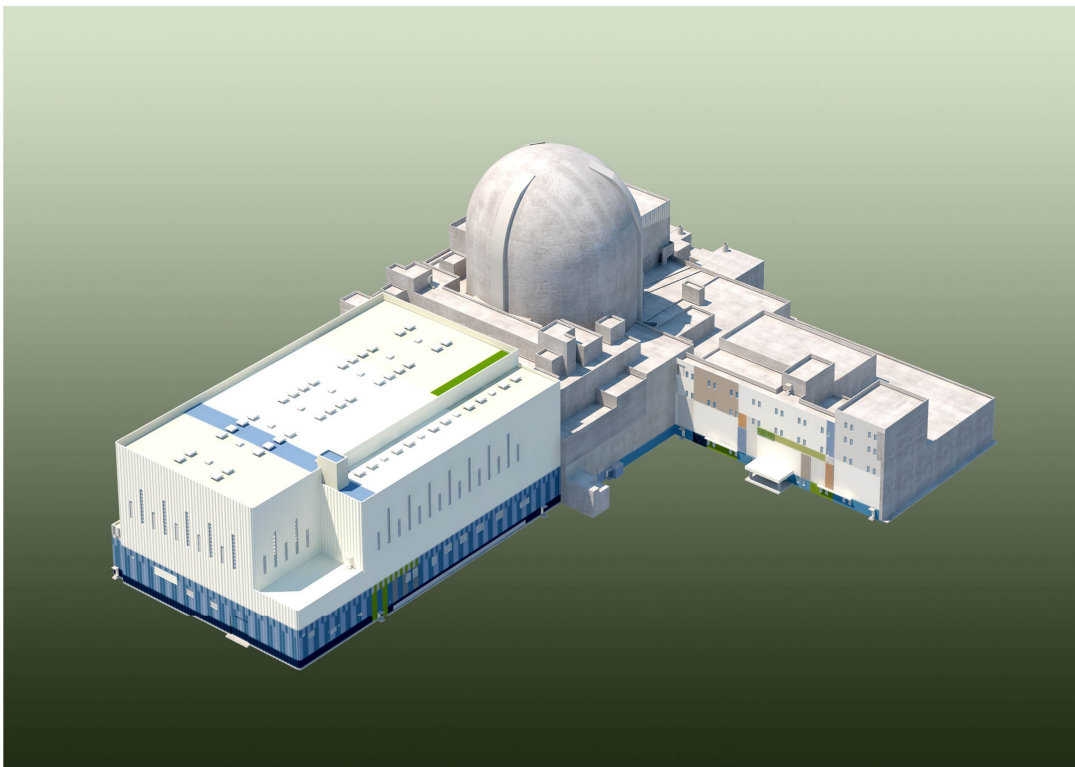


APR1400
DESIGN CONTROL DOCUMENT TIER 2

CHAPTER 7
INSTRUMENTATION AND CONTROLS

APR1400-K-X-FS-14002-NP
REVISION 3
AUGUST 2018



© 2018

KOREA ELECTRIC POWER CORPORATION
&
KOREA HYDRO & NUCLEAR POWER CO., LTD

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 of Korea Hydro & Nuclear Co., Ltd.

Copying, using, or distributing the information in this document in whole or in part is permitted only to 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

<u>NUMBER</u>	<u>TITLE</u>	<u>PAGE</u>
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	7.1-4
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(h)(2)	7.1-11
7.1.2.3	Conformance with 10 CFR 50.55a(h)(3)	7.1-11
7.1.2.4	Conformance with 10 CFR 50.34(f)(2)(v).....	7.1-12
7.1.2.5	Conformance with 10 CFR 50.34(f)(2)(xi).....	7.1-12
7.1.2.6	Conformance with 10 CFR 50.34(f)(2)(xii).....	7.1-12
7.1.2.7	Conformance with 10 CFR 50.34(f)(2)(xiv).....	7.1-12
7.1.2.8	Conformance with 10 CFR 50.34(f)(2)(xvii).....	7.1-12
7.1.2.9	Conformance with 10 CFR 50.34(f)(2)(xviii).....	7.1-12
7.1.2.10	Conformance with 10 CFR 50.34(f)(2)(xix).....	7.1-13
7.1.2.11	Conformance with 10 CFR 50.34(f)(2)(xx).....	7.1-13
7.1.2.12	Conformance with 10 CFR 50.62	7.1-13
7.1.2.13	Conformance with GDC 1	7.1-13

APR1400 DCD TIER 2

7.1.2.14	Conformance with GDC 2	7.1-13
7.1.2.15	Conformance with GDC 4	7.1-13
7.1.2.16	Conformance with GDC 10	7.1-13
7.1.2.17	Conformance with GDC 13	7.1-14
7.1.2.18	Conformance with GDC 15	7.1-14
7.1.2.19	Conformance with GDC 16	7.1-14
7.1.2.20	Conformance with GDC 19	7.1-14
7.1.2.21	Conformance with GDC 20	7.1-14
7.1.2.22	Conformance with GDC 21	7.1-14
7.1.2.23	Conformance with GDC 22	7.1-15
7.1.2.24	Conformance with GDC 23	7.1-15
7.1.2.25	Conformance with GDC 24	7.1-15
7.1.2.26	Conformance with GDC 25	7.1-15
7.1.2.27	Conformance with GDC 28	7.1-15
7.1.2.28	Conformance with GDC 29	7.1-15
7.1.2.29	Conformance with GDC 33	7.1-15
7.1.2.30	Conformance with GDC 34	7.1-16
7.1.2.31	Conformance with GDC 35	7.1-16
7.1.2.32	Conformance with GDC 38	7.1-16
7.1.2.33	Conformance with GDC 41	7.1-16
7.1.2.34	Conformance with GDC 44	7.1-16
7.1.2.35	Conformance with SRM on SECY-93-087, Item II.Q.....	7.1-16
7.1.2.36	Conformance with SRM on SECY-93-087, Item II.T	7.1-16
7.1.2.37	Conformance with NRC RG 1.22	7.1-17
7.1.2.38	Conformance with NRC RG 1.47	7.1-18
7.1.2.39	Conformance with NRC RG 1.53, as Augmented by IEEE Std. 379.....	7.1-18
7.1.2.40	Conformance with NRC RG 1.62	7.1-19
7.1.2.41	Conformance with NRC RG 1.75, as Augmented by IEEE Std. 384.....	7.1-19
7.1.2.42	Conformance with NRC RG 1.97	7.1-20
7.1.2.43	Conformance with NRC RG 1.105	7.1-20

APR1400 DCD TIER 2

7.1.2.44	Conformance with NRC RG 1.118, as Augmented by IEEE Std. 338.....	7.1-21
7.1.2.45	Conformance with NRC RG 1.151	7.1-21
7.1.2.46	Conformance with NRC RG 1.152	7.1-22
7.1.2.47	Conformance with NRC RG 1.168	7.1-23
7.1.2.48	Conformance with NRC RG 1.169	7.1-23
7.1.2.49	Conformance with NRC RG 1.170	7.1-23
7.1.2.50	Conformance with NRC RG 1.171	7.1-23
7.1.2.51	Conformance with NRC RG 1.172	7.1-23
7.1.2.52	Conformance with NRC RG 1.173	7.1-24
7.1.2.53	Conformance with NRC RG 1.180	7.1-24
7.1.2.54	Conformance with NRC RG 1.189	7.1-24
7.1.2.55	Conformance with NRC RG 1.204	7.1-24
7.1.2.56	Conformance with NRC RG 1.206	7.1-24
7.1.2.57	Conformance with BTP 7-1	7.1-24
7.1.2.58	Conformance with BTP 7-2	7.1-25
7.1.2.59	Conformance with BTP 7-3	7.1-25
7.1.2.60	Conformance with BTP 7-4	7.1-25
7.1.2.61	Conformance with BTP 7-5	7.1-25
7.1.2.62	Conformance with BTP 7-6	7.1-25
7.1.2.63	Conformance with BTP 7-8	7.1-25
7.1.2.64	Conformance with BTP 7-9	7.1-25
7.1.2.65	Conformance with BTP 7-10	7.1-26
7.1.2.66	Conformance with BTP 7-11	7.1-26
7.1.2.67	Conformance with BTP 7-12	7.1-26
7.1.2.68	Conformance with BTP 7-13	7.1-26
7.1.2.69	Conformance with BTP 7-14	7.1-26
7.1.2.70	Conformance with BTP 7-17	7.1-26
7.1.2.71	Conformance with BTP 7-18	7.1-27
7.1.2.72	Conformance with BTP 7-19	7.1-27
7.1.2.73	Conformance with BTP 7-21	7.1-27
7.1.2.74	Conformance with DI&C-ISG-04.....	7.1-27

APR1400 DCD TIER 2

7.1.3	Digital Instrumentation and Control Systems Software Design Process	7.1-27
7.1.4	Combined License Information	7.1-28
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	7.2-12
7.2.1.4	Reactor Trip Initiation Signals	7.2-13
7.2.1.5	Manual Reactor Trip and Actuated Devices	7.2-22
7.2.1.6	Bypasses	7.2-23
7.2.1.7	Interlocks	7.2-25
7.2.1.8	Redundancy	7.2-26
7.2.1.9	Diversity and Defense-in-Depth	7.2-27
7.2.1.10	Vital Instrument Power Supply	7.2-28
7.2.1.11	System Arrangement	7.2-28
7.2.2	Design Basis Information	7.2-28
7.2.2.1	Single Failure Criterion	7.2-28
7.2.2.2	Quality of Components and Modules	7.2-28
7.2.2.3	Independence	7.2-29
7.2.2.4	Diversity and Defense-in-Depth	7.2-30
7.2.2.5	System Testing and Inoperable Surveillance	7.2-30
7.2.2.6	Use of Digital Systems	7.2-31
7.2.2.7	Setpoint Determination	7.2-32
7.2.2.8	Equipment Qualification	7.2-33
7.2.3	Analysis	7.2-33
7.2.3.1	Failure Modes and Effects Analysis	7.2-33
7.2.3.2	Safety Analysis	7.2-34
7.2.3.3	Test and Inspection	7.2-34
7.2.3.4	Multiple Setpoints	7.2-34
7.2.3.5	Conformance to General Design Criteria	7.2-34

APR1400 DCD TIER 2

7.2.3.6	Conformance with IEEE Std. 603.....	7.2-34
7.2.3.7	Conformance with IEEE Std. 7-4.3.2	7.2-35
7.2.4	Combined License Information.....	7.2-35
7.2.5	References	7.2-35
7.3	Engineered Safety Features Systems.....	7.3-1
7.3.1	System Description.....	7.3-1
7.3.1.1	Engineered Safety Features Actuation System Measurement Channels	7.3-3
7.3.1.2	Engineered Safety Features Actuation System Initiation Logic.....	7.3-4
7.3.1.3	Actuation Logic.....	7.3-4
7.3.1.4	Component Control Logic	7.3-9
7.3.1.5	Bypasses	7.3-17
7.3.1.6	Interlocks.....	7.3-18
7.3.1.7	Redundancy.....	7.3-18
7.3.1.8	Emergency Diesel Generator Loading Sequencer	7.3-19
7.3.1.9	Actuated Systems	7.3-22
7.3.1.10	Vital Instrument Power Supply	7.3-26
7.3.1.11	Component Interface Module	7.3-27
7.3.2	Design Basis Information.....	7.3-27
7.3.2.1	Single Failure Criterion.....	7.3-27
7.3.2.2	Quality of Components and Modules	7.3-28
7.3.2.3	Independence	7.3-28
7.3.2.4	Diversity and Defense-in-Depth	7.3-29
7.3.2.5	System Testing and Inoperable Surveillance	7.3-29
7.3.2.6	Use of Digital Systems.....	7.3-32
7.3.2.7	Setpoint Determination	7.3-32
7.3.2.8	Equipment Qualification	7.3-32
7.3.2.9	System Drawings	7.3-33
7.3.3	Analysis.....	7.3-33
7.3.3.1	Failure Modes and Effects Analysis.....	7.3-33
7.3.3.2	Conformance with IEEE Std. 603.....	7.3-33

APR1400 DCD TIER 2

7.3.3.3	Conformance with IEEE Std. 7-4.3.2	7.3-34
7.3.3.4	Analysis for Additional Postulated Failure	7.3-34
7.3.3.5	Periodic Testing Method	7.3-34
7.3.4	Combined License Information.....	7.3-34
7.3.5	References	7.3-35
7.4	Systems Required for Safe Shutdown	7.4-1
7.4.1	System Description.....	7.4-2
7.4.2	Design Basis Information.....	7.4-9
7.4.2.1	Single Failure Criterion.....	7.4-10
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.....	7.4-11
7.4.2.6	System Drawings	7.4-11
7.4.3	Analysis	7.4-11
7.4.3.1	Conformance with IEEE Std. 603 and IEEE Std. 7-4.3.2.....	7.4-11
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	Combined License Information.....	7.4-12
7.4.5	References	7.4-12
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.....	7.5-8
7.5.1.3	Bypassed and Inoperable Status Indication	7.5-10
7.5.1.4	Alarm System.....	7.5-12
7.5.1.5	Safety Parameter Display System	7.5-13
7.5.1.6	Information Systems Associated with the Emergency Response Facility and Emergency Response Data System.....	7.5-14
7.5.2	Design Basis Information.....	7.5-14

APR1400 DCD TIER 2

7.5.2.1	Accident Monitoring Instrumentation.....	7.5-14
7.5.2.2	Inadequate Core Cooling Monitoring	7.5-17
7.5.2.3	Bypassed and Inoperable Status Indication	7.5-17
7.5.2.4	Alarm System.....	7.5-17
7.5.2.5	Safety Parameter Display System	7.5-18
7.5.2.6	Information Systems Associated with the Emergency Response Facility and Emergency Response Data System.....	7.5-18
7.5.3	Analysis	7.5-18
7.5.4	Combined License Information.....	7.5-18
7.5.5	References	7.5-19
7.6	Interlock Systems Important to Safety	7.6-1
7.6.1	System Description.....	7.6-1
7.6.1.1	Shutdown Cooling System Suction Line Isolation Valve Interlocks.....	7.6-1
7.6.1.2	Shutdown Cooling System Suction Line Relief Valve Interlocks.....	7.6-2
7.6.1.3	Safety Injection Tank Isolation Valve Interlocks	7.6-3
7.6.1.4	Component Cooling Water Non-essential Supply and Return Header Isolation Valves Interlocks.....	7.6-4
7.6.1.5	CCW Cross Connection Line Isolation Valve Interlocks.....	7.6-5
7.6.1.6	Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps.....	7.6-6
7.6.2	Design Basis Information.....	7.6-7
7.6.2.1	Applicable Codes and Regulations	7.6-7
7.6.2.2	Conformance with IEEE Std. 603.....	7.6-11
7.6.2.3	System Testing and Inoperable Surveillance	7.6-16
7.6.2.4	Use of Digital Systems.....	7.6-17
7.6.3	Analysis	7.6-17
7.6.3.1	Interlocks to Prevent Overpressurization of Low- Pressure Systems.....	7.6-17

