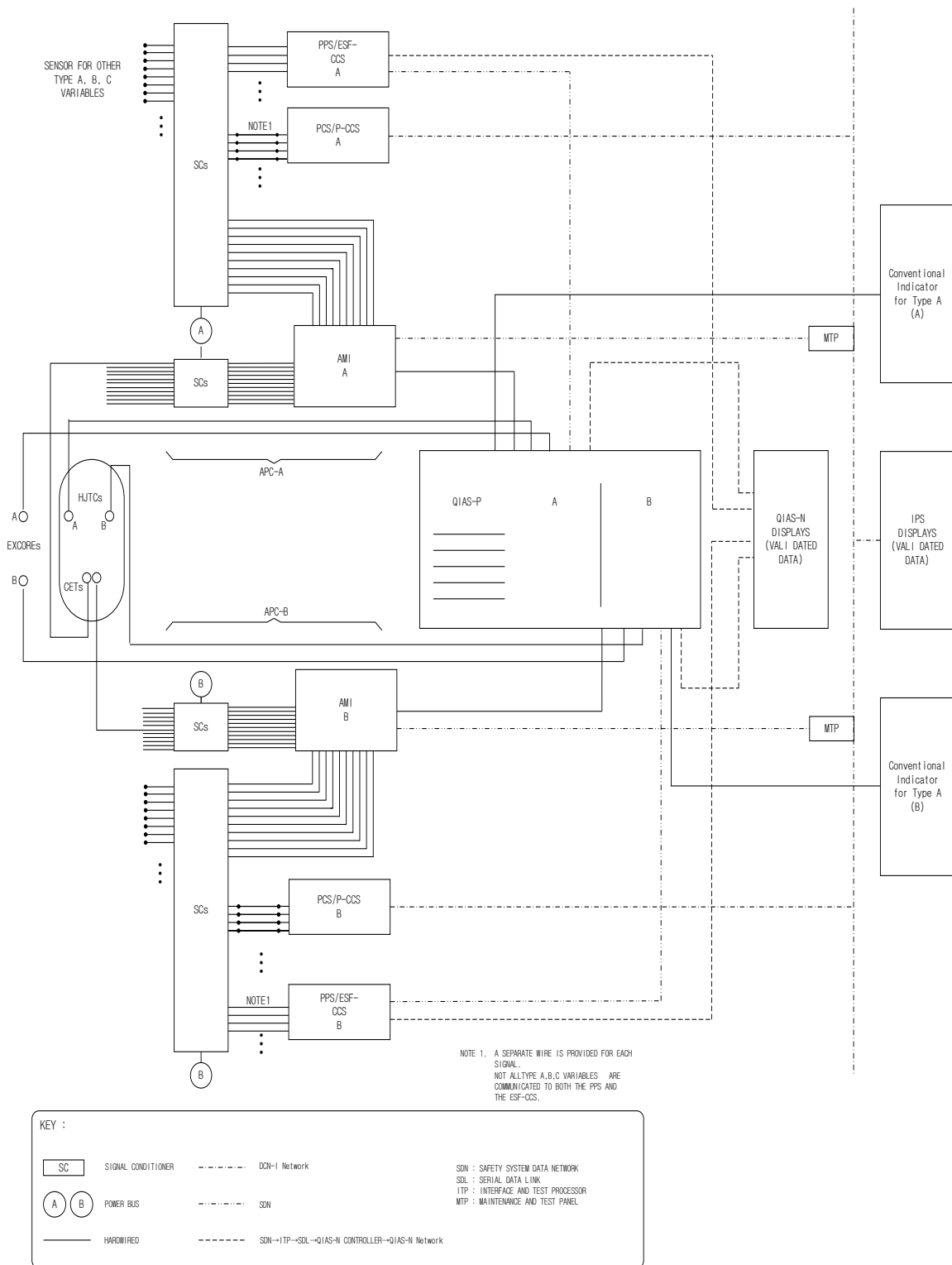


Figure 7.5-1 Diverse Display of Accident Monitoring Type A, B, and C Variables

APR1400 DCD TIER 2

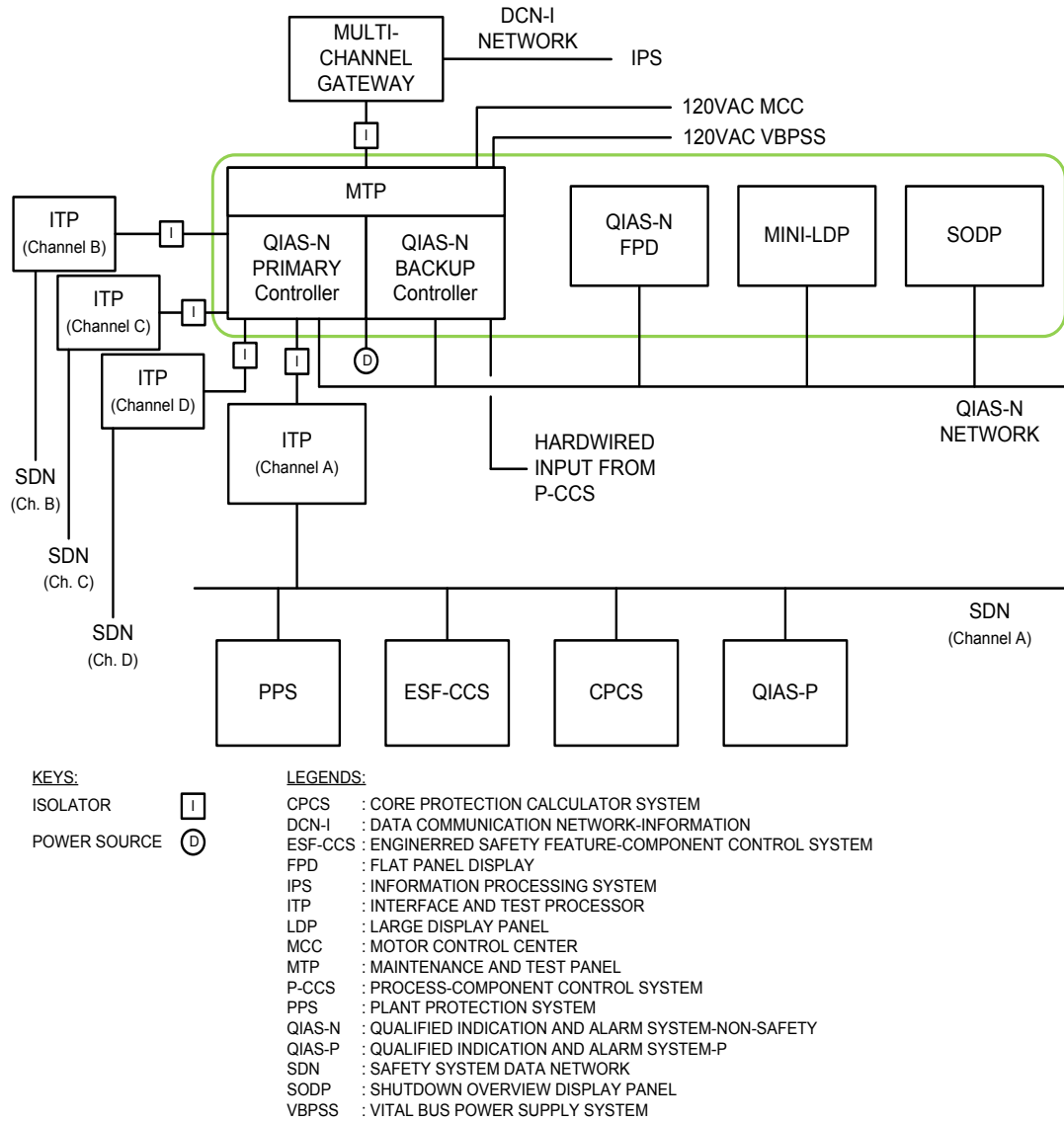


Figure 7.5-2 QIAS-N Block Diagram

APR1400 DCD TIER 2

7.6 Interlock Systems Important to Safety

7.6.1 System Description

This section describes interlock systems important to safety that are credited in the safety analysis to:

- a. Prevent over-pressurization of low-pressure systems
- b. Prevent over-pressurization of the reactor coolant system (RCS) during low-temperature operations of the reactor vessel
- c. Provide reasonable assurance of the availability of safety injection tank (SIT) isolation valves
- d. Provide reasonable assurance of the availability of component cooling water (CCW) supply and return header tie line isolation
- e. Preclude inadvertent inter-ties between redundant or diverse safety systems

Bypassed and inoperable status of all interlocks is provided via the bypassed and inoperable status indication (BISI), as described in Section 7.5.

7.6.1.1 SCS Suction Line Isolation Valve Interlocks

The shutdown cooling system (SCS) is a low-temperature and low-pressure system used to remove decay heat from the RCS. The initial phase of a cooldown of the RCS is accomplished using the steam generator (SG) down to at least 176.7 °C (350 °F) and 31.6 kg/cm²A (450 psia). Below these values, the SCS is used to cool the RCS to refueling temperature and to maintain these conditions for extended periods.

An interlock associated with the SCS suction line isolation valves prevents the isolation valves from being opened at RCS pressures above 31.6 kg/cm²A (450 psia). The interlock setpoint is calculated considering tolerances necessary to provide reasonable assurance that the pressure at the valves does not exceed the low temperature over-pressurization protection (LTOP) valve setpoint when the SCS is aligned to the RCS for normal shutdown cooling.

APR1400 DCD TIER 2

Each SCS suction line has independent, redundant motor-operated isolation valves to prevent over-pressurization and provide isolation between the RCS and the SCS. Refer to Table 7.6-1.

The interlocks prevent the suction line isolation valves from being opened if the RCS pressure has not decreased below the setpoint. Refer to Figure 5.4.7-3, Sheet 2 of 2, for the flow diagram of the isolation valves.

The interlocks do not prevent achieving cold shutdown from the MCR after a single failure.

The RCS pressure signals used for these interlocks are provided by physically independent pressurizer pressure safety channels (see Figures 7.6-1A, 7.6-1B, and 7.6-1C).

No single failure can prevent the operator from aligning the valves, on at least one suction line, for shutdown cooling after the RCS pressure requirements are satisfied. In addition, no single failure can result in a suction line being spuriously opened. The SCS design is described in Subsection 5.4.7. SCS suction line isolation valves are described in Subsection 5.4.7.2.2 and valve tests are described in Subsection 5.4.7.4.

7.6.1.2 SCS Suction Line Relief Valve Interlocks

Overpressure protection of the RCS during low temperature conditions is provided by the relief valves located in the SCS suction lines.

Each SCS suction line relief valve protects the primary system components given a failure that initiated the pressure transient. Each SCS suction line relief valve provides sufficient pressure relief capacity to mitigate the most limiting LTOP events during low temperature conditions.

One relief valve is installed in each SCS suction line to provide LTOP for the RCS when the SCS is aligned to the RCS to provide decay heat removal during plant shutdown and startup operations.

The relief valves are located inside the containment and connected to the in-containment refueling water storage tank (IRWST).

The LTOP pressure is the SCS suction line relief valve setpoint pressure adjusted to provide a margin to avoid lifting and to compensate for measuring inaccuracies during normal

APR1400 DCD TIER 2

operation. Because the LTOP relief valve setpoint pressure is much lower than the design pressure of the SCS, these valves also provide overpressure protection of the SCS.

During heatup, the RCS pressure is maintained below the LTOP pressure until the RCS cold leg temperature exceeds the LTOP disable temperature.

During cooldown, the RCS pressure is maintained below the LTOP pressure once the RCS cold leg temperature reaches the LTOP enable temperature.

The SCS suction line relief valve is a self-actuating spring-loaded liquid relief valve, and control circuitry is not required. The valve opens when the RCS pressure exceeds its setpoint. Refer to Table 7.6-1. The relief valves on the SCS have an accumulation of 10 percent of the set pressure.

No single failure of an isolation valve or its associated interlock prevents one relief valve from performing its intended function.

The SCS suction line relief valves are described in Subsection 5.4.7.2.2, and the valve tests are described in Subsection 5.4.7.4.

7.6.1.3 SIT Isolation Valve Interlocks

The safety injection system (SIS) is designed to inject borated water into the RCS upon receipt of the SIAS (see Section 7.3) and to provide RCS cooling in conjunction with other systems following an accident. The SIS is described in Section 6.3.

The SITs inject borated water into the RCS if system pressure drops below SIT pressure.

During normal operation, each tank has a motor-operated isolation valve that is normally open with power removed from its motor circuit to eliminate the possibility of spurious isolation.

As the RCS pressure is reduced during plant shutdown, the low pressurizer pressure trip setpoint is reduced to avoid inadvertent initiation of safety injection, the SITs are depressurized to a value below the SCS entry pressure, and the isolation valves are closed.

The SIT permissive interlocks are used to allow isolation of the SITs below the pressure required for mitigation following a loss of coolant accident (LOCA). See Figure 7.6-2 for the interlock logic.

APR1400 DCD TIER 2

The isolation valves are manually closed when RCS pressure drops below the setpoint in Table 7.6-1 so that the SITs cannot cause over-pressurization of the SCS while the SITs are maintained above atmospheric pressure.

As RCS pressure increases, the valves automatically reopen at the set pressure.

The opening of the SIT isolation valves provides reasonable assurance that the SITs are available for injection during plant startup.

If the isolation valves are closed and an SIAS is initiated, the isolation valves automatically open. The SIAS overrides the interlock or any manual signal.

The alarm associated with the SITs is activated if the RCS pressure is increased to the determined values and the SITs have not been repressurized.

Physically separate and independent signals are provided for SIT isolation valve interlocks. Refer to Section 6.3 for SIS and Subsections 6.3.4 and 3.9.6.3.1 for valve tests.

7.6.1.4 CCW Supply and Return Header Tie Line Isolation Interlocks

The CCW system removes heat from all safety components required for normal power plant operation, and normal and emergency shutdown of the plant, and transfers the heat to the essential service water through the CCW heat exchangers. The CCW system also provides cooling water for some non-safety components required for plant operation.

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two series electric motor operated valves and can be remotely operated.

These valves are automatically closed on an SIAS or low-low CCW surge tank level signal. The valve closure times are set to prevent complete loss of surge tank volume due to a break in the non-safety piping. These valves can be manually opened and closed from the main control room.

Cooling water may be supplied to the post-accident primary sample cooler rack by the function of the ESFAS overriding to open non-essential supply and return header isolation valves of the other division under the discretion of the operator during post-accident condition.

APR1400 DCD TIER 2

The design of the CCW system is described in Subsection 9.2.2, and a flow diagram of the isolation valves (CC-V-143, 144, 145, 146, 147, 148, 149, and 150) is provided in Figure 9.2.2-1. The setpoint and function of CCW isolation valves are described in Table 7.6-2.

A single interlock failure may result in valve malfunction within a single division, but this does not adversely affect the other division. These interlocks provide reasonable assurance of the independence between essential supply and return headers, and non-essential supply and return headers.

The interlocks for these valves are shown in Figure 7.6-3. The signal path for the surge tank interlock is from local level transmitters to the ESF-CCS loop controller for control of these valves.

7.6.1.5 Interlocks Required to Preclude Inadvertent Inter-ties between Redundant or Diverse Safety Systems

Because there is no connection between the CCW safety divisions, the APR1400 design does not include interlocks to prevent inadvertent inter-ties between redundant or diverse safety systems. Therefore, this is not applicable.

7.6.2 Design Basis Information

This subsection describes the criteria for the interlock systems that are important to safety and that operate to reduce the probability of events such as a LOCA or LTOP and to maintain safety systems in a state that provide reasonable assurance of their availability in an accident. Compliance with applicable GDC is described in Subsection 7.6.2.1, and compliance with IEEE Std. 603 (Reference 1) is described in Subsection 7.6.2.2.

7.6.2.1 Applicable Codes and Regulations

The interlock systems important to safety comply with the following codes and regulations:

- a. 10 CFR 50.34(f)(2)(v), “Additional TMI-Related Requirements.”

The BISI described in Subsection 7.6.1 is designed in accordance with 10 CFR 50.34(f)(2)(v) (Reference 2).

APR1400 DCD TIER 2

The BISI of the interlock systems important to safety is available on the information processing system (IPS) and qualified indication and alarm system - non-safety (QIAS-N).

b. 10 CFR 50.55a(a)(1), “Quality Standards.”

The interlock systems important to safety are defined as safety grade according to ANSI/ANS-51.1 (Reference 3). This is for compliance with IEEE Std. 603, Clause 5.3.

The interlock systems important to safety are tested and inspected to quality standards commensurate with the importance of the safety function to be performed in accordance with 10 CFR 50.55a(a)(1) (Reference 4).

c. 10 CFR 50.55a(h), “Protection and Safety Systems.”

The important to safety interlock systems described in Subsections 7.6.1.1, 7.6.1.3, and 7.6.1.4 are designed in accordance with 10 CFR 50.55a(h)(2) (Reference 5) as follows :

The interlock systems important to safety consist of four independent channels except the SCS suction line relief valves, which consist of two channels. The protection channel is physically separated and electrically isolated from the other protection channels. All equipment/components used for safety related functions are qualified as safety related. The failures of non-safety systems cannot prevent any interlock system important to safety from performing its safety function.

The operating bypass and trip bypass status for the all interlocks except SCS suction line relief valve interlock is available for display at the IPS display and operator module (OM) in the main control room (MCR).

d. 10 CFR 50, Appendix A, General Design Criterion (GDC) 1, “Quality Standards and Records.”

The important to safety interlock systems discussed in Subsections 7.6.1.1 through 7.6.1.4 are designed in accordance with GDC 1 (Reference 6) in compliance with IEEE Std. 603, Clause 5.3. Compliance with GDC 1 is described in Subsection 7.1.2.

APR1400 DCD TIER 2

- e. GDC 2, “Design Bases for Protection Against Natural Phenomena.”

The interlock systems important to safety are designated as seismic Category I to provide protection against seismic and other natural phenomena, such as wind, tornado, and flood.

- f. GDC 4, “Environmental and Dynamic Effects Design Bases.”

The interlock systems important to safety are qualified to accommodate the effects of environmental conditions and designed to withstand the dynamic effects of missiles, pipe whipping, and discharging fluids. Under the LOCA condition, the interlock systems valves operate for 182 days of post-accident operability period.

- g. GDC 10, “Reactor Design.”

The interlock systems important to safety contribute to reactor design margin by providing conservatism in setpoint calculations and fault-tolerant features. Compliance with GDC 10 is described in Subsections 7.6.1.1 through 7.6.1.4.

- h. GDC 13, “Instrumentation and Control.”

The interlock systems important to safety comply with GDC 13, as described in Subsections 7.6.1.1, 7.6.1.3 and 7.6.1.4, and maintain interlock variables within safe states by observing the setpoint conditions as depicted in Figures 7.6-1A through 7.6-3 and as shown in Tables 7.6-1 and 7.6-2.

- i. GDC 15, “Reactor Coolant System Design.”

The interlock systems important to safety to prevent over-pressurization of the RCS are designed in compliance with GDC 15, as described in Subsections 7.6.1.1 and 7.6.1.2.

- j. GDC 16, “Containment Design.”

The leak-tightness of the containment system and short-term and long-term performance following a LOCA are designed in compliance with GDC 16, as described in Section 6.2.

APR1400 DCD TIER 2

k. GDC 19, “Control Room.”

Instrumentation and control systems for the all interlock systems important to safety except SCS suction line relief valve interlock in the MCR are designed in compliance with GDC 19 to maintain in a safe condition under accident conditions (refer to Figures 7.6-1A through 7.6-3).

The SCS suction line relief valves are not required to comply with 10 CFR 50.34(f)(2)(xi) (Reference 7) addressing TMI Action Plan Item II.D.3. Because the requirement for position indication has been applied only to safety and relief valves directly connected to the RCS, SCS suction line relief valves, which are located in the SCS line and normally isolated from the RCS, are not applicable to the TMI requirement II.D.3.

l. GDC 24, “Separation of Protection and Control Systems.”

Compliance with GDC 24 presents the characteristics described in IEEE Std. 603 as follows:

1) Single failure criterion

The all interlocks important to safety are designed to comply with the single failure criterion.

2) Physical, electrical, and communications independence

Complete physical, electrical, and communication isolations for the interlock systems important to safety are maintained between redundant safety channels, and between the safety system and non-safety system.

3) Control protection interaction

All interlocks important to safety are isolated in normal operation to prevent an unnecessary initiation of a protective action and to limit non-safety system interactions with safety systems.

4) Auxiliary features

Not applicable in Section 7.6.

APR1400 DCD TIER 2

5) Power sources

The channels of all interlock systems important to safety receive AC power from the four independent A, B, C, D channels of the vital bus power supply system (VBPSS). All interlock systems important to safety do not share the power between channels.

m. GDC 25, “Protection System Requirements for Reactivity Control Malfunctions.”

GDC 25 is not applicable to Section 7.6. Protection system requirements for reactivity control malfunctions are met by opening of the reactor trip switchgear system (RTSS) circuit breakers, which is described in Section 7.2.

n. GDC 28, “Reactivity Limits.”

GDC 28 is not applicable to Section 7.6. The function related to reactivity limits is implemented by the chemical and volume control system (CVCS), which is described in Subsection 9.3.4, and has no interlock system important to safety.

o. GDC 33, “Reactor Coolant Makeup.”

GDC 33 is not applicable to Section 7.6. The reactor coolant makeup function is implemented by the CVCS, which is described in Subsection 9.3.4, and has no interlock system important to safety.

p. GDC 34, “Residual Heat Removal.”

The interlock systems important to safety are designed in compliance with GDC 34, as described in Subsections 7.6.1.1 and 7.6.1.2.

q. GDC 35, “Emergency Core Cooling.”

The interlock systems important to safety are designed in compliance with GDC 35, as described in Subsections 7.6.1.1 through 7.6.1.3.

r. GDC 38, “Containment Heat Removal.”

The containment heat removal function implemented by the containment spray system (CSS), which is described in Subsections 6.2.5 and 6.5.2, is designed in compliance with GDC 38.

APR1400 DCD TIER 2

- s. GDC 41, “Containment Atmosphere Cleanup.”

The containment atmosphere cleanup function implemented by the CSS and containment hydrogen control system, which is described in Subsections 6.2.5 and 6.5.2, are designed in compliance with GDC 41.

- t. GDC 44, “Cooling Water.”

The CCW supply and return header tie line isolation interlocks are designed in accordance with GDC 44. Compliance with GDC 44 is described in Subsection 7.6.1.4.

7.6.2.2 Conformance to IEEE Std. 603

This subsection describes the compliance of only for the interlocks with IEEE Std. 603. The valves and piping of SCS are addressed in Subsection 5.4.7, and SIS and its requirements are addressed in Section 6.3.

- a. Single Failure Criterion (Clause 5.1)

All interlocks important to safety comply with the single failure criterion and are described in Subsections 7.6.1.1 through 7.6.1.4.

- b. Completion of Protective Action (Clauses 5.2 and 7.3)

This requirement is not applicable in Section 7.6.

- c. Quality (Clause 5.3)

The sensors for the all interlocks meet the same quality requirements imposed on the protection system sensors.

- d. Equipment Qualification (Clause 5.4)

The interlocks important to safety described in Subsections 7.6.1.1 through 7.6.1.4 are implemented using Class 1E qualified components.

- e. System Integrity (Clause 5.5)

APR1400 DCD TIER 2

All interlocks are designed to maintain functional capability during accident environments. In case of SCS suction line isolation valve interlocks, failure of one interlock does not prevent opening a path or closing both paths of the SCS. In case of SIT isolation valve interlocks, failure of an interlock does not preclude safety injection during accident conditions.

f. Independence (Clause 5.6)

The interlocks important to safety are performed in independent and redundant divisions. Independence and redundancy are described in Subsections 7.6.1.1 through 7.6.1.4.

The method for identifying power and signal cables and cable trays dedicated to the instrumentation, control, and electrical equipment associated with the isolation valves is described in Subsection 7.3.2.3, and complies with NRC RG 1.75 (Reference 8) as described in Subsection 7.1.2.

g. Capability for Testing and Calibration (Clauses 5.7 and 6.5)

Complete testing capability of the SCS isolation valve interlocks and SIT isolation valve interlocks exists. The tests are performed in conjunction with inspection of the valves. The tests, using the built-in ESF-CCS test logic, include testing of the interlock logic, valve control circuits, and actuation of the individual valves. This testability is equivalent to the testability required for ESF circuits.

Testing is accomplished sequentially for each valve by inserting a test signal simulating a decreased pressure condition while holding the control switch in the open position to the point where the valve partially opens. It is further tested by manually reclosing the valve, simulating an increased pressure condition, and observing that the valve does not open when the hand switch is moved to the open position.

h. Information Display (Clause 5.8)

The readout consists of individual and validated pressure indication on the QIAS-N and IPS.

i. Control of Access (Clause 5.9)

APR1400 DCD TIER 2

Access is controlled by the administrative procedures.

j. Repair (Clause 5.10)

Components are accessible for repair. One channel can be placed out of service for maintenance without jeopardizing the isolation of the SCS or the availability of the SITs.

k. Identification (Clause 5.11)

The instrumentation and cables associated with the interlocks are uniquely identified. The channels are identified to distinguish between redundant channels of safety related equipment.

l. Auxiliary Features (Clause 5.12)

This requirement is not applicable to Section 7.6.

m. Multi-unit stations (Clause 5.13)

This requirement is not applicable to Section 7.6.

n. Human Factors Considerations (Clause 5.14)

The interlock systems are designed for operator and maintenance personnel to accomplish their assigned functions successfully during the various plant conditions.

o. Reliability (Clause 5.15)

The interlock systems are designed to operate during accident environmental conditions.

p. Automatic Control (Clauses 6.1 and 7.1)

The SCS suction line isolation valve interlock and SCS suction line relief valve interlock is not applicable to this requirement.

The SIT isolation valve interlock is designed to open the valve automatically when the RCS pressure exceeds the setpoint listed in Table 7.6-1.

APR1400 DCD TIER 2

The CCW supply and return header tie line isolation interlocks are designed to close the valve automatically on the CCW surge tank low-low level signal.

q. Manual Control (Clauses 6.2 and 7.2)

The manual control for the SCS suction line and SIT isolation valve interlocks is allowed when the RCS pressure is below the setpoint in Table 7.6-1.

The SCS suction line relief valve interlock is not applicable to this requirement.

The CCW supply and return header tie line isolation interlocks can override the automatic close signal by a manual operation from the MCR.

r. Interaction between the Sense and Command Features and Other Systems (Clause 6.3)

The SIT isolation valves are opened automatically when the RCS pressure is greater than the setpoint listed in Table 7.6-1 and by the SIAS signal.

The SCS suction line isolation valve interlock, SCS suction line relief valve interlock, and CCW supply and return header tie line isolation interlocks are not applicable to this requirement.

s. Derivation of System Inputs (Clause 6.4)

The pressurizer pressure is the sensed parameter for the SCS suction line isolation valve interlock, SCS suction line relief valve interlock, and SIT isolation valve interlock.

The CCW surge tank level is the sensed parameter for the CCW supply and return header tie line isolation interlocks.

t. Operating Bypasses and Maintenance Bypass (Clauses 6.6, 6.7, 7.4, and 7.5)

Removal of one channel for testing does not degrade system reliability. Failure of one of the remaining channels during a test outage does not generate an unacceptable situation, since valve position indication monitoring, with alarms and administrative controls, effectively precludes inadvertent opening or closing of the valves by the operator.

APR1400 DCD TIER 2

u. Setpoints (Clause 6.8)

The permissive open setpoint of the SCS suction line isolation valves is provided to prevent opening the LTOP relief valves.

The multiple setpoints are not required to the SCS suction line relief valve interlock, SIT isolation valve interlock, and CCW supply and return header tie line isolation interlocks.

v. Power Source Requirements (Clause 8)

The channels of all interlock systems important to safety receive non-interrupt AC power from the VBPSS. The power of all interlocks is provided with single phase 120 Vac from four independent A, B, C, D channel inverters.

7.6.2.3 System Testing and Inoperable Surveillance

The system testing and inoperable surveillance of the interlocks important to safety are described in Subsections 3.9.6.3.1 and 3.9.6.3.6.

System testing complies with the criteria of IEEE Std. 338 (Reference 9), which is endorsed by NRC RG 1.22 (Reference 10) and NRC RG 1.118 (Reference 11). Test intervals and their bases are included in the Technical Specifications (Chapter 16).

7.6.2.4 Use of Digital Systems

The interlocks important to safety are implemented in the ESF-CCS group controller and loop controller. The ESF-CCS loop controller interfaces with controlled plant components and reflects the result of combining the interlock control signals.

7.6.3 Analysis

7.6.3.1 Interlocks to Prevent Over-pressurization of Low-Pressure Systems

The SCS suction line isolation valve interlock is described in Subsection 7.6.1.1. The interlocks to prevent over-pressurization of low-pressure systems meet the design bases in Subsection 7.6.2.

APR1400 DCD TIER 2

7.6.3.2 Interlocks to Prevent Over-pressurization of the Reactor Coolant System during Low-Temperature Operations of the Reactor Vessel

The SCS suction line relief valve interlock is described in Subsection 7.6.1.2. There is no interlock for SCS suction line relief valves, since the valves are spring-loaded relief valves. The interlocks to prevent over-pressurization of the reactor coolant system during low-temperature operations of the reactor vessel meet the design bases in Subsection 7.6.2.

7.6.3.3 Interlocks for SIT Isolation Valves

The SIT isolation valve interlock is described in Subsection 7.6.1.3. The interlocks for SIT isolation valves meet the design bases in Subsection 7.6.2.

7.6.3.4 Interlocks for Supply and Return Header Isolation Valves

The CCW supply and return header isolation valve interlocks are described in Subsection 7.6.1.4. The interlocks required to isolate safety systems from non-safety systems meet the design bases in Subsection 7.6.2.

7.6.4 Combined License Information

No COL information is required with regard to Section 7.6.

7.6.5 References

1. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers.
2. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3].
3. ANSI/ANS 51.1-1983, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants."
4. 10 CFR 50.55a(a)(1), "Domestic Licensing of Production and Utilization Facilities, Codes and Standards, Quality Standards for Systems Important to Safety."
5. 10 CFR 50.55a(h)(2), "Codes and Standards, Protection Systems."
6. 10 CFR 50, Appendix A, "General Design Criteria for Nuclear Power Plants."

APR1400 DCD TIER 2

7. 10 CFR 50.34(f)(2)(xi), “Direct Indication of Relief and Safety Valve Position,” [II.D.3].
8. NRC RG 1.75, Rev. 3, “Criteria for Independence of Electrical Safety Systems,” 2005.
9. IEEE Std. 338-1987, “Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems.”
10. NRC RG 1.22, “Periodic Testing of Protection System Actuation Functions,” 1972.
11. NRC RG 1.118, Rev. 3, “Periodic Testing of Electrical Power and Protection Systems,” 1995

APR1400 DCD TIER 2

Table 7.6-1

Shutdown Cooling System and Safety Injection Tank Interlock

System	Setpoint	Function
Shutdown Cooling System		
Suction line isolation valves: SI-655, SI-656, SI-651, SI-652, SI-653, SI-654 ⁽⁴⁾	$\leq 31.64 \text{ kg/cm}^2 \text{A}$ (450 psia) ⁽¹⁾	Permits valves to be opened by the operator.
Suction line relief valves: SI-179, SI-189 ⁽⁴⁾	37.3 kg/cm^2 (530 psig) ⁽²⁾	Prevents or mitigates over pressurization of the SCS. (Refer to Table 5.2-3 for design parameter of SCS suction line relief valves)
Safety Injection Tank		
Isolation valves: SI-614, SI-624, SI-634, SI-644 ⁽⁴⁾	$> 42.2 \text{ kg/cm}^2 \text{A}$ (600 psia) ⁽³⁾	Valves are automatically opened.
	$< 33.4 \text{ kg/cm}^2 \text{A}$ (475 psia) ⁽³⁾	Permits valves to be closed by the operator.
	SIAS	Automatically opens the valves if the valves are closed. Sends an open signal if valves are open that overrides a closing signal.

(1) The interlock setpoint is established so that the set pressure of the SCS relief valves (SI-179 and SI-189) is not exceeded upon opening of the suction line valves.

(2) Refer to Table 5.2-3 for design parameter of SCS suction line relief valves.

(3) Refer to Subsection 6.3.2.2.2.

(4) Refer to Figure 6.3.2-1 (Sheet 3 of 3) for the P&ID of the valves.

APR1400 DCD TIER 2

Table 7.6-2

CCW Supply and Return Header Tie Line Isolation Interlocks

System	Setpoint	Function
Component Cooling Water System		
Non-essential supply header isolation valves CC-V-143, CC-V-144, CC-V-145, CC-V-146 ⁽¹⁾	SIAS CCW surge tank low-low level signal ⁽²⁾	Close to terminate CCW flow to the nonessential equipment in the event of an accident
Non-essential return header isolation valves CC-V-147, CC-V-148, CC-V-149, CC-V-150 ⁽¹⁾	SIAS CCW surge tank low-low level signal ⁽²⁾	Isolate the nonessential return headers in the event of an accident

(1) The valve closure times are selected to prevent the CCW surge tank from being emptied in the event of a break in the non-safety piping. The automatic close signal can be overridden by a manual operation from the MCR to cool the post-accident primary sample cooler rack in the other division, if necessary. The interlock valves are listed in Table 9.2.2-5. Refer to Figure 9.2.2-1 for the flow diagram of the valves.

(2) Refer to Subsection 9.2.2.5.4.

APR1400 DCD TIER 2

TAG NO.	DESCRIPTION	CHANNEL	COMPONENT	PZR PRESS
SI-655	SHUTDOWN COOLING SYSTEM SUCTION LINE ISOLATION VALVE	A	MOV(FULL THROW)	P-103A
SI-656	SHUTDOWN COOLING SYSTEM SUCTION LINE ISOLATION VALVE	B	MOV(FULL THROW)	P-104B

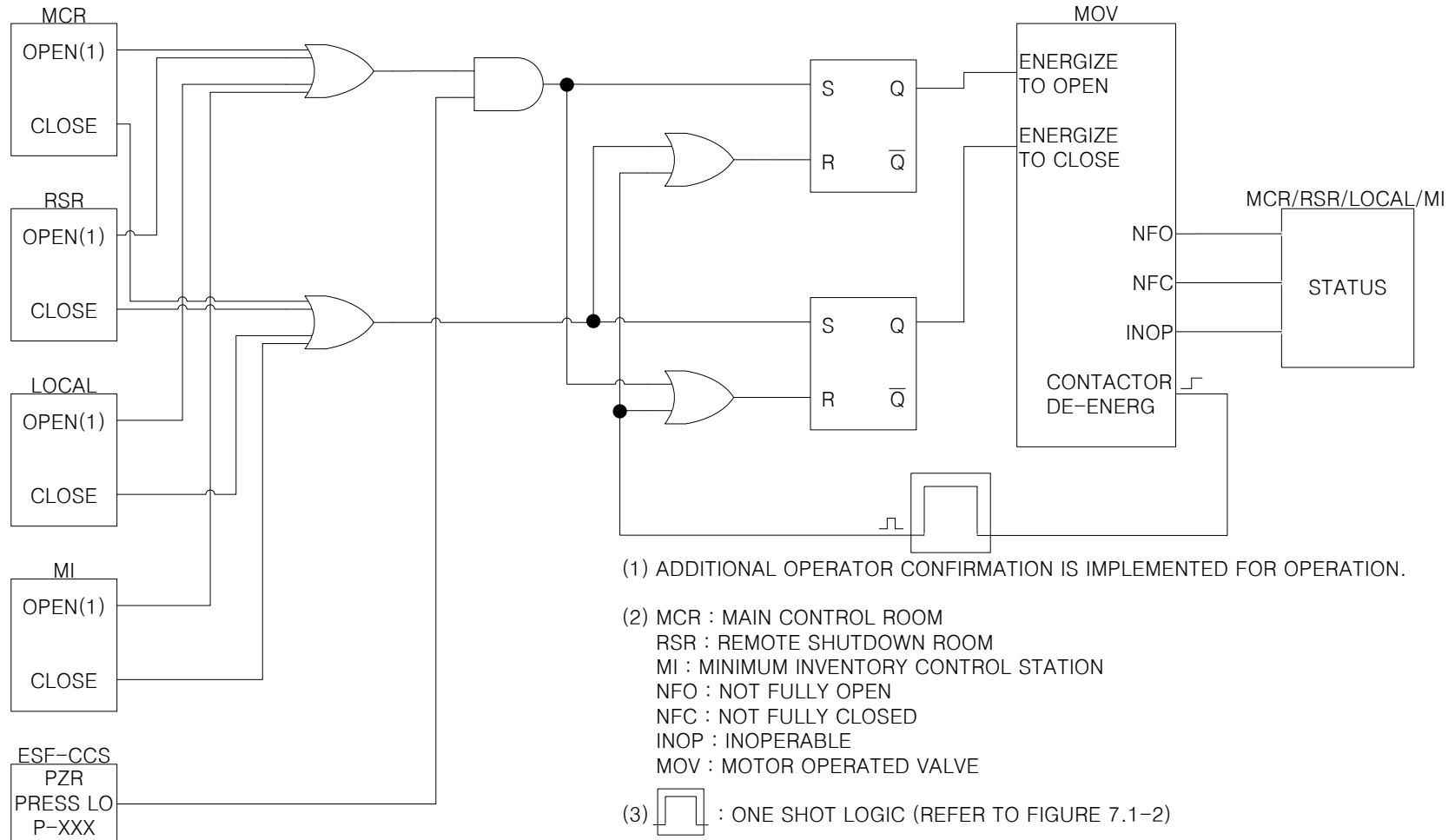


Figure 7.6-1a Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

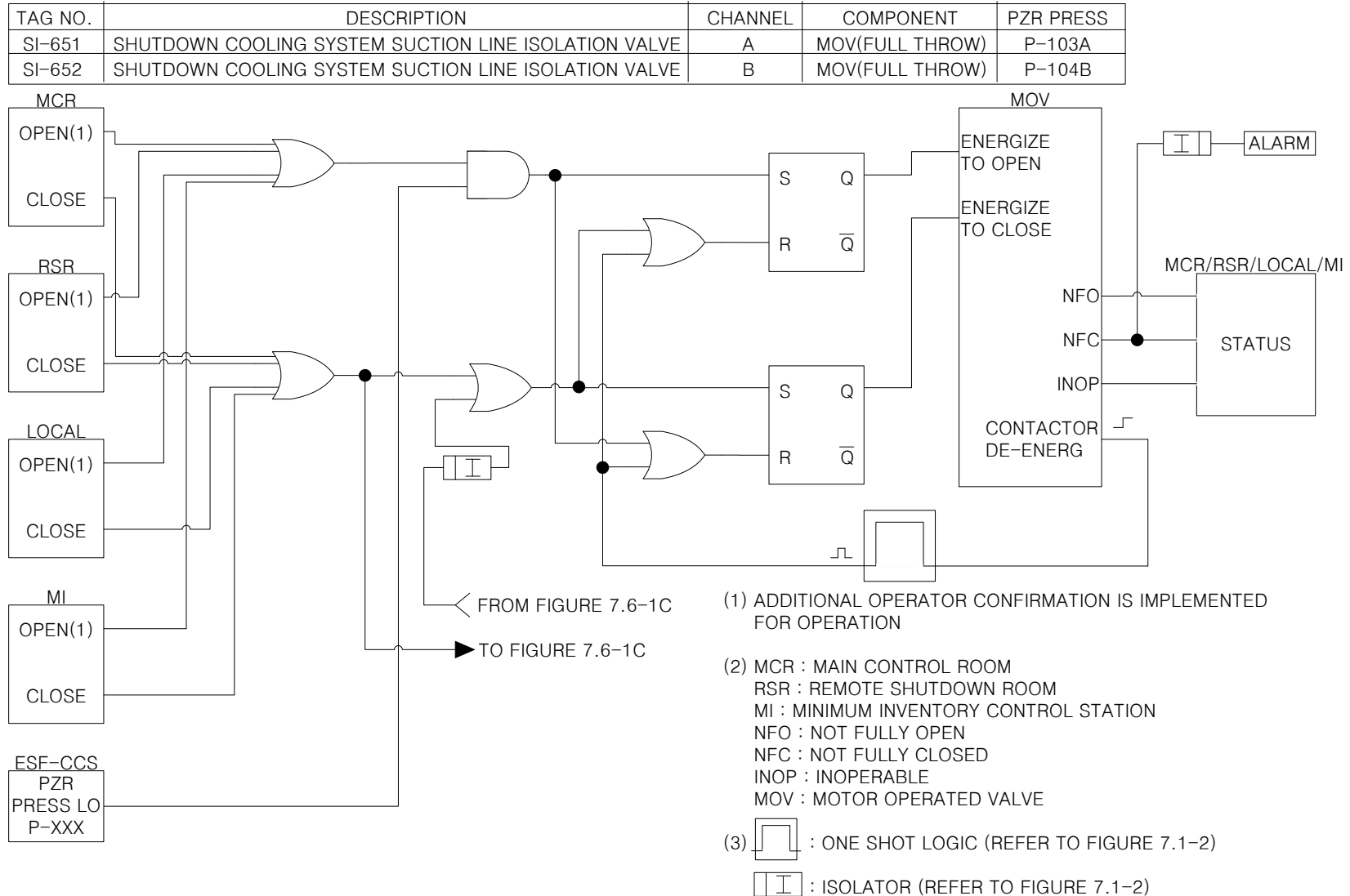


Figure 7.6-1b Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

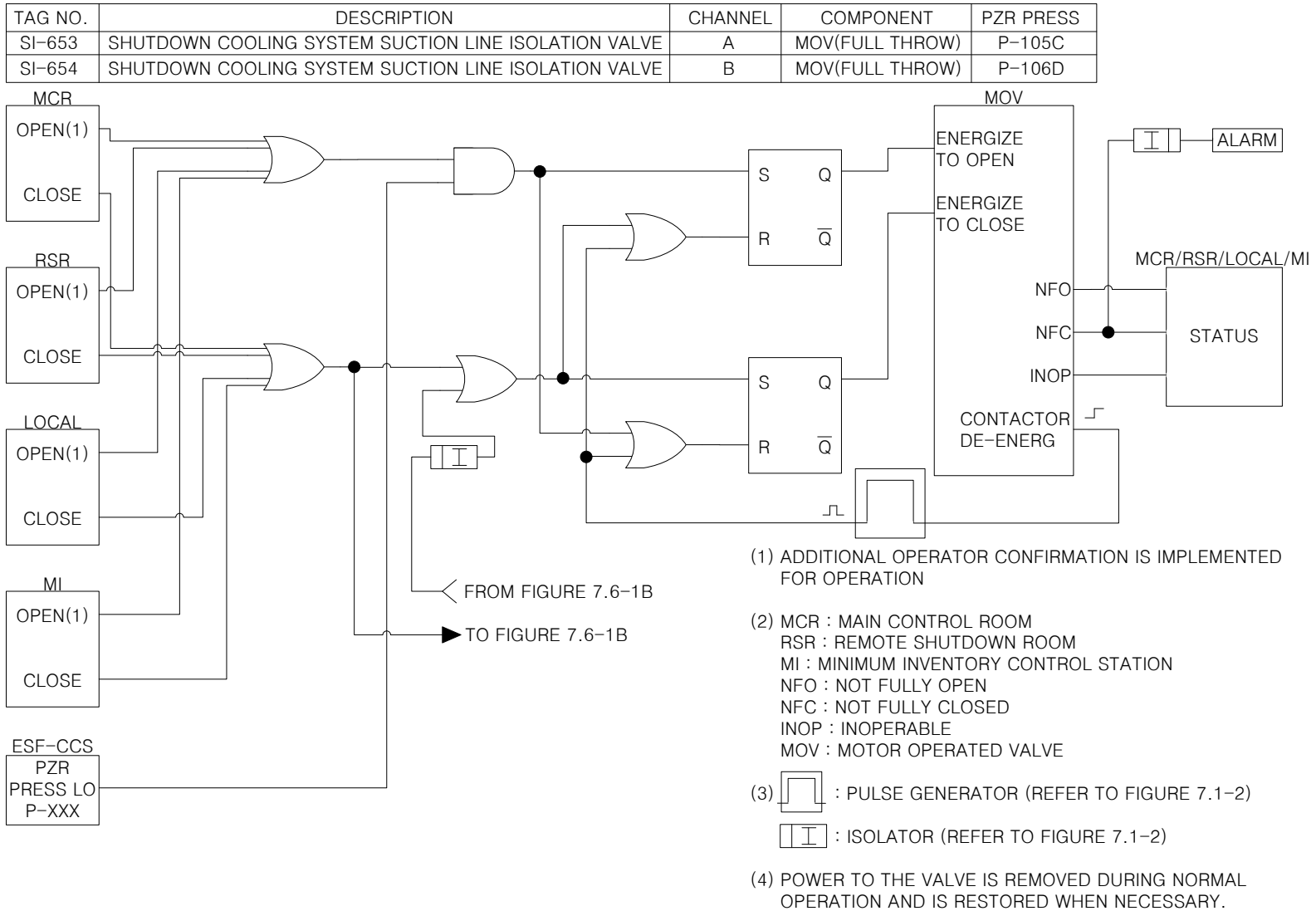


Figure 7.6-1c Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

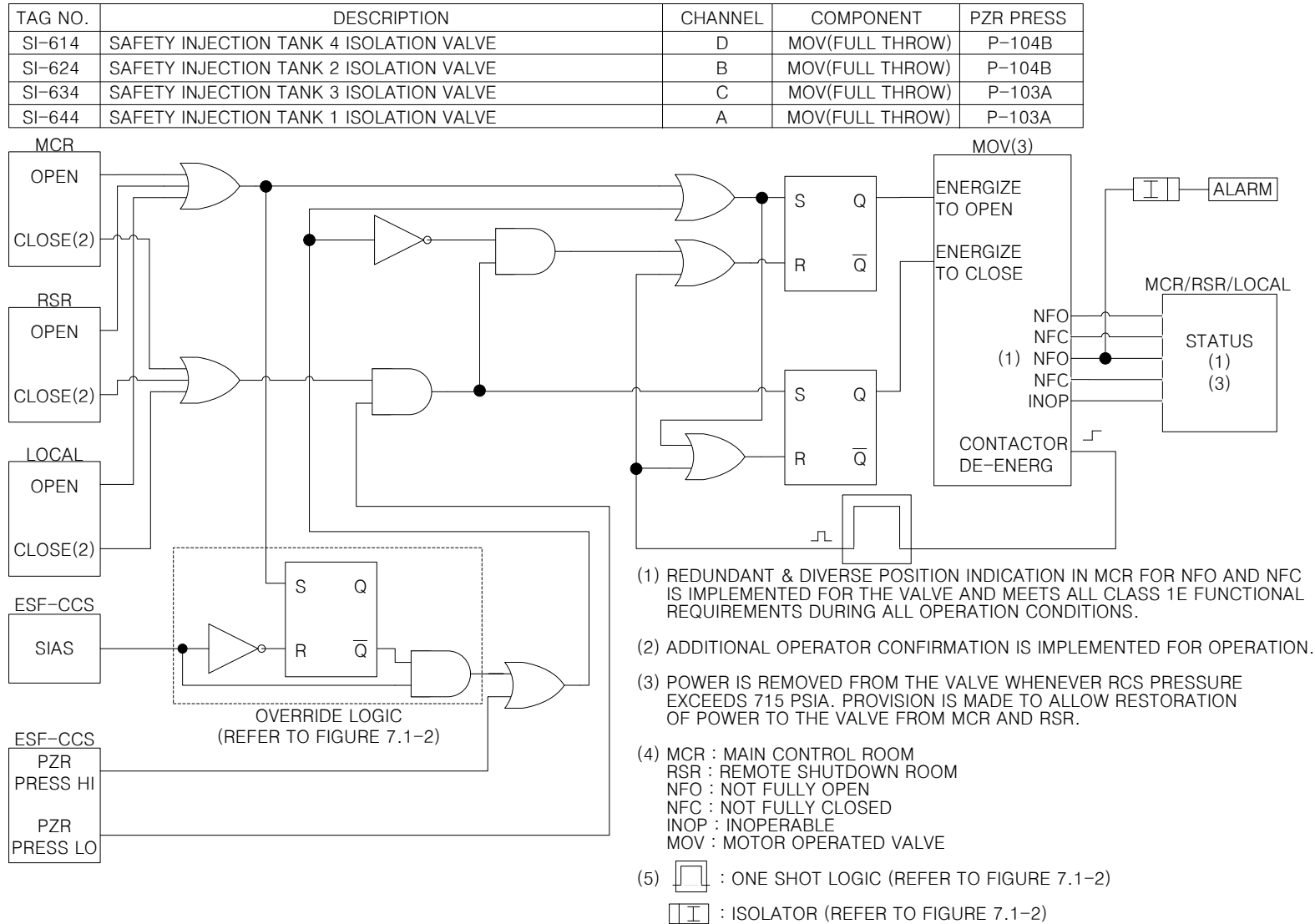


Figure 7.6-2 Interlocks for Safety Injection Tank Isolation Valve

APR1400 DCD TIER 2

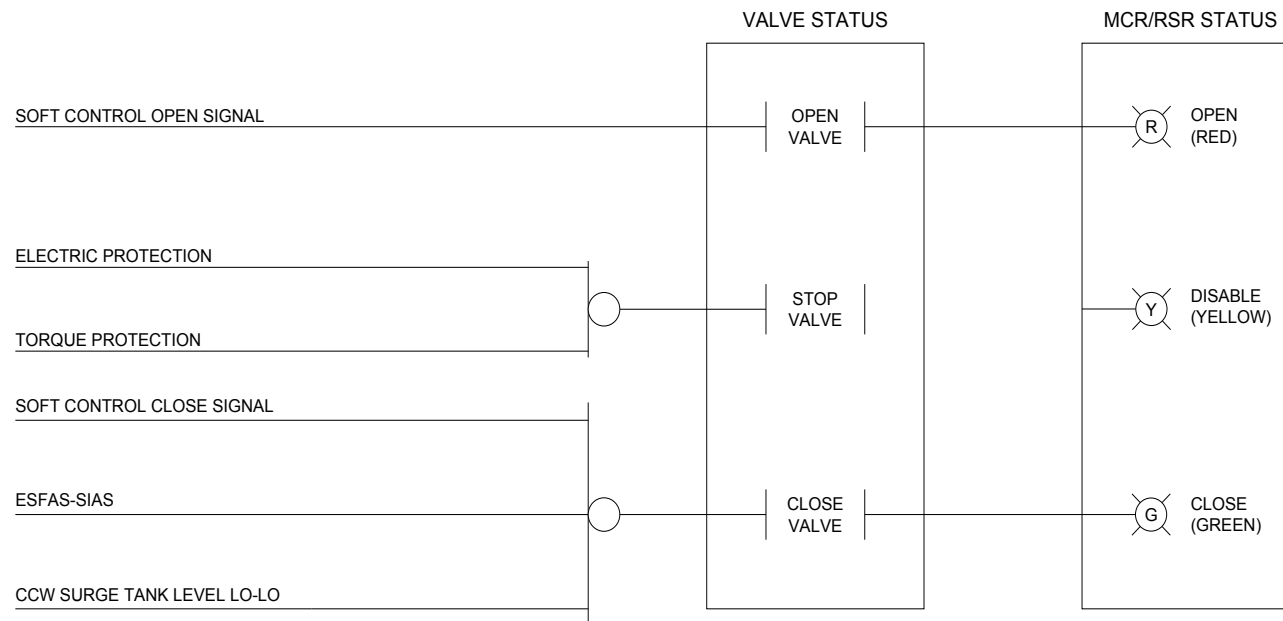


Figure 7.6-3 Interlocks for CCW Supply and Return Header Isolation Valve

APR1400 DCD TIER 2

7.7 Control Systems Not Required for Safety

7.7.1 Description

Plant information, monitoring, and control systems not essential for the plant safety are described in this section.

Non-safety systems that interface with safety systems are designed so that credible failures in the systems do not impact the operation of safety systems.

Interfaces between safety and non-safety systems use isolation devices to maintain electrical independence. Isolation devices are considered part of the safety system and are qualified as Class 1E.

In general, the non-safety-related control system sensors and signal conditioning devices are separated from those used in safety-related control systems. Where safety-related devices provide parameters for control and monitoring, signal isolation is provided between the safety systems and the non-safety-related control and monitoring systems.

The information processing system (IPS) and the qualified indication and alarm system-non-safety (QIAS-N) receive data from safety-related and non-safety systems through a fiber-optic network that provides the isolation.

The human-system interface (HSI) design for both safety systems and non-safety systems in the main control room (MCR) and the remote shutdown room (RSR) is subject to the human factors engineering (HFE) design processes described in Chapter 18. Non-safety consoles are designed to maintain structural integrity so that no missile hazards are generated as a result of a seismic event.

To provide reasonable assurance that the non-safety control system failures do not cause initiating anticipated operational occurrences (AOOs) that have not been considered in the safety analysis, control functions are distributed to the separate non-safety controller groups. The initiating AOOs due to a controller group failure are in Table 7.7-1.

7.7.1.1 Control Systems

The non-safety control systems consist of the power control system (PCS) and the process-component control system (P-CCS). The PCS includes the reactor regulating system (RRS),

APR1400 DCD TIER 2

the digital rod control system (DRCS), and the reactor power cutback system (RPCS). The P-CCS includes the NSSS process control system (NPCS) and balance of plant (BOP) control systems. The NPCS consists of the feedwater control system (FWCS), steam bypass control system (SBCS), pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), and other miscellaneous NSSS control systems.

The control systems are implemented on a digital platform that is diverse from the safety common platform. Control of physical and electronic access to digital computer-based control system software and data prevents changes by unauthorized personnel.

The reactivity feedback properties of the NSSS inherently cause reactor power to match the total NSSS load. The resulting reactor coolant temperature is a controlled parameter adjusted by changes in the total reactivity implemented through the control element assembly (CEA) position changes or through the boric acid concentration changes in the primary coolant.

The ability of the NSSS to follow the turbine load changes is dependent on the ability of the control systems or the operator to adjust reactivity, feedwater flow, bypass steam flow, reactor coolant inventory, and energy content of the pressurizer such that NSSS conditions remain within normal operating limits.

Except as limited by the xenon conditions, the major control systems described below provide the capability to follow the load changes automatically. These automatic systems also provide the capability to accommodate load rejections of any magnitude.

a. Reactivity control systems

The reactor reactivity is controlled by adjustments of CEAs for rapid reactivity changes or by adjustment of boric acid concentration for slow reactivity changes. The boric acid is used to compensate for the long-term effects of fuel burnup and changes in fission product concentration.

The boric acid concentration can be used within limits to load follow. Since boric acid concentrations changes occur slowly, operator action is acceptable for boric acid concentration control. The CEAs can be controlled manually by the operator or automatically to maintain the programmed reactor coolant temperature and power level during boric acid concentration changes within the limits of CEA travel.

APR1400 DCD TIER 2

The PCS integrates the control systems that control the reactor power level, which include the RRS, DRCS, and RPCS.

Providing control limits and interlocks prevents abnormal power and temperature conditions that could result from excessive control rod withdrawal initiated by a control system malfunction or by an operator.

Table 7.7-2 summarizes the DRCS control limits and interlocks.

The RRS automatically adjusts reactor power and reactor coolant temperature to follow the turbine load transients within the established limits. Figure 7.7-1 shows that the RRS receives a turbine load index signal (linear indication of load) and reactor coolant temperature signals.

The desired average temperature is determined by a reference temperature (T_{REF}) program that is inputted with the turbine load index. The hot leg and cold leg temperature signals are averaged (T_{AVG}) in the RRS. The T_{REF} signal is then subtracted from the T_{AVG} signal to provide a temperature error signal. Power range neutron flux is subtracted from the turbine load index to provide compensation to the $T_{AVG} - T_{REF}$ error signal generated.

This resulting error signal is fed to a CEA rate program to determine whether the CEAs are to be adjusted at a high or low rate, and to a CEA motion demand program that determines if the CEAs are to be withdrawn, inserted, or held. The outputs of the rate and motion demand programs are used by the DRCS.

If the temperature error signal is high (i.e., T_{AVG} is higher than T_{REF} or the cold leg temperature (T_{COLD}) is higher than a limit), the RRS provides an automatic withdrawal prohibit (AWP) signal to the DRCS. The withdrawal of CEAs causes the T_{AVG} to increase. Prohibiting a withdrawal prevents an increase in the error signal.