APR1400 DCD TIER 2

7.6.3.2	Interlocks to Prevent Overpressurization of the Reactor Coolant System during Low-Temperature Operations of the Reactor Vessel	7.6-17
7.6.3.3	Interlocks for Safety Injection Tank Isolation Valves	7.6-17
7.6.3.4	Interlocks for Component Cooling Water Non- essential Supply and Return Header Isolation Valves.....	7.6-17
7.6.3.5	Interlocks for Component Cooling Water Cross Connection Line Isolation Valves	7.6-18
7.6.3.6	Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps.....	7.6-18
7.6.4	Combined License Information.....	7.6-18
7.6.5	References	7.6-18
7.7	Control Systems Not Required for Safety.....	7.7-1
7.7.1	Description	7.7-1
7.7.1.1	Control Systems	7.7-2
7.7.1.2	Main Control Room Facility	7.7-21
7.7.1.3	Large Display Panel	7.7-26
7.7.1.4	Information Processing System	7.7-27
7.7.1.5	Nuclear Steam Supply System Integrity Monitoring System.....	7.7-37
7.7.2	Design Basis Information.....	7.7-37
7.7.2.1	Safety Classification	7.7-38
7.7.2.2	Effects of Control System Operation upon Accidents	7.7-38
7.7.2.3	Effects of Control System Failures	7.7-38
7.7.2.4	Effects of Control System Failures Caused by Accidents.....	7.7-39
7.7.2.5	Environmental Control System.....	7.7-39
7.7.2.6	Use of Digital Systems.....	7.7-39
7.7.2.7	Independence	7.7-39
7.7.2.8	Diversity and Defense-in-Depth	7.7-40
7.7.2.9	Potential for Inadvertent Actuation	7.7-40
7.7.2.10	Control of Access.....	7.7-41
7.7.3	Analysis	7.7-41

APR1400 DCD TIER 2

7.7.4	Combined License Information.....	7.7-41
7.7.5	References	7.7-42
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 Engineered Safety Features Actuation Switches	7.8-4
7.8.1.3	Diverse Indication System	7.8-4
7.8.2	Design Basis Information.....	7.8-5
7.8.2.1	Diverse Protection System	7.8-5
7.8.2.2	Diverse Manual Engineered Safety Features Actuation Switches	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
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	Safety System Data Network for Safety Systems.....	7.9-2
7.9.1.2	Serial Data Link for Safety Systems	7.9-3
7.9.1.3	Data Communication Network-Information Network 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	7.9-11

APR1400 DCD TIER 2

7.9.2.5	Control of Access	7.9-12
7.9.2.6	Single Failure Criterion.....	7.9-12
7.9.2.7	Independence	7.9-12
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.....	7.9-13
7.9.2.11	Electromagnetic Interference and Radio-Frequency Interference Susceptibility	7.9-13
7.9.2.12	Diversity and Defense-in-Depth	7.9-13
7.9.2.13	Seismic Hazards	7.9-14
7.9.3	Analysis	7.9-14
7.9.4	Combined License Information.....	7.9-14
7.9.5	References	7.9-14

APR1400 DCD TIER 2

LIST OF TABLES

<u>NUMBER</u>	<u>TITLE</u>	<u>PAGE</u>
Table 7.1-1	Regulatory Requirements Applicability Matrix.....	7.1-37
Table 7.2-1	Reactor Protection System Operating Bypass Permissive	7.2-38
Table 7.2-2	Reactor Protection System Monitored Plant Variable Ranges	7.2-39
Table 7.2-3	Reactor Protection System Sensors.....	7.2-40
Table 7.2-4	Reactor Protection System Design Inputs.....	7.2-41
Table 7.2-5	Reactor Protective Instrumentation Response Time	7.2-43
Table 7.2-6	Critical Function Success Path Diversity	7.2-45
Table 7.2-7	Failure Modes and Effects Analysis for the Plant Protection System	7.2-46
Table 7.3-1	ESFAS Operating Bypass Permissive.....	7.3-38
Table 7.3-2	Design Basis Events Requiring ESF System Action	7.3-39
Table 7.3-3	Monitored Variables for ESFAS Signals	7.3-40
Table 7.3-4	ESFAS Sensors	7.3-41
Table 7.3-5A	NSSS ESFAS Setpoints and Margins to Actuation	7.3-42
Table 7.3-5B	BOP ESFAS Setpoints and Margins to Actuation	7.3-43
Table 7.3-6	ESFAS Variable Ranges	7.3-44
Table 7.3-7	ESF Response Time	7.3-45
Table 7.3-8	Failure Modes and Effects Analysis for the Engineered Safety Features-Component Control System	7.3-48
Table 7.4-1	Remote Shutdown Console Instrumentation and Controls for Hot Shutdown.....	7.4-15
Table 7.4-2	Remote Shutdown Console Instrumentation and Controls for Cold Shutdown.....	7.4-19
Table 7.5-1	Accident Monitoring Instrumentation Variables	7.5-21
Table 7.5-2	Basis and Analysis of Selection for AMI Variables	7.5-27
Table 7.6-1	Shutdown Cooling System and Safety Injection Tank Interlock	7.6-20
Table 7.6-2	CCW Non-essential Supply and Return Header Isolation Valves and Cross Connection Line Isolation Valves.....	7.6-21

APR1400 DCD TIER 2

Table 7.7-1	Control Groups for the NSSS Control Functions.....	7.7-44
Table 7.7-2	Control Limit and Interlocks on Digital Rod Control System	7.7-45
Table 7.8-1	Diverse Protection System Parameter	7.8-17
Table 7.8-2	Diverse Functions Remain Available after the Software CCF of Safety Instrumentation and Control Systems.....	7.8-18
Table 7.8-3	Diverse Actuation Signals.....	7.8-19
Table 7.8-4	Display and Control Parameters for the DIS.....	7.8-20
Table 7.8-5	Safe State of ESF Components for State-Based Priority	7.8-22

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	7.1-43
Figure 7.1-2	Symbol & Legend Diagram	7.1-44
Figure 7.2-1	PPS Basic Block Diagram.....	7.2-71
Figure 7.2-2	PPS Measurement Channel Functional Diagram (Pressurizer Pressure Narrow Range)	7.2-72
Figure 7.2-3	Reed Switch Position Transmitter Assembly Schematic	7.2-73
Figure 7.2-4	CEA Position Signal Flow for CPCS.....	7.2-74
Figure 7.2-5	Ex-Core Neutron Monitoring System (Safety Channel).....	7.2-75
Figure 7.2-6	Reactor Coolant Pump Shaft Speed Sensing System.....	7.2-76
Figure 7.2-7	Core Protection Calculator Functional Block Diagram	7.2-77
Figure 7.2-8	PPS Bistable Trip Logic Functional Block Diagram	7.2-78
Figure 7.2-9	Reactor Trip Switchgear System Interface Diagram	7.2-79
Figure 7.2-10	PPS Channel A Trip Path Diagram.....	7.2-80
Figure 7.2-11	RPS Testing Overlap.....	7.2-81
Figure 7.2-12	Interface and Test Processor Block Diagram.....	7.2-82
Figure 7.2-13	PPS Channel Contact Bistable Interface Diagram	7.2-83
Figure 7.2-14	Plant Protection System Interface Logic Diagram for Division D	7.2-84
Figure 7.2-15	Reactor Trip Initiation Diagram.....	7.2-85
Figure 7.2-16	Manual Reactor Trip Initiation Diagram.....	7.2-86
Figure 7.2-17	Functional Logic Diagram for Variable Overpower	7.2-87
Figure 7.2-18	Functional Logic Diagram for High Logarithmic Power Level.....	7.2-88
Figure 7.2-19	Functional Logic Diagram for High Local Power Density	7.2-89
Figure 7.2-20	Functional Logic Diagram for Low Departure from Nucleate Boiling Ratio	7.2-90
Figure 7.2-21	Functional Logic Diagram for High Pressurizer Pressure	7.2-91
Figure 7.2-22	Functional Logic Diagram for Low Pressurizer Pressure	7.2-92

APR1400 DCD TIER 2

Figure 7.2-23	Functional Logic Diagram for Low Steam Generator Water Level.....	7.2-93
Figure 7.2-24	Functional Logic Diagram for Low Steam Generator Pressure.....	7.2-94
Figure 7.2-25	Functional Logic Diagram for High Containment Pressure	7.2-95
Figure 7.2-26	Functional Logic Diagram for High Steam Generator Water Level.....	7.2-96
Figure 7.2-27	Functional Logic Diagram for Low Reactor Coolant Flow	7.2-97
Figure 7.2-28	Functional Logic Diagram for Reactor Trip Signal Generation	7.2-98
Figure 7.2-29	Functional Logic Diagram for DNBR/LPD Operating Bypass Permissive	7.2-99
Figure 7.2-30	Functional Logic Diagram for Low Pressurizer Pressure Operating Bypass Permissive.....	7.2-100
Figure 7.2-31	Functional Logic Diagram for High Logarithmic Power Level Operating Bypass Permissive.....	7.2-101
Figure 7.2-32	Functional Logic Diagram for CWP	7.2-102
Figure 7.3-1	Simplified Functional Diagram of the ESF-CCS.....	7.3-69
Figure 7.3-2	Block Diagram of the ESF-CCS	7.3-70
Figure 7.3-3	ESF-CCS Simplified Logic Diagram for 2-out-of-4 Actuation.....	7.3-71
Figure 7.3-4	ESFAS Functional Logic (SIAS).....	7.3-72
Figure 7.3-5	ESFAS Functional Logic (CSAS).....	7.3-73
Figure 7.3-6	ESFAS Functional Logic (CIAS).....	7.3-74
Figure 7.3-7	ESFAS Functional Logic (MSIS)	7.3-75
Figure 7.3-8	ESFAS Functional Logic (AFAS-1 and AFAS-2).....	7.3-77
Figure 7.3-9	ESFAS Functional Logic (FHEVAS)	7.3-78
Figure 7.3-10	ESFAS Functional Logic (CPIAS)	7.3-79
Figure 7.3-11	ESFAS Functional Logic (CREVAS).....	7.3-80
Figure 7.3-12	CLD for a Solenoid-Operated Valve.....	7.3-81
Figure 7.3-13	CLD for a Modulating Valve with Solenoid Operator.....	7.3-82
Figure 7.3-14	Motor-Operated Valve Functional Interface Design.....	7.3-83
Figure 7.3-15	CLD for a Full Stroke Motor-Operated Valve	7.3-84
Figure 7.3-16	CLD for a Throttling Motor-Operated Valve.....	7.3-85

APR1400 DCD TIER 2

Figure 7.3-17	CLD for a Non-reversing Motor Starter Operated Component	7.3-86
Figure 7.3-18	CLD for a Circuit Breaker Operated Component	7.3-87
Figure 7.3-19	CLD for a Modulating Component	7.3-88
Figure 7.3-20	CLD for a Electro-Hydraulic Motor Damper.....	7.3-89
Figure 7.3-21	EDG Loading Sequencer – Control Logic Diagram	7.3-90
Figure 7.3-22	ESF-CCS Simplified Test Logic Diagram	7.3-94
Figure 7.3-23	Radiation Monitoring System Measurement Channel Functional Diagram.....	7.3-95
Figure 7.3-24	ESF-CCS Actuation Test Logic Diagram	7.3-96
Figure 7.4-1	Interface Diagram for Division A MCR/RSR master transfer switches	7.4-20
Figure 7.4-2	Interface Diagram for Division AB MCR/RSR master transfer switches	7.4-21
Figure 7.4-3	MCR/RSR Master Transfer Logic (Division A).....	7.4-22
Figure 7.4-4	Layout of Remote Shutdown Room.....	7.4-23
Figure 7.5-1	Diverse Display of Accident Monitoring Type A, B and C Variables	7.5-35
Figure 7.5-2	QIAS-N Block Diagram.....	7.5-36
Figure 7.5-3	HSI Primary and Backup Means.....	7.5-37
Figure 7.6-1A	Interlocks for Shutdown Cooling System Suction Line Isolation Valve	7.6-22
Figure 7.6-1B	Interlocks for Shutdown Cooling System Suction Line Isolation Valve	7.6-23
Figure 7.6-1C	Interlocks for Shutdown Cooling System Suction Line Isolation Valve	7.6-24
Figure 7.6-2	Interlocks for Safety Injection Tank Isolation Valve	7.6-25
Figure 7.6-3	Interlocks for Component Cooling Water Non-essential Supply and Return Header Isolation Valves in the Division I and Cross Connection Line Isolation Valves	7.6-26
Figure 7.6-4	Interlocks for Component Cooling Water Non-essential Supply and Return Header Isolation Valves in the Division II	7.6-27

APR1400 DCD TIER 2

Figure 7.6-5	Interlocks for Both Shutdown Cooling Pump and Containment Spray Pump	7.6-28
Figure 7.7-1	Reactor Regulating System Block Diagram	7.7-46
Figure 7.7-2	Digital Rod Control System - Reactor Protection System Interface Block Diagram	7.7-47
Figure 7.7-3	Pressurizer Pressure Control System Block Diagram	7.7-48
Figure 7.7-4	Pressurizer Level Control System Block Diagram	7.7-49
Figure 7.7-5	Feedwater Control System Block Diagram	7.7-50
Figure 7.7-6	Steam Bypass Control System Block Diagram	7.7-51
Figure 7.7-7	Reactor Power Cutback System Simplified Block Diagram	7.7-52
Figure 7.7-8	Process-Component Control System Simplified Block Diagram	7.7-53
Figure 7.7-9	Core Operating Limit Supervisory System Functional Diagram	7.7-54
Figure 7.7-10	Ex-Core Neutron Flux Monitoring System Startup and Control Channel Flow Diagram	7.7-55
Figure 7.7-11	N-16 Detection and Alarm Logic	7.7-56
Figure 7.7-12	HSI Information Processing Block Diagram	7.7-57
Figure 7.7-13	Layout of Main Control Room	7.7-58
Figure 7.7-14	I&C System Architecture for the RCC Panel	7.7-59
Figure 7.7-15	Configuration of Workstation Disable Switch	7.7-60
Figure 7.8-1	Diverse Protection System Block Diagram	7.8-24
Figure 7.8-2	Diverse Reactor Trip, Turbine Trip, AFWS and SIS Actuation	7.8-25
Figure 7.8-3	Diverse Reactor Trip and Turbine Trip	7.8-26
Figure 7.8-4	Diverse AFWS Actuation	7.8-27
Figure 7.8-5	Diverse SIS Actuation	7.8-28
Figure 7.8-6	DMA Switches Block Diagram	7.8-29
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

APR1400 DCD TIER 2

CCF	common-cause failure
CCG	control channel gateway
CCW	component cooling water
CCWS	component cooling water system
CEA	control element assembly
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

APR1400 DCD TIER 2

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
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
EDS	external data communication system
EMI	electromagnetic interference
ENFMS	ex-core neutron flux monitoring system
EOF	emergency operations 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

APR1400 DCD TIER 2

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
FPC	front panel control
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 monitoring system
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

APR1400 DCD TIER 2

ISG	Interim Staff Guidance
ITA	important-to-availability
ITP	interface and test processor
ITS	important-to-safety
IVMS	internal vibration monitoring system
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
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
NDL	nuclear data link

APR1400 DCD TIER 2

NERC	nuclear emergency response center
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	pipng 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
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
RCC	remote control center
RCGV	reactor coolant gas vent
RCGVS	reactor coolant gas vent system

APR1400 DCD TIER 2

RCP	reactor coolant pump
RCPB	reactor coolant pressure boundary
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	Secretary of the Commission, Office of the NRC

APR1400 DCD TIER 2

SG	steam generator
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

APR1400 DCD TIER 2

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 the safety systems and (2) non-qualified distributed control system (DCS) platform for the data processing system and non-safety control systems. In addition, independent systems such as the turbine/generator (T/G) control and protection system, the nuclear steam supply system (NSSS) monitoring system, 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.

All figures provided in Chapter 7 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference.

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 described in Section 8 of the Safety I&C System Technical Report (Reference 2) is loaded with the APR1400-specific application software to implement various 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 as described in the Software Program Manual Technical Report (Reference 1). The qualified PLC platform applies to the following safety systems:

- a. Plant protection system (PPS)

APR1400 DCD TIER 2

- b. Core protection calculator system (CPCS)
- c. Engineered safety features – component control system (ESF-CCS)
- d. ESF-CCS soft control module (ESCM)
- e. Qualified indication and alarm system – P (QIAS-P)

The specific design information of the qualified PLC platform is described in Common Qualified Platform Topical Report (Reference 77), APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items (Reference 78), and Common Q Platform Supplemental Information in Support of the APR1400 Design Certification (Reference 79).

The Safety I&C System Technical Report 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 independent platforms that are diverse from the safety-qualified PLC platform: ex-core neutron flux monitoring system (ENFMS) (see Subsection 7.2.1.1.c), auxiliary process cabinet – safety (APC-S) (see Subsection 7.2.1), safety portion of radiation monitoring system (RMS) (refer to Section 11.5 and Subsection 12.3.4) and component interface module (CIM) (see Subsection 7.3.1.11).

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 the 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 the NSSS process control system (NPCS)

APR1400 DCD TIER 2

- 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 important plant parameters and maintains diversity from the IPS.

Some I&C functions are not installed on a common PLC and DCS platform. These functions are implemented in independent 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 or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety systems. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety and non-safety data communication systems. The safety and non-safety data communication systems are diverse.

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.

APR1400 DCD TIER 2

7.1.1.1 Plant Protection System

The PPS is a safety system that includes electrical, electronic, network, mechanical devices, and circuits and performs the following protective functions:

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 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 shut down.

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

APR1400 DCD TIER 2

- c. Safety injection system (SIS)
- d. Auxiliary feedwater system (AFWS)
- e. Containment spray system (CSS)
- 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, the safety portion of the RMS, 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. AFWS

APR1400 DCD TIER 2

- b. Main steam system (MSS) – atmospheric dump
- c. Shutdown cooling system (SCS)
- d. Safety injection system (SIS)
- e. Manual actuation of pressurizer pilot operated safety relief valve (POS RVs)
- f. Reactor coolant gas vent system (RCGVS)

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

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

APR1400 DCD TIER 2

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

The QIAS-P processors and display processors are dedicated to continuously monitor and display AMI Type A, B and C variables.

The QIAS-N displays AMI Type A, B and C variables. The QIAS-N also displays selected Type D and E variables.

The IPS displays all AMI variables.

b. Inadequate core cooling (ICC) monitoring instrumentation

The ICC monitoring instrumentation provides an unambiguous, easy-to-interpret indication of ICC. The design follows the guidance of II.F.2 of NUREG-0737 (Reference 4). The safety parameter display system (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 (BISI)

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 systems are redundantly implemented by the IPS and QIAS-N. The IPS and QIAS-N are independent and diverse from each other. Therefore, any single alarm system failure will not cause a total loss of the plant's alarm system.

e. Safety parameter display system

APR1400 DCD TIER 2

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 No. 1 (Reference 75).

- 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), and emergency operations 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 No. 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) non-essential supply and return header isolation valve interlocks
- e. CCW cross connection line isolation valve interlocks
- f. Interlocks for both shutdown cooling pumps and containment spray pumps

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-

APR1400 DCD TIER 2

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 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
- b. Diverse manual ESF actuation switches
- c. Diverse indication system

Diverse I&C systems are described in Section 7.8.

7.1.1.9 Data Communication Systems

Data communication systems provide high-speed and reliable communications between each segment of a division, between divisions, 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 for safety systems

APR1400 DCD TIER 2

- b. Serial data link for safety systems
- c. Data communication network – information network 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 7.1.2.74 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, the General Design Criteria (GDC) in 10 CFR Part 50, Appendix A (Reference 20), standards, and other documents used in the design of the systems listed in Subsection 7.1.1. Compliance with 10 CFR Part 50 and 52 is described in Section 3.1 of the Safety I&C System Technical Report. Compliance with 10 CFR Part 50, Appendix A, General Design Criteria is described in Section 3.2 of the Safety I&C System Technical Report. Compliance with IEEE Std. 603 (Reference 8) is described in Appendix A of the Safety I&C System Technical Report.

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.

APR1400 DCD TIER 2

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.

7.1.2.1.5 Interlocks

The interlocks for safety instrumentation are described in Subsections 7.2.1.7 and 7.3.1.6 and Section 7.6.

7.1.2.1.6 Bypasses

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

7.1.2.1.7 Diversity

The diversity for safety instrumentation is described in Subsections 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(h)(2)

Not Applicable.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.55a(h)(3) (Reference 10) as described in Section 3.1 of the Safety I&C System Technical Report 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 provided in the Safety I&C System Technical Report.

APR1400 DCD TIER 2

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(v) (Reference 11) as described in Section 3.1 of the Safety I&C System Technical Report. 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 with 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.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xi) (Reference 12), as described in Subsection 7.5.1.1.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xii) (Reference 13) as described in Section 3.1 of the Safety I&C System Technical Report. The automatic and manual initiation of the auxiliary feedwater system is described in Subsection 7.3.1.9.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xiv) (Reference 14). The containment isolation function, including reset of the function, is described in Subsection 7.3.1.9.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xvii) (Reference 15), as described in Subsection 7.5.1.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xviii) (Reference 16), as described in Subsection 7.5.1.2.

APR1400 DCD TIER 2

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xix) (Reference 17), as described in Subsection 7.5.1.1.

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

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.34(f)(2)(xx) (Reference 18), as described in Subsection 7.5.2.1.

7.1.2.12 Conformance with 10 CFR 50.62

The applicable I&C systems listed in Table 7.1-1 meet the requirements of 10 CFR 50.62 (Reference 19). The conformance with 10 CFR 50.62 is described in the Diversity and Defense-in-Depth Technical Report.

7.1.2.13 Conformance with GDC 1

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 1 (Reference 20) as described in Section 3.2 of the Safety I&C System Technical Report. The quality assurance program description complies with the requirements of 10 CFR Part 50, Appendix B (Reference 21).

7.1.2.14 Conformance with GDC 2

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 2 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.15 Conformance with GDC 4

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 4 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.16 Conformance with GDC 10

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 10 as described in Section 3.2 of the Safety I&C System Technical Report.

APR1400 DCD TIER 2

7.1.2.17 Conformance with GDC 13

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 13 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.18 Conformance with GDC 15

The applicable I&C systems listed in Table 7.1-1 meets the requirement of GDC 15 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.19 Conformance with GDC 16

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 16 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.20 Conformance with GDC 19

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 19 as described in Section 3.2 of the Safety I&C System Technical Report. 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.

7.1.2.21 Conformance with GDC 20

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 20. The protection function is described in Sections 7.2 and 7.3.

7.1.2.22 Conformance with GDC 21

The applicable I&C systems listed in Table 7.1-1 are designed to meet the requirement of GDC 21 (Reference 20). Clause 5.1 of IEEE Std. 603 corresponds to the requirement that no single failure results in loss of the protection function as stated in GDC 21. The protection system is designed to conform to Clause 5.1 of IEEE Std. 603. Conformance to IEEE Std. 603, Clause 5.1 is described in Section A.5.1 of the Safety I&C System Technical Report. The protection system is designed to meet the requirement that removal from service of any component or channel shall not result in loss of the required minimum redundancy; Sections 7.2.1.8 and 7.3.1.7 describe the safety systems' compliance.

APR1400 DCD TIER 2

7.1.2.23 Conformance with GDC 22

The applicable I&C systems listed in Table 7.1-1 are designed to meet the requirement of GDC 22 as described in Subsections 7.2.2.3 and 7.3.2.3. Conformance to functional diversity criteria of GDC 22 is also described in Section 3.1.18. 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.

7.1.2.24 Conformance with GDC 23

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 23. Failure modes and effects analysis for protection systems is described in Subsections 7.2.3.1 and 7.3.3.1.

7.1.2.25 Conformance with GDC 24

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 24 as described in A.5.6 of the Safety I&C System Technical Report. Electrical isolation, physical separation, and communication independence are maintained between redundant safety divisions and between the safety system and non-safety system.

7.1.2.26 Conformance with GDC 25

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 25 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.27 Conformance with GDC 28

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 28 as described in Subsections 7.6.2.1 and 7.7.1.1.

7.1.2.28 Conformance with GDC 29

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 29 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.29 Conformance with GDC 33

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 33 as described in Section 3.2 of the Safety I&C System Technical Report.

APR1400 DCD TIER 2

7.1.2.30 Conformance with GDC 34

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 34 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.31 Conformance with GDC 35

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 35 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.32 Conformance with GDC 38

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 38 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.33 Conformance with GDC 41

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 41 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.34 Conformance with GDC 44

The applicable I&C systems listed in Table 7.1-1 meet the requirements of GDC 44 as described in Section 3.2 of the Safety I&C System Technical Report.

7.1.2.35 Conformance with SRM on SECY-93-087, Item II.Q

Analyses and design features for diversity and defense-in-depth for the instrumentation and control systems are provided in accordance with the Staff Requirements Memorandum (SRM) on SECY-93-087, Item II.Q (Reference 22), as referenced by NUREG-0800, BTP 7-19 (Reference 70). The analyses and design features address postulated safety system CCFs and are described in the Diversity and Defense-in-Depth Technical Report.

7.1.2.36 Conformance with SRM on SECY-93-087, Item II.T

The alarm systems are required to meet the redundancy, independence, and safety alarm system requirements in accordance with SRM on SECY-93-087, Item II.T (Reference 5). The APR1400 design complies with the requirements as follows:

APR1400 DCD TIER 2

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 processors also provide redundant processing in a hot standby configuration. Multi-divisional 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-division 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 IPS and QIAS-N are isolated from each other with qualified isolation devices so a failure of the IPS will not affect the QIAS-N.

c. Safety alarm system requirements

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

7.1.2.37 Conformance with NRC RG 1.22

The I&C systems that are applicable to NRC RG 1.22 (Reference 24), 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

APR1400 DCD TIER 2

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. The provisions for operating bypass and trip channel bypass are provided. 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.

7.1.2.38 Conformance with NRC RG 1.47

The I&C systems that are applicable to NRC RG 1.47 (Reference 25), as shown in Table 7.1-1, comply with the recommendations of NRC RG 1.47. A discussion of the application of the BISI is described in Subsection 7.5.1.3.

7.1.2.39 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 26), as augmented by IEEE Std. 379 (Reference 27) 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.

APR1400 DCD TIER 2

7.1.2.40 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. Conformance with NRC RG 1.62 (Reference 28) 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.
- 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.

7.1.2.41 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 29) as endorsed by NRC RG 1.75 (Reference 30) 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 divisions of the RPS and ESFAS, which provides the separation and independence necessary to meet the requirements of Clause 5.6 of IEEE Std. 603.

APR1400 DCD TIER 2

The independence and separation of redundant Class 1E circuits within and between the PPS assemblies or ESF-CCS assemblies are accomplished primarily by using fiber-optic technology. The optical technology provides reasonable assurance that no single credible electrical fault in a PPS division will prevent the circuitry in any other redundant division 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 divisions in the redundant ESF systems. The component control logic for each division is contained in a separate cabinet. The redundant cabinets are physically separated from each other by locating them in separate zones.

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

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

The digital data sent from the safety system to non-safety systems (e.g., IPS, QIAS-N) for status monitoring, alarm, and display are isolated from the safety system. Fiber-optic isolation and other techniques are used to provide reasonable assurance that no credible failures on the non-Class 1E side of the isolation device will affect the PPS side and that the independence of the PPS will not be jeopardized.

7.1.2.42 Conformance with NRC RG 1.97

The design of the accident monitoring instrumentation system (the QIAS-P, QIAS-N, and IPS) is described in Subsection 7.5.1.1. The design complies with NRC RG 1.97.

7.1.2.43 Conformance with NRC RG 1.105

The setpoint methodology (Reference 72) follows the methodology in ANSI/ISA S67.04 (Reference 34) as endorsed by NRC RG 1.105 (Reference 35) except for the setpoints calculation using CPC Setpoint Analysis Methodology Technical Report (Reference 82).

APR1400 DCD TIER 2

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 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.

7.1.2.44 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 36), as augmented by IEEE Std. 338 (Reference 37) 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 divisions 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 divisions.

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.

7.1.2.45 Conformance with NRC RG 1.151

Instrument sensing lines comply with NRC RG 1.151 (Reference 38). Compliance with NRC RG 1.151 is described in Section 1.9.

APR1400 DCD TIER 2

7.1.2.46 Conformance with NRC RG 1.152

NRC RG 1.152 (Reference 32) states that the requirements set forth in IEEE Std. 7-4.3.2 (Reference 31) provide methods for designing, verifying, and implementing software and for validating computer systems in safety systems in nuclear power plants.

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

The Secure Development and Operational Environment (SDOE) for APR1400 Computer-Based I&C Safety Systems Technical Report (Reference 83) describes compliance to SDOE guidance of NRC RG 1.152 Revision 3. The design features and processes are applicable to all safety systems implemented on the common safety qualified PLC platform: PPS, ESF-CCS, CPCS, and QIASP.

Clause 5.3.3 of IEEE Std. 7-4.3.2 requires V&V of software in accordance with IEEE Std. 1012 (Reference 33), 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 is qualified as safety-critical (SC) or important-to-safety (ITS) 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 and high local power density. 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 described in Subsection 7.5.1.1, is assigned to the ITS class. The ITS class 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

APR1400 DCD TIER 2

Software Program Manual Technical Report. The design and V&V for SC and ITS class software are described in the Software Program Manual Technical Report.

7.1.2.47 Conformance with NRC RG 1.168

The I&C systems that are applicable to NRC RG 1.168 (Reference 39), as shown in Table 7.1-1, comply with IEEE Std. 1028 (Reference 40) and IEEE Std. 1012 as endorsed by NRC RG 1.168. The activities associated with conformance to NRC RG 1.168 are described in the Software Program Manual Technical Report.

7.1.2.48 Conformance with NRC RG 1.169

The I&C systems that are applicable to NRC RG 1.169 (Reference 41), as shown in Table 7.1-1, comply with NRC RG 1.169, which endorses IEEE Std. 828 (Reference 42). The activities associated with conformance to NRC RG 1.169 are described in the Software Program Manual Technical Report.

7.1.2.49 Conformance with NRC RG 1.170

The I&C systems that are applicable to NRC RG 1.170 (Reference 43), as shown in Table 7.1-1, comply with IEEE Std. 829 (Reference 44), as endorsed by NRC RG 1.170. The activities associated with compliance to NRC RG 1.170 are described in the Software Program Manual Technical Report.