The DRCS uses automatic CEA motion demand signals from the RRS or manual motion signals from the DRCS soft control display on the information flat panel display (FPD) to convert these signals to direct current pulses that are transmitted to the control element drive mechanism (CEDM) coils to cause CEA motion.

APR1400 DCD TIER 2

The SBCS generates an AWP signal whenever SBCS demand for opening the turbine bypass valves exists. The AWP signal is sent to the DRCS to block its response to the RRS demands for withdrawing CEAs and thus preventing an increase in reactor power when there is excess energy in the NSSS.

A reactor trip initiated by either the reactor protection system (RPS) or the diverse protection system (DPS) causes the input motive power to be removed from the DRCS, which causes all CEAs to be inserted by gravity as shown in Figure 7.7-2.

There are five modes of control: sequential group movement in manual and automatic control, manual group movement, manual individual CEA movement, and standby. Sequential group movement functions such that, when the moving group reaches a programmed low (or high) position, the next group begins inserting (or withdrawing), thus providing for overlapping motion of the regulating groups. The initial group stops upon reaching its lower (or upper) limit. Applied successively to all regulating groups, the procedure allows a smooth continuous rate of change of reactivity. The DRCS group sequencing logic necessitates that the preceding group reach a specified limit before the next group is permitted to move. The DRCS and IPS monitor proper sequential motion and provide an alarm for out of sequence conditions.

The DRCS also includes normal CEA control limits and CEA interlocks for all CEAs and part-strength CEAs (PSCEAs). The CEA control limits include both the upper group stop (UGS) and the lower group stop (LGS) for full-strength CEAs and the PSCEAs. Control limits are provided to automatically terminate CEA motion upon reaching the CEA limits of travel. Whenever the DRCS receives an upper electrical limit (UEL) or lower electrical limit (LEL) interlock signals from the reed switch position transmitters (RSPTs), it prohibits the withdrawal or the insertion of the appropriate CEA. These UEL and LEL interlock signals are provided to automatically terminate CEA motion upon reaching the CEA upper and lower limits of travel.

The shutdown CEAs are moved in the manual control mode only, with either individual or group movement. The DRCS soft control permits withdrawal of no more than one shutdown group at any time.

APR1400 DCD TIER 2

The PSCEAs are normally moved manually, with either individual or group movement.

During plant startup and shutdown, and all cases where power is below a preset value, manual control is used. Automatic control of the regulating CEAs by the RRS can be selected by the operator only when power exceeds the preset value. Manual control can be used to override automatic control at any time.

The DRCS includes pulse counting to infer each CEA position by electronically monitoring the mechanical actions within each CEDM to determine when a CEDM has raised or lowered the CEA. The pulse counting CEA position signal associated with each CEA is reset to zero whenever the rod drop contact (located within the RSPT housing) is closed. This permits the pulse counting system to automatically reset the position to zero, whenever a reactor trip occurs or whenever a CEA is dropped into the core. This CEA position information is used in MCR displays. The displays provide CEA group information and individual CEA position information.

The DRCS also provides the IPS with each CEA position from the pulse counting system for use in the CEA monitoring displays and alarms and the core operating limit supervisory system (COLSS) as described in Subsection 7.7.1.4.

The DRCS receives a CEA withdrawal prohibit (CWP) signal from the PPS. This signal stops withdrawal motion of all CEAs. It can be overridden by the operator with the DRCS soft control display on the information FPD in the MCR.

The CWP interlock is interfaced to the protection systems via optical isolation to provide reasonable assurance of separation and independence.

b. Pressurizer pressure and level control systems

Pressurizer pressure control system

The PPCS maintains the reactor coolant system (RCS) pressure within specified limits by the use of pressurizer heaters and spray valves. The pressurizer provides a water/steam surge volume to minimize pressure variations due to density changes in the coolant.

APR1400 DCD TIER 2

A pressurizer pressure error signal is generated by comparing a pressure signal with a pressure setpoint and is used in a proportional-integral controller to control the proportional heaters as shown in Figure 7.7-3. The heaters are operated to maintain the pressurizer pressure as required. The operator can take manual control to regulate the pressure.

The pressurizer pressure error signal is also sent to a spray valve program. This provides a signal to the spray valves to control their opening. Since reactor coolant is cooler than the water/steam mixture, reactor coolant sprayed in causes some steam to condense in the pressurizer and thereby reduce the system pressure. The operator can take manual control of the spray valves to control the pressure.

If the proportional heaters are being used and system pressure is still decreasing, the backup heaters would be automatically energized. The operator can also manually energize these backup heaters.

The control system has a low-level interlock and a high-pressure interlock. The low-level interlock shuts off all the heaters when the level falls below a setpoint. If the pressurizer pressure reaches a high setpoint, all heaters are de-energized to provide reasonable assurance that the heaters will not cause the pressure to increase further.

Pressurizer level control system

The PLCS minimizes changes in the RCS coolant inventory by using the charging control valve and letdown orifice isolation valves in the chemical and volume control system (CVCS) described in Subsection 9.3.4. It also maintains a proper vapor volume in the pressurizer to accommodate surges during transients. Figure 7.7-4 shows the PLCS diagram.

During normal operation the level setpoint is programmed as a function of RCS T_{AVG} in order to minimize required charging and letdown flow. The T_{AVG} goes through a level setpoint program and the setpoint program signal is compared to the actual level signal. The level error signal is sent to a proportional-integral controller and comparators to control the charging control valve and letdown orifice isolation valves.

APR1400 DCD TIER 2

If the level error is high, the selected charging control valve is throttled back. If the level error is low, the charging control valve is open. If the level error exceeds a preset setpoint at which the charging control valve is not sufficient to control the level error, the letdown orifice isolation valves are opened or closed to control letdown flow.

The operator can manually control the level by controlling the charging control and letdown orifice isolation valves. The PLCS soft control display on the information FPD allows a selection of the charging control valve operated by the PLCS.

c. Feedwater control system

The FWCS automatically controls the steam generator downcomer water level from startup mode to full power operation. The steam generator level is controlled during the following conditions:

- 1) Steady-state operations
- 2) One percent per minute turbine load ramps between 5 percent and 15 percent NSSS power, and 5 percent per minute turbine load ramps between 15 percent and 100 percent NSSS power
- 3) One percent turbine load steps between 5 percent and 15 percent NSSS power, and 10 percent turbine load steps between 15 percent and 100 percent NSSS power
- 4) Loss of one of three operating feedwater pumps
- 5) Load rejection of any magnitude

The description of the FWCS refers to only one steam generator. Each FWCS controls the level in its corresponding steam generator. See Figure 7.7-5 for the FWCS block diagram and Subsection 10.4.7 for condensate and feedwater system descriptions.

The steam generator level signal is compensated by the difference between the downcomer feedwater flow and calculated steam flow signals (below a control mode transfer setpoint) or by the difference between the total feedwater flow and

APR1400 DCD TIER 2

total steam flow signals (above the control mode transfer setpoint) to generate a flow demand signal.

Below a valve transfer setpoint for NSSS power, the flow demand signal is sent to a downcomer valve program where a downcomer valve demand signal is generated. The programmed signal or a manual control signal from the operator controls the downcomer valve position. When the FWCS is in this control mode, the economizer control valve closes and the pump speed setpoint nears its minimum value.

As NSSS power increases above the valve transfer setpoint, 10 percent of the full power main feedwater flow rate goes to the downcomer valve while the remainder of the feedwater is injected into the economizer valve. The feedwater demand signal goes to an economizer valve program, which produces a valve demand signal that controls the economizer valve. This signal can also be manipulated manually using a soft control display.

The signal also goes to a high select function that selects the higher of the feedwater demand signals from FWCS 1 and FWCS 2 and passes it to the pump program. The sum of the pump program output and a valve differential pressure compensation signal generates a pump speed setpoint signal that is directed to the feedwater pumps. The operator can manipulate the signal manually using a soft control display.

The feedwater system has three 55 percent capacity turbine-driven main feedwater pumps that are operating normally. The FWCS automatically controls the steam generator level during a loss of one of three operating feedwater pumps.

d. Steam bypass control system

The turbine bypass system consists primarily of the turbine bypass valves and the SBCS. The SBCS main controller controls the positioning of the turbine bypass valves through which steam is bypassed around the turbine into the unit condenser.

The system is designed to increase plant availability by making full utilization of turbine bypass capacity to remove excess NSSS thermal energy following turbine load rejections. This is achieved by the selective use of turbine bypass valves and the controlled release of steam. This avoids unnecessary reactor trips and prevents

APR1400 DCD TIER 2

the opening of pressurizer or main steam safety valves. Refer to Figure 7.7-6 for the SBCS block diagram.

The RPCS is used in conjunction with the SBCS to reduce the required turbine bypass valve capacity. Additionally, the SBCS provides an even load on the reactor as the turbine is brought up to load during turbine loading. The system removes excess NSSS energy, and controls the rate of temperature change during reactor heatup and cooldown.

The following three types of valve signals are generated for each turbine bypass valve: a modulation signal that controls the flow rate through the valve, a quick opening signal that causes the valve to fully open in a short time, and a valve permissive signal that is required for the preceding two signals to operate the bypass valve.

In the modulation mode, a steam flow signal is sent to a program that develops a main steam header pressure setpoint. At the same time, the pressurizer pressure generates a pressurizer pressure bias program. The two program signals and the measured main steam header pressure are compared to provide an error signal that goes to the controller. The controller demand, or a manual signal provided by the operator, is passed to an electro-pneumatic converter on each turbine bypass valve. This converts the electrical signal to an air signal that is passed through the first solenoid valve to the air actuated turbine bypass valve as shown in Figure 7.7-6.

In the quick opening mode, the steam flow signal is biased based on pressurizer pressure and is sent to a change detector. The change detector output is compared to a threshold value so that, if the change signal exceeds the threshold, a quick opening signal is produced. The quick opening signal energizes the solenoid, which blocks the modulated air signal and applies the full air system pressure to quickly open the valve.

A permissive signal is also produced by the separate SBCS permissive controller to limit the effect of SBCS main controller failure. Refer to Table 7.7-1. This signal is provided by control logic identical to that described above except that the output of the permissive controller is converted to a binary signal and fed into an OR function with the quick opening signal. If a permissive signal is present, it opens the second solenoid valve and allows either the modulated or the quick open

APR1400 DCD TIER 2

air signal to be applied to the pneumatically operated bypass valves. When the permissive signal is removed, the control air is vented to the atmosphere and the valve is quickly closed. When turbine condenser pressure exceeds a preset value, the turbine bypass valves are prevented from opening.

Reactor power cutback demand signals are generated at a higher threshold by the same functions that produce the valve quick opening signals. These redundant signals are sent to the RPCS.

e. Reactor power cutback system

The NSSS normally operates with minor perturbations in power and flow that are handled by the control systems described above. Certain large plant imbalances can occur, however, such as a large turbine load rejection, turbine trip, or loss of two of the three operating main feedwater pumps. Under these conditions, the RPCS maintains the NSSS within the control band ranges by a rapid reduction of NSSS power at a rate that is greater than that provided by the normal high-speed CEA insertion. See Figure 7.7-7 for functional block diagram of the RPCS.

The RPCS is a control system designed to accommodate certain types of imbalances by providing a “step” reduction in reactor power. The step reduction in reactor power is accomplished by the simultaneous dropping of one or two preselected groups of full strength regulating CEAs into the core. The CEA groups are dropped in their normal sequence of insertion. The RPCS also provides control signals to the turbine to rebalance turbine and reactor power following the initial reduction in reactor power as well as to restore the SG water level and pressurizer pressure to their normal controlled values. The system accommodates either large load rejections or loss of two main feedwater pumps.

The RPCS receives two of each of the following signals: reactor power cutback demand signals from the SBCS and loss of two feedwater pumps. A 2-out-of-2 logic is required to actuate the system for load rejections. The operator has the capability to manually actuate the system.

The predetermined pattern of appropriate CEA groups for use in the reactor power cutback is accomplished by CEA selection logic in the IPS. This logic utilizes NSSS power, CEA positions, and coolant temperatures, and provides the RPCS with the CEA groups selected for dropping during reactor power cutback. If the

APR1400 DCD TIER 2

IPS CEA selection logic is inoperable, the RPCS control logic can switch to the manual select mode. In the manual select mode, the operator inputs the CEA group drop selection through the RPCS soft control display. This feature increases the availability of the system.

The RPCS actuation initiates the dropping of the preselected pattern of CEAs upon receiving 2-out-of-2 coincidence signals indicating large turbine load rejection or loss of two feedwater pumps. There are inhibits in the DRCS to prevent the possibility of the RPCS dropping CEA groups that are not intended to drop for a reactor power cutback (e.g., part-strength groups, shutdown groups). Subsequent insertion of other groups either automatically by the RRS or manually by the operator occurs as necessary.

f. Boron control system

Information is supplied to the operator to allow regulation and monitoring of the boron concentration in the RCS. The RCS boron control is accomplished by dilution and boron addition using the CVCS. Refer to Subsection 9.3.4 for a description of the CVCS. To allow the operator to maintain the required boron concentration in the RCS, the volume control tank contents are maintained at a prescribed boron concentration either manually or automatically. To assist the operator in maintaining the proper boric acid concentration, indications of boron concentration are displayed as parts per million (ppm) on the QIAS-N and the IPS. These signals are supplied by the boronometer. Information on the FPD indicates reactor makeup water flow and boric acid makeup flow, which can be used to determine whether boron addition or dilution is occurring.

The boronometer detects the boron concentration by passing reactor coolant around a neutron source. Around the source are BF_3 neutron detectors. As the boron concentration decreases, the neutron flux increases.

At power, the boron concentration and the CEA position affect reactor coolant temperature. Because of the long time required to change the boron concentration, the boron is used for long-term effects such as fuel burnup and fission product build up. Boron concentration control is also used for load following. By adjusting the boron concentration, the CEAs can be withdrawn to provide an adequate shutdown margin. Boron control is provided by use of the P-CCS.

APR1400 DCD TIER 2

g. In-core instrumentation system

The in-core instrumentation system consists of core exit temperature (CET) instrumentation and in-core nuclear instrumentation.

The CET instrumentation consists of 61 thermocouples at fixed core outlet positions that measure the fuel assembly coolant outlet temperatures in the core.

Likewise, the in-core nuclear instrumentation consists of fixed in-core neutron flux detectors that are spaced radially and axially in sufficient numbers to permit the representative flux mapping of the entire core.

The in-core nuclear instrumentation is used to monitor the core power distribution, and the detectors are fixed in place at all times during operation.

There are 61 fixed in-core neutron flux detector assemblies with five self-powered Rhodium detectors and one background detector in each location. The 61 assemblies are distributed in the reactor core to optimize a core power distribution monitoring capability.

The five Rhodium detectors are axially distributed along the length of the core at 10, 30, 50, 70, and 90 percent of core height. This permits representative three-dimensional flux mapping of the core.

The Rhodium detectors produce a delayed beta current proportional to the neutron activation of the detectors that is proportional to the neutron flux in the detector region.

The signals from the fixed in-core neutron flux detector assemblies are processed by the fixed in-core detector amplifier system (FIDAS) and are sent to the IPS for monitoring and display. The IPS performs the background, beta decay delay, and Rhodium depletion compensation using in-core nuclear instrumentation signal processing programs.

The in-core nuclear instrumentation performs the following functions:

- 1) Provides data to determine the gross power distribution in the core during different operating conditions from 20 percent to 100 percent power

APR1400 DCD TIER 2

- 2) Provides data to estimate fuel burn-up in each fuel assembly
- 3) Provides data for the evaluation of thermal margins in the core

The fixed in-core neutron flux detectors can be used to assist in the calibration of the ex-core detectors by providing azimuthal and axial power distribution information.

The safety-related ex-core neutron flux monitoring system is used to provide indication of the flux power and axial distribution for the RPS.

h. Ex-core neutron flux monitoring system (non-safety channel)

The ex-core neutron flux monitoring system (ENFMS) includes two startup and control channels for startup and control. Each startup and control channel consists of one ENFMS detector assembly, one preamplifier assembly, and one startup and control signal processing drawer. The detector assembly and preamplifier assembly are shared with the corresponding safety channel. Each startup and control signal processing drawer processes the signals from any one of three safety channel preamplifier assemblies through the qualified isolators and provides the signal outputs for startup range monitoring and reactor power control. The startup and control channel flow diagram is shown in Figure 7.7-10.

Two startup signal processing drawers consist of logarithmic amplifier and test circuitry. Each drawer provides the startup channel neutron flux signal (readout and audio count rate information) to the reactor operator for use during extended shutdown periods, initial reactor startup, startup after extended shutdown periods, and following reactor refueling operations. The drawers have no direct control or protection functions.

Two control signal processing drawers consist of linear amplifier and test circuitry. Each drawer provides the neutron flux information in the power operating range of 0 percent to 125 percent to the RRS for use during automatic turbine load-following operation.

Startup and control signal processing drawers are independent of the safety channels.

APR1400 DCD TIER 2

i. Boron dilution alarm system

Reactivity control in the reactor core is affected, in part, by soluble boron in the RCS. The boron dilution alarm system (BDAS) utilizes the ENFMS startup channel neutron flux signals to detect a possible inadvertent boron dilution event while in Modes 3-6. The BDAS has two separate channels to provide reasonable assurance of detection and alarming of the event, and alarm signals are provided to the QIAS-N and the IPS.

When neutron flux signals increase (during Mode 3-6) to equal or greater than the calculated alarm setpoint, alarm signals are generated. The alarm setpoint is periodically lowered automatically to be a fixed amount above the current neutron flux signal setpoint. The alarm setpoint only follows decreasing or steady flux levels, not an increasing signal. The current neutron flux indication and alarm setpoint are available on the operator console in the MCR. There is also a reset capability to allow the operator to acknowledge the alarm and reinitialize the system.

j. Turbine control system

The turbine control system is described in Subsection 10.2.2.

k. P-CCS

The P-CCS controls non-safety components such as pumps, valves, heaters, and fans. It provides process variables and P-CCS status information to the IPS and QIAS-N.

The components are properly assigned to the group controller for system-level control and loop controller for component level control to minimize the plant impact due to system or component failures as shown in Figure 7.7-8.

Standardized logics for system or component are provided for the various types of components.

The group controller performs supervisory control of groups of components such as an alternate ac generator control system or T/G control system and provides

APR1400 DCD TIER 2

system-level status information to the IPS and QIAS-N. The P-CCS has master transfer function to disable MCR controls and to enable RSR controls.

The P-CCS loop controllers are located in the vicinity of the controlled component. The loop controller and internal data communications are redundant.

The P-CCS has soft control human-system interfaces (HSIs) on the information FPD.

1. Reduced inventory instrumentation

The following system is provided to aid in the prevention of a loss of shutdown cooling. The RCS reduced inventory instrumentation system provides a means of monitoring RCS water level, RCS temperature, SCS flow rate and temperatures, SCS pump and containment spray pump operation status, and SCS valve position during shutdown operations.

The refueling water level instrumentation includes wide and narrow range differential pressure sensors, ultrasonic level meters, and local sight glasses that monitor the level in each RCS hot leg. Additionally HJTC probes monitor level in the RV. These systems are also used to monitor RCS level during shutdown operations. The differential pressure sensors provide continuous redundant narrow and wide range indication during reduced inventory operations. Narrow range differential pressure sensors measure RCS level in the hot leg region. The narrow range instrumentation includes low, low-low, and high level alarms that annunciate in the MCR. The wide range differential pressure sensors measure RCS level from hot leg bottom to approximately 10 percent PZR level. The wide range differential pressure instrumentation is indicated in the MCR. The HJTC instrumentation also includes a low-level alarm that annunciates in the MCR.

The sight glasses provide a local measurement of the RCS level in the hot leg region. The sight glasses also provide low, low-low, and high level alarms that annunciate in the MCR. The ultrasonic level provides a measurement of the RCS level in the hot leg region. The ultrasonic level measurement also provides low and low-low level alarms that annunciate in the MCR.

APR1400 DCD TIER 2

The above-mentioned indication and alarms allow the operator to monitor the RCS level from the MCR during shutdown operations that require reduced RCS inventory.

RCS temperature is measured using the existing CET temperatures, HJTC unheated sensor temperatures, and RCS hot leg RTD temperatures. The CETs and HJTC unheated sensors have a high alarm. The RTDs have a high-level alarm annunciation. The CETs provide a high alarm for reduced inventory operation. The HJTC unheated sensor temperature is not available when the head is off.

Each train of the SCS has a measurement of SCS flow. This measurement provides indication of return flow to the RCS when either the SCS pump or containment spray (CS) pump is being used for shutdown cooling. Low flow is annunciated in the MCR.

To monitor the performance of the SCS and CS pumps, pump suction pressure, discharge pressure, and motor current are monitored and annunciated in the MCR.

The performance of the SCS heat exchanger is monitored and annunciated by measuring the temperature in the inlet and return lines. Valve position indication provides indication of the system lineup and provides the status of the available flow paths.

m. Steam generator tube rupture detection instrumentation

Instrumentation for steam generator tube rupture (SGTR) detection incorporates N-16 gamma detection with a scintillation detector and microprocessor based signal conditioning and processing on each main steam line of SG. The detection system alerts the operator of a SG tube leak condition during power operation and identifies which SG is affected.

The N-16 radiation detection and monitoring equipment further enhances the diagnosis of SG tube leaks or ruptures and provides the operator with more accurate information to assess the condition of the plant. Detectors are mounted close to the main steam lines in the auxiliary building to detect radioactivity due to a SG tube leak or rupture.

APR1400 DCD TIER 2

To provide reasonable assurance that a detected condition is not missed, the N-16 detection system latches the alarm when an initial increased N-16 condition is detected, since the detected condition may clear as soon as the reactor is tripped or shutdown. This feature preserves the information to support subsequent diagnostic or control responses. To provide reasonable assurance that an alarm acknowledgment does not reset this latch, the alarm latch needs to be reset manually by an operator. The detection and alarm logic for N-16 is shown in Figure 7.7-11.

n. Control signal validation

Where there are more than two identical process parameter inputs including control and protection systems, a valid process representative value (PRV) calculated in the IPS can be used to select a valid control signal, where necessary.

The control system takes action based on a sensor signal that is selected by a PRV that reflects good process signals. Therefore, there are fewer challenges to plant safety due to control system errors, since failed sensors are detected and eliminated before they adversely impact control system performance.

The signal validation logic functions as follows:

- 1) A PRV for an input channel selection is received from the IPS.
- 2) Input channels are compared to each other for a deviation check.
- 3) If the deviation between the input channels is within an acceptable level, the average value of the input channels is selected. If the deviation exceeds an acceptable level, the input channel that has less deviation from the PRV is used as the controlling signal within the control system(s).
- 4) When the PRV is out of predetermined operating range, an alarm is generated. The operator can select an input channel to be used.

o. Severe accident systems

The following systems are provided to address severe accident conditions:

- 1) Cavity flooding system (CFS)

APR1400 DCD TIER 2

2) Hydrogen mitigation system (HMS)

3) Remote control center (RCC)

a) Cavity flooding system

The CFS provides a means of directing flow from the in-containment refueling water storage tank (IRWST) to flood the reactor cavity in the event of a severe accident. The CFS is controlled manually from the MCR. Electrical power distribution is defined in Section 8.3.

IRWST instrumentation includes three level transmitters that provide independent level readout in the MCR. Level indication allows the operator to monitor the effect of any actions taken to flood the holdup volume tank (HVT) and reactor cavity.

Four isolation valves are provided in the spillway pipes between the IRWST and the HVT. Each valve has limit switches to indicate valve position on the ESF-CCS soft control module (ESCM) and information FPD in the MCR. Two valves are powered from Vital A power, and the other two are powered from Vital B power.

The HVT includes a level switch in each of the two sumps to alert the operator of the presence of water. Three level transmitters are also provided to indicate HVT level in the MCR.

Two isolation valves are provided to transfer water from the HVT to the reactor cavity. Each valve is provided with limit switches to indicate valve position in the MCR. One valve is powered from Vital A power, and one is powered from Vital B power.

Reactor cavity instrumentation consists of three level transmitters that provide indication of reactor cavity level in the MCR. A level switch in the sump provides an alarm in the MCR to alert the operator of the presence of water in that area.

b) Hydrogen mitigation system

APR1400 DCD TIER 2

The HMS allows adiabatic, controlled burning of hydrogen at low concentrations during degraded core accident conditions. Channelized HMS igniters are manually actuated from the MCR.

The HMS controls and instrumentation are described in Subsection 6.2.5. Electrical power distribution is described in Section 8.3.

c) Remote control center

The RCC against aircraft impact is designed in accordance with 10 CFR 50.150. The minimum equipment needed to maintain the reactor for 24 hours is provided to accomplish hot standby plant condition. The operator can shut down the reactor from the MCR ten minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to RCC using a transfer switch located in the MCR. The RCC is located separately from the MCR so that aircraft impact to the MCR does not adversely affect the RCC operation integrity.

The RCC panel has channelized Class 1E control and the associated signals are routed from Class 1E component. The non-Class 1E signals are routed from hardwired switches to the P-CCS loop controller as well as to the motor control center (MCC) through multiplexers.

7.7.1.2 MCR Facility

The MCR facilities are composed of the following major functional units:

- a. The MCR includes the MCR operator consoles, a large display panel (LDP), safety console, and adjacent offices.
- b. The computer room contains the IPS that monitors plant performance, drives various display units, and logs plant data.
- c. The RSR is designed to achieve an orderly plant shutdown and is isolated from the MCR.
- d. The technical support center (TSC) relieves the MCR operators of peripheral duties and communications and serves to reduce congestion in the MCR. The TSC is described in Section 13.3.

APR1400 DCD TIER 2

- e. The MCR facilities include I&C equipment rooms, non-Class 1E power/equipment rooms, and Class 1E power/equipment rooms.

The MCR is designed to accommodate NUREG-0800 Section 9.5.1.1 (Reference 1), which requires consideration of the exposure to fires that cause damage or require personnel evacuation. Redundant channels of Class 1E equipment are designed to accommodate separation by locating them in different unmanned I&C equipment rooms. Transfer switches are provided in RSR and I&C equipment rooms for transfer of controls from MCR to RSR. The I&C systems and HSI design prevents faults from either location from propagating to plant systems outside the MCR or RSR.

Refer to Section 3.11 for the definition of environmental design requirements (temperature, humidity, radiation, pressure) relevant to the I&C systems and HSI equipment. Monitoring of the environmental condition of the area where the equipment cabinets are located is provided by the HVAC system, which is described in Section 9.4, and by the fire protection system, which is described in Section 9.5.

The arrangements, layouts, and information displays and controls for MCR operator consoles, auxiliary panels, safety console, LDP, and remote shutdown console (RSC) are designed, verified, and validated in accordance with the human factors design criteria. A typical MCR overview is shown in Figure 7.7-13, and the layout of the MCR is shown in Figure 7.7-14.

MCR and Consoles

Compliance with GDC 19 is achieved by implementation of the MCR.

The main operating area of the MCR is designed to continuously accommodate the normal and shift operating staff defined in Chapter 18 during emergencies.

The MCR, which includes offices adjacent to the main operating area, is able to accommodate the operating staff as defined in Chapter 18.

The MCR provides operator consoles, safety console, LDP, auxiliary panel, and other equipment necessary for the safe and reliable operation of the plant.

Each operator console contains information FPDs, pointing devices, and ESCMs.

APR1400 DCD TIER 2

The safety console contains ESCMs, a mini LDP, QIAS-N FPDs, QIAS-P FPDs, a diverse indication system display, operator modules, diverse manual ESF actuation switches, minimum inventory switches including reactor trip switches, and manual ESF system-level actuation switches.

The MCR operator consoles and safety console are seismically qualified to perform their safety functions during and following a seismic event.

The MCR operator consoles and safety console are designed to provide reasonable assurance of an adequate HSI while meeting requirements for independence of redundant circuits.

To minimize the potential for multiple channel damage within the MCR console or RSC, the following design features are employed:

- a. Low energy circuits (switch contact and lamps) are used to the maximum extent practical.
- b. Fire retardant non-metallic materials meeting UL-94 rating or equivalent are used throughout the MCR operator consoles, LDP, safety console, and RSC enclosures. The enclosures are equipped with smoke detectors. Fire-resistant insulation material for MCR operator consoles, safety console, and RSC wiring meets the applicable requirements of IEEE Std. 383.
- c. Electrical independence of channelized circuits is maintained throughout the MCR operator consoles and safety console enclosures.

Although the design features above minimize the potential for multiple redundant channel damage, the following design features accommodate such a catastrophic event:

- a. All MCR circuits are properly isolated from the electronics to which they interface. Similarly, all RSC circuits are properly isolated from the electronics. Therefore, the MCR operator consoles, LDP, safety console, and RSC circuits are inherently isolated from each other.
- b. All MCR operator consoles, safety console, and RSC circuits are designed passively. Momentary contacts are used for all switches with the memory of MCR operator consoles and safety console commands retained only in electronics

APR1400 DCD TIER 2

located in the I&C equipment rooms. This passive design is used for discrete state component controls, setpoint change commands, and position change commands from process controllers for analog components. This passive design provides reasonable assurance that transfer of control from the MCR to the RSR (or vice versa) is bumpless (i.e., no setpoints or component states are affected). This design also provides reasonable assurance that all open circuit failures have no impact on control setpoints, modes, or component states.

The MCR, RSR, and I&C equipment rooms are located in separate fire zones. Therefore, the plant can be safely shut down with a catastrophic fire in the MCR, the RSR, or any one of the I&C equipment rooms.

Transfer switches are provided in the RSR and I&C equipment rooms for transfer of control from the MCR to the RSR. If a fire is detected within the MCR consoles, as indicated by an early warning smoke detector, the operator actuates the switches. Actuation of the switches initiates each channel of the ESF-CCS and each channel of the P-CCS to perform a soft transfer to deactivate the MCR consoles as a control interface and to activate the RSC control interface. The MTP provides interlocks for performing the transfer of control from the MCR to the RSR.

TSC and ERF Interfaces

The guidance for the TSC and the ERF is defined in NUREG-0696. The guidance provides basic design and qualification criteria for the onsite TSC, operation support center (OSC), the near-site emergency operations facility (EOF), and the emergency response data system (ERDS).

NRC RG 1.97 (Reference 2) specifies associated design criteria for monitoring accident situations. The SPADES+ provides the capability for integrated human factors presentation and retrieval of accident monitoring information.

The IPS provides the necessary interfaces with the TSC, EOF, and ERDS to make the same information that is available to the operating staff available to other interested personnel. The IPS equipment includes workstations and printers installed as shown in Figure 7.7-12 and described further in Subsection 7.7.1.4.

7.7.1.3 LDP

The large display panel (LDP) provides a single location to allow for a quick assessment of key information on critical safety functions. The LDP displays information that both the operators and supervisory personnel use for quickly assessing the status of the plant.

The LDP indicates existence of key alarms, deviations from control setpoints, key parameter values, and system operational status in a schematic representation. The LDP is implemented as a large board mimic display located in the front of operator console in the MCR.

The plant systems represented on the LDP are the major heat transport path systems and systems that are required to support the major heat transport process. The systems include the required bypassed and inoperable status indications (BISIs) that are required per NRC RG 1.47 (Reference 3).

a. LDP configuration

The LDP is configured with fixed mimic sections and variable display sections.

b. LDP display

The LDP display is driven by the IPS. Component and system status, operable condition and deviations from control setpoints are calculated by the IPS and transmitted to the LDP. Individual validated key parameters, alarm and parameter trends are based on calculations by the IPS for display on the LDP.

In the event of failure of the IPS, the operator uses the mini LDP driven by QIAS-N on the safety console. The QIAS-N provides alarms, values, and trends. The operator uses QIAS-N displays to assess operational availability and performance of the plant systems.

The mini-LDP is designed to maintain physical integrity during seismic events.

HFE considerations and features of the LDP are described in Subsection 18.7.

7.7.1.4 IPS

The information processing system (IPS) is a computer based system that provides operational means for monitoring and control of the plant. The information is derived from other I&C systems and self-contained algorithms called application programs. The IPS makes the information available to the plant operating staff both on a real-time and historical basis.

The IPS is designed to enhance overall power plant operability, availability, and efficiency. These are accomplished through the use of integrated plant information displays and advanced alarm design. Analysis of data assists the operating staff in operating the plant within specified limits while evaluating the performance of the reactor core, primary and secondary plant systems and components.

The IPS performs a supervisory monitoring and control function for the NSSS and BOP steam and electrical production processes. It allows the operating staff to obtain detailed plant data by use of its HSI displays. These HSI devices are integrated into the MCR in a manner that meets the Style Guide (Reference 4) that is described in Chapter 18.

The major functions performed by the IPS include plant wide data acquisition, validation of sensed parameters, execution of NSSS application programs and BOP performance calculations, monitoring of plant safety and general status, presentation of status and calculation results on IPS displays, provision of logs, and determination of alarm conditions.

a. IPS functions

The IPS performs comprehensive algorithmic processing of input data. Output results from this processing are transmitted externally to other systems, as required, and is made available to the operating staff via IPS displays and the LDP.

The major functions performed by the IPS include:

- 1) Acquires plant I/O data from the other plant systems via a data communication network
- 2) Performs application processing on the acquired data via NSSS, BOP and general plant monitoring program tasks

APR1400 DCD TIER 2

- 3) Provides detailed plant process data to the operating staff via IPS displays and the LDP
- 4) Provides data archive and retrieval functions
- 5) Provides safety parameter displays to assist the operating staff during abnormal or accident conditions and provides this data to the staff in the MCR, RSR, TSC and EOF
- 6) Processes for alarm signals and alarm controls including cross check with the QIAS-N alarms
- 7) Generates log reports
- 8) Supports the operating staff's control actions including selection of control objects
- 9) Performs on-line diagnostics for continuous self-health monitoring
- 10) Performs signal validation on input signals
- 11) Determines a representative value for a given parameter being sensed by multiple sensors
- 12) Accommodates a failure of any single hardware element so that no single failure within the IPS can disable any of the aforementioned functions; hardware redundancy coupled with continuous on-line diagnostics provides high availability

The advanced alarm processing described in Section 18.7 is built into the IPS to minimize the number of alarms (via alarm grouping and prioritization) and generation of spurious alarms (nuisance alarms). Alarm priority categories are established to inform the operating staff of the relative importance of any alarm.

The IPS is designed with sufficient alarm buffer so that no alarm is "lost" during a high influx of alarms.

b. IPS configuration

APR1400 DCD TIER 2

The IPS consists of redundant servers, display devices, data storage devices, printers, and other support devices. The redundant servers perform application processing of the received data and transmit computed results to the IPS display and the LDP.

The IPS architecture is based on a distributed fault tolerant design. A data communications network acquires plant process data from other plant systems and transmits it to the IPS.

The IPS is configured as follows:

IPS servers

The IPS application functions and alarm processing functions are executed via redundant IPS servers. One server is the primary (active) unit and the other is a dedicated backup. If the primary IPS server experiences a failure, its dedicated backup server assumes all processing tasks of the failed unit. The IPS servers communicate with LDP, operator consoles, and engineering stations via data communication network.

The IPS application functions minimize processor loading, simplify task scheduling, and minimize the potential for unintended interactions among application tasks.

Engineering station

An engineering station is used for engineering tasks such as configuring application software and developing building graphics and databases. In addition, the station supports maintenance, testing, and system diagnostics of the IPS.

Information flat panel displays

Information FPD consists of a flat panel display, pointing device, display processor and communication interface. Each information FPD is driven by a dedicated display processor.

The display system communicates with the IPS servers and engineering station over a data communication network. The ESCMs connected to the information FPD are physically and electrically isolated from the IPS.

APR1400 DCD TIER 2

If a data communication error occurs, an appropriate message is generated. Diagnostic tests are then performed to identify the cause of the data communication error.

IPS software is composed of modular and structured programs. The developed code is confirmed for consistency throughout the source listings.

c. IPS environmental qualification

The IPS is a non-safety system that performs non-safety related functions, and is not required to operate during or after a seismic event. However, the IPS is seismically qualified for structural integrity so that no control room missile hazards result as a consequence of a seismic event.

Qualification is performed by test and/or analysis. The IPS is designed to operate over the environmental range specified for the MCR equipment per Sections 3.10 and 3.11. The IPS cabinets are provided with a temperature switch and associated alarm in the MCR to alert the operator if the temperature within a cabinet reaches the upper limit specified for the environment in that location.

d. Application programs

The nuclear application programs noted herein are implemented in the IPS and provide information to assist the operator with maintaining the plant within specified limits and with evaluating the performance of the reactor core.

SPADES+

The SPADES+ application program provides the operator with functions to continuously monitor the status of the critical safety functions and to assess the success paths that are available to maintain control of the critical plant functions. SPADES+ information is organized within the plant process information hierarchy in a manner that supports the plant-specific implementation of an emergency operating procedure (EOP). SPADES+ is designed to meet the criteria for safety parameter display system (SPDS) set forth in NUREG-0696 and NUREG-0737, Supplement 1.

APR1400 DCD TIER 2

SPADES+ monitors the status of the critical safety functions during normal, abnormal, and emergency operating conditions and provides alarms when any of the critical safety functions is not being maintained.

SPADES+ provides the capability to display the status of the following critical safety functions:

- 1) Core reactivity control
- 2) Maintenance of vital auxiliaries
- 3) Reactor coolant system inventory control
- 4) Reactor coolant system pressure control
- 5) Core heat removal
- 6) Reactor coolant system heat removal
- 7) Containment isolation
- 8) Containment temperature and pressure control
- 9) Containment combustible gas control (Radioactive emissions control)

SPADES+ provides the capability to display the success path status for each critical safety function and initiates an alarm when the function becomes inoperable.

Core Operating Limit Supervisory System

The COLSS consists of process instrumentation and algorithms used to continually monitor the limiting conditions for operation (LCO). A description of COLSS algorithms and a discussion of the treatment of COLSS input information are provided in Reference 5. The COLSS continuously calculates departure from nucleate boiling ratio (DNBR) margin, linear heat rate margin, total core power, core average axial shape index, and azimuthal tilt magnitude, and compares the calculated values to the LCO on the parameters. If a LCO is exceeded for any of these parameters, COLSS alarms are initiated and operator action is taken as required by the Technical Specifications.

APR1400 DCD TIER 2

The limiting safety system settings, core power operating limits, axial shape index, and azimuthal tilt operating limits are specified so that the following criteria are met:

- 1) The safety limit is not exceeded as a result of any anticipated operational occurrence (AOO).
- 2) The consequences of postulated accidents (PAs) are acceptable.

The RPS functions to initiate a reactor trip at the specified limiting safety system settings. The COLSS is not required for plant safety since it does not initiate any direct safety-related function during AOOs or PAs. The Technical Specifications define the LCOs required to provide reasonable assurance that reactor core conditions during operation are no more severe than the initial conditions assumed in the safety analyses and in the design of the low DNBR and high local power density trips. The COLSS serves to monitor reactor core conditions in an efficient manner, and provides indication and alarm functions to aid the operator in maintenance of core conditions within the LCOs of Technical Specifications.

The COLSS algorithms are executed in the IPS. The calculation speed and capacity of the IPS enable numerous separate plant operating parameters to be integrated into three easily monitored parameters: (1) margin to a core power limit (based upon DNBR limits, COLSS linear heat rate, and licensed power limits); (2) azimuthal tilt; and, (3) axial shape index.

If the COLSS is not provided, maintenance of reactor core parameters within the LCOs, as defined by the Technical Specifications, would be accomplished by monitoring and alarming on the separate non-safety related process parameters used in the COLSS calculations. Therefore, the essential difference in using COLSS in lieu of previous monitoring concepts is the integration of many separate process parameters into a few easily monitored parameters. The conciseness of the COLSS displays on the IPS has distinct operational advantages because the number of parameters that are monitored by the operator is reduced.

The following COLSS parameters are continually available to the operator via the information FPD.

- 1) Linear heat rate core power operating limit

APR1400 DCD TIER 2

- 2) DNBR core power operating limit
- 3) Total core power
- 4) Margin between core power and nearest core power operating limit
- 5) Axial shape index

The COLSS alarms are initiated if:

- 1) Core power exceeds a core power operating limit
- 2) Axial shape index exceeds its limits
- 3) Azimuthal tilt exceeds the azimuthal tilt limit

Technical Specifications for the reactor core provide an alternate means of monitoring the LCOs in the event that the IPS is out of service. When the IPS is out of service, Technical Specifications specify that the core protection calculator (CPC) DNBR calculation be used to monitor the margin to the DNBR limit.

A functional block diagram of the COLSS is provided in Figure 7.7-9.

Control element assembly application program

The CEA application program is provided to help the operator monitor CEA-related Technical Specifications as follows:

- 1) Power-dependent insertion limits are operating limits on the allowable insertion of the full-strength (regulating) CEAs as a function of reactor power.
- 2) Individual CEA position sensing and group position calculations are performed by the DRCS, and the results of calculations are transmitted to the IPS for the other applications.
- 3) The CEA application program monitors the insertion and withdrawal sequence of CEA groups.
- 4) The CEA application program monitors the insertion and withdrawal sequence of CEA groups. A contact output signal for out-of-sequence

APR1400 DCD TIER 2

alarming is generated if improper sequence or separation between CEA groups is detected.

- 5) CEA exposures are calculated every hour and reported once a day.

Deviation and setpoint monitoring program

The IPS performs deviation and setpoint monitoring for two multichannel, separate systems: the core protection calculator system (CPCS) and the plant protection system (PPS). Data received from these systems consist of sensor inputs, setpoints, and calculated values.

Reactor coolant pressure boundary leakage program

The IPS calculates and records reactor coolant pressure boundary (RCPB) leakage. Leakage detection systems are described in Subsection 5.2.5.

The IPS calculates reactor coolant total leak rate, identified leak rate, and unidentified leak rate at normal operation.

The application programs described above are intended to assist the plant operator in the supervision or analysis of plant conditions.

Computer-based procedure system

The computer-based procedure (CBP) system is an application program and is used to display procedures during normal, abnormal, and post-accident plant operating conditions.

- e. Interface applications

The IPS interface applications are as follows:

Interface with soft control for non-safety components

The information FPD provides the soft control displays related to non-safety controls. The soft control interacts with the control system that performs plant control functions. The IPS does not perform any direct plant control functions; however, the IPS displays and the soft controls are interfaced functionally.

APR1400 DCD TIER 2

The information FPD provides an interface with the soft control such that a controllable plant component can be designated on an IPS display. The soft control display automatically presents the appropriate control template for the selected component on a mimic display page in the information FPD. The soft control is described in Section 18.7.

Interface with LDP

The IPS provides plant information periodically to the LDP as follows:

- 1) Plant process status including status of major plant systems, status of major system components, and values of parameters calculated by the IPS
- 2) Alarm and status data for fixed alarm tiles on the LDP including critical safety function, and bypassed and inoperable status indication (BISI) status information

IPS display pages are shown on the variable display area of the LDP.

The IPS provides an interface with the LDP so that alarms appearing on IPS display pages are acknowledged via an IPS display and also on the LDP.

Interface with ESCM

The Information FPD provides an interface with the ESCM such that it calls up a control template on the ESCM display. When a component symbol in the system mimic display on the information FPD is selected by the operator, the identification of the component is transmitted via a serial data link to the dedicated ESCM. In response to the identification information, the ESCM presents the control template for the selected component or variable.

f. Historical data storage and retrieval

All plant input parameters for the IPS are stored for review at two resolution rates as follows:

- 1) High resolution: All input points are stored in every second for 48 hours
- 2) Low resolution: All input points are stored in every minute for 2 weeks

APR1400 DCD TIER 2

Both high and low resolution rates of historical data can be transferred to the secondary storage by operator's demand. Operators can specify the time spans of the available historical data to be backed up in the secondary storage.

The historical data stored in a disk or other media are utilized for trending in the information FPDs and the LDP.

7.7.1.5 NSSS Integrity Monitoring System

The NSSS integrity monitoring system (NIMS) detects selected conditions that indicate deterioration or that could lead to deterioration of the RCS pressure boundary.

The NIMS is a non-safety monitoring system that consists of the internals vibration monitoring system (IVMS), acoustic leak monitoring system (ALMS), loose parts monitoring system (LPMS), and RCP vibration monitoring system (RCPVMS).

The IVMS monitors the motion of the reactor internals by using the ex-core neutron flux signals from the ENFMS detectors and provides diagnostic information that can be used to evaluate the reasons for changes in the motion of the reactor internals.

The ALMS detects a leak at specific locations or within specific components in the primary pressure boundary and provides information that is used to determine changes in the leak rate from specified components or at specified locations.

The LPMS detects the presence of loose part impacts within the major NSSS components, including the reactor vessel, steam generators, and RCP, and provides diagnostic information that allows plant system engineers to evaluate the impact location, energy, and mass of loose parts. The system is designed in compliance with NRC RG 1.133 (Reference 6).

The RCPVMS monitors the vibration levels of RCP motor and pump bearing assemblies. The RCPVMS also monitors the rotation speed and displacements of the RCP shafts.

The alarms generated by each system are provided to the operators in the MCR.

The failure of the NIMS has no effect on the function of the safety system.

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 non-safety control system design is based on the following design considerations.

7.7.2.1 Safety Classification

The control systems described in Section 7.7 are classified as non-safety systems. The safety analysis of Chapter 15 does not rely on the operability of any non-safety system control functions to provide reasonable assurance of safety. For safe shutdown, non-safety system control functions are not required, as described in Section 7.4.

7.7.2.2 Effects of Control System Operation upon Accidents

In the safety analysis addressed in Chapter 15, the effects of both control system action and inaction are considered in assessing the transient response of the plant for accidents and AOOs. If a non-safety control system helps to mitigate a transient, then the analysis of that transient assumes the system is in the manual mode of operation. The non-safety control system is assumed to be in the automatic mode of operation if that mode of operation makes the consequences of a transient more adverse.

7.7.2.3 Effects of Control System Failures

The control system failures due to failure do not cause plant conditions that are more severe than those described in Chapter 15. The results of the failure evaluation of control systems and the single failure list for the safety analysis are provided in Subsection 15.0.0.4 and Table 15.0-4. The safety analysis of Chapter 15 does not require these systems to remain functional.

Control groups and postulated events due to a single failure of a control group are described in Table 7.7-1.

7.7.2.4 Effects of Control System Failures Caused by Accidents

For the non-safety system, the controllers are located in mild environment locations and are not affected by AOOs and PAs. The worst-case non-safety control system single failure

APR1400 DCD TIER 2

that would aggravate the accident condition is assumed in the Chapter 15 safety analysis to accommodate the effects of non-safety control system failures that can be caused by accident conditions.

7.7.2.5 Environmental Control System

Environmental controls are provided to protect equipment from temperature, humidity, radiation, and ventilation conditions. Heating, ventilation, and air conditioning (HVAC) systems are provided as required throughout all areas for personal comfort, personnel safety protection, and equipment functional protection. Additional information for HVAC functions and ambient temperature control where I&C equipment is located is described in Section 9.4.

7.7.2.6 Use of Digital Systems

The non-safety control system and the safety system utilize different software and different platforms. The non-safety control system application software is developed using a structured process similar to that applied to the development of the safety system application software. This process includes a necessary quality program, including software V&V in accordance with the significance of control system. The software classes of the non-safety control systems are described in the [*Software Program Manual Technical Report (Reference 7).*]*

7.7.2.7 Independence

The non-safety control system is physically, electrically, and functionally independent of safety system.

7.7.2.8 Defense-in-Depth and Diversity

The non-safety control system and safety system are implemented on diverse platforms to preclude common-cause failure (CCF), which is described in the Diversity and the Defense-in-Depth Technical Report (Reference 8). A CCF in non-safety control systems is not considered.

The diverse protective functions that are designed to protect against potential CCF of the PPS and ESF-CCS are described in Section 7.8.

APR1400 DCD TIER 2

The control systems that are credited in the CCF Coping Analysis Technical Report (Reference 9) have sufficient quality to perform their intended functions.

7.7.2.9 Potential for Inadvertent Actuation

The non-safety control system design limits the potential for inadvertent actuation and challenges of safety system functions as follows:

- a. Non-safety control systems and safety systems use different hardware and software.
- b. The control systems have physical and electrical isolation and maintain communication independence from the safety system.
- c. Safety functions are not controlled by non-safety soft controls on the information FPD.
- d. For important control functions, multiple sensors are used, and a control signal validation algorithm is applied.
- e. The non-safety control system includes a control limit and interlocks that limit erroneous control actions, as shown in Table 7.7-2.
- f. Non-safety soft control is designed so that the demand signals are generated by two operator positive actions.

7.7.2.10 Control of Access

Equipment related to control systems not required for safety is administratively controlled by key locked doors on the equipment cabinets to protect against unauthorized access. The indication of access to the cabinets by door switches is provided in the MCR.

Access to the cabinets is normally required only during system testing, calibration or maintenance.

In addition to the security provisions provided by the above, system software is protected against unauthorized alterations. The protection includes setpoints and software coding by an administrative control of access to software media by the plant owner. Access to

APR1400 DCD TIER 2

workstations within the facility that have an access to control systems not required for safety is administratively controlled or password controlled.

7.7.3 Analysis

The safety analysis in Chapter 15 for AOOs and PAs does not require the operability of the non-safety control system. In addition, non-safety control system action/inaction and a single failure are bounded by the Chapter 15 analysis.

The plant control systems and equipment are designed for high reliability during steady-state operation and anticipated transient conditions. The control systems include the necessary features for manual and automatic control of process variables within prescribed normal operating limits. The control systems are powered by non-Class 1E redundant vital instrument buses where necessary to limit the potential for inadvertent actuation and challenges to safety functions.

Non-Class 1E systems that interface with Class 1E systems are designed so that credible failures in the control and monitoring systems do not impact the operation of Class 1E systems. The control system has physical and electrical isolation, and maintains communication independence from the safety system.

The HSI for MCR and RSR is designed in accordance with the Style Guide. These criteria meet the applicable TMI Action Plan guidance.

7.7.4 Combined License Information

No COL information is required with regard to Section 7.7.

7.7.5 References

1. NUREG-0800, "Standard Review Plan," March 2007.
2. NRC RG 1.97, Rev. 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," 2006.
3. NRC RG 1.47, Rev. 1, "Bypassed and Inoperable Status indication for Nuclear Power Plant Safety Systems," 2010.

APR1400 DCD TIER 2

4. APR1400-E-J-T(NR)-12005-P, “Style Guide,” September 2013.
5. CEN-312-P, Revision 1-P, “Overview Description of the Core Operating Limit Supervisory System (COLSS),” Combustion Engineering, Inc., November 1986.
6. NRC RG 1.133, “Loose-Part Detection Program for the Primary System of Light-Water-Cooled Reactors,” May 1981.
7. *[APR1400-Z-J-NR-13003-P, “Software Program Manual Technical Report,” September 2013.]**
8. APR1400-Z-J-EC-13002-P, “Diversity and Defense-in-Depth Technical Report,” September 2013.
9. APR1400-Z-A-NR-13008-P, “CCF Coping Analysis Technical Report,” September 2013.

Table 7.7-1

Controller Grouping in the NSSS Control System

Controller Group	Control System	Postulated Event Due to a Single Failure in the Corresponding Controller Group ⁽¹⁾					
		Excessive or Deficient Feedwater Flow	Full Open of Any One TBV	Excessive Charging Flow or Deficient PZR Spray	Uncontrolled CEA Withdrawal	Inadvertent Deboration	Related Section
Group 1 Controller	SG 1 Feedwater Control (FWCS 1)	×					15.1.2
Group 2 Controller	SG 2 Feedwater Control (FWCS 2)	×					15.1.2
Group 3 Controller	PZR Pressure Control (PPCS)			×			15.5.2
Group 4 Controller	PZR Level Control (PLCS)			×			15.5.2
Group 5 Controller	Turbine Bypass Control (SBCS Main)		× ⁽²⁾				15.1.4
Group 6 Controller	Turbine Bypass Control (SBCS Permissive)		×				15.1.4
Group 7 Controller	Reactor Makeup Control (CVCS)					×	15.4.6
Group 8 Controller	Control Rod Control (RRS)				×		15.4.1, 15.4.2
Group 9 Controller	Control Rod Control (DRCS)				× ⁽²⁾		15.4.1, 15.4.2

(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 or safety systems, to limit the effect of this single controller failure.

APR1400 DCD TIER 2

Table 7.7-2

Control Limit and Interlocks on Digital Rod Control System

Related Section	Conditions of Interlocks	Functions
7.7.1.1	Upper Electrical Limit (UEL) and Lower Electrical Limit (LEL) signals from Reed Switch Position Transmitter (RSPT).	Interlock: Blocks control rod withdrawal or insertion on automatic, manual group and manual individual DRCS control modes.
7.7.1.1	Automatic Withdrawal Prohibit (AWP) signals from RRS and SBCS when T_{AVG} is much higher than T_{REF} , T_{COLD} is high, or any opening demand of TBVs is generated in accordance with excessive energy in the NSSS.	Interlock: Blocks control rod withdrawal on automatic DRCS control mode.
7.7.1.1	Upper Group Stop (UGS) and Lower Group Stop (LGS) function in the DRCS	Control Limit: Blocks control rod withdrawal or insertion on automatic and manual group DRCS control modes.
7.2.1.7, 7.7.1.1	CEA Withdrawal Prohibit (CWP) signal from PPS. Refer to Subsection 7.2.1.7.	Interlock: Blocks control rod withdrawal on automatic, manual group and manual individual DRCS control modes.