7.1.2.50 Conformance with NRC RG 1.171

The I&C systems that are applicable to NRC RG 1.171 (Reference 45), as shown in Table 7.1-1, comply with IEEE Std. 1008 (Reference 46), as endorsed by NRC RG 1.171. The activities associated with conformance to NRC RG 1.171 are described in the Software Program Manual Technical Report.

7.1.2.51 Conformance with NRC RG 1.172

The I&C systems that are applicable to NRC RG 1.172 (Reference 47), as shown in Table 7.1-1, comply with IEEE Std. 830 (Reference 48), as endorsed by NRC RG 1.172. The activities associated with conformance to NRC RG 1.172 are described in the Software Program Manual Technical Report.

APR1400 DCD TIER 2

7.1.2.52 Conformance with NRC RG 1.173

The I&C systems that are applicable to NRC RG 1.173 (Reference 49), as shown in Table 7.1-1, comply with IEEE Std. 1074 (Reference 50), as endorsed by NRC RG 1.173. The activities associated with conformance to NRC RG 1.173 are described in the Software Program Manual Technical Report.

7.1.2.53 Conformance with NRC RG 1.180

The I&C systems that are applicable to NRC RG 1.180 (Reference 51), as shown in Table 7.1-1, are designed, tested, qualified, and installed to conform with the requirements and guidance specified in NRC RG 1.180. The equipment qualification plan is described in Section 6 of the Safety I&C System Technical Report.

7.1.2.54 Conformance with NRC RG 1.189

The I&C systems that are applicable to NRC RG 1.189 (Reference 52), as shown in Table 7.1-1, are designed in accordance with NRC RG 1.189. The details of the conformance with NRC RG 1.189 are provided in Chapter 9.

7.1.2.55 Conformance with NRC RG 1.204

The I&C systems that are applicable to NRC RG 1.204 (Reference 53), as shown in Table 7.1-1, comply with IEEE Std. 1050 (Reference 76), as endorsed by NRC RG 1.204. The details of the conformance with NRC RG 1.204 are provided in Chapter 8.

7.1.2.56 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 54) together with NUREG-0800 (Reference 23) in order for NRC to evaluate and confirm the safety evaluation.

7.1.2.57 Conformance with BTP 7-1

The I&C systems that are applicable to BTP 7-1 (Reference 55), as shown in Table 7.1-1, are designed in accordance with BTP 7-1.

APR1400 DCD TIER 2

7.1.2.58 Conformance with BTP 7-2

The I&C systems that are applicable to BTP 7-2 (Reference 56), as shown in Table 7.1-1, are designed in accordance with BTP 7-2, as described in Subsection 7.6.1.3 and Figure 7.6-2.

7.1.2.59 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 57) is not applicable.

7.1.2.60 Conformance with BTP 7-4

The I&C systems that are applicable to BTP 7-4 (Reference 58), as shown in Table 7.1-1, are designed in accordance with BTP 7-4.

7.1.2.61 Conformance with BTP 7-5

The I&C systems that are applicable to BTP 7-5 (Reference 59), as shown in Table 7.1-1, are designed in accordance with BTP 7-5.

7.1.2.62 Conformance with BTP 7-6

The APR1400 does not have a recirculation mode. Therefore, BTP 7-6 (Reference 60) is not applicable.

7.1.2.63 Conformance with BTP 7-8

The I&C systems that are applicable to BTP 7-8 (Reference 61), as shown in Table 7.1-1, are designed in accordance with BTP 7-8.

7.1.2.64 Conformance with BTP 7-9

The I&C systems that are applicable to BTP 7-9 (Reference 62), as shown in Table 7.1-1, are designed in accordance with BTP 7-9.

APR1400 DCD TIER 2

7.1.2.65 Conformance with BTP 7-10

The I&C systems that are applicable to BTP 7-10 (Reference 63), as shown in Table 7.1-1, are designed in accordance with BTP 7-10, as described in Subsection 7.1.2.42.

7.1.2.66 Conformance with BTP 7-11

The I&C systems that are applicable to BTP 7-11 (Reference 64), as shown in Table 7.1-1, are designed in accordance with BTP 7-11.

7.1.2.67 Conformance with BTP 7-12

The I&C systems that are applicable to BTP 7-12 (Reference 65), as shown in Table 7.1-1, are designed in accordance with BTP 7-12.

7.1.2.68 Conformance with BTP 7-13

The I&C systems that are applicable to BTP 7-13 (Reference 66), as shown in Table 7.1-1, are designed in accordance with BTP 7-13.

7.1.2.69 Conformance with BTP 7-14

The I&C systems that are applicable to BTP 7-14 (Reference 67), as shown in Table 7.1-1, are designed in accordance with BTP 7-14.

7.1.2.70 Conformance with BTP 7-17

The I&C systems that are applicable to BTP 7-17 (Reference 68), as shown in Table 7.1-1, are designed in accordance with BTP 7-17. Test provisions for the 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 are qualified in accordance with IEEE Std. 7-4.3.2, as endorsed by NRC RG 1.152, and are assigned to ITS software class.

The justification for this deviation is described in Subsection 7.1.2.46.

APR1400 DCD TIER 2

7.1.2.71 Conformance with BTP 7-18

The I&C systems that are applicable to BTP 7-18 (Reference 69), 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 qualified as described in the Safety I&C System Technical Report. 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.

7.1.2.72 Conformance with BTP 7-19

The I&C systems that are applicable to BTP 7-19 (Reference 70), as shown in Table 7.1-1, are designed in accordance with BTP 7-19. Compliance to this BTP is addressed in the Diversity and Defense-in-Depth Technical Report.

7.1.2.73 Conformance with BTP 7-21

The I&C systems that are applicable to BTP 7-21 (Reference 71), 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 Response Time Analysis of Safety I&C System Technical Report (Reference 74).

7.1.2.74 Conformance with DI&C-ISG-04

The compliance of the safety I&C systems with DI&C-ISG-04 (Reference 73) 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 these processes. The software quality assurance program is implemented in accordance with 10 CFR Part 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. The software development process is carried out throughout the software life cycle, which consists of the following:

- a. Concept phase
- b. Requirements phase
- c. Design phase
- d. Implementation phase
- e. Test phase
- f. Installation and checkout phase
- g. Operation and maintenance phase

Software is classified based on the functionality and importance related to safety, as described in the Software Program Manual Technical Report. The software that is used within the APR1400 I&C systems is assigned to one of the following classes:

- a. SC (Protection)
- b. ITS
- c. Important-to-availability (ITA)
- d. General purpose

7.1.4 Combined License Information

- COL 7.1(1) The COL applicant is to provide the software installation plan, the software training plan, and the software operation and maintenance plan for the safety I&C systems, as described in the Software Program Manual Technical Report.
- COL 7.1(2) The COL applicant is to provide justifiable software reliability data for software used in the digital I&C systems (i.e., PPS and DPS).

APR1400 DCD TIER 2

7.1.5 References

1. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.
2. APR1400-Z-J-NR-14001-P, "Safety I&C System," Rev. 3, KEPCO & KHNP, May 2018.
3. Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Rev. 4, U.S. Nuclear Regulatory Commission, June 2006.
4. NUREG-0737, "Clarification of TMI Action Plan Requirements," Item II.F.2, "Instrumentation for detection of inadequate core cooling," U.S. Nuclear Regulatory Commission, November 1980.
5. Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs" Item II.T, "Control Room Annunciator (Alarm) Reliability," U.S. Nuclear Regulatory Commission, July 21, 1993.
6. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, 1981.
7. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
8. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.
9. 10 CFR 50.55a(h)(2), "Codes and Standards, Protection Systems," U.S. Nuclear Regulatory Commission.
10. 10 CFR 50.55a(h)(3), "Codes and Standards, Safety Systems," U.S. Nuclear Regulatory Commission.
11. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3], U.S. Nuclear Regulatory Commission.

APR1400 DCD TIER 2

12. 10 CFR 50.34(f)(2)(xi), “Direct Indication of Relief and Safety Valve Position,” [II.D.3], U.S. Nuclear Regulatory Commission.
13. 10 CFR 50.34(f)(2)(xii), “Auxiliary Feedwater System Automatic Initiation and Flow Indication,” [II.E.1.2] U.S. Nuclear Regulatory Commission.
14. 10 CFR 50.34(f)(2)(xiv), “Containment Isolation Systems,” [II.E.4.2], U.S. Nuclear Regulatory Commission.
15. 10 CFR 50.34(f)(2)(xvii), “Accident Monitoring Instrumentation,” [II.F.1], U.S. Nuclear Regulatory Commission.
16. 10 CFR 50.34(f)(2)(xviii), “Instrumentation for Detection of Inadequate Core Cooling,” [II.F.2], U.S. Nuclear Regulatory Commission.
17. 10 CFR 50.34(f)(2)(xix), “Instruments for Monitoring Plant Conditions Following Core Damage,” [II.F.3], U.S. Nuclear Regulatory Commission.
18. 10 CFR 50.34(f)(2)(xx), “Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves,” [II.G.1], U.S. Nuclear Regulatory Commission.
19. 10 CFR 50.62, “Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water Cooled Nuclear Power Plants,” U.S. Nuclear Regulatory Commission.
20. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” U.S. Nuclear Regulatory Commission.
21. 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” U.S. Nuclear Regulatory Commission.
22. Staff Requirements Memorandum on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs” Item II.Q, “Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems,” U.S. Nuclear Regulatory Commission , July 21, 1993.

APR1400 DCD TIER 2

23. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)," U.S. Nuclear Regulatory Commission, various dates and revisions.
24. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions," U.S. Nuclear Regulatory Commission, February 1972.
25. Regulatory Guide 1.47, "Bypassed and Inoperable Status indication for Nuclear Power Plant Safety Systems," Rev. 1, U.S. Nuclear Regulatory Commission, February 2010.
26. Regulatory Guide 1.53, "Application of the Single-Failure Criterion to Safety Systems," Rev. 2, U.S. Nuclear Regulatory Commission, November 2003.
27. IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 2000.
28. Regulatory Guide 1.62, "Manual Initiation of Protective Actions," Rev. 1, U.S. Nuclear Regulatory Commission, June 2010.
29. IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers, 1992.
30. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Rev.3, U.S. Nuclear Regulatory Commission, February 2005.
31. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.
32. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.
33. IEEE Std. 1012-2004, "IEEE Standard for Software Verification and Validation," Institute of Electrical and Electronics Engineers, 2004.
34. ANSI/ISA S67.04-1994, "Setpoints for Nuclear Safety-Related instrumentation," International Society of Automation, 1994.

APR1400 DCD TIER 2

35. Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation," Rev. 3, U.S. Nuclear Regulatory Commission, December 1999.
36. Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," Rev. 3, U.S. Nuclear Regulatory Commission, April 1995.
37. IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems," Institute of Electrical and Electronics Engineers, 1987.
38. Regulatory Guide 1.151, "Instrument Sensing Lines," Rev. 1, U.S. Nuclear Regulatory Commission, July 2010.
39. Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Rev. 2, U.S. Nuclear Regulatory Commission, July 2013.
40. IEEE Std. 1028-2008, "IEEE Standard for Software Reviews and Audits," Institute of Electrical and Electronics Engineers, 2008.
41. Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Rev. 1, U.S. Nuclear Regulatory Commission, July 2013.
42. IEEE Std. 828-2005, "IEEE Standard for Software Configuration Management Plans," Institute of Electrical and Electronics Engineers, 2005.
43. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety systems of Nuclear Power Plants," Rev. 1, U.S. Nuclear Regulatory Commission, July 2013.
44. IEEE Std. 829-2008, "IEEE Standard for Software and System Test Documentation," Institute of Electrical and Electronics Engineers, 2008.
45. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Rev. 1, U.S. Nuclear Regulatory Commission, July 2013.

APR1400 DCD TIER 2

46. IEEE Std. 1008-1987 (reaffirmed 2002), “IEEE Standard for Software Unit Testing,” Institute of Electrical and Electronics Engineers, 1987.
47. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Rev. 1, U.S. Nuclear Regulatory Commission, July 2013.
48. IEEE Std. 830-1998 (reaffirmed 2009), “IEEE Recommended Practice for Software Requirements Specifications,” Institute of Electrical and Electronics Engineers, 1998.
49. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,” Rev. 1, U.S. Nuclear Regulatory Commission, July 2013.
50. IEEE Std. 1074-2006, “IEEE Standard for Developing Software Life Cycle Processes,” Institute of Electrical and Electronics Engineers, 2006.
51. Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.
52. Regulatory Guide 1.189, “Fire Protection for Nuclear Power Plants,” Rev. 2, U.S. Nuclear Regulatory Commission, October 2009.
53. Regulatory Guide 1.204, “Guidelines for Lightning Protection of Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, November 2005.
54. Regulatory Guide 1.206, “Combined License Applications for Nuclear Power Plants (LWR Edition),” U.S. Nuclear Regulatory Commission, June 2007.
55. NUREG-0800, Standard Review Plan, BTP 7-1, “Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
56. NUREG-0800, Standard Review Plan, BTP 7-2 “Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.

APR1400 DCD TIER 2

57. NUREG-0800, Standard Review Plan, BTP 7-3, "Guidance on Protection System Trip Point Changes for the Operation With Reactor Coolant Pumps Out of Service," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
58. NUREG-0800, Standard Review Plan, BTP 7-4, "Guidance on Design Criteria for Auxiliary Feedwater Systems," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
59. NUREG-0800, Standard Review Plan, BTP 7-5, "Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
60. NUREG-0800, Standard Review Plan, BTP 7-6, "Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
61. NUREG-0800, Standard Review Plan, BTP 7-8, "Guidance for Application of Regulatory Guide 1.22," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
62. NUREG-0800, Standard Review Plan, BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
63. NUREG-0800, Standard Review Plan, BTP 7-10, "Guidance on Application of Regulatory Guide 1.97," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
64. NUREG-0800, Standard Review Plan, BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
65. NUREG-0800, Standard Review Plan, BTP 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
66. NUREG-0800, Standard Review Plan, BTP 7-13, "Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors," Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.

APR1400 DCD TIER 2

67. NUREG-0800, Standard Review Plan, BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
68. NUREG-0800, Standard Review Plan, BTP 7-17, “Guidance on Self-Test and Surveillance Test Provisions,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
69. NUREG-0800, Standard Review Plan, BTP 7-18, “Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
70. NUREG-0800, Standard Review Plan, BTP 7-19, “Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems,” Rev. 6, U.S. Nuclear Regulatory Commission, July 2012.
71. NUREG-0800, Standard Review Plan, BTP 7-21, “Guidance on Digital Computer Real-Time Performance,” Rev. 5, U.S. Nuclear Regulatory Commission, March 2007.
72. APR1400-Z-J-NR-14005-P, “Setpoint Methodology for Safety-Related Instrumentation,” Rev. 2, KEPCO & KHNP, January 2018.
73. DI&C-ISG-04, “Highly Integrated Control Rooms – Communications Issues (HICRc),” Rev. 1, U.S. Nuclear Regulatory Commission, 2009.
74. APR1400-Z-J-NR-14013-P, “Response Time Analysis of Safety I&C System,” Rev. 2, KEPCO & KHNP, January 2018.
75. NUREG-0737, Supplement No. 1, “Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability,” U.S. Nuclear Regulatory Commission, 1983.
76. IEEE Std. 1050-1996, “IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations,” Institute of Electrical and Electronic Engineers, 1996.
77. WCAP-16097-P-A, “Common Qualified Platform Topical Report,” Rev. 3, Westinghouse Electric Corporation, February 2013.