APR1400 DCD TIER 2

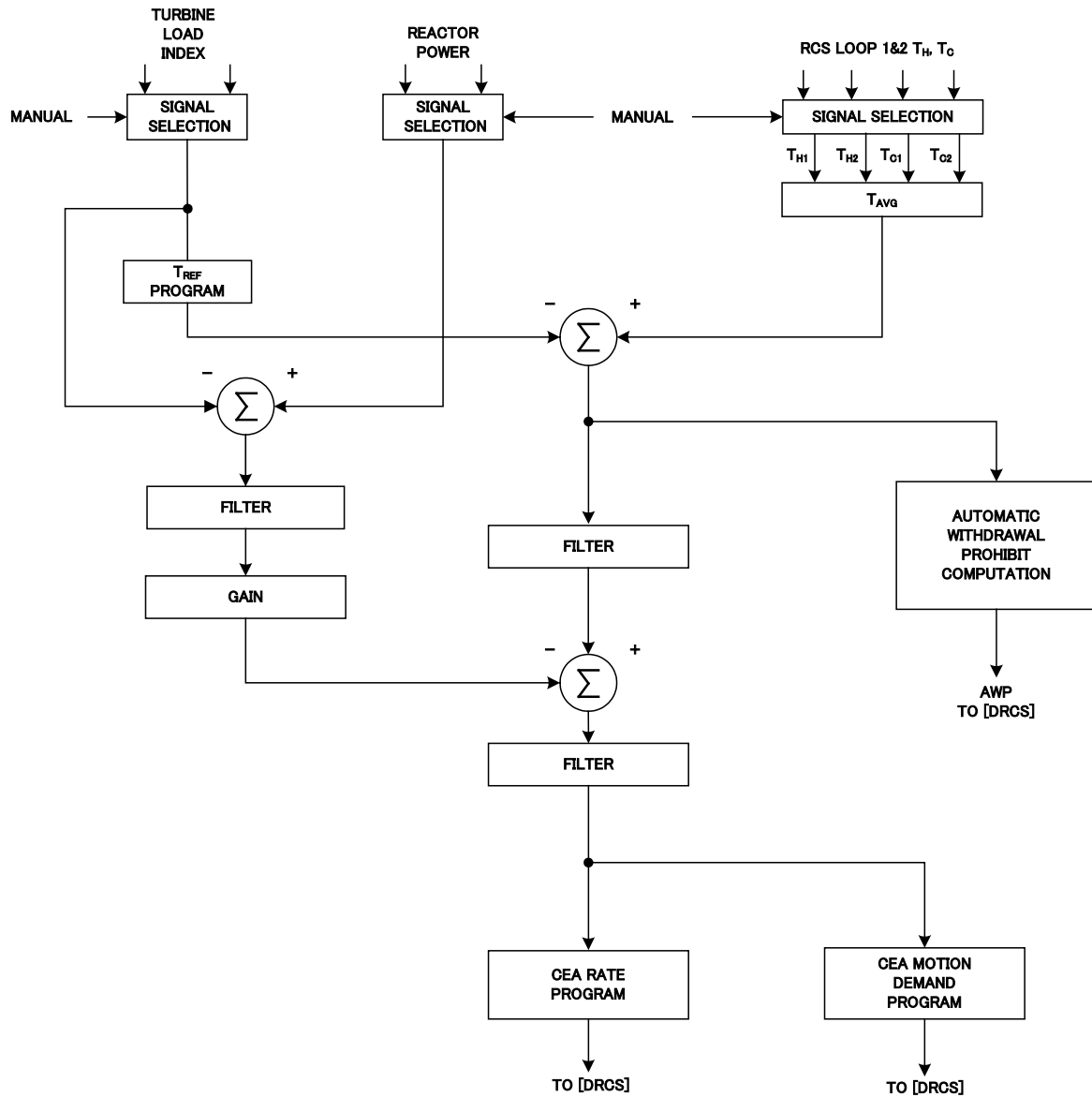


Figure 7.7-1 Reactor Regulating System Block Diagram

APR1400 DCD TIER 2

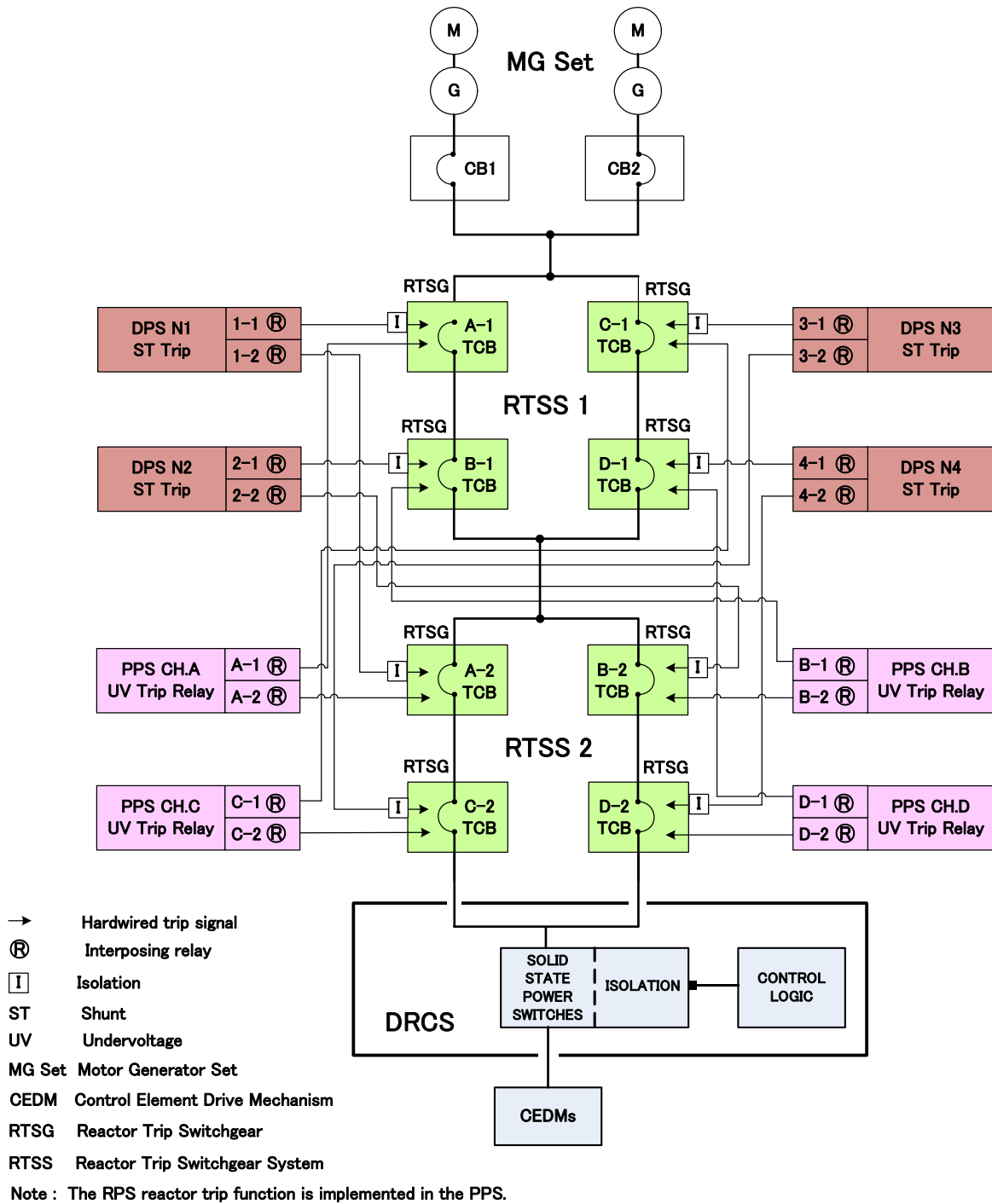


Figure 7.7-2 Digital Rod Control System - Reactor Protection System Interface Block Diagram

APR1400 DCD TIER 2

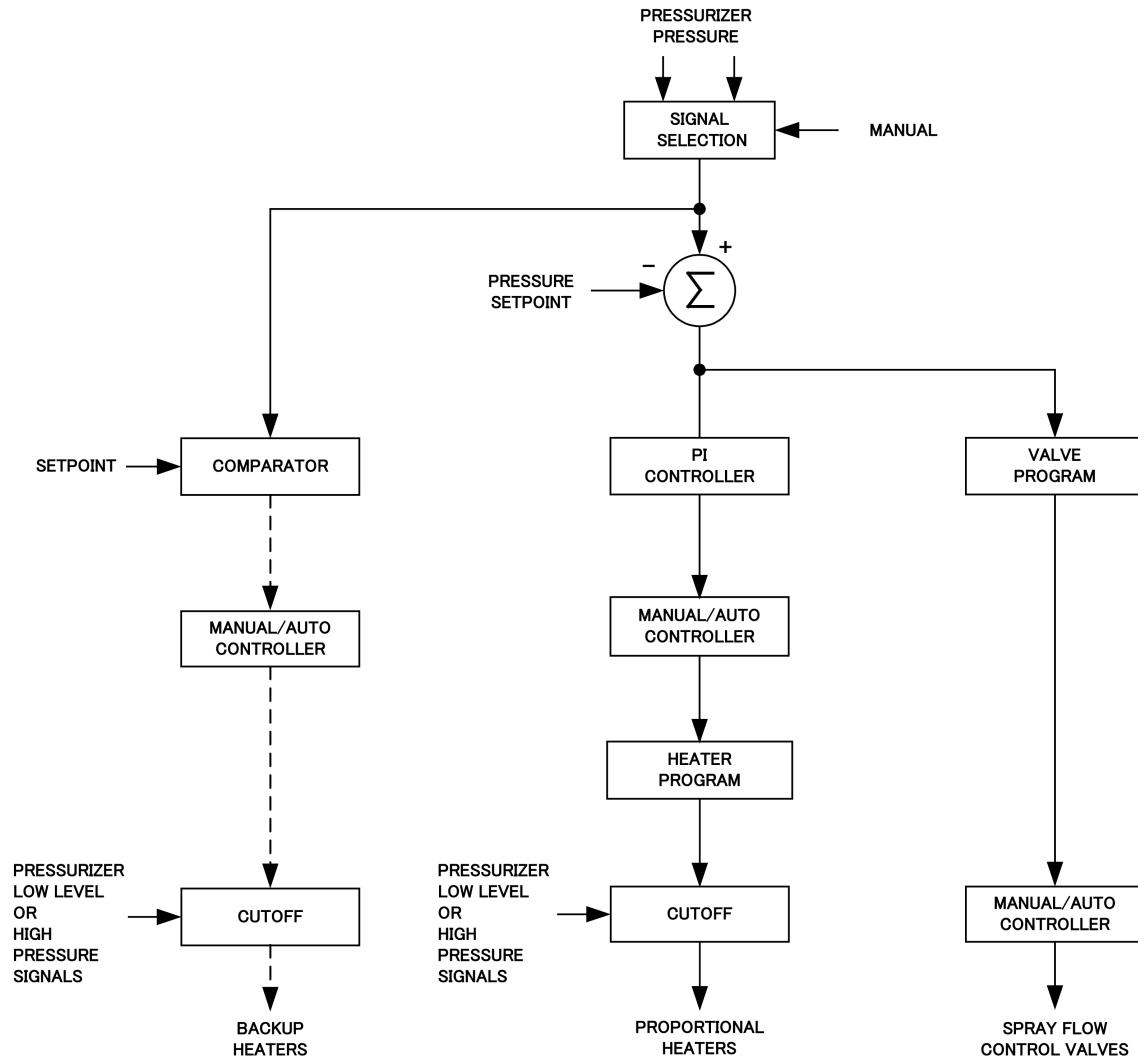


Figure 7.7-3 Pressurizer Pressure Control System Block Diagram

APR1400 DCD TIER 2

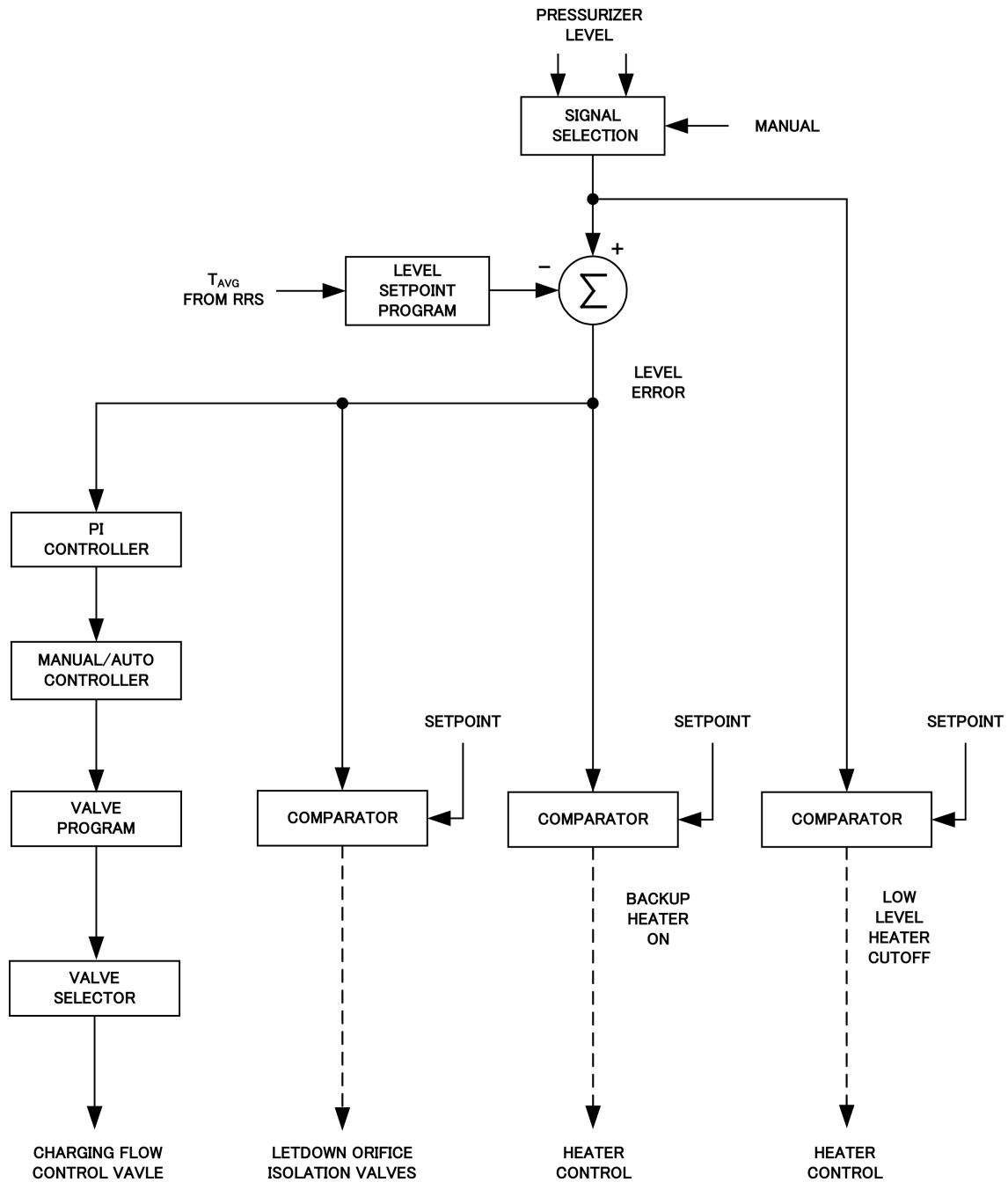


Figure 7.7-4 Pressurizer Level Control System Block Diagram

APR1400 DCD TIER 2

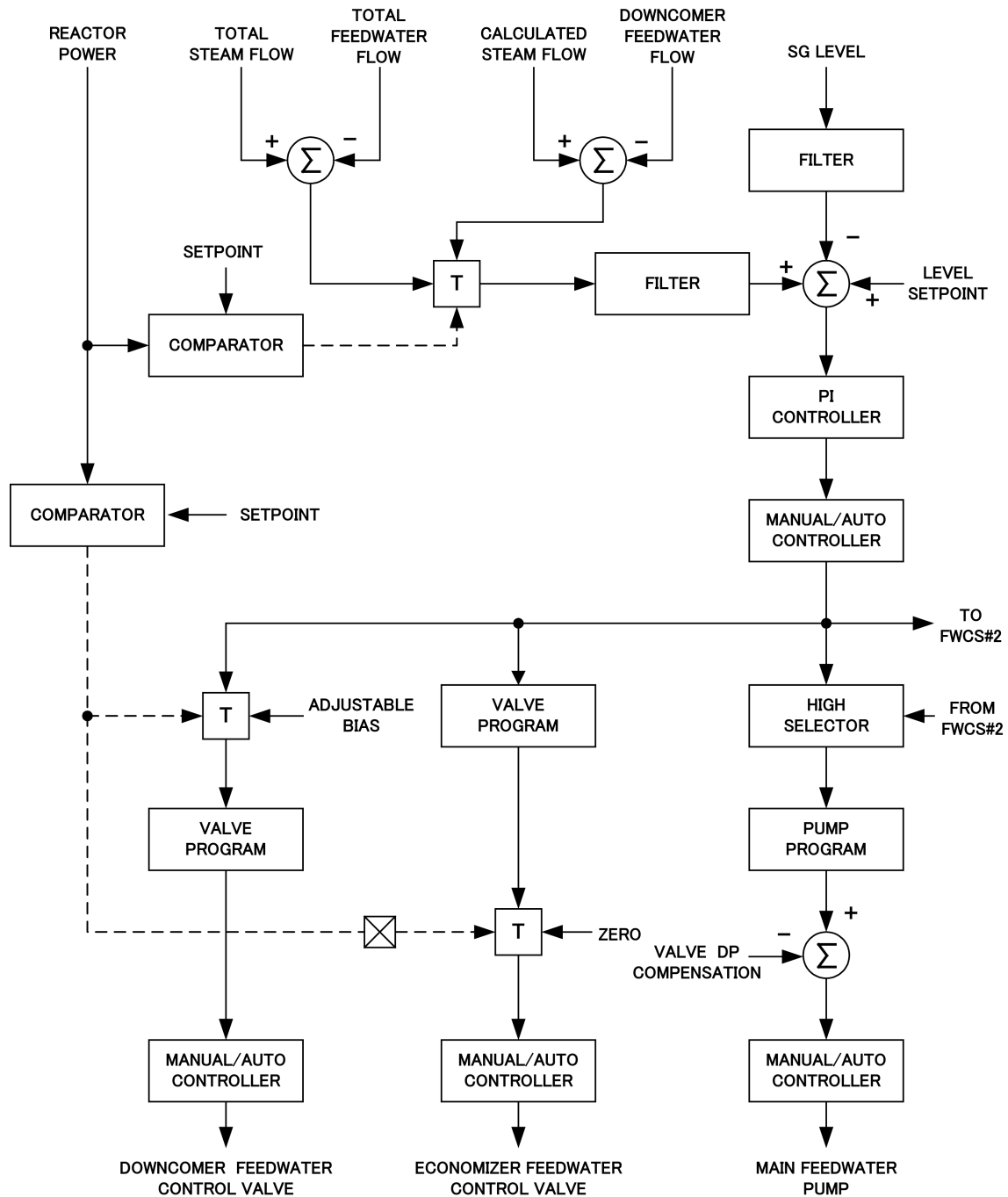
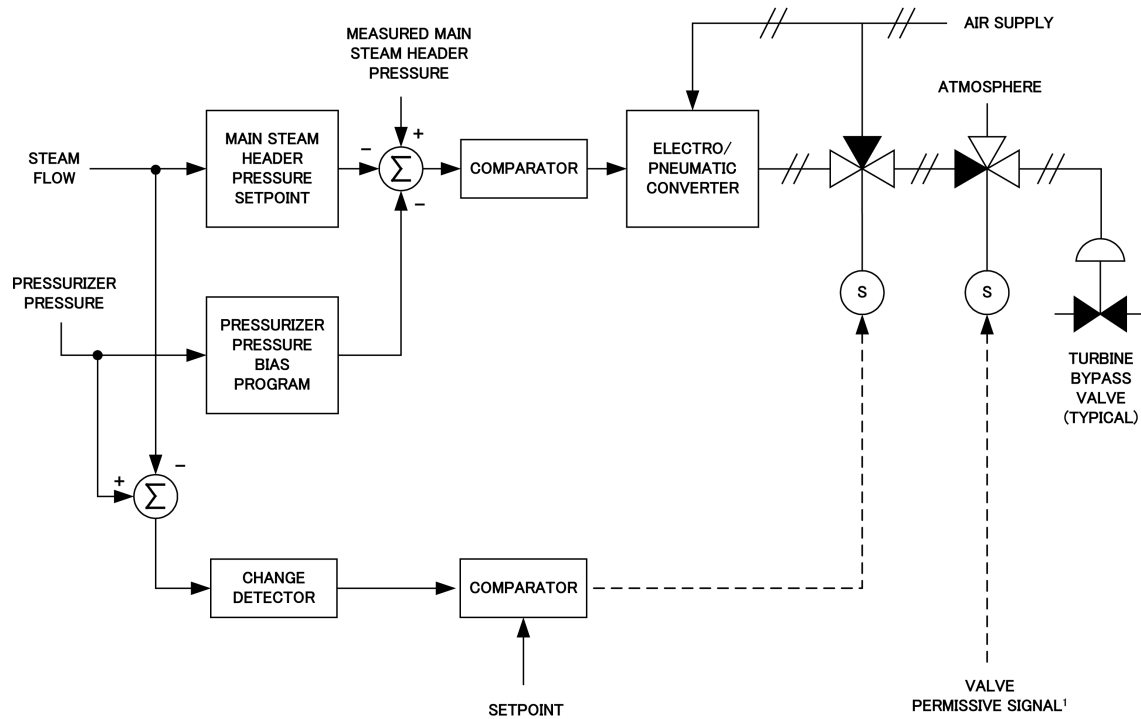


Figure 7.7-5 Feedwater Control System Block Diagram

APR1400 DCD TIER 2



NOTE 1 :

THE VALVE PERMISSIVE SIGNAL FROM A SEPARATE PERMISSIVE CONTROLLER IS PRODUCED BY SIMILAR CIRCUITRY.

Figure 7.7-6 Steam Bypass Control System Block Diagram

APR1400 DCD TIER 2

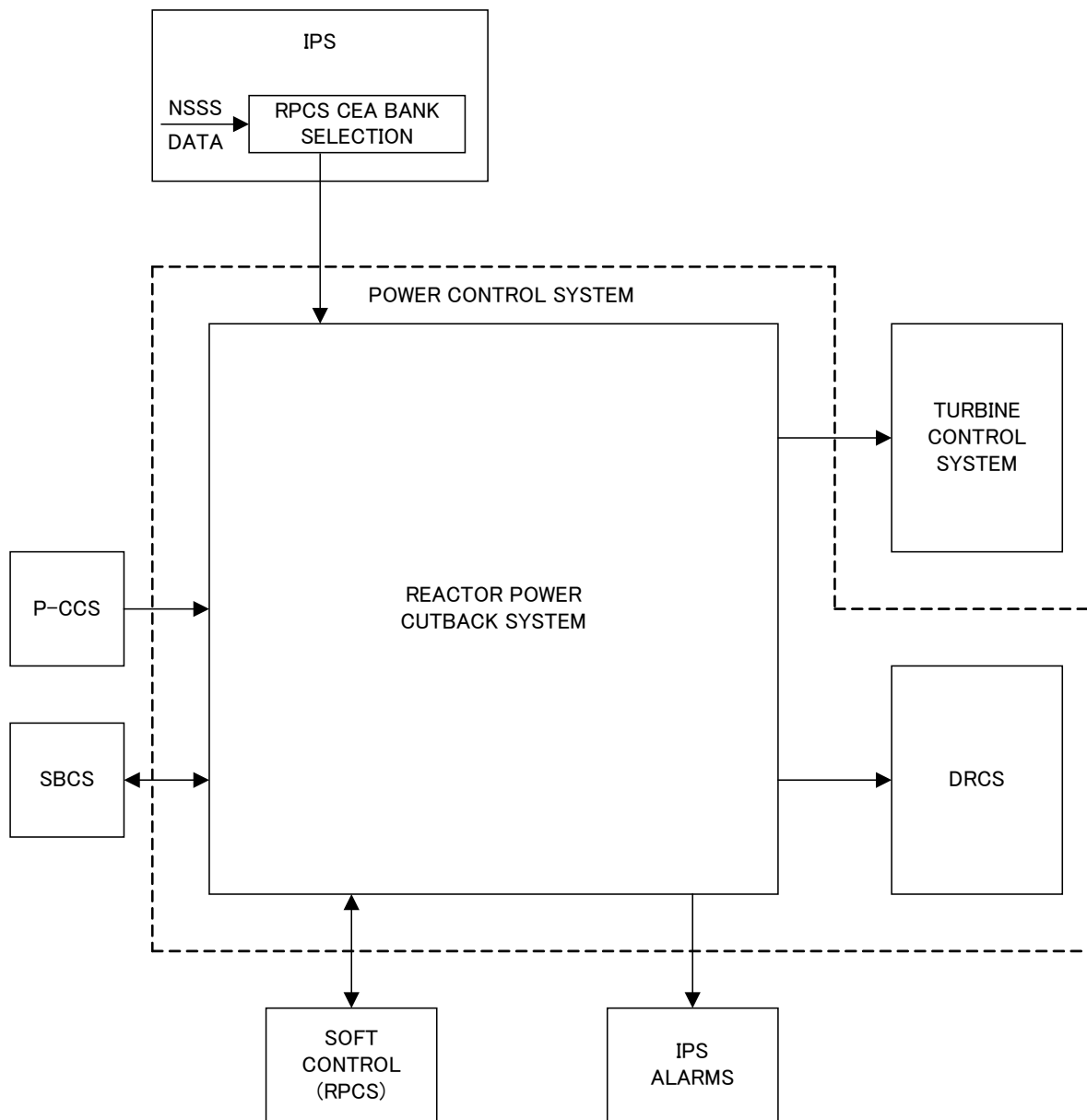
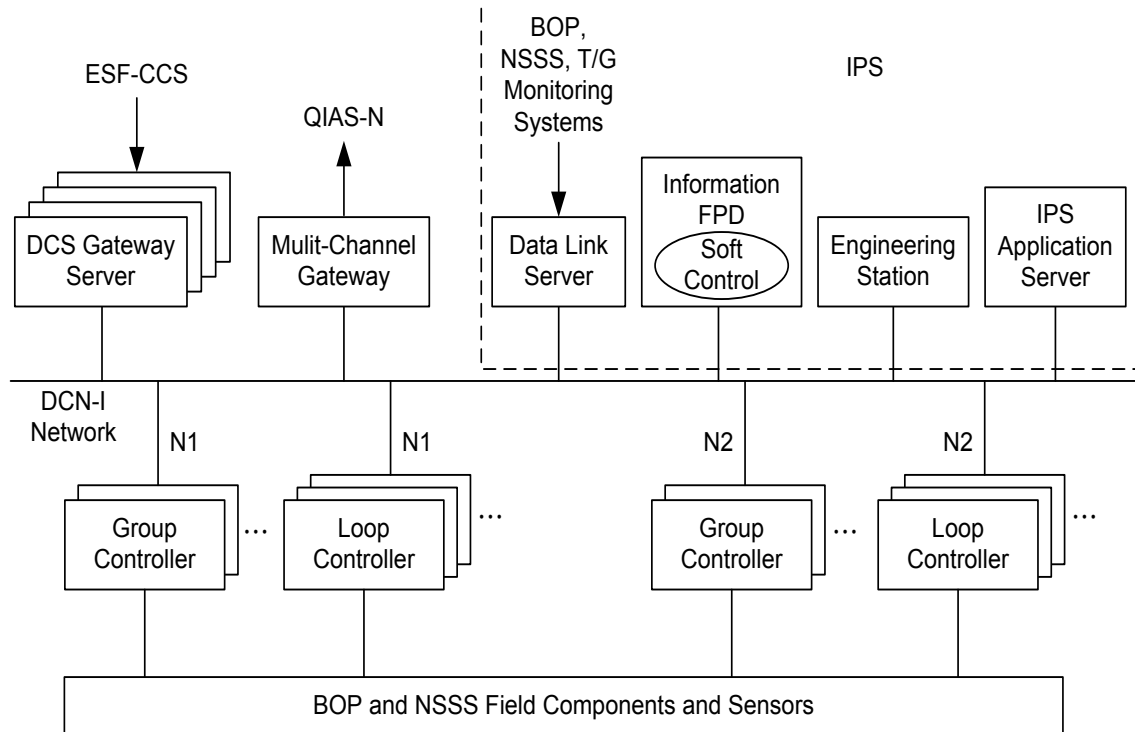


Figure 7.7-7 Simplified Block Diagram Reactor Power Cutback System

APR1400 DCD TIER 2



Abbreviations:

DCN-I : Data Communication Network
-Information

ESF-CCS : Engineered Safety Features
-Component Control System

FPD : Flat Panel Display

IPS : Information Processing System

QIAS-N : Qualified Indication and
Alarm System – Non-safety

Notes:

- (1) A duplicate subset of the main control room workstation are also located in the remote shutdown room.
- (2) Data communication networks are redundant between all controllers and the human system interfaces.