APR1400 DCD TIER 2

78. APR1400-A-J-NR-14003-P (WCAP-17926-P), “APR1400 Disposition of Common Q Topical Report NRC Generic Open Items and Plant Specific Action Items,” Rev. 0, KEPCO & KHNP, October 2014.
79. APR1400-A-J-NR-14004-P (WCAP-17922-P), “Common Q Platform Supplemental Information in Support of the APR1400 Design Certification,” Rev. 2, KEPCO & KHNP, May 2017.
80. IEEE Std. 497-2002, “IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2002.
81. EPRI TR-102323, “Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants,” Electric Power Research Institute, 1997.
82. APR1400-F-C-NR-14001-P, “CPC Setpoint Analysis Methodology for APR1400,” Rev. 3, KEPCO & KHNP, June 2018.
83. APR1400-E-J-NR-17001-P, “Secure Development and Operational Environment for APR1400 Computer-Based I&C Safety Systems,” KEPCO & KHNP, September 2017.

APR1400 DCD TIER 2

Table 7.1-1 (1 of 6)

Regulatory Requirements Applicability Matrix

Applicable Criteria		Title	I&C System							Section in APR1400 DCD	
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS		
10 CFR Part 50											
1	50.55a(h)(2)	Protection Systems									Not Applicable
2	50.55a(h)(3)	Safety Systems	×	×	×						7.2, 7.3, 7.5, 7.6, 7.9
3	50.34(f)(2)(v)	Bypass and Inoperable Status Indication	×	×	×	×					7.2, 7.3, 7.5, 7.6, 7.9
4	50.34(f)(2)(xi)	Direct Indication of Relief and Safety Valve Position				×					7.5
5	50.34(f)(2)(xii)	Auxiliary Feedwater System Automatic Initiation and Flow Indication	×	×	×						7.2, 7.3, 7.5
6	50.34(f)(2)(xiv)	Containment Isolation Systems	×	×	×						7.2, 7.3, 7.5
7	50.34(f)(2)(xvii)	Accident Monitoring Instrumentation			×	×					7.5
8	50.34(f)(2)(xviii)	Instrumentation for the Detection of Inadequate Core Cooling			×						7.5
9	50.34(f)(2)(xix)	Instruments for Monitoring Plant Conditions Following Core Damage			×						7.5
10	50.34(f)(2)(xx)	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves			×						7.4, 7.5
11	50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram								×	7.8
10 CFR Part 50, Appendix A GDC											
12	GDC 1	Quality Standards and Records	×	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
13	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

APR1400 DCD TIER 2

Table 7.1-1 (2 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
14	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
15	GDC 10	Reactor Design	×	×			×	×		7.2, 7.3, 7.6, 7.7
16	GDC 13	Instrumentation and Control	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
17	GDC 15	Reactor Coolant System Design	×	×			×	×		7.2, 7.3, 7.6, 7.7
18	GDC 16	Containment Design		×						7.3, 7.6
19	GDC 19	Control Room	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
20	GDC 20	Protection System Functions	×	×						7.2, 7.3
21	GDC 21	Protection System Reliability and Testability	×	×						7.2, 7.3, 7.9
22	GDC 22	Protection System Independence	×	×						7.2, 7.3, 7.9
23	GDC 23	Protection System Failure Modes	×	×						7.2, 7.3, 7.9
24	GDC 24	Separation of Protection and Control Systems	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9
25	GDC 25	Protection System Requirements for Reactivity Control Malfunctions	×							7.2, 7.6
26	GDC 28	Reactivity Limits					×			7.6, 7.7
27	GDC 29	Protection against Anticipated Operational Occurrences	×	×			×	×		7.2, 7.3, 7.7, 7.9
28	GDC 33	Reactor Coolant Makeup	×	×						7.2, 7.3, 7.6
29	GDC 34	Residual Heat Removal	×	×						7.2, 7.3, 7.4, 7.6
30	GDC 35	Emergency Core Cooling	×	×						7.2, 7.3, 7.4, 7.6
31	GDC 38	Containment Heat Removal	×	×						7.2, 7.3, 7.4, 7.6
32	GDC 41	Containment Atmosphere Cleanup	×	×						7.2, 7.3, 7.6
33	GDC 44	Cooling Water		×						7.3, 7.6

APR1400 DCD TIER 2

Table 7.1-1 (3 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
Staff Requirements Memoranda										
34	SRM on SECY-93-087, Item II.Q	Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems	×	×					×	7.2, 7.3, 7.8, 7.9
35	SRM on SECY-93-087, Item II.T	Control Room Annunciator (Alarm) Reliability				×				7.5, 7.9
NRC Regulatory Guides										
36	NRC RG 1.22	Periodic Testing of Protection System Actuation Functions	×	×						7.2, 7.3,, 7.9
37	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
38	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
39	NRC RG 1.62	Manual Initiation of Protective Actions	×	×					×	7.2, 7.3, 7.8
40	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
41	NRC RG 1.97	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants			×	×				7.5
42	NRC RG 1.105	Setpoints for Safety-Related Instrumentation ⁽¹⁾	×	×	×	×				7.2, 7.3, 7.4, 7.5, 7.6, 7.9
43	NRC RG 1.118	Periodic Testing of Electric Power and Protection Systems	×	×	×	×				7.2, 7.3, 7.4, 7.5, 7.6, 7.9
44	NRC RG 1.151	Instrument Sensing Lines	×	×	×					7.2, 7.3, 7.5,
45	NRC RG 1.152	Criteria for Digital Computers in Safety Systems of Nuclear Power Plants	×	×	×					7.2, 7.3, 7.5, 7.9

APR1400 DCD TIER 2

Table 7.1-1 (4 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
46	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
47	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
48	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
49	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
50	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
51	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
52	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
53	NRC RG 1.189	Fire Protection for Nuclear Power Plants								Refer to Chapter 9 (Subsection 9.5.1)
54	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
55	NRC RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants	×	×	×	×	×	×	×	Refer to Chapter 8 (Subsection 8.3.1.1.8)

APR1400 DCD TIER 2

Table 7.1-1 (5 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
56	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										
57	BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System		×						7.6
58	BTP 7-2	Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines		×						7.6
59	BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service								Not Applicable
60	BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems		×						7.3
61	BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors	×				×			7.2, 7.7
62	BTP 7-6	Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode								Not Applicable
63	BTP 7-8	Guidance for Application of NRC RG 1.22	×	×						7.2, 7.3, 7.9
64	BTP 7-9	Guidance on Requirements for Reactor Protection System Anticipatory Trips	×							7.2
65	BTP 7-10	Guidance on Application of NRC RG 1.97			×	×				7.5
66	BTP 7-11	Guidance on Application and Qualification of Isolation Devices	×	×	×					7.2, 7.3, 7.5, 7.9
67	BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6,

APR1400 DCD TIER 2

Table 7.1-1 (6 of 6)

Applicable Criteria		Title	I&C System							Section in APR1400 DCD
			RTS	ESF System	QIAS-P	QIAS-N	PCS	P-CCS	DAS	
68	BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	×	×	×					7.2, 7.3, 7.4, 7.5
69	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
70	BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	×	×	×					7.2, 7.3, 7.4, 7.5, 7.6, 7.9
71	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
72	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
73	BTP 7-21	Guidance on Digital Computer Real-Time Performance	×	×	×	×	×	×	×	7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 7.9

(1) Except for the setpoints calculation using CPC Setpoint Analysis Methodology Technical Report (Reference 82 in Subsection 7.1.5).

APR1400 DCD TIER 2

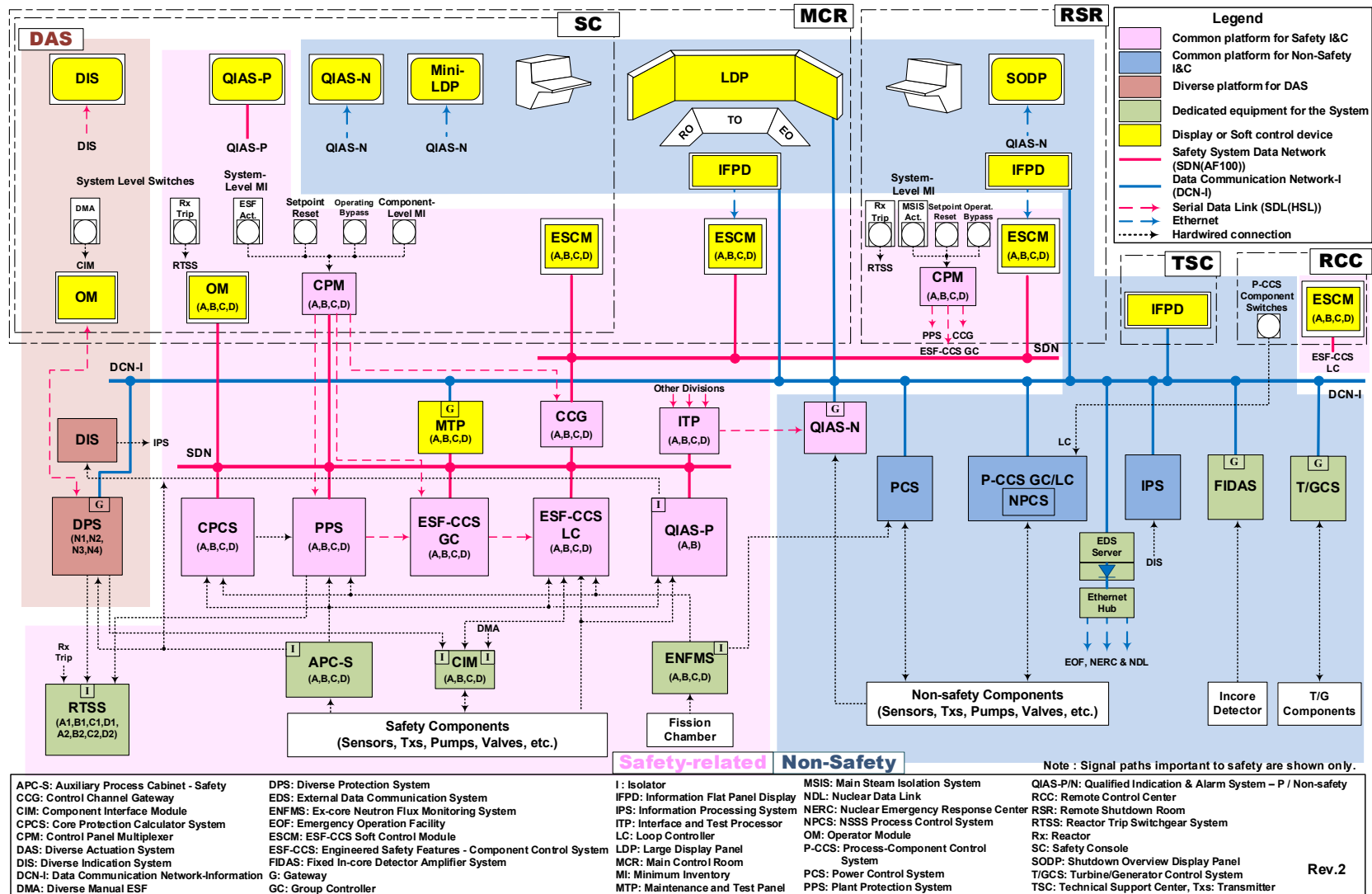


Figure 7.1-1 APR1400 I&C System Overview Architecture

APR1400 DCD TIER 2

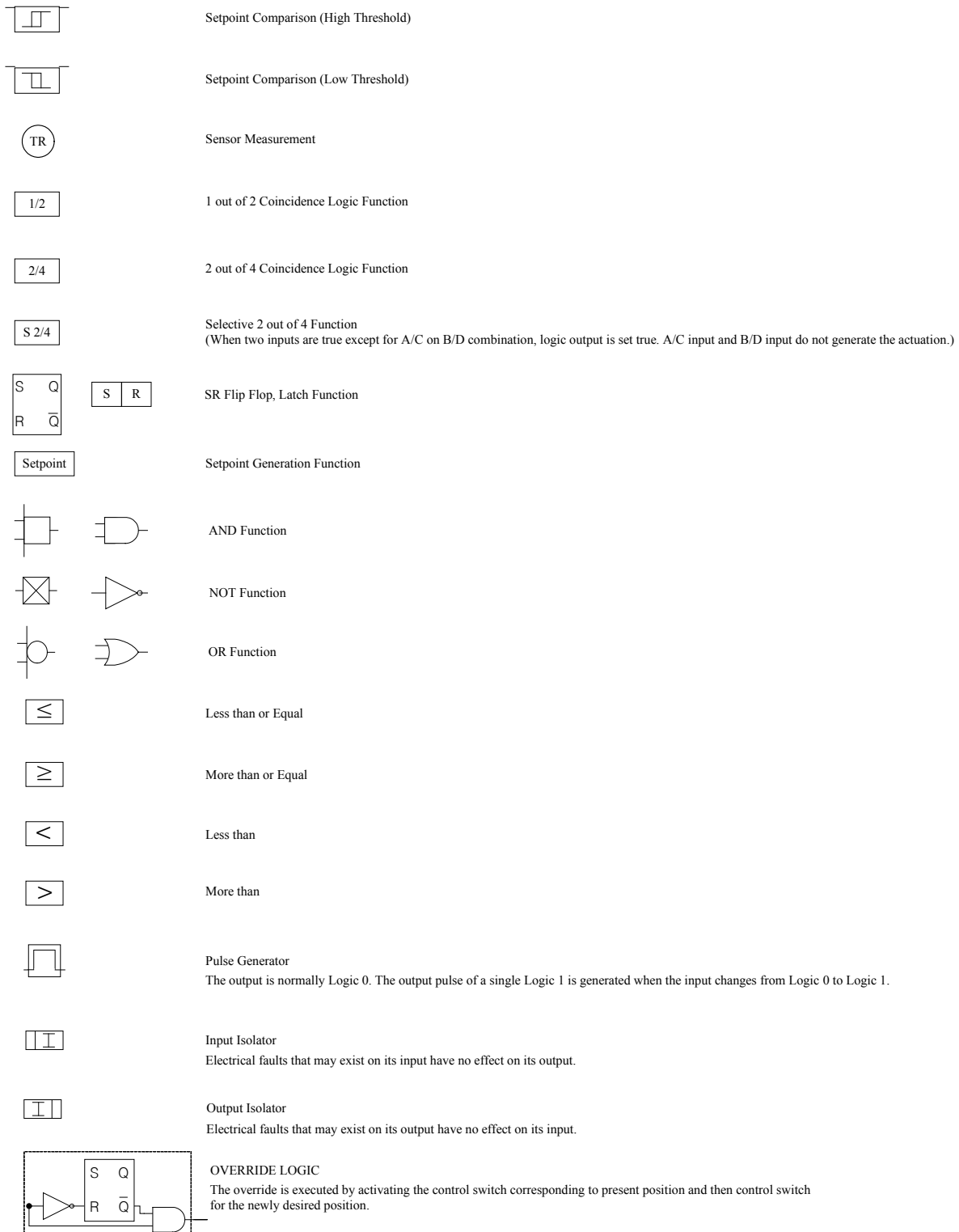


Figure 7.1-2 Symbol & Legend Diagram (1 of 2)

APR1400 DCD TIER 2




	Isolator Output is electrically isolated from input
	ON Delay Output exists only when input has been continuously present for a present time and remains present
	Light R-RED - Operating, Flowing or Increasing. G-Green - Not operating, Not flowing or decreasing. O-Orange - Manual, Synchronize, or Operator information. Y-Yellow - Trouble/Disable

Figure 7.1-2 Symbol & Legend Diagram (2 of 2)

APR1400 DCD TIER 2

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, four divisions of 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 ESF system consists of four channels of sensors, and APC-S cabinets, four divisions of the engineered safety features actuation system (ESFAS) initiation portion of the PPS cabinets, and the ESF-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 provide assistance in mitigating the consequences of postulated accidents (PAs). Four measurement channels with electrical isolation and physical separation are provided for each parameter to generate the trip signals, with the exception of the two channel control element assembly (CEA) position indication used in the CPCS.

APC-S functions include signal conditioning/splitting for the safety field sensor signals shared by the PPS, CPCS, and ESF-CCS loop controller (LC), or safety systems and non-safety systems, and provide isolation when signals are split to the non-safety system.

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 divisions. Each PPS division is located in a divisionalized instrumentation and control (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 divisions.

Each division is designed based on a programmable logic controller (PLC) platform. The BPs (two redundant processors per channel) perform A/D conversion, signal compensation

APR1400 DCD TIER 2

(if required), engineering unit conversion, and generate trip signals if the process values exceed their respective setpoints. The BP provides trip signals to the LCL processors in the four redundant divisions, as shown in Figure 7.2-10.

The LCL processors (four redundant processors per division) determine the LCL output state based on the state of the eight bistable trip signals and their respective trip channel bypasses. For the RPS, the LCL outputs are transmitted to the RTSS through the selective 2-out-of-4 initiation circuit (see Section 7.2.1.3 for a description of the logic). 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 division. The four reactor trip signals are combined using 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 division (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 divisionalized 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 division 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 human system interface (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.

APR1400 DCD TIER 2

The maintenance and test panel (MTP) and the interface and test processor (ITP) cabinet is located in a divisionalized 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 bypass, 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 communication gateway function to send a selected safety system division 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 division 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 parameters, as shown in Table 7.2-2, are measured with four redundant and independent process instrument channels with the exception of the two channel CEA position indication used in the CPCS. The number of RPS sensors is listed in Table 7.2-3.

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

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

b. CEA position measurements

APR1400 DCD TIER 2

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 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 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 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

APR1400 DCD TIER 2

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 of the CPCS is shown in Figure 7.2-7.

c. Ex-core neutron flux measurements

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, preamplifier assembly, and 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 a 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 I&C equipment rooms. Physical separation and electrical isolation between redundant channels are provided.

APR1400 DCD TIER 2

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 in Figure 7.2-6. Each scanning device produces a voltage pulse signal. The pulse train that is input to the CPCS to calculate flow rate is based on 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, cold leg temperatures, and 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, density of cold leg coolant, and 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 hardwired 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

APR1400 DCD TIER 2

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 isolated one-way SDL communication.

Each CPC receives the following inputs:

- 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 a Core Protection Calculator System for the APR1400 (Reference 1) which includes the CPCS Improvement Program (Reference 30):

- 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 (In the CPCS, flow information is derived from reactor coolant pump speed and density of the coolant in the hot leg because no method that directly measures the flow information is available in modern engineering.)
- 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

APR1400 DCD TIER 2

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
- 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) LPD high trip and pre-trip
- 3) CEA withdrawal prohibit
- 4) CPC auxiliary trips (see Table 7.2-4)

The outputs to the IPS are as follows:

- 1) DNBR margin
- 2) LPD margin
- 3) Calibrated neutron flux power
- 4) CPC measurement factor and calculation results values

APR1400 DCD TIER 2

- 5) Trip-buffer and snapshot reports

The outputs to the QIAS-N are as follows:

- 1) DNBR margin
- 2) LPD margin
- 3) Axial shape index
- 4) DNBR
- 5) Compensated LPD
- 6) Cold leg temperature
- 7) Hot leg temperature

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. The COL applicant is to provide site-specific CPCS startup test requirement (COL 7.2(1)).

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 with the segregation based upon which initiating event is mitigated by the input signal, 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.

APR1400 DCD TIER 2

The trip output signal of the bistable logic is sent to the LCL processors via the SDL in the four protective divisions. 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 contain 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.

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

APR1400 DCD TIER 2

switches on the safety console or remote shutdown console (RSC) based on the master transfer switch status.

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 sets of two redundant LCL processors for the RPS in each division. The LCL processors for the RPS generate 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 division 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.

Eight RTSGs are connected with 2-out-of-4 configuration, as shown in Figure 7.2-9. A full 2-out-of-4 RTSG configuration with eight RTSGs meets the single failure criterion during maintenance and testing.

There are separate initiation circuits for undervoltage and shunt trip initiation. The PPS provides the undervoltage trip signals, and the diverse protection system (DPS) provides the shunt trip signals to each RTSG for diversity.

The RTSS consists of two sets of four reactor trip switchgears (RTSS 1 and RTSS 2). The PPS interfaces with the undervoltage trip device and the DPS interfaces with the shunt trip device. The RTSGs in RTSS 1 are supplied from a different manufacturer than the RTSGs in RTSS 2, thereby providing reasonable assurance that a different actuation mechanism is used in the RTCBs in the two different sets of RTSGs.

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.

Two pairs of manual trip switches are provided in the MCR, and one pair of manual trip switches is provided in the RSR for reactor trip. These manual reactor trip switch signals are connected directly to the undervoltage trip device of the trip circuit breaker (TCB) in each RTSG.

APR1400 DCD TIER 2

7.2.1.4 Reactor Trip Initiation Signals

Figure 7.2-14 illustrates the logic for the RPS and ESFAS functions. 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), which is unidirectional from the PPS to the TCS via a hardwired connection, when any variable trip initiation occurs.

- a. Variable overpower

APR1400 DCD TIER 2

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 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 ENFMS safety channel. The trip can be 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 LPD reaches a preset value. The preset value is less than that value that would cause fuel centerline melting. The calculation of the peak LPD is performed by the CPCs, which compensates the calculated peak LPD 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 LPD.

The calculated trip provides reasonable assurance that the core peak LPD 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 LPD trip. The trip can 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

- a) Neutron flux power and hot pin axial power distribution from the ENFMS

APR1400 DCD TIER 2

- 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 LPD 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 can 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.

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.

APR1400 DCD TIER 2

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 ENFMS
- 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
- f) Core inlet temperature from reactor coolant cold leg temperature measurements
- g) Core outlet temperature from reactor coolant hot leg temperature measurements
- h) Penalty factors from CEACs for CEA deviation within a subgroup
- i) 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 DNBR is shown in Figure 7.2-20. The functional logic for the operating bypass permissive is shown in Figure 7.2-29.

- e. High pressurizer pressure

APR1400 DCD TIER 2

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 overpressurization 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 to trip the reactor when required during plant cooldown.

The trip can be 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

Reactor coolant pressure from wide range pressurizer pressure measurements

APR1400 DCD TIER 2

2) Purpose

To provide a reactor trip to assist the ESF systems in the event of reduction in system pressure such as a loss of coolant accident (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 steam generator (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

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 setpoint can be manually decreased to a fixed increment below the 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. The 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 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 SG 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.

For turbine trip, each PPS division interfaces with the TCS as follows:

Two (2) sets of contact signals are provided per division in the reactor trip switchgear system (RTSS). A total of eight (8) output signals are generated. The contact signal, as a momentary signal type, is provided through hardwired connections. Isolation is achieved by using Class 1E isolation relays within the RTSS.

The two sets of contact signals from each division in the RTSS are inputted to two P-CCS cabinets through hardwired connections. The P-CCS cabinets have 2-out-of-4 voting logic to prevent spurious turbine trip due to single P-CCS cabinet failure. The results of the 2-out-of-4 voting logic in the P-CCS cabinets are provided to the TCS to initiate turbine trip.

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 TCBs, 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).

APR1400 DCD TIER 2

A minimum of two divisions of RPS trips are required for a reactor trip. The RPS initiation relays in each division 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 operating bypass can be requested either from the MCR or from the RSR based on the master transfer switch status. The following operating bypasses are provided:

1) DNBR/LPD operating bypass

The DNBR and LPD operating 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 operating bypass removal function is provided.

2) Low pressurizer pressure bypass

APR1400 DCD TIER 2

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

- a) System tests at low pressure
- b) Heatup and cooldown with shutdown CEAs withdrawn

The operating bypass can 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 can be 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 results in a 2-out-of-3 coincidence logic in the LCL.

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 divisions.

APR1400 DCD TIER 2

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 the LCL digital input modules. 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 administrative procedure. The coincidence logic becomes 2-out-of-3 coincidence logic. The all-bypass function for bypassing all parameters in one channel is 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 hardwired cable between LCLs in all divisions. 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 by administrative procedure 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 by administrative procedure. The function enable key switch is interlocked for testing.

d. ENFMS test interlock

APR1400 DCD TIER 2

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
- 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 the 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 divisions of coincidence logics
- e. Redundant coincidence logics in each division

APR1400 DCD TIER 2

- f. Four redundant divisions 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 divisions of the RPS allow a division functional test during power operation while still meeting the single failure criteria.

7.2.1.9 Diversity and Defense-in-Depth

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

- 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 (one set of four RTSGs supplied by a different manufacturer than the other set of four RTSGs).
- 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.

APR1400 DCD TIER 2

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 divisions of the RPS 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 preclude protective action at the system level in accordance with NRC RG 1.53 (Reference 4).

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 RPS continues to meet the single failure criterion. The time duration the channel may be out of service is specified in the Technical Specifications.

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

7.2.2.2 Quality of Components and Modules

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

The I&C used for the RPS are designed in accordance with the QA program that meets the requirements of 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 the safety system

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

Both BP and LCL processors within the PPS include a communication processor, separate from the function processor.

The data flow between redundant PPS divisions is buffered at the outgoing side of the communication processor of the BP and at the incoming side of the communication processor of the LCL processor to ensure independence of the redundant safety divisions.

One way communication over fiber optic cable is used to ensure communication independence and electrical isolation between redundant portions of the safety system.

The PPS divisions receive ac power from the vital bus power supply system. The PPS does not share the power between divisions.

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 Class 1E qualified isolation devices or fiber-optic cables so that any failure in a non-safety system does not cause loss of the 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.

APR1400 DCD TIER 2

7.2.2.4 Diversity and Defense-in-Depth

The diversity and defense-in-depth analysis is described in Reference 3. The diversity features of the PPS are 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 meets the guidance of IEEE Std. 338 (Reference 9), which is endorsed by NRC RG 1.118 (Reference 11). The testing also complies with NRC RG 1.22 (Reference 10).

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

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

Bypasses and inoperable status of safety systems displayed at the MTP and OM meets the guidance of 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.

Manual testing is interlocked by administrative procedure for testing only one channel at a time.

c. CPCS test

APR1400 DCD TIER 2

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

The checks of trip logic by the trip signal generated from the CPCS are performed by tripping the 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 two pairs of manual trip pushbuttons on the safety console or one pair of manual trip pushbuttons on the RSC, observing an RTSG trip, and closing the RTSG prior to the next manual trip test.

Figure 7.2-16 shows the signal path for the 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 reactor trip pushbuttons 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 Safety-Related Instrumentation Technical Report and CPC Setpoint Analysis Methodology Technical Report (References 14 and 29).

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

CPC setpoint is determined as the analytical limit. The overall uncertainty factors, which are the combined uncertainty in a CPC channel, are applied directly in the CPC DNBR and LPD calculation.

The setpoint methodology meets the guidance of ANSI/ISA S67.04 (Reference 15), as endorsed by NRC RG 1.105 (Reference 16) except for the CPC setpoints which conforms with CPC Setpoint Analysis Methodology Technical Report (Reference 29).

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 the Response Time Analysis of Safety I&C System Technical Report (Reference 17).

APR1400 DCD TIER 2

7.2.2.8 Equipment Qualification

The RPS meets the requirements of IEEE Std. 323 (Reference 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).

The RPS that is designed and tested to minimize both the emission and susceptibility of EMI and RFI meets the guidance of 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 modes and effects analysis (FMEA), to demonstrate how the analyses satisfy the requirements of the applicable GDC (see Table 7.1-1), IEEE Std. 603 (Reference 24), and IEEE Std. 7-4.3.2 (Reference 25).

Compliance with the 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 FMEA meets the guidance 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 divisions. Independence provides reasonable assurance that a single failure cannot propagate between divisions within the safety system or between the safety system and non-safety system.

The FMEA demonstrates that:

- a. As a result of the four division 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.

APR1400 DCD TIER 2

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

The results of a 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:

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 AOOs.

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 PAs 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 Multiple Setpoints

Multiple setpoints comply with the restrictive setpoint requirement of IEEE Std. 603, as described in Reference 26.

7.2.3.5 Conformance to General Design Criteria

Conformance 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 with IEEE Std. 603

Conformance with IEEE Std. 603 is described in Reference 26.

APR1400 DCD TIER 2

7.2.3.7 Conformance with IEEE Std. 7-4.3.2

Conformance with IEEE Std. 7-4.3.2 is described in Reference 26.

7.2.4 Combined License Information

COL 7.2(1) The COL applicant is to provide site-specific CPCS startup test requirement.

7.2.5 References

1. APR1400-F-C-NR-14003-P, "Functional Design Requirements for a Core Protection Calculator System for the APR1400," Rev. 1, KEPCO & KHNP, March 2017.
2. Regulatory Guide 1.62, "Manual Initiation of Protection Action," Rev. 1, U.S. Nuclear Regulatory Commission, June 2010.
3. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
4. Regulatory Guide 1.53, "Application of the Single Failure Criterion to Safety Systems," Rev. 2, U.S. Nuclear Regulatory Commission, November 2003.
5. ASME NQA-1a-2009, Subpart 2.2, "Quality Assurance Requirements for Packaging, Shipping, Receiving, Storage, and Handling of Items for Nuclear Facilities," The American Society of Mechanical Engineers, 2009.
6. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.
7. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Rev. 3, U.S. Nuclear Regulatory Commission, February 2005.
8. Regulatory Guide 1.151, "Instrument Sensing Lines," Rev. 1, U.S. Nuclear Regulatory Commission, July 2010.
9. IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 1987.

APR1400 DCD TIER 2

10. Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions,” U.S. Nuclear Regulatory Commission, February 1972.
11. Regulatory Guide 1.118, “Periodic Testing of Electric Power and Protection Systems,” Rev. 3, U.S. Nuclear Regulatory Commission, April 1995.
12. Regulatory Guide 1.47, “Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, February 2010.
13. APR1400-Z-J-NR-14004-P, “Uncertainty Methodology and Application for Instrumentation,” Rev. 2, KEPCO & KHNP, January 2018.
14. APR1400-Z-J-NR-14005-P, “Setpoint Methodology for Safety-Related Instrumentation,” Rev. 2, KEPCO & KHNP, January 2018.
15. ANSI/ISA S67.04-1994, “Setpoint for Nuclear Safety-Related Instrumentation,” International Society of Automation, 1994.
16. Regulatory Guide 1.105, “Setpoints for Safety-Related Instrumentation,” Rev. 3, U.S. Nuclear Regulatory Commission, December 1999.
17. APR1400-Z-J-NR-14013-P, “Response Time Analysis of Safety I&C System,” Rev. 2, KEPCO & KHNP, January 2018.
18. IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2003.
19. IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2005.
20. Regulatory Guide 1.89, “Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants,” Rev. 1, U.S. Nuclear Regulatory Commission, June 1984.
21. Regulatory Guide 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” U.S. Nuclear Regulatory Commission, March 2007.