Figure 7.7-8 Process-Component Control System Simplified Block Diagram

APR1400 DCD TIER 2

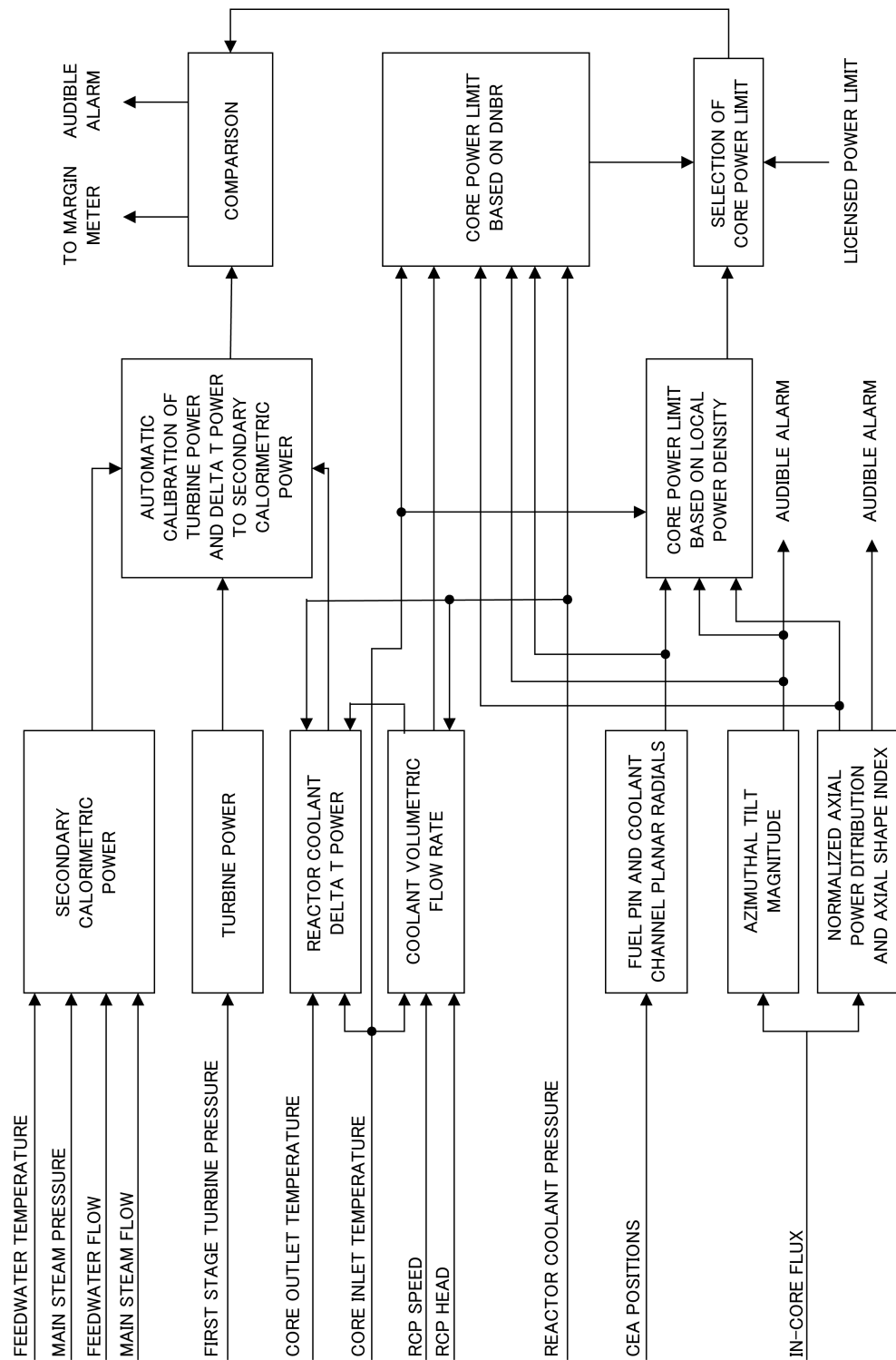
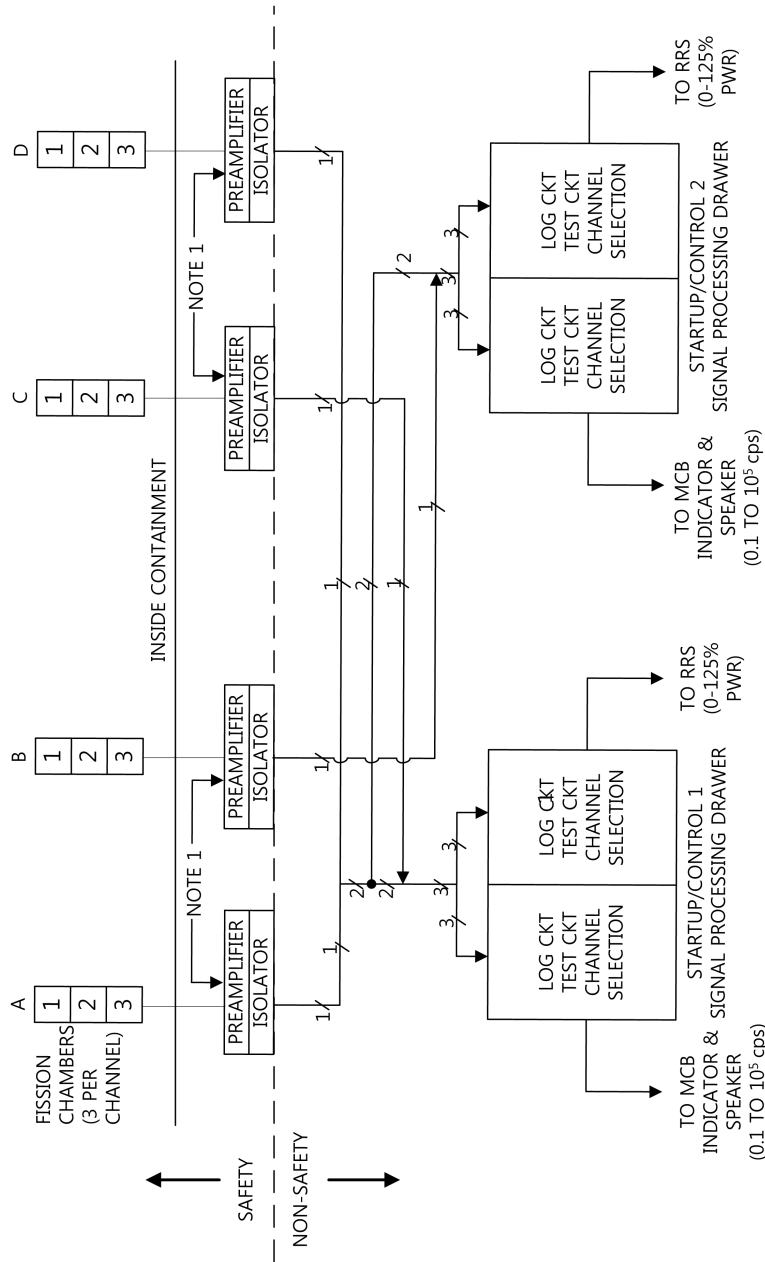


Figure 7.7-9 Core Operation Limit Supervisory System Functional Diagram



NOTE

1. FISSION CHAMBERS WHICH ARE SAFETY SENSORS PROVIDE THE NEUTRON FLUX SIGNALS FOR STARTUP CHANNEL AND CONTROL CHANNEL.
2. THE PREAMPLIFIER PROVIDES SIGNALS FOR STARTUP AND CONTROL FUNCTION THROUGH QUALIFIED ISOLATOR.
3. THE NUMBER SPECIFIED NEAR LINE IS CHANNEL QUANTITY.

Figure 7.7-10 Ex-Core Neutron Flux Monitoring System Startup and Control Channel Flow Diagram

APR1400 DCD TIER 2

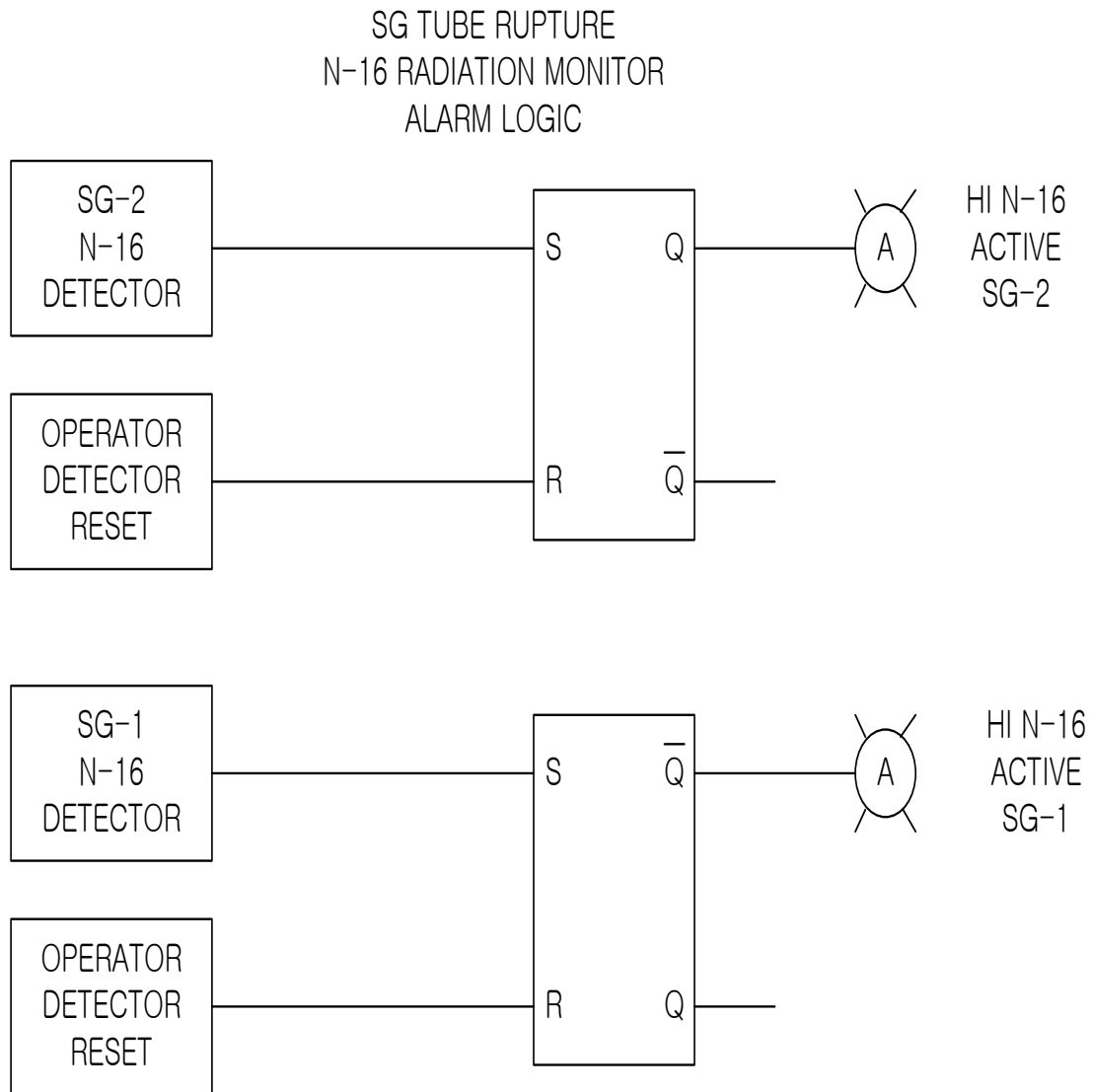


Figure 7.7-11 N-16 Detection and Alarm Logic

APR1400 DCD TIER 2

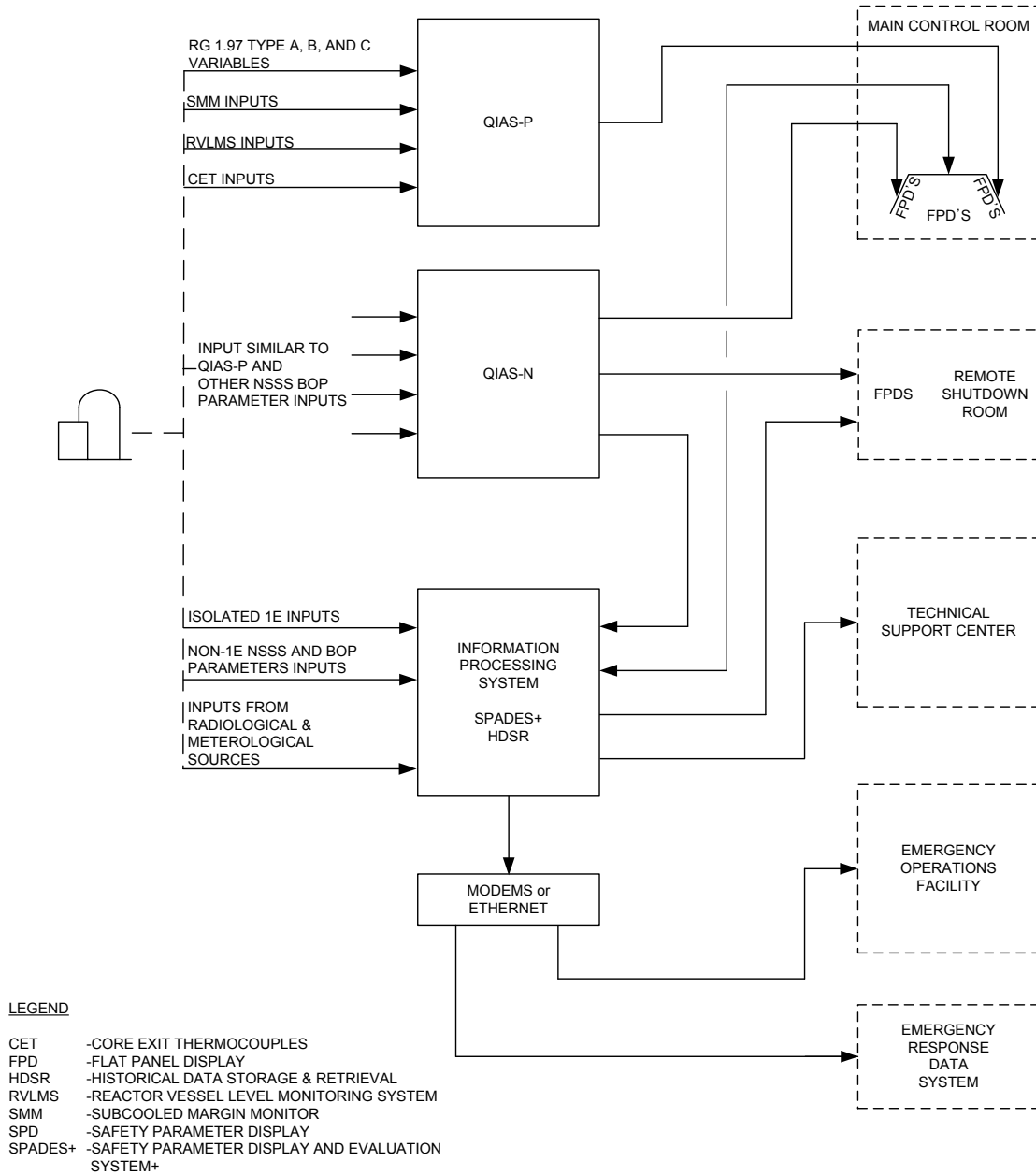


Figure 7.7-12 HSI Information Processing Block Diagram

APR1400 DCD TIER 2

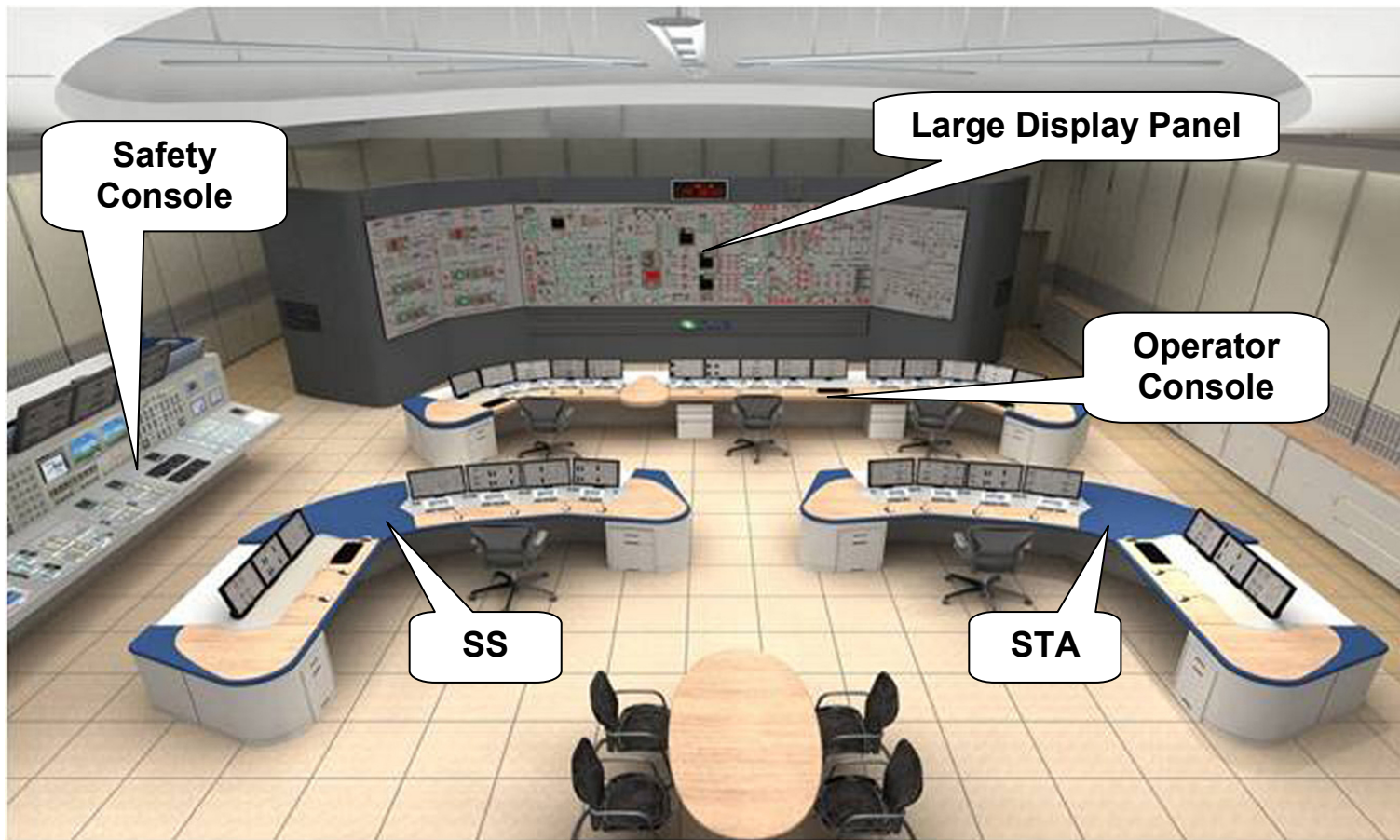


Figure 7.7-13 Typical Main Control Room Overview

APR1400 DCD TIER 2

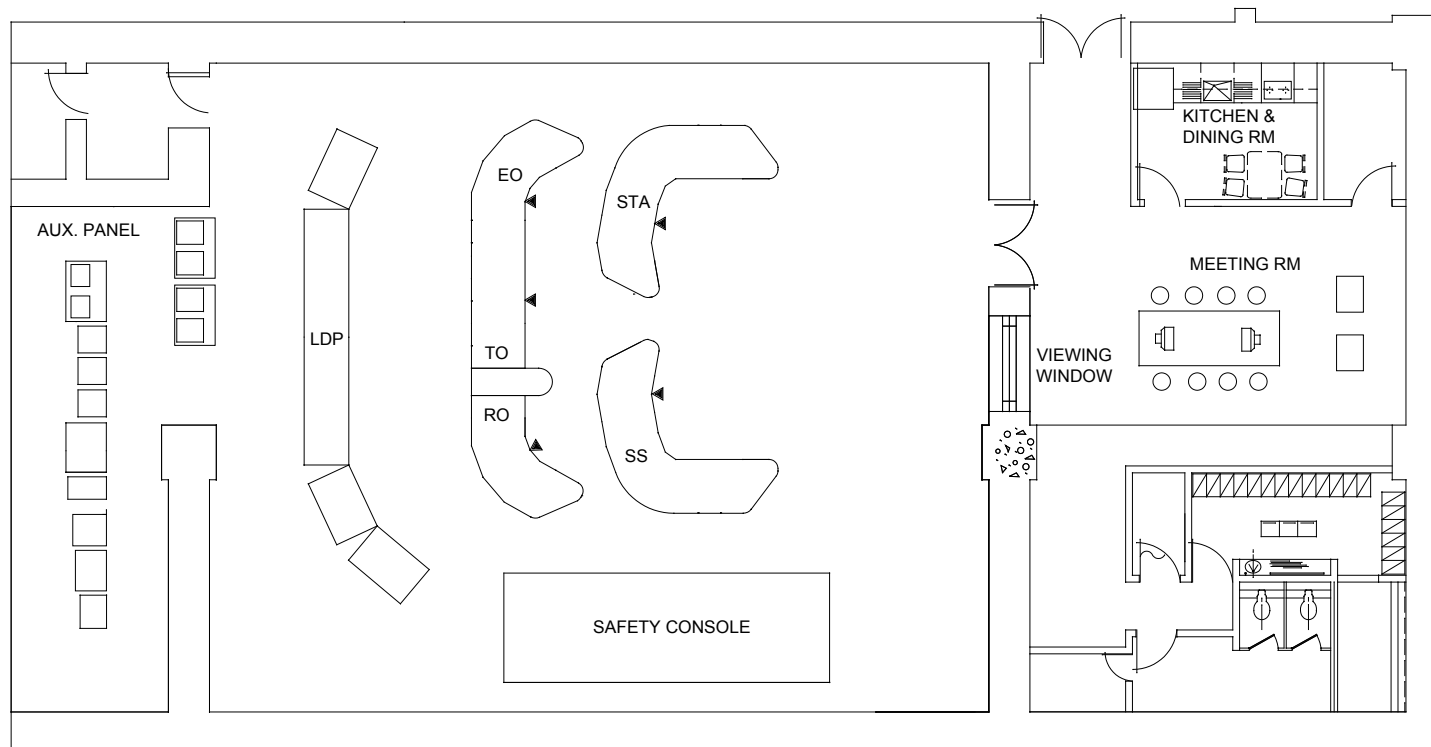


Figure 7.7-14 Layout of Main Control Room

7.8 Diverse Instrumentation and Control Systems

The diverse actuation system (DAS) consists of the diverse I&C systems that are provided to protect against potential common-cause failure (CCF) of the plant protection system (PPS) and engineered safety features-component control system (ESF-CCS). The design has sufficient diversity and defense-in-depth to tolerate the following beyond design basis events:

- a. Anticipated transients without scram (ATWS), which is defined as an anticipated operational occurrence (AOO) followed by failure of the reactor trip portion of the PPS.
- b. An AOO or a postulated accident (PA) concurrent with a software CCF that prevents the safety I&C systems from performing their required functions.

The DAS consists of the diverse protection system (DPS), the diverse manual ESF actuation (DMA) switches, and the diverse indication system (DIS).

For the ATWS mitigation, the DPS is provided in compliance with 10 CFR 50.62 (Reference 1). In addition, the DPS, DIS, and DMA switches are provided to comply with SECY-93-087 (Reference 2). The DPS and DMA switches are independent and diverse from the PPS and ESF-CCS. The DMA switches are located in the MCR for system-level manual actuation of critical safety functions.

A reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation functions are included in the DPS. These functions are provided to assist the mitigation of the effects of a postulated CCF within the PPS and ESF-CCS. The DMA switches are provided to permit the operator to actuate ESF systems in a timely manner from the MCR after a postulated CCF of the PPS and ESF-CCS. In addition, the DIS provides diverse indications to monitor critical variables and control the heater power for proper HJTC output signal level, when the CCF of digital I&C safety systems occurs.

APR1400 DCD TIER 2

7.8.1 System Description

7.8.1.1 Diverse Protection System

The DPS augments the PPS to address 10 CFR 50.62 requirements for the reduction of risk from ATWS events. In addition, the DPS assists the mitigation of the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS.

The DPS design includes a reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation functions.

The DPS reactor trip provides a simple and diverse mechanism to decrease the risk from the ATWS events and mitigates the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS, concurrent with a steam line break inside containment.

The DPS turbine trip is automatically initiated whenever the DPS reactor trip conditions are met.

The DPS auxiliary feedwater system (AFWS) actuation provides additional reasonable assurance that an ATWS event could be mitigated if it occurred.

The DPS safety injection system (SIS) actuation assists the mitigation of the effects of large break loss of coolant accident (LOCA) event with a concurrent software CCF within the PPS and ESF-CCS.

The DPS automatic trip/actuation setpoints are specified to provide reasonable assurance that the PPS initiates an automatic trip/actuation signal prior to the DPS if a postulated software CCF has not degraded the PPS.

The DPS is composed of four channels with one cabinet per channel, and each is located in a separate room. Each DPS channel is powered from two redundant non-Class 1E vital buses that are independent from Class 1E vital buses. Each DPS channel can be tested manually without causing component actuation during plant operations.

APR1400 DCD TIER 2

Reactor Trip Signal

The DPS initiates an automatic reactor trip when either pressurizer pressure or containment pressure exceeds a predetermined value (see Table 7.8-1). The DPS also initiates a reactor trip on turbine trip (RTOTT) if the RPCS is out of service. The DPS RTOTT can be manually enabled from the DPS operator module (DPS-OM) in the MCR.

The DPS design uses a 2-out-of-4 logic to open the trip circuit breakers of the reactor trip switchgear system (RTSS), thus removing motive power to the control element drive mechanisms (CEDMs) as shown in Figures 7.8-1 and 7.8-2. For reactor trip, the DPS energizes the shunt trip coil of the RTSS trip circuit breakers while the PPS de-energizes the undervoltage trip coil to cause the RTSS trip circuit breakers to open.

The DPS manual reactor trip is provided to permit the operator to trip the reactor from the DPS-OM in the MCR.

Turbine Trip Signal

The DPS turbine trip is automatically initiated whenever the DPS reactor trip conditions are met. The DPS turbine trip signal is automatically generated with a three-second time delay after initiation of the DPS reactor trip signal. A block diagram of the reactor trip/turbine trip circuitry is shown in Figure 7.8-2. Refer to Figure 7.8-3 for the DPS turbine trip signal.

Auxiliary Feedwater System Actuation Signal

The DPS initiates the AFWS actuation when the level in either of the two SGs decreases below a predetermined value (see Table 7.8-1). Each auxiliary feedwater actuation signal (AFAS) generated independently by the DPS and ESF-CCS is logically combined in the ESF-CCS, using “hardwired OR” circuits in the component interface module (CIM), so that either system can actuate the auxiliary feedwater. Isolation is provided at the ESF-CCS to maintain electrical isolation between the DPS and ESF-CCS. Refer to Figure 7.8-4 for the DPS-AFAS.

APR1400 DCD TIER 2

Safety Injection System Actuation Signal

The DPS also initiates the SIS actuation when the pressure decreases below a predetermined value (see Table 7.8-1). Each safety injection actuation signal (SIAS) generated independently by the DPS and ESF-CCS is logically combined in the CIM, so that either system can actuate the SIS. Isolation is provided at the ESF-CCS to maintain electrical isolation between the DPS and the ESF-CCS. Refer to Figure 7.8-5 for the DPS-SIAS.

7.8.1.2 Diverse Manual ESF Actuation Switch

The DMA switches permit the operator to manually actuate ESF systems from the MCR after a postulated CCF of the PPS and ESF-CCS.

Diverse manual ESF actuation signals consist of the SIAS, main steam isolation signal (MSIS), containment isolation actuation signal (CIAS), containment spray actuation signal (CSAS), AFAS-1, and AFAS-2. Table 7.8-3 identifies diverse automatic and manual actuation signals. The DMA signals are hardwired to the CIM and are independent and diverse from the safety system.

Each DMA signal actuates necessary ESF systems to perform the ESF functions.

7.8.1.3 Diverse Indication System

The DIS provides functions to monitor critical variables following a postulated software CCF of digital I&C safety systems. As the DIS receives its hard-wired signal inputs from isolators in the auxiliary process cabinet-safety (APC-S) as well as in qualified indication and alarm system – P (QIAS-P) channel A, the DIS is independent and diverse from the QIAS-P.

The DIS provides control functions of heater power for the proper heated junction thermocouple (HJTC) output signal level to assist the mitigation of the effects of a postulated software CCF of the QIAS-P. The control function is manually transferred from the QIAS-P to the DIS by the DIS manual transfer switch.

The DIS display and the DIS manual transfer switch are located on the MCR safety console. The DIS cabinet is classified as non-seismic equipment. However, the DIS HSI equipment

APR1400 DCD TIER 2

on the MCR safety console are qualified as seismic Category II and powered by non-class 1E vital bus.

7.8.2 Design Bases

7.8.2.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO followed by failure of the reactor trip portion of the protection system. In addition, the DPS is designed to include functions to assist the mitigation of the effects of a postulated software CCF of the PPS and ESF-CCS, concurrent with AOOs and postulated accidents.

Quality

The DPS is the non-safety system designed with augmented quality, as defined by Generic Letter 85-06 (Reference 3). The software associated with the DPS is identified as important to safety (ITS) as described in the *[Software Program Manual Technical Report (Reference 4)]**.

System Testing

The DPS testing covers the trip path from sensor input to the RTSS. The system test does not affect the DPS functions.

The DPS has manual and manually initiated automatic test functions through the DPS maintenance and test panel (MTP). The manually initiated automatic test is performed periodically during power operation, and a manual test is performed during shutdown.

During the manually initiated automatic test, the DPS trip outputs are automatically bypassed and the fixed test signals are inserted to cause a channel trip for each process parameter in the DPS.

During the manual test, the DPS trip outputs are not automatically bypassed and the fixed test signals, inserted through manual test selection, cause a channel trip for each process parameter. The channel trip signals generated by manual test initiate the final actuation devices.

APR1400 DCD TIER 2

During the refueling period, the response time verification tests are performed for the DPS to confirm that the DPS response times are maintained within the acceptable range.

Trip Channel Bypass

A trip channel bypass of the DPS is provided in each channel through the DPS-OM and MTP to allow for the maintenance, repair, test, and calibration during operation to avoid inadvertent actuation of the protective action. When a trip channel is bypassed for test or maintenance, the bypass status is indicated in the MCR. The logic converts to 2-out-of-3 while a channel is bypassed.