APR1400 DCD TIER 2

22. Regulatory Guide 1.180, Rev. 1, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.
23. IEC 61000-4-2, “Electromagnetic Compatibility – Testing and Measurement Techniques - Electrostatic Discharge Immunity Test,” International Electrotechnical Commission, 1992.
24. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 1991.
25. IEEE Std. 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2003.
26. APR1400-Z-J-NR-14001-P, “Safety I&C System,” Rev. 3, KEPCO & KHNP, May 2018.
27. IEEE Std. 352-1987, “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems,” Institute of Electrical and Electronics Engineers, 1987.
28. IEEE Std. 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” Institute of Electrical and Electronics Engineers, 2000.
29. APR1400-F-C-NR-14001-P, “CPC Setpoint Analysis Methodology for APR1400,” Rev. 3, KEPCO & KHNP, June 2018.
30. CEN-310-P-A, “CPC and Methodology Changes for the CPC Improvement Program,” Combustion Engineering, Inc., April 1986.

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 operating bypass permissive	Disable low DNBR and high LPD trips by manual operation of bypass switch	If power is $< 10^{-4} \%$	Automatic if power is $\geq 10^{-4} \%$	Allows low power testing and CEA withdrawal under non-critical state
Low pressurizer pressure operating bypass permissive	Disables low pressurizer pressure trip, SIAS, and CIAS by manual operation of bypass switch	If pressure is $< 28.12 \text{ kg/cm}^2\text{A}$ (400 psia)	Automatic if pressure is $\geq 35.15 \text{ kg/cm}^2\text{A}$ (500 psia)	-
High log power level operating bypass permissive	Disables high logarithmic power level trip by manual operation of bypass switch	If power is $> 10^{-3} \%$	Automatic if power is $\leq 10^{-3} \%$	Bypassed during reactor startup
CPC CWP operating bypass permissive	Disables CPCS CWP signals by automatic operation of bypass	If power is $< 10^{-4} \%$	Automatic if power is $\geq 10^{-4} \%$	CWP by high 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 (2,250)	175 (2,489)
Pressurizer pressure (wide range), kg/cm ² A (psia)	0 (0)	158.2 (2,250)	210.9 (3,000)
CEA positions	Full in	NA	Full out
Reactor coolant pump speed, rpm	0	1,190	1,320
Steam generator water level (wide range), % ⁽¹⁾	0	77	100
Steam generator water level (narrow range), % ⁽²⁾	0	50	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)	2,110 (30)	5,000 (71)

(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	4/steam generator	Cold leg piping connected to steam generators	CPCS (for generating high LPD and low DNBR)
Hot leg temperature	Precision RTD	4/steam generator	Hot leg piping connected to steam generators	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
Steam generator pressure	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)		158.2 (2,250)	167.1 (2,377)	Fixed	8.9 (126.6)
Low pressurizer pressure, kg/cm ² A (psia)		158.2 (2,250)	127.3 ^{(4), (5)} (1,810)	Variable	30.9 (439.5)
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⁾		50.0	90.0	Fixed	40.0
Low reactor coolant flow, cmH ₂ O (psid)	Min	2,100 (30)	730.9 (10.4)	Rate limited Variable	1,346.3 (19.1)
	Rate	0/second	3.0/second ⁽⁸⁾ (0.043)		3.4/second (0.048)
	Step	NA	646.7 band (9.2)		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 ⁽⁹⁾				
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 (2,250)	127.3 (1,810) to 168.0 (2,389)	Fixed	+9.8 (139.4) –30.9 (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	6 % / min		6 % / min
Decreasing rate	0	90 % / min		90 % / min
Band ⁽²⁾	NA	15 % band		NA
Low pressure, kg/cm ² A (psia) and DNBR	158 (2,250) and 2.0	141.7 (2,015) and 1.45	Fixed	16.3 (235) and 0.55

(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

(8) For the low reactor coolant flow (LRCF) reactor trip setpoint, the process used to calculate the trip setpoint and generate a trip by comparing it with the input value occurs simultaneously. That is, the digital data from which the trip setpoint is created is the same as that used to establish the trip. Therefore, no uncertainty factor exists that would affect the trip setpoint, and the nominal trip setpoint for LRCF is identical to the allowable value in Technical Specifications (Chapter 16), Table 3.3.1-1.

(9) Both the DNBR and LPD trips are initiated in the CPCS for any condition of the CPC auxiliary trips.

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	≤ 0.7 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. Reactor 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.

APR1400 DCD TIER 2

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	Reactor coolant pumps	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 depressuri- zation	1. Safety injection 2. Rapid depressuri- zation 3. Reactor coolant gas vent	1. Shutdown cooling 2. Safety injection 3. Rapid depressuri- zation	1. Auxiliary feedwater 2. Atmospheric dump valves 3. Safety injection 4. Rapid depressuri- zation	CIAS actuation	CNMT spray	Monitoring only	1. Vital ac and dc from onsite source 2. Emergency diesel generators 3. Safety -related CCW

(1) PCS or P-CCS is applicable.

(2) PPS or ESF-CCS is applicable.

APR1400 DCD TIER 2

Table 7.2-7 (1 of 25)

Failure Modes 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 on PPS	Remarks and Other Effects
1-1	Ex-core neutron flux detector	a) Low output	Loss of high power supply source	<ul style="list-style-type: none">• Data loss• Incorrect data• Detection failure of high neutron flux level	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	The resulting reactor trip coincidence logic on variable overpower, high logarithmic power, DNBR/LPD becomes 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	<ul style="list-style-type: none">• 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	The resulting reactor trip coincidence logic on variable overpower, high logarithmic power, DNBR/LPD becomes 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.
1-2	Pressurizer pressure (wide range)	a) One signal turns on due to failure (high level signal)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• High-level pressure signal is input to bistable logic.• Low pressurizer pressure bistable logic does not generate trip under trip condition.	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	The resulting coincidence logic for reactor trip, CIAS, and SIAS becomes 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)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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	The resulting coincidence logic for reactor trip, CIAS and SIAS becomes 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.
1-3	Pressurizer pressure (narrow range)	a) Signal turns on (high level signal)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• The resulting reactor trip coincidence logic on low DNBR becomes 2-out-of-2 coincidence logic.• The resulting reactor trip coincidence on high pressurizer pressure becomes 1-out-of-2 coincidence logic.• The resulting CWP coincidence logic on high pressurizer pressure becomes 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)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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 DNBR channel	Three-channel redundancy	<ul style="list-style-type: none">• The resulting reactor trip coincidence logic on low DNBR becomes 1-out-of-2 coincidence logic.• The resulting reactor trip coincidence logic on high pressurizer pressure becomes 2-out-of-2 coincidence logic.• The resulting CWP coincidence logic on high pressurizer pressure becomes 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.

APR1400 DCD TIER 2

Table 7.2-7 (2 of 25)

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
1-4	Steam generator-1 level signal, Steam generator-2 level signal (wide range)	a) Signal turns off (low level signal)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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	The resulting coincidence logic for reactor trip and AFAS on affected low steam generator level becomes 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)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• High-level signal is input to bistable logic.• Low steam generator level bistable logic does not generate trip on affected steam generator.	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	<ul style="list-style-type: none">• The resulting coincidence logic for reactor trip and AFAS on affected low steam generator level becomes 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.
1-5	Steam generator-1 level signal, Steam generator-2 level signal (narrow range)	a) Signal turns off (low level signal)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	The resulting coincidence logic for reactor trip and MSIS on high steam generator level becomes 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)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• 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	The resulting coincidence logic for reactor trip and MSIS on affected high steam generator level becomes 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.
1-6	Steam generator-1 pressure signal, Steam generator-2 pressure signal	a) One signal unnecessarily turns off (low level signal)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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	The resulting coincidence logic for reactor trip and MSIS on steam generator pressure becomes 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)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	The resulting coincidence logic for reactor trip and MSIS on low steam generator pressure becomes 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.
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)	<ul style="list-style-type: none">• Sensor failure• Component failure	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Alarm: comparison of three channels• Periodic test	Three-channel redundancy	The resulting reactor trip coincidence logic on affected low steam generator flow becomes 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)	<ul style="list-style-type: none">• Sensor failure• DC power supply failure• Open circuit	<ul style="list-style-type: none">• 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	The resulting reactor trip coincidence logic on affected low steam generator flow becomes 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.

APR1400 DCD TIER 2

Table 7.2-7 (3 of 25)

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
1-8	Containment pressure signal (narrow range)	a) Signal turns on (high level signal)	Component failure	<ul style="list-style-type: none">High-level pressure signal is input to bistable logic.Bistable logic initiates channel trip of high containment pressure for RPS, SIAS, CIAS, and MSIS.	<ul style="list-style-type: none">RPS and ESF channel indication and pre-trip/alarm for high containment pressure channel	Three-channel redundancy	<ul style="list-style-type: none">The resulting reactor trip coincidence logic on high containment pressure becomes 1-out-of-2 coincidence logic.The resulting coincidence logic for CIAS, SIAS, and MSIS on high containment pressure becomes 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)	<ul style="list-style-type: none">Sensor failureDC power supply failureOpen circuit	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Alarm: comparison of three channelsPeriodic test	Three-channel redundancy	<ul style="list-style-type: none">The resulting reactor trip coincidence logic on high containment pressure becomes 2-out-of-2 coincidence logic.The resulting coincidence logic for CIAS, SIAS, and MSIS regarding high containment pressure becomes 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.
1-9	Containment pressure signal (wide range)	a) Signal turns on (high level signal)	<ul style="list-style-type: none">Sensor failureComponent failure	<ul style="list-style-type: none">High-level pressure signal is input to bistable logic.Bistable logic initiates channel trip for CSAS.	<ul style="list-style-type: none">ESF channel indication and pre-trip/alarm for high-high containment pressure channel	Three-channel redundancy	The resulting CSAS coincidence logic becomes 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)	<ul style="list-style-type: none">Sensor failureDC power supply failureOpen circuit	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Alarm: comparison of three channelsPeriodic test	Three-channel redundancy	The resulting CSAS coincidence logic becomes 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.
1-10	Ex-core neutron flux measurement channel (ENFMS)	a) ENFMS test interlock contact turns off due to failure.	<ul style="list-style-type: none">Open circuitMechanical failure	<ul style="list-style-type: none">Relay output for ENFMS test interlock is de-energized.Unnecessary channel trip of LPD and DNBR.	Alarm	Three-channel redundancy on LPD and DNBR	The resulting reactor trip coincidence logic on LPD and DNBR becomes 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	<ul style="list-style-type: none">Relay output for ENFMS test interlock is not de-energized upon failure of signal processing drawer of or test for ENFMS.Loss of failure alarmBistable 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	The resulting reactor trip coincidence logic on LPD and DNBR can becomes 2-out-of-2 coincidence logic.	
		c) Logarithmic power bistable contact of 10-3% turns off due to failure.	<ul style="list-style-type: none">Open circuitMechanical failure	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Periodic testChannel trip alarmNo bypass permissive indication light for high logarithmic power	Three-channel redundancy	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Bistable relay is energized Operator can apply bypass on high logarithmic power bistable with power being below 10⁻³%.	<ul style="list-style-type: none">Alarm: comparison of three channelsPeriodic test	Three-channel redundancy	The resulting reactor trip coincidence logic on high logarithmic power becomes 2-out-of-2 coincidence logic.	

APR1400 DCD TIER 2

Table 7.2-7 (4 of 25)

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
1-10	ENFMS (Continued)	e) Logarithmic power bistable contact of 10 ⁻⁴ % turns off due to failure (CPCS, CWP).	<ul style="list-style-type: none">Open circuitMechanical failure	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Alarm: comparison of three channelsPeriodic test	Three-channel redundancy	Trip occurs in one channel on LPD, DNBR, and CWP at low power and the resulting coincidence logic becomes 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).	<ul style="list-style-type: none">Contact arc and fixing	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Bypass permission indication of CPCSPeriodic test	Three-channel redundancy	The resulting reactor trip coincidence logic and CWP logic on LPD or DNBR becomes 2-out-of-2 coincidence logic.	
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.	<ul style="list-style-type: none">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	The resulting DNBR/LPD logic of RPS becomes 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	<ul style="list-style-type: none">For in range failures, possible DNBR/LPD channel trip on quality margin ⁽¹⁾.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, the resulting DNBR/LPD logic of RPS becomes 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.	<ul style="list-style-type: none">For out of range failures: DNBR/LPD channel auxiliary trip, CPC sensor failure indication / annunciation, CPC trouble indication/ annunciationSensor input cross channel comparison	Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 1-out-of-2 coincidence logic.	
		d) Low level signal (in range)	Sensor Failure	<ul style="list-style-type: none">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: <ul style="list-style-type: none">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.	

(1) Quality : the mass fraction of vapor in the mixture.
Quality margin: the difference between the quality limit and the calculated quality.

APR1400 DCD TIER 2

Table 7.2-7 (5 of 25)

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
2-2	Analog input cold leg temperature (Continued)	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	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 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	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Sensor input cross channel comparison, possible DNBR trip/pre-trip, NI-Delta T power deviation alarm.• Possible aux trip possible sensor failure alarm	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 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, CPC channel trouble annunciation.	<ul style="list-style-type: none">• CPC sensor failure indication/annunciation, Increase in Delta T power, DNBR/LPD channel auxiliary trip sensor input cross channel comparison• CPC trouble indication / annunciation	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 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: <ul style="list-style-type: none">• Sensor input cross-channel comparison, possible DNBR trip/pre-trip, NI-Delta T power deviation alarm.• Possible aux. trip• Possible sensor failure alarm	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 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.
2-3	Reactor coolant pump flow	a) Low pulse rate input, loss of transmission (out of range)	Power Supply or pulse amplifier failure	<ul style="list-style-type: none">• Out of range interpreted as low flow.• DNBR/LPD channel trip on low flow.	<ul style="list-style-type: none">• DNBR/LPD Channel trip• Sensor input cross channel comparison	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 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	<ul style="list-style-type: none">• Decrease in thermal power. Change in calculated DNBR.• Possible NI-Delta T Power deviation alarm.	<ul style="list-style-type: none">• Sensor cross channel comparison• Possible NI-Delta T Power deviation alarm	<ul style="list-style-type: none">• Three-channel redundancy	For in range failures not resulting in a channel trip, the resulting RPS logic becomes 2-out-of-2 coincidence logic.	
		c) High pulse rate input (out of range)	Pulse amplifier failure	<ul style="list-style-type: none">• DNBR/LPD channel Trip on low flow.• Excessively high speed input exceeding module range limit interpreted as error.	<ul style="list-style-type: none">• DNBR/LPD channel Trip• Sensor input cross channel comparison. CPCS sensor failure indication and annunciation	<ul style="list-style-type: none">• Single PPS channel trip• Three-channel redundancy	The resulting DNBR/LPD logic of RPS becomes 1-out-of-2 coincidence logic.	
		d) High pulse rate input (in range)	Pulse amplifier failure	<ul style="list-style-type: none">• Increase in thermal power. Change in calculated DNBR.• Possible NI-Delta T power deviation alarm.	<ul style="list-style-type: none">• Sensor cross channel comparison• Possible NI-Delta T power deviation alarm	<ul style="list-style-type: none">• Three-channel redundancy	For in range failures not resulting in a channel trip, the resulting RPS logic becomes 2-out-of-2 coincidence logic.	