Operating Bypass

The DPS provides the operating bypasses for the SIAS. The DPS-SIAS operating bypass can be manually enabled during the RCS heatup and cooldown. The DPS-SIAS operating bypass is provided in each channel by using the DPS-OM in the MCR. The DPS-SIAS is also automatically defeated by the actuation of MCR-RSR control transfer, which enables the plant operation in the remote shutdown room (RSR). When the DPS-SIAS operating bypass is enabled, the bypass status is indicated in the MCR.

Use of Digital System

The DPS is implemented on a platform that is diverse from the safety system common platform.

Single failure

Because the DPS is classified as a non-safety system, it is not required to meet the single failure criterion for actuation. The DPS consists of four channels, and it has 2-out-of-4 coincidence logic for the trip actuation. Therefore, the DPS can minimize the inadvertent actuations, and it has fault-tolerant capabilities. The DPS has two operator modules (DPS-OM) on the safety console. In addition, each DPS-OM can be used to control and monitor all four DPS channels. Therefore, if one DPS-OM fails, another DPS-OM can be used.

APR1400 DCD TIER 2

Environmental Qualification

DPS equipment is qualified to perform its intended protective function to the required environments of design basis events (including the main steam line break (MSLB) and LOCA).

Independence from the Protection System

The DPS is electrically isolated and physically separated from the protection system. The engineered safety feature actuation signals initiated by the DPS are isolated in the protection system. The DPS receives the hard-wired process signal inputs from isolators in the APC-S. The qualified isolation devices are part of the safety system.

Diversity

The DPS is diverse from the sensor output to the trip device in the final actuation equipment used to interrupt motive power to CEDMs. The DPS final actuation equipment for reactor trip is the trip circuit breakers of the RTSS. The RTSS consist of RTSS 1 and 2 provided by different manufacturers. The DPS reactor trip energizes the shunt trip coils of the RTSS trip circuit breakers. The PPS reactor trip de-energizes the undervoltage trip coils of the RTSS trip circuit breakers.

The DPS is diverse from the sensor output to the CIM of ESF-CCS for engineered safety feature actuation such as auxiliary feedwater actuation and safety injection actuation.

Defense-in-Depth and Diversity

The defense-in-depth and diversity (D3) approach is based on the following principles:

- a. Minimize the potential for software CCF
- b. Cope with software CCFs concurrent with AOOs and postulated accidents

The DPS is implemented to prevent adverse effects and impacts to the safety system. The DPS assists the mitigation of the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS.

APR1400 DCD TIER 2

The DPS design complies with the following regulatory documents to provide reasonable assurance of adequate performance of its protective functions:

- a. GDC 1, 13, 19, and 24 of Appendix A 10 CFR 50
- b. IEEE Std. 603, Clause 5.6.3
- c. 10 CFR 50.62
- d. Staff Requirements Memorandum on SECY 93-087 II.Q
- e. NUREG-0800, Chapter 7, Branch Technical Position 7-19

7.8.2.2 Diverse Manual ESF Actuation Switch

The DMA switches are provided to permit the operator to manually actuate system-level ESF functions from the MCR.

The DMA switches are diverse from the manual and automatic logic functions performed by digital equipment in the PPS and ESF-CCS.

Basic design bases are described as follows:

Quality

The DMA switches provide the non-safety functions, but they are designed with augmented quality, as defined by Generic Letter 85-06. The DMA switches are designed with Class 1E qualified hardware and are seismically qualified. The DMA switches are energized using Class 1E power.

System Testing

A channel functional test is performed for the DMA switches by manual actuation of each function. This testing is performed during plant outages to verify that the actuation switch can actuate the components.

APR1400 DCD TIER 2

Environmental Qualification

The DMA switches are qualified to perform their intended protective function during AOOs and design basis events.

Independence from the Protection System

The DMA switches are connected directly to fan-out devices in the MCR safety console to distribute the system-level switch signals to individual component controls. The signals are hard-wired to the CIM in the ESF-CCS cabinet. The DMA switches compose a non-safety system, but they are designed with Class 1E hardware and are energized using Class 1E power. Therefore, isolation devices are not necessary for interfacing the DMA switch outputs to the CIM.

Single Failure

Because the DMA switches compose a non-safety system, they do not need to meet the single failure criterion for actuation.

Diversity

The DMA switches are diverse from the manual and automatic logic functions performed by digital equipment in the PPS and ESF-CCS. The DMA switches are connected through conventional hardware circuits.

Defense-in-Depth and Diversity

The DMA switches are designed to comply with the regulatory position in SECY 93-087 II.Q and with BTP 7-19 (Reference 5). The DMA switches provide manual control capability that is used in the event of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS.

To implement adequate diversity for ESF-CCS, the DMA switches that are not based on software are used to assist in maintaining the following plant critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and

APR1400 DCD TIER 2

containment integrity. The switches in the MCR provide for system-level actuation, as shown in Table 7.8-3.

The DMA switches are hard-wired downstream of the ESF-CCS LC to the CIM level, and are independent and diverse from the ESF-CCS.

7.8.2.3 Diverse Indication System

The DIS displays parameters required for the operator to assess the plant condition and to take corrective action, if necessary. The displayed parameters are selected on the following bases:

- a. A subset of the accident monitoring instrumentation (AMI) parameters
- b. The inadequate core cooling monitoring (ICCM) parameters
- c. The parameters needed for the operator to place and maintain the plant in a safe shutdown condition

The associated variables that are displayed by the DIS are shown in Table 7.8-4.

The DIS is designed to meet the independence requirements so that any failures occurring within the DIS cannot affect digital safety systems by receiving input signals from digital safety systems through qualified isolators. In addition, the DIS is designed to meet the diversity requirements by implementing the system on a diverse platform.

The system is designed in compliance with the applicable criteria of GDCs 1, 13, and 19. Compliance with GDCs 1, 13, and 19 is described in the Diversity and Defense-in-Depth Technical Report (Reference 6).

Quality

The DIS is the non-safety system designed with augmented quality, as defined by Generic Letter 85-06. The software associated with the DIS is identified as ITS as described in the [Software Program Manual Technical Report]*.

APR1400 DCD TIER 2

System Testing

A functional test is performed for the DIS during plant outages to verify the DIS function.

Use of Digital Systems

The DIS is implemented on a platform that is diverse from the digital safety system common platform.

Environmental Qualification

The DIS equipment is qualified to perform its intended function during design basis events.

Independence from the Protection System

The DIS is isolated from the QIAS-P and APC-S, in accordance with the independence requirements of IEEE Std. 603 (Reference 7) and IEEE Std. 384 (Reference 8), so that a credible fault originating in the DIS cannot propagate to or adversely affect the safety system.

Single Failure

Because the DIS is a non-safety system, it does not need to meet the single failure criterion.

Diversity

The DIS is diverse from the digital safety system common platform in compliance with the SRM on SECY-93-087 and BTP 7-19.

Defense-in-Depth and Diversity

The DIS provides sufficient information for the operator to perform safety functions following a postulated software CCF of safety systems.

APR1400 DCD TIER 2

7.8.3 Analysis

7.8.3.1 General

An evaluation is performed to show the capability of the plant design to cope with the event initiators in Chapter 15 concurrent with a postulated software CCF of the digital type PPS and ESF-CCS.

Credit is taken for the DPS providing an automatic reactor trip on high pressurizer pressure or high containment pressure, an automatic actuation of the auxiliary feedwater actuation on low SG level, and an automatic actuation of the safety injection actuation on low pressurizer pressure. Manual operator action is credited if the action time has been determined based on sufficient information and time for the operator to detect, analyze, and act to mitigate the events with the CCF of the PPS and ESF-CCS.

a. Anticipated transients without scram

In accordance with 10 CFR 50.62, the DPS is diverse from the reactor trip system to initiate reactor trip, turbine trip, and auxiliary feedwater actuation.

Compliance with 10 CFR 50.62 is addressed in the Diversity and Defense-in-Depth Technical Report.

b. Adequacy of Manual controls and displays

The DIS and DMA switches provide means for the operator to take manual actions necessary for the mitigation of AOOs and postulated accidents analyzed in Chapter 15 concurrent with software CCF, to place the nuclear plant in a safe shutdown condition, and monitor and maintain the critical safety functions.

The DIS and DMA switches are also designed for all credited manual operator actions. The DIS and DMA switches are designed, verified, and validated in accordance with the HFE program described in Chapter 18.

Adequacy of manual control and displays is addressed in the CCF Coping Analysis Technical Report (Reference 9).

c. Compliance with BTP 7-19

APR1400 DCD TIER 2

The compliance with BTP 7-19 is provided in the Diversity and Defense-in-Depth Technical Report.

7.8.3.2 Scope of Evaluation

The CCF prevents both the PPS and ESF-CCS from providing any actuation or control (automatic and manual) or from causing spurious actuation of their associated safety equipment. Table 7.8-2 shows the plant functions and systems that are not affected by the CCF in the PPS and ESF-CCS.

Operator response is necessary to accomplish subsequent recovery actions following each event. Diversity in the plant equipment and software provides reasonable assurance that adequate instrumentation and controls are available for the timely diagnosis and mitigation of design basis events with a concurrent postulated software CCF in the PPS and ESF-CCS.

The postulated CCF may cause the displayed data on the QIAS-P and QIAS-N to be invalid, which would cause the PPS and ESF-CCS data that are passed to the IPS to be invalid. The data passed from the IPS from the other systems except the PPS and ESF-CCS would be valid and would be processed for display and alarm. Moreover, the data provided to the DIS are processed to display the parameters that are listed in Table 7.8-4.

7.8.3.3 Evaluation of Design Basis Events

- a. The qualitative evaluation assesses the D3 capability of the plant design in responding to event initiators, which are the design basis events presented in Chapter 15, with a concurrent postulated software CCF of the PPS and ESF-CCS.

The qualitative evaluation assumes that the automatic actuations of safety functions in the PPS and ESF-CCS and the capability for manual actuation using these systems are precluded or the software CCF causes spurious actuation. The evaluation uses realistic assumptions regarding initial operating conditions and assumes continued operability of the RCPs (except the events in which the event initiator is loss of power to the RCPs or the actual failure of the RCPs) and the control systems. The qualitative evaluation results are compared to the acceptance criteria for each event initiator.

The results of the qualitative evaluation analyses are presented in the CCF Coping Analysis Technical Report (Reference 9).

APR1400 DCD TIER 2

b. Quantitative analysis

A detailed, quantitative analysis using qualified computer programs is conducted for the event requiring further detailed quantitative analyses in order to determine their compliance with the acceptance criteria.

The results of the quantitative evaluation analyses are presented in the CCF Coping Analysis Technical Report.

7.8.4 Combined License Information

No COL information is required with regard to Section 7.8.

7.8.5 References

1. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."
2. SECY-93-087, "Policy, Technical, and Licensing Issue Preparing to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," April 2, 1993.
3. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related."
4. [APR1400-Z-J-NR-13003-P, "*Software Program Manual Technical Report*," September 2013.]*
5. BTP 7-19, Rev. 6, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," July 2012.
6. APR1400-Z-J-EC-13002-P, "Diversity and Defense-in-Depth Technical Report," September 2013.
7. IEEE Std. 603-1991, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
8. IEEE Std. 384-1992, "Standard Criteria for Independence of Class 1E Equipment and Circuits."

APR1400 DCD TIER 2

9. APR1400-Z-A-NR-13008-P, “CCF Coping Analysis Technical Report,” September 2013.
10. *[APR1400-Z-J-NR-13004-P, “Uncertainty Methodology and Application for Instrumentation Technical Report,” April 2013.]**
11. *[APR1400-Z-J-NR-13005-P, “Setpoint Methodology for Plant Protection System Technical Report,” April 2013.]**

APR1400 DCD TIER 2

Table 7.8-1

Diverse Protection System Parameter

Monitored Variable	Type	Number of Sensors	Sensor Range	Nominal Setpoint ⁽¹⁾	Response Time (in seconds)
Pressurizer pressure for reactor trip	Pressure transmitter	4	105 to 175 kg/cm ² A (1,494 to 2,489 psia)	168.7 kg/cm ² A (2,399 psia)	≤ 0.85
Pressurizer pressure for SIAS	Pressure transmitter	4	7.03 to 155.38 kg/cm ² A (100 to 2,200 psia)	114.6 kg/cm ² A (1,630 psia)	≤ 1.25 ⁽²⁾
Containment pressure for reactor trip	Pressure transmitter	4	−300 to 1200 cmH ₂ O (−4 to 17 psig)	257 cmH ₂ O (3.6 psig)	≤ 1.25
Steam generator level (wide range) for AFAS	Differential pressure transmitter	4/steam generator	0 to 100 % WR	22.2 % WR	≤ 1.15 ⁽²⁾
Turbine tripped status for reactor trip	Electro-hydraulic control header pressure switch	4	Contact	Contact	N/A

(1) The uncertainty methodology and the setpoint methodology are provided in References 10 and 11. DPS has different setpoints from PPS so that PPS actuates prior to DPS. Refer to Tables 7.2-4 and 7.3-5A for PPS and ESF-CCS setpoints.

(2) The response time includes the sensor and the DPS but does not include the final actuation device.

APR1400 DCD TIER 2

Table 7.8-2

Diverse Functions Remain Available After the CCF

Functions available	Related System	Operation Mode
1. Diverse protection system <ul style="list-style-type: none"> • Reactor trip on high pressurizer pressure • Reactor trip on high containment pressure • Auxiliary feedwater actuation on low steam generator level • Manual reactor trip by the DPS-OM • Safety injection actuation on low pressurizer pressure • Turbine trip on DPS reactor trip (3-second time delay) 	DPS	Automatic or manual
2. NSSS control system <ul style="list-style-type: none"> • Steam bypass control system • Feedwater control system • Pressurizer level control system • Pressurizer pressure control system • Reactor regulating system • Reactor power cutback system • Digital rod control system 	NPCS, PCS	Automatic or manual
3. Manual reactor trip (in the MCR/RSR) ⁽¹⁾	RTSS	Manual
4. Diverse manual ESF actuation (at a system level)	CIM (located in ESF-CCS cabinet)	Manual
5. Manual actions taken locally (at the component)	—	Manual
6. Indications, displays and alarms (except the PPS and the ESF-CCS information) provided by the IPS	IPS	—
7. Displays provided by the DIS	DIS	—
8. HJTC heater power control provided by the DIS	DIS	Automatic after manual transfer

(1) Refer to Subsection 7.2.1.5.

APR1400 DCD TIER 2

Table 7.8-3

Diverse Actuation Signals

System	Actuation Signal	Number of Sensors or Switches	Act. Logic
DPS	DPS reactor trip on high pressurizer pressure	4 PZR pressure sensors	2/4
	DPS reactor trip on high containment pressure	4 Cont. pressure sensors	2/4
	DPS AFAS on low steam generator level	4 SG level sensors (WR)	2/4
	DPS SIAS on low pressurizer pressure	4 PZR pressure sensors (WR)	2/4
	DPS turbine trip	DPS reactor trip output with 3-second time delay	2/4
	DPS manual reactor trip	4 soft control switches	2/4
PPS	PPS manual reactor trip	4 switches	2/4
DMA switches	Diverse manual AFAS-1	1 switch (channel A)	1/1
	Diverse manual AFAS-2	1 switch (channel B)	1/1
	Diverse manual SIAS	2 switches (channels A and C)	1/1
	Diverse manual MSIS-1A	1 switch (channel A)	1/1
	Diverse manual MSIS-1B	1 switch (channel A)	1/1
	Diverse manual MSIS-2A	1 switch (channel A)	1/1
	Diverse manual MSIS-2B	1 Switch (channel A)	1/1
	Diverse manual CSAS	2 switches (channels A and C)	1/1
	Diverse manual CIAS	1 switch (channel A)	1/1

APR1400 DCD TIER 2

Table 7.8-4 (1 of 2)

Display and Control Parameters for the DIS

No	Parameter Description
1	Representative Core Exit Temperature
2	Reactor Vessel Water Level-Head
3	Reactor Vessel Water Level-Plenum
4	Upper Head Temperature
5	Upper Head Temperature Saturation Margin
6	Upper Head Pressure Saturation Margin
7	RCS Temperature Saturation Margin
8	RCS Pressure Saturation Margin
9	CET Temperature Saturation Margin
10	CET Pressure Saturation Margin
11	Containment Pressure (Accident Monitoring Instrumentation)
12	Containment Temperature
13	Containment Water Level
14	Containment Hydrogen Concentration
15	IRWST Temperature
16	IRWST Level
17	IRWST Hydrogen Concentration
18	PZR Level
19	PZR Pressure
20	RCS Hot Leg Temperature (T_h)
21	RCS Cold Leg Temperature (T_c)
22	Reactor Power
23	Steam Generator 1 Level Protective (WR)
24	Steam Generator 2 Level Protective (WR)
25	Steam Generator 1 Pressure Protective (WR)
26	Steam Generator 2 Pressure Protective (WR)

APR1400 DCD TIER 2

Table 7.8-4 (2 of 2)

No	Parameter Description
27	SI Flow to DVI 1A
28	SI Flow to DVI 2B
29	CS Pump 1 Flow
30	Charging Line Flow
31	AFW Flow Rate to S/G 1
32	AFW Flow Rate to S/G 2
33	AFWST A Level
34	AFWST B Level
35	Auxiliary Building Sump Level
36	SIT 1 Pressure (WR)
37	Containment Air Radiation (Iodine)
38	HJTC Heater Power

APR1400 DCD TIER 2

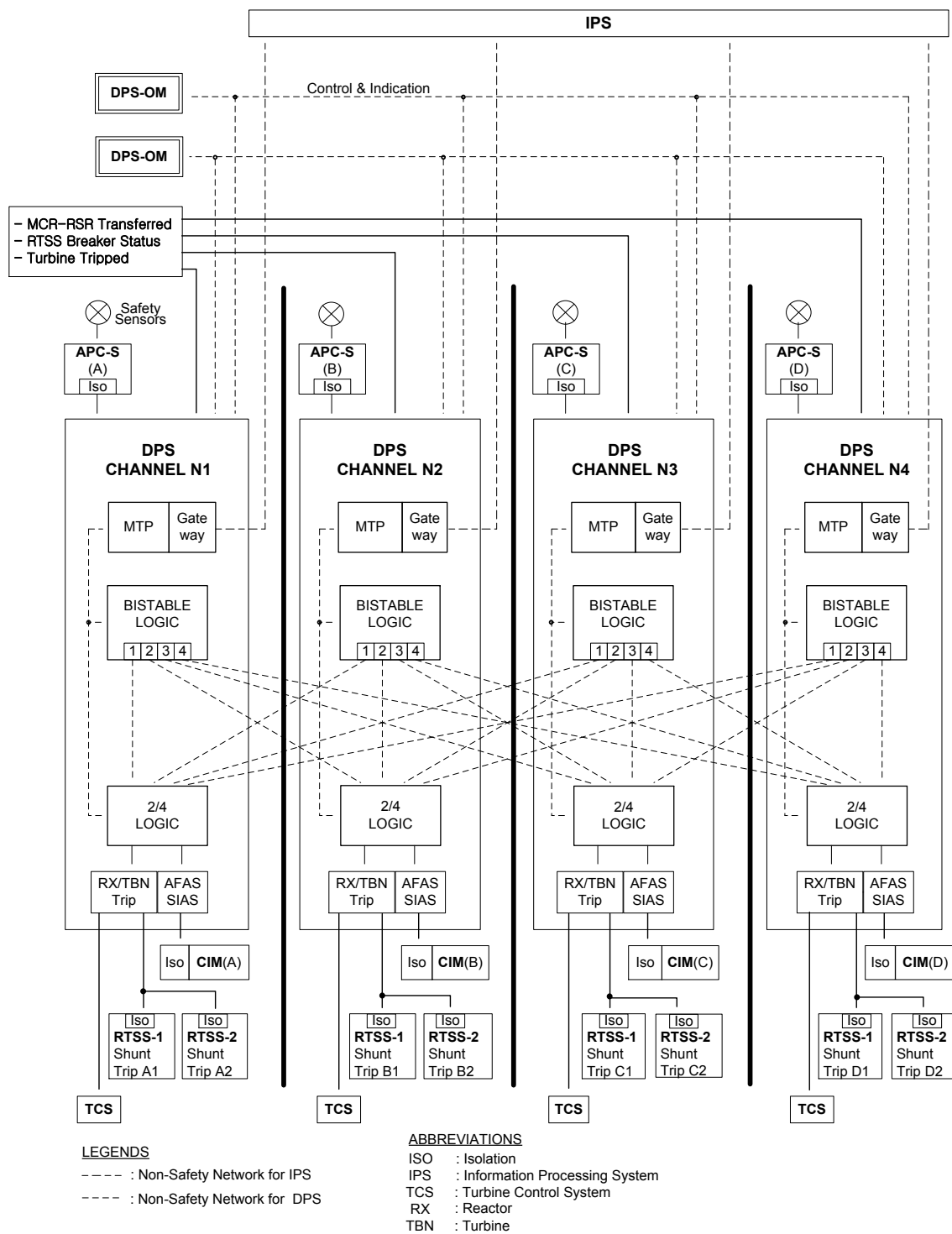


Figure 7.8-1 Diverse Protection System Block Diagram

APR1400 DCD TIER 2

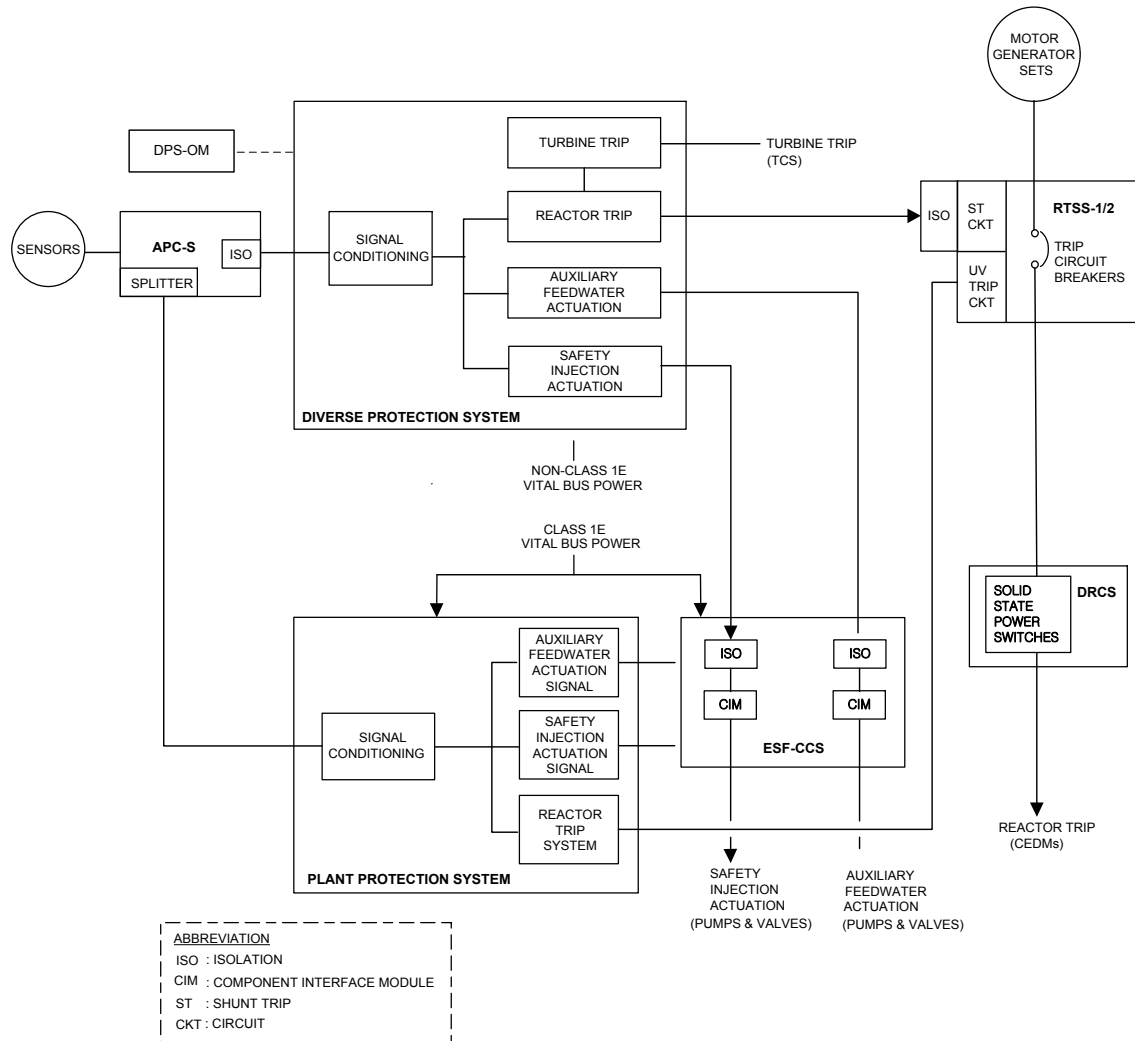
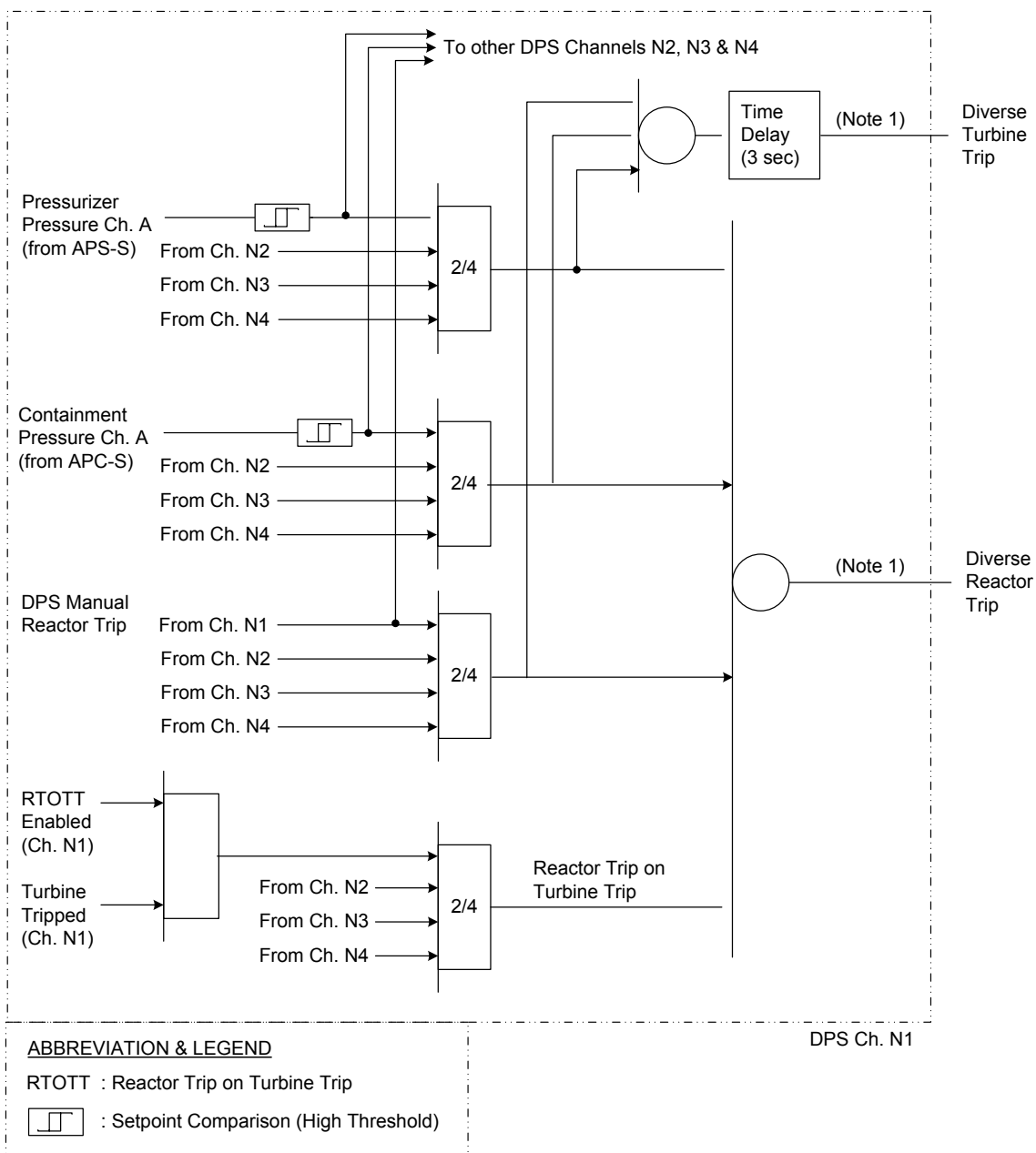


Figure 7.8-2 Diverse Reactor Trip, Turbine Trip, AFWs and SIS Actuation

APR1400 DCD TIER 2



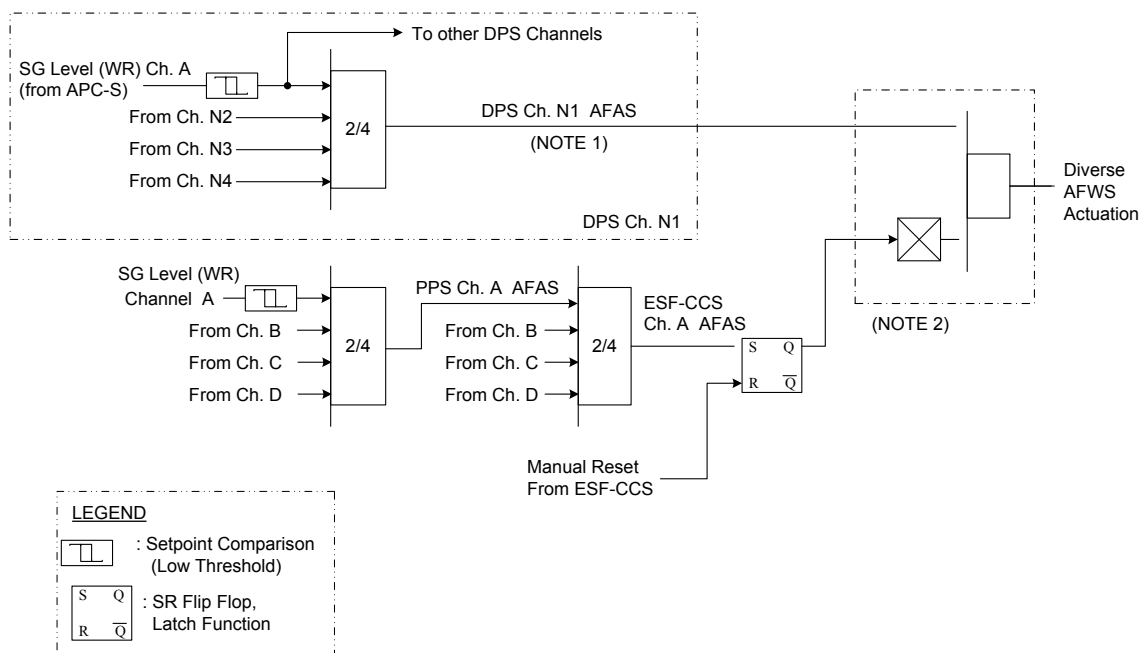
Notes: 1. DPS Reactor Trip and Turbine Trip signals are automatically cleared if process signal is returned to normal value.

2. This diagram is for the DPS Channel N1. Channels N2, N3 and N4 are the same as Channel N1.

3. Refer to Reference 3.2.2.1 for details.

Figure 7.8-3 Diverse Reactor Trip and Turbine Trip

APR1400 DCD TIER 2

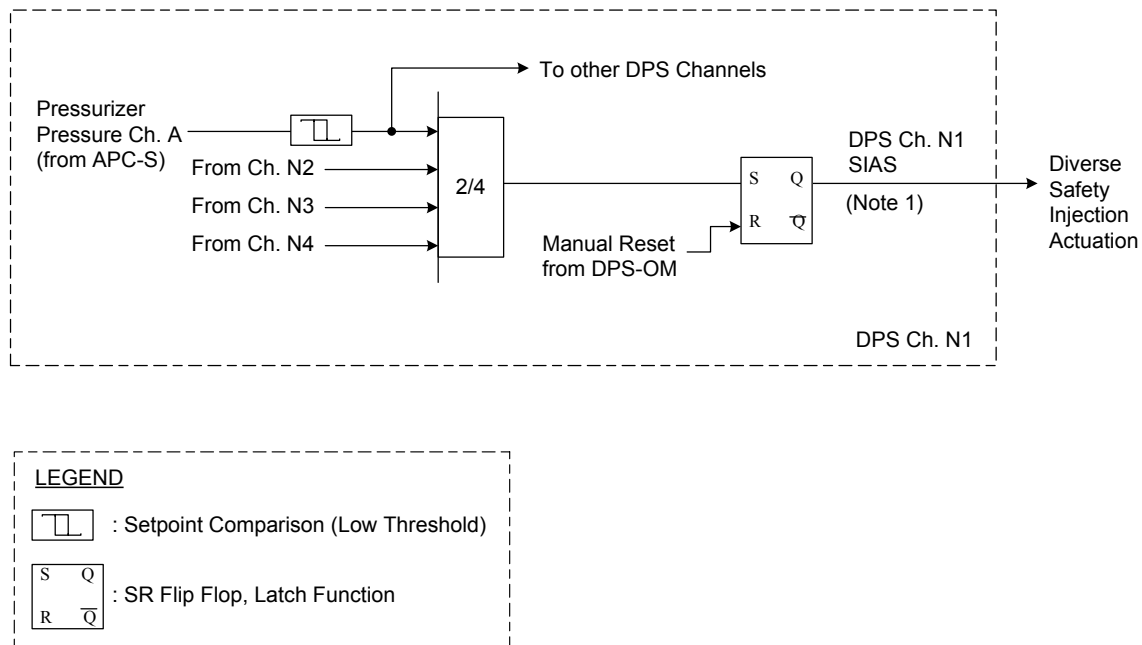


Notes:

1. The DPS-AFAS components cycle its operation, which is ON if SG level goes below Low Setpoint, and OFF if SG level is above the Low Setpoint plus Hysteresis.
2. This hardwired logic is implemented in ESF-CCS for Auxiliary Feedwater isolation valves. Refer to Figure 10.4.9-1(Sheet 2 of 3).
3. This diagram is for the DPS Channel N1. Channels N2, N3, and N4 are the same as Channel N1.

Figure 7.8-4 Diverse AFWS Actuation

APR1400 DCD TIER 2



- Notes: 1. The DPS-SIAS is latched signal which is ON and maintained (or latched) if Pressurizer Pressure goes below Low Setpoint, and can be OFF if Manual Reset signal is generated by the DPS-OM.
2. This diagram is for the DPS Channel N1. Channels N2, N3, and N4 are the same as Channel N1.
3. Refer to Reference 3.2.2.1 for details.

Figure 7.8-5 Diverse SIS Actuation

7.9 Data Communication Systems

Data communication systems provide high-speed and reliable communications between various systems. Data communication systems consist of hardware, protocols, and information systems.

Data communication systems are designed to provide accurate, reliable, and timely transfer of data within protection systems, between control and protection systems and information systems, or within the information systems.

The information processing system (IPS) and qualified indication and alarm system - non-safety (QIAS-N) acquire information from data communication networks, process the data and provide information to the display devices and other peripherals.

7.9.1 System Description

Data communication systems consist of three kinds of data communication networks or links with different protocols:

- a. Safety system data network (SDN), which is qualified seismically and environmentally and based on important to safety (ITS) software
- b. Serial data link (SDL), which is qualified seismically and environmentally and based on safety critical (SC) software
- c. Data communication network-information (DCN-I), which is not qualified and based on important to availability (ITA) software

Data communication systems provide data communication for intra-channel communications within a safety channel, between safety channels, from safety system to non-safety system, and within non-safety systems. All of these systems are designed to have physical separation, electrical isolation, and communication independence between safety channels and between safety systems and non-safety systems. Refer to Figure 7.9-1 for an illustration of the interconnections of the three communication networks.

7.9.1.1 SDN for Safety Systems

The SDN is used for communication between safety systems within one channel. Intra-channel communications are a separated and isolated SDN. The SDN is a broadcasting network with deterministic characteristics. Each SDN is fully redundant.

The SDN provides data communication as follows:

a. Plant protection system (PPS)

Bistable processors and local coincidence logic (LCL) processors send status data to maintenance and test panel (MTP), operator module (OM), and interface and test processor (ITP) through the SDN.

Bistable processors and LCL processors receive testing data from MTP through the SDN.

b. Core protection calculator system (CPCS)

The CPCS sends data for monitoring all processors, including inputs and calculated output to MTP, OM, and ITP through the SDN.

c. Engineered safety features – component control system (ESF-CCS)

ESF-CCS loop controller (LC) sends engineered safety features (ESF) component status information to MTP through the SDN.

Group controller (GC) sends status data to MTP and ITP through the SDN.

d. Qualified indication and alarm system – P (QIAS-P)

The QIAS-P processor transmits the value and system status to the IPS and qualified and indication alarm system – non-safety (QIAS-N) through the MTP and ITP, which provide data communication isolation function and electrical isolation function. The QIAS-P processor is connected to the QIAS-P display, MTP, and ITP through the SDN.

e. ESF-CCS soft control module (ESCM)

APR1400 DCD TIER 2

The ESCM sends component control signals to the control channel gateway (CCG) through the SDN.

The ESCM receives the information data from the CCG through the SDN.

f. ITP

The ITP receives status data from safety systems through the SDN.

g. MTP

The MTP receives status data from safety systems and sends testing data and setpoint data through the SDN.

h. OM

The OM receives status data from safety systems and sends testing data and setpoint data through the SDN. The setpoint data are sent to the CPCS.

i. Control panel multiplexer (CPM)

The CPM communicates with the bistable processor (BP), ITP, ESF-CCS GC, and LC for receiving status information through the SDN.

j. CCG

The CCG transfers component control signals to the ESF-CCS LC through the SDN. The CCG receives the feedback data from the ESF-CCS LC through the SDN.

7.9.1.2 SDL for Safety Systems

The SDL is a serial data link that can be used for predefined data transmissions between each processor within a channel. The SDL also used to transmit broadcast data to other channels and non-safety systems. The SDL meets the communication isolation requirements of IEEE Std. 7-4.3.2 (Reference 1). The SDL is designed to fulfill communication independence in accordance with DI&C-ISG-04 guidance (Reference 2) so that a failure of the SDL in a channel does not adversely affect the operation of other channels.

APR1400 DCD TIER 2

The SDLs use fiber optic modems and cables to provide electrical isolation.

The SDL provides data communication as follows:

a. PPS

SDL for LCL voting logic

There are two sets of cross channel communication SDLs per redundant PPS channels. Each bistable processor transmits data to the LCL processors through the SDL.

SDL for ESF-CCS GC voting logic (actuation logic)

Each LCL processor transmits ESFAS initiation signals to the GCs for 2-out-of-4 voting logic through the SDL.

b. CPCS

The CPCS consists of a core protection calculator (CPC) rack with two processor modules (CPC processor and auxiliary CPC processor) and a control element assembly (CEA) calculator (CEAC) rack 1 and 2 (each with a CEAC and a CEA position processor (CPP)).

The CPP transmits CEA position signals to the CPP and CEAC processor through CPPs in the same channel and other channels using the SDLs.

The CPP transmits target CEA position signals to the CPC in the same channel through the SDLs.

The CEAC transmits penalty factors and target CEA position signals to CPC in the same channel via the SDLs.

c. ESF-CCS

The ESF-CCS consists of a control network that delivers control signals and information network that delivers status and monitoring signals. The control network is implemented by the SDLs.

APR1400 DCD TIER 2

The ESF-CCS control signals are transmitted to the LCs from the GCs through the SDLs.

Control signals from the safety console manual switches are connected to the CPM, and the commands are delivered to the ESF-CCS GCs (system-level and component-level) through the SDL. The component control signals initiated by minimum inventory switches are transmitted to the ESF-CCS LCs via the ESF-CCS GCs through the SDL.

The operating bypass and setpoint reset switch signals are also transmitted to the PPS BP via the channelized CPM through the SDLs.

7.9.1.3 DCN-I for Non-safety Systems

The DCN-I provides non-safety data communication to integrate the data from safety and non-safety systems. The signal connections for the DCN-I is as follows:

- a. IPS server
- b. IPS workstation
- c. Engineering station
- d. Computer-based procedure (CBP) system server
- e. Distributed control system (DCS) gateway to be interfaced with MTP in each safety channel
- f. Multi-channel gateway to be interfaced with ITP in each safety channel
- g. P-CCS controller
- h. Balance of plant (BOP) monitoring systems
- i. Turbine/generator (T/G) control system
- j. Power control system (PCS) controller
- k. NSSS process control system (NPCS) controller

APR1400 DCD TIER 2

- l. Fixed in-core detector amplifier system (FIDAS)
- m. NSSS integrity monitoring system (NIMS)

The DCN-I is independent of the QIAS-N network. The DCN-I uses different data communication hardware and protocols from the QIAS-N network.

All data paths between the DCN-I and safety systems via information gateways are fiber optic cables to provide reasonable assurance of electrical isolation.

The DCN-I is a partially redundant network. Each control and safety system that interfaces with the DCN-I is via multiple (multi-channel) or redundant data communication paths, such that a single failure in the data communication path does not cause a total loss of data transmission capability between these systems and the DCN-I. The IPS server processors interface with the DCN-I via a redundant data communication path, such that a single failure in the data communication path does not cause the loss of data transmission capability between the IPS server processors and the DCN-I. The IPS server processors communicate with the IPS display systems through the DCN-I.

The evaluation is performed to provide reasonable assurance that the throughput, capacity, response time, and data accuracy of DCN-I meet the requirements of the supported I&C systems. Expected error rates and their effects upon system safety, reliability, and performance are also evaluated.

7.9.1.4 Data Communication for Safety and Non-Safety Systems

Data Communication from Safety System to Non-safety System

- a. MTP

The MTP transmits data to the IPS through the fiber optic cable uni-directionally. Failure of the MTP does not prevent the safety functions from performing their intended functions.

APR1400 DCD TIER 2

b. ITP

The ITP sends the status and alarm information to the QIAS-N through the SDL uni-directionally. Failure of the ITP does not prevent the safety systems from performing their intended functions.

c. DCS Gateway Server

The DCS gateway server performs data communication functions from safety systems to non-safety systems with isolation using fiber optic.

Data Communication from Non-safety System to Safety System

Ethernet communication is used to communicate from the information flat panel display (FPD) to ESCM. The connection does not transfer any safety or control information to perform any safety or control functions. The signal from the information FPD provides information to the ESCM only to support manual actions performed by the operator. This signal is used for bringing up the control template on the ESCM display and is not used for performing any automatic safety functions. Therefore, the ESF-CCS channel does not rely on information from the information FPD to accomplish its function.

Compliance of DI&C-ISG-04 regarding communication from the information FPD to the ESCM is described in Appendix C of the Safety I&C System Technical Report (Reference 3).

Data Communication from Safety Systems to the QIAS-N

a. QIAS-N network

The QIAS-N network is used for signal connections as follows:

- 1) QIAS-N controller
- 2) QIAS-N display
- 3) QIAS-N MTP

APR1400 DCD TIER 2

The QIAS-N network and the DCN-I are independent from each other. The QIAS-N network utilizes different data communication hardware and protocols from the DCN-I.

All data paths between the QIAS-N network and safety systems by way of information gateways are fiber optic cables to provide reasonable assurance of electrical isolation. The QIAS-N network is seismically qualified.

The QIAS-N network is a redundant network. The QIAS-N controller interfaces with QIAS-N network by way of a redundant data communication path, such that a single failure in the communication path does not cause a loss of data transmission capability between the QIAS-N and the QIAS-N network.

The QIAS-N communicates with display devices such as a mini-large display panel (mini-LDP), QIAS-N FPDs and shutdown overview display panel (SODP) for QIAS-N over a redundant data communication network. These displays are associated with a server that communicates with the QIAS-N by way of the QIAS-N network.

The QIAS-N MTP performs its data communication function from the DCN-I network to the QIAS-N network for isolation through the fiber optic cable.

An evaluation is performed to provide reasonable assurance that the throughput, capacity, latency, and data accuracy of the QIAS-N network meet the requirements of the QIAS-N. Expected error rates and their effects upon system safety, reliability, and performance are also evaluated. The error rates include errors in device addressing and signal data attributes.

b. Communications between IPS and QIAS-N

The data communication path by way of a gateway device is connected between the QIAS-N network and the DCN-I for IPS. Electrical isolation is maintained between the QIAS-N network and the DCN-I by way of the gateway and the fiber optic cable that provides isolation. Since the electrical isolation is maintained between the IPS and the QIAS-N, a failure of the IPS does not adversely affect the QIAS-N, and vice versa.

APR1400 DCD TIER 2

An evaluation is performed to provide reasonable assurance that the throughput, capacity, response time, and data accuracy of the communications between IPS and QIAS-N meet the requirements of the supported I&C systems. Potential errors and their impact upon system reliability and performance are evaluated.

7.9.2 Design-Basis Information

The section describes the design criteria for the data communication systems that meet design basis requirements such as quality of components, software quality, performance requirements, and hazards. Compliance with DI&C-ISG-04 is described in Appendix C of the Safety I&C System Technical Report.

7.9.2.1 Quality of Components and Modules

The safety classification of components and modules used in the data communication systems are as follows:

- a. The components and modules in the PPS, CPCS, ESF-CCS, and QIAS-P data communication system that perform the protection functions are designed as Class 1E.
- b. The components and modules in the P-CCS and PCS data communication system are designed as non-Class 1E.
- c. The components and modules in the IPS, DCN-I, and QIAS-N data communication network are designed as non-Class 1E.

For the quality classification of components and modules, refer to Table 3.2-1.

7.9.2.2 Data Communication Systems Software Quality

Details of the software quality for the data communication systems are as follows:

- a. The SDL software quality embedded in the safety grade processors (PPS bistable processor, LCL processor, CPC, CEAC, CPP, and ESF-CCS GC/LC, ESCM and CPM) for performing RPS and ESFAS functions is SC.

APR1400 DCD TIER 2

- b. The SDN software quality embedded in the processors, MTP, ITP, OM, and QIAS-P is ITS.

Data communication system software quality for the interfaces between IPS and QIAS-N is as follows:

- a. The DCN-I software quality embedded in the P-CCS, PCS, QIAS-N and IPS is ITA.

*[Data communication system software is developed and tested in accordance with the Software Program Manual Technical Report (Reference 4).]**

7.9.2.3 Performance Requirements

The data communication systems are designed with a sufficient performance margin to perform its designed functions under conditions of maximum load. Conditions of maximum load are based on plant events that cause the highest data transmission loading. Considerations of failures, operating staff actions, automatic test features, and other issues are evaluated. The data communication systems perform their safety functions in a deterministic manner.

- a. Real-time performance

A real-time performance analysis for each function is performed for demonstrating the actual system response time is less than the response time requirements.

- b. System deterministic timing

All protocols of the data communication systems allow calculation of deterministic response time. The deterministic timing considers data rates, data bandwidths, and data precision requirements for normal and abnormal operation. The data communication system application software is designed to be deterministic (repetitive and non-interrupt). The function of the application program is predictable and reproducible. The execution sequence of an application is not influenced by internal decision logic or external interruption. The execution sequence of an application program is repeated at predetermined intervals.

- c. Time delays within the data communication system

APR1400 DCD TIER 2

The delays of data transport due to data communication in the data communication system are included in response time. The response time calculations are validated by vendor test and site test to verify the performance.

APR1400 DCD TIER 2

d. Data rates and bandwidth

The data rates and bandwidths for data communication system are provided to implement a deterministic data communication.

e. Interfaces with other data communication systems

The interface from the data communication systems to external networks allows the data communication with emergency operating facility (EOF), technical support center (TSC) and the NRC via emergency response data system (ERDS).

f. Test results

The factory acceptance test and integration test for the data communication system demonstrate that the data communication system meets applicable qualification requirements in the Safety I&C System Technical Report.

g. Communication protocols

The data communication systems adopt communication protocols to support the interfaces with other data communication systems or the other parts of the I&C system. Additional information on the data communication protocols used in each network of the data communication system including capabilities, bandwidth, and data rates are provided in related system design documents.

7.9.2.4 Potential Hazards

The data communication system is designed to support self-testing and surveillance testing, therefore potential hazards to the data communication system and from the data communication system do not prevent operation of the safety functions.

All data communication system errors and failures are analyzed in the failure modes and effects analysis (FMEA).

7.9.2.5 Control of Access

Equipment related to the data communication systems are administratively controlled by key- locked doors on equipment cabinets to protect against unauthorized access. The indication of access to the cabinets by door switches is provided in the MCR.

APR1400 DCD TIER 2

Access to the cabinets is normally required only during system testing, calibration, and/or maintenance. In addition to the security provisions provided by the above, system software is protected against unauthorized alterations. The protection includes setpoints and software coding by an administrative control of access to software media by the plant owner. Access to the data communication systems is administratively or password controlled.

7.9.2.6 Single Failure Criterion

The SDN and SDL in each channel are physically separated and functionally isolated from other channels. A single failure within the SDN and SDL does not affect a required safety function. The FMEA for the PPS and the ESF-CCS provides the failure effects and analysis for the failure of communication modules, as shown Tables 7.2-7 and 7.3-8.

The data communication systems are designed so the requirements of the single failure criterion are satisfied. The FMEA shows that a single failure does not adversely affect other systems and channels such as redundant PPS channels or ESF-CCS channels.

7.9.2.7 Independence

The data communication systems are designed to maintain the independence between the safety channels, and between the safety and non-safety channels. The fiber optic cables are used to meet the isolation and independence requirements outlined in NRC RG 1.75 (Reference 5) and other applicable standards. Exceptions for the SDL are discussed in Appendix C in the Safety I&C System Technical Report.

7.9.2.8 Fail Safe Failure Modes

Fail safe failure modes for data communication systems are designed as part of the design of the PPS and ESF-CCS. Detection of a failure of the data communication systems is indicated in the MCR and RSR.

7.9.2.9 System Testing and Surveillances

Data communication systems have the diagnostic capability to detect most failures. System testing and inoperable surveillance in accordance with the Technical Specifications detect additional failures.

APR1400 DCD TIER 2

7.9.2.10 Bypass and Inoperable Status Indications

The redundant network can be switched automatically. The bypassed and inoperable status indications for the data communication systems display operational status. The failure of data communication systems is indicated on display and alarm systems.

7.9.2.11 EMI/RFI Susceptibility

The SDN and SDL equipment is qualified in accordance with MIL Std. 461E and IEC 61000 Part 4 Series as endorsed by NRC RG 1.180 (Reference 6). The testing of the equipment is performed for both conducted and radiated signals as follows:

- a. EMI/RFI emissions
- b. EMI/RFI susceptibility / immunity
- c. Surge withstand capability

The DCN-I equipment is tested for EMI/RFI emission so that any safety equipment is not affected.

7.9.2.12 Defense-In-Depth and Diversity

Data communication systems were postulated to fail as a result of a software common-cause failure of the safety systems. The results of the analysis of the postulated failure are provided in the Diversity and Defense-in-Depth Technical Report (Reference 7).

7.9.2.13 Seismic Hazards

The SDN and SDL are qualified as seismic Category I. The DCN-I is seismically qualified as seismic Category II.

7.9.3 Analysis

The data communication systems comply with the recommendations in the regulatory guides and industry codes and standards that are applicable to these systems, are in compliance with the guidance of GDC 1, and meet the requirements of 10 CFR 50.55a(a)(1) (Reference 8).

APR1400 DCD TIER 2

A reliability model is created to represent the hardware implementation of the data communication systems. The model is used to determine the estimated reliability and availability of data communication systems. The analysis is based on reliability data provided by equipment manufacturers.

The FMEA demonstrates that failures in data communication systems do not adversely affect the safety function or cause erroneous safety function actuation.

The results of the analysis of the data communication systems are provided in Appendix C of the Safety I&C System Technical Report.

7.9.4 Combined License Information

No COL information is required with regard to Section 7.9.

7.9.5 References

1. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
2. DI&C-ISG-04, Rev. 1, "Highly-Integrated Control Rooms – Communications Issues (HICRc)," 2009.
3. APR1400-Z-J-EC-13001-P, "Safety I&C System Technical Report," September 2013.
4. *[APR1400-Z-J-NR-13003-P, "Software Program Manual Technical Report," September 2013.]**
5. NRC RG 1.75, Rev. 3, "Criteria for Independence of Electrical Safety Systems," 2005.
6. NRC RG 1.180, Rev. 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," 2003.
7. APR1400-Z-J-EC-13002-P, "Diversity and Defense-in-Depth Technical Report," September 2013.
8. 10 CFR 50.55a(a)(1), "Codes and Standards, Quality Standards for Systems Important to Safety."

APR1400 DCD TIER 2

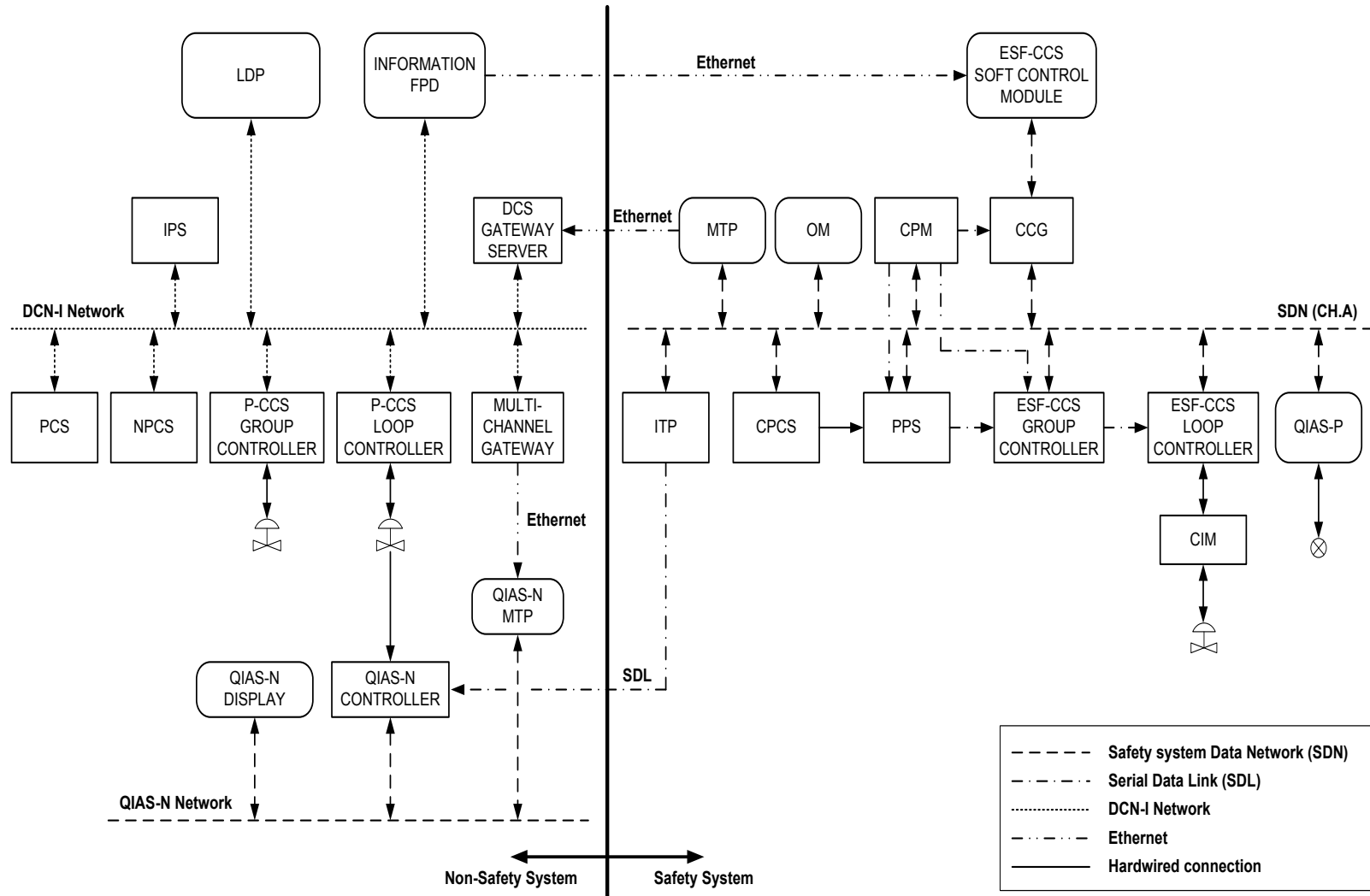


Figure 7.9-1 Data Communication Block Diagram