APR1400 DCD TIER 2

Table 7.2-7 (6 of 25)

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
2-4	Non-target CEA position	a) Low level signal caused by failure (out of range)	<ul style="list-style-type: none">Shorted resistorFailed reed switchesPower 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.	<ul style="list-style-type: none">CEAC sensor failure indication/annunciation. CEA Position display depictionCPC 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.	<ul style="list-style-type: none">If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS.CEAC uses last good ⁽¹⁾ 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 good PF from failed CEAC, or current PF from operable CPC, whichever is larger.The resulting RPS logic becomes 2-out-of-2 coincidence logic on a channel trip.	
		b) Low-level signal caused by 12 finger CEA failure (in range)	Shorted resistor, failed reed switches, power supply malfunction.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">All channel DNBR/LPD trips are possible for 12 finger CEAsSingle PPS trip in the corresponding channel due to the PF and subgroup deviation alarm in the other channels for 4 finger CEAsRSPT input cross channel comparison within each channel	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Plant is shutdown due to the DNBR and LPD trip for 12 finger CEAs.Single channel PPS trip for 4 finger CEAs and the resulting RPS logic becomes 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.	<ul style="list-style-type: none">Subgroup deviation alarm occurs in all channelsRSPT input cross channel comparison within each channel	<ul style="list-style-type: none">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.	
		d) High-level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction	<ul style="list-style-type: none">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 three 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.	<ul style="list-style-type: none">CEAC sensor failure indication/annunciation on OM and MTP. CEA position display depictionCPCS 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.	<ul style="list-style-type: none">If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS.CEAC uses last good 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 PF from failed CEAC, or current PF from operable CPC, whichever is larger.The resulting RPS logic becomes 2-out-of-2 coincidence logic on a channel trip.	

(1) Last good PF/Position : Last PF/Position value which is received from the sending processor when the quality is good.

APR1400 DCD TIER 2

Table 7.2-7 (7 of 25)

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
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.	<ul style="list-style-type: none">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 shut down due to the DNBR and LPD trip.	
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	<ul style="list-style-type: none">Single PPS channel tripThree-channel redundancy	The resulting RPS logic for function becomes 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.	<ul style="list-style-type: none">DNBR/LPD channel trips are possible. The RPCB flag is set, and a CWP generated.RSPT input cross channel comparison within each channel	<ul style="list-style-type: none">Single PPS channel tripThree-channel redundancy	The resulting RPS logic for function becomes 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.	<ul style="list-style-type: none">Single PPS channel tripThree-channel redundancy	The resulting RPS logic for function becomes 1-out-of-2 coincidence logic.	
		d) High level signal caused by failure (in 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.	<ul style="list-style-type: none">Three-channel redundancy	If no DNBR/LPD channel trip occurs, the resulting RPS logic for function becomes 2-out-of-2 coincidence logic.	
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	<ul style="list-style-type: 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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Single RPS channel tripThree-channel redundancy logic	The resulting RPS trip logic for DNBR/LPD and CWP becomes 1-out-of-2 coincidence logic.	<ul style="list-style-type: none">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.
		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 resulting RPS trip logic for DNBR/LPD and CWP becomes 2-out-of-2 coincidence logic.	

APR1400 DCD TIER 2

Table 7.2-7 (8 of 25)

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
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	<ul style="list-style-type: none">No effect on RPS channel trip logic.The resulting CWP logic becomes 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	<ul style="list-style-type: none">No effect on RPS channel trip logic.The resulting CWP logic becomes 2-out of-2 coincidence logic.	
		c) Discrete input ON (Untripped)	Contact failure	Bistable logic not tripped	Periodic test	Three-channel redundancy	The resulting coincidence logic becomes 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.	The resulting coincidence logic becomes 1-out-of-2 coincidence logic for the affected variable.	
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	<ul style="list-style-type: none">DNBR/LPD channel trip/pre-tripCPC Fail annunciators and indication at OM/MTPCPC Trouble indication at OM/MTPDiagnostics indicate DO module failure.Local DO Module Fault lamp on, green Run lamp off	<ul style="list-style-type: none">Single PPS channel tripThree-channel redundancy	The resulting RPS logic for function becomes 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.	<ul style="list-style-type: none">Channel DNBR/LPD channel trip and pre-trip, CWP, also CPC Fail, annunciation CPC trouble indication on OM/MTPCPC processor fault lamp on, green Run lamp out	<ul style="list-style-type: none">Single PPS channel tripThree-channel redundancy	The resulting RPS logic becomes 1-outof-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. * Unrecognized software malfunctions: Software failures which cannot be detected by system and application diagnostics.
		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.	<ul style="list-style-type: none">Four channel comparisonDNBR/LPD margin indication of QIAS-N and IPS	<ul style="list-style-type: none">Three-channel redundancy	The resulting RPS logic becomes 2-outof-2 coincidence logic (assuming no channel trip).	
2-11	Aux CPC processor module (PM)	a) OFF; processor off	Loss of module power; software execution stops	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Channel trouble annunciation and indication on the OM/MTPAux CPC processor fault lamp on, green run lamp out	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Aux CPC does not perform a safety function.No effect on PPS.No compensating provisions required.	None	

APR1400 DCD TIER 2

Table 7.2-7 (9 of 25)

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
2-12	CEAC 1 processor module (PM) processor section	a) OFF; processor off	Loss of module power; software execution stops	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">CEAC 1 fail indication on OM/MTPChannel trouble indication / annunciation CEAC 1 processor fault lamp on, green run lamp out	Two redundant CEACs in each channel.	<ul style="list-style-type: none">Affected CPC uses the last good PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger.If the other CEAC is failed/declared inoperable ⁽³⁾/or in test, a large pre-selected ⁽²⁾ 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;	<ul style="list-style-type: none">Possible inconsistency in CEA position with respect to other CEAC/pulse count.Failure to properly indicate CEA motion.	<ul style="list-style-type: none">Cross channel comparison of CEA position	Two redundant CEACs in each channel.	<ul style="list-style-type: none">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.The resulting RPS logic becomes 2-outof-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. *Improper CEA positions: Erroneous CEA positions which cannot generate the DNBR/LPD trip.
2-13	CEAC 2 processor module (PM) processor section	a) OFF; processor off	Loss of module power; software execution stops	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">CEAC 2 Fail indication on OM/MTPChannel Trouble annunciation CEAC 2 processor fault lamp on, green run lamp out	Two redundant CEACs in each channel.	<ul style="list-style-type: none">Affected CPC uses the last good 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-selected 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.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">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.
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.	<ul style="list-style-type: none">CPP1 watchdog timer timeout, CPP trouble OM/MTP indication, channel Trouble annunciation.Loss of alternate source of RSPT 1 CEA position transmission to CEAC 1 in all four channels.Loss of preferred source of target CEA position in channel of origin.Loss of receive ports for alternate CEA position to CEAC 1.	<ul style="list-style-type: none">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 inputRun lamp out on affected CPPDiagnostics identify loss of SDL input to CPC.WDT in the affected CPP provide failure to CPC	<ul style="list-style-type: none">CPPs 1 and 2 are redundant in each channel.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.	None. CEAC 1 in all channels normally receives CEA position from CPP2. Target CEA position input in affected channel is switched from the CEAC 1 to CPC SDL to the CEAC 2 to CPC SDL. Loss of CPP 1 receives ports in channels A and B disables the alternate source of SDL input to CEAC 1. This has no effect on CEAC 1 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.
		b) ON; Erroneous CEA position transmitted*	Unrecognized hardware or software malfunction	<ul style="list-style-type: none">Failure to provide proper alternate source of CEA position in CEAC 1 in all channels.Possible failure of preferred source of target CEA position transmission in channel of origin	<ul style="list-style-type: none">Possible erroneous target CEA position indicationIf problem is due to processor failure, this is detected by on line diagnostics and a CPP trouble/ CPP WDT time out.	<ul style="list-style-type: none">CPP1 is alternate source for CEAC 1 position indication, and is normally not selected.CPP1 is preferred source of target CEA position, and target CEA position may be improper in one CPC channel.3-channel redundancy.	None. If target CEA position is improper, one CPC channel is inoperable, and RPS logic is in 2-out-of-2 coincidence logic.	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 * Erroneous CEA position transmitted: When CEA values are different from reading values transmitted from the analog input modules to the CPP/CEAC/CPC processors.

APR1400 DCD TIER 2

Table 7.2-7 (10 of 25)

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
2-14a	CEA Position Processor 2 in Channels A or B. Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	<ul style="list-style-type: none">• CPP2 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation• Loss of primary source of RSPT 1 CEA position transmission to CEAC 1 in all four channels• Loss of alternative source of Target CEA position in channel of origin• Loss of receive ports for primary CEA position to CEAC 1	<ul style="list-style-type: none">• 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• Run lamp out on affected CPP• Diagnostics identify loss of SDL input to CPC.• WDT in the affected CPP	<ul style="list-style-type: none">• CPPs 1 and 2 are redundant in each channel.• CPP 1 in channels A and B is alternative source of CEAC 1 CEA position in all channels. CPP 1 in channels A and B is primary source of Target CEA position.	None. CEAC 1 in all channels is switched from CEA positions from CPP2 to CPP1. CPC in all channels normally receives Target CEA position input from the CEAC 1 to CPC SDL Loss of CPP 2 ports in channels C and D disables the primary source of SDL input to CEAC 1.	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	<ul style="list-style-type: none">• Failure to provide proper primary source of CEA position in CEAC 1 in all channels.• Possible failure of alternative source of target CEA position transmission in channel of origin	Possible erroneous target CEA position indication	<ul style="list-style-type: none">• CPP2 is proper alternative source for Target CEA position indication, and is normally not selected.• CPP2 is preferred source of CEA position, and CEAC1 receiving CEA positions from CPP2 may be improper in all channels.• 2 CEAC redundancy	None. If CEA position in CEAC1 is improper, CEAC1 in all channels is inoperable, and CEAC2 in all channels are operable. RPS remains in 2-out-of-3 coincidence logic.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
2-14b	CEA Position Processor 1 in Channels C or D. Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	<ul style="list-style-type: none">• CPP1 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation• Loss of primary source of RSPT 1 CEA position transmission to CEAC 2 in all four channels• Loss of primary source of Target CEA position in channel of origin• Loss of receive ports for primary CEA position to CEAC 2	<ul style="list-style-type: none">• 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• Run lamp out on affected CPP• Diagnostics identify loss of SDL input to CPC.• WDT in the affected CPP	<ul style="list-style-type: none">• CPPs 1 and 2 are redundant in each channel.• CPP 2 in channels C and D is alternative source of CEAC 2 CEA position in all channels, and alternate source of Target CEA position.	None. CEAC 2 in all channels is switched for CEA positions from CPP1 to CPP2. Target CEA position input in affected channel is switched from the CEAC 1 to CPC SDL to the CEAC 2 to CPC SDL. Loss of CPP 1 ports in channels C and D disables the alternative source of SDL input to CEAC 1.	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	<ul style="list-style-type: none">• Failure to provide proper primary source of CEA position in CEAC 2 in all channels.• Possible failure of primary source of target CEA position transmission in channel of origin	Possible erroneous target CEA position indication	<ul style="list-style-type: none">• CPP2 is alternative source for Target CEA position indication, and is normally not selected.• CPP1 is primary source of CEA position, and CEAC2 receiving CEA positions from CPP1 may be improper in all channels.• 2 CEAC redundancy	None. If CEA position in CEAC2 is improper, CEAC2 in all channels is inoperable, and CEAC1 in all channels are operable. RPS remains in 2-out-of-3 coincidence logic.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.

APR1400 DCD TIER 2

Table 7.2-7 (11 of 25)

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
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	<ul style="list-style-type: none">• CPP 2 watchdog timer timeout, CPP trouble OM/MTP indication, channel trouble annunciation.• Loss of alternate source of RSPT 2 CEA position transmission to CEAC 2 in all four channels.• Loss of alternate source of target CEA position in channel of origin.• Loss of receive ports for alternate CEA position to CEAC 2.	<ul style="list-style-type: none">• 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• Run 2 lamp out on affected CPP• Diagnostics identify loss of SDL input to CPC.• WDT in the affected CPP provide failure to CPC	<ul style="list-style-type: none">• 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, CPP 1 provides preferred source of target CEA position in the affected channel. These are unaffected by a failure of CPP 2. 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.
		b) ON; Erroneous CEA position transmitted, but processor remains functional.	Unrecognized hardware or software malfunction	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.
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	<ul style="list-style-type: none">• SDL diagnostics indicate SDL failure, channel trouble indication on OM/MTP, trouble annunciation• CPC uses last good PF from inoperable CEAC versus current PF from operable CEAC.• Target CEA position sent to CPC over remaining link	<ul style="list-style-type: none">• Channel trouble indicated on OM/MTP in affected channel(s)• Diagnostics identify nature of failure.	<ul style="list-style-type: none">• Redundant CEAC to CPC SDL provides PFs and Target CEA position input.• One channel has one inoperable CEAC.• All others channels fully operable.	<ul style="list-style-type: none">• One channel has one inoperable CEAC.• Other channels fully operable.• RPS remains in 2-out-of-3 coincidence logic.	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	<ul style="list-style-type: none">• SDL diagnostics indicate SDL failure, channel trouble indication on OM/MTP, trouble annunciation• Both CEACs fail. CPC uses pre-selected PF on loss of both CEACs.• Likely channel trip if at high power levels• If SDL failure also causes loss of target CEA position transmission, CPC Fail and DNBR/LPD channel trip occurs.	<ul style="list-style-type: none">• CPC Fail indicated on OM/MTP in affected channel(s)• Diagnostics identify nature of failure• Channel trip (DNBR/LPD trip/pre-trip/CWP) likely	<ul style="list-style-type: none">• On loss of both CEACs, CPC channel uses pre-selected penalty.• Trip likely at high power levels.• Loss of Target CEA position input causes aux trip (DNBR/LPD)• Three channel redundancy in PPS	<ul style="list-style-type: none">• One channel has two inoperable CEACs. Likely channel trip.• The resulting RPS logic becomes 1-out of- 2 coincidence logic.	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.

APR1400 DCD TIER 2

Table 7.2-7 (12 of 25)

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
2-18	Loss of all SDL within a single CPC channel	Off, no transmission	Loss of fiber-optic modem power	<ul style="list-style-type: none">Channel trouble indication on OM/MTP in receiving channelsDNBR/LPD trip in failed channel due to loss of target CEA positionCPC fail indicated at OM/MTPFailure of one CEAC in other operable CPC channels	<ul style="list-style-type: none">SDL include diagnostics to detect failures by receiving processor.Channel trouble indicated on OM/MTP in receiving channel(s)One CEAC failed in other channels.Both CEACs failed in inoperable channel DNBR/LPD trips in failed channel.CPC fail indication on OM/MTPDiagnostics in receiving processors identify nature of failure	<ul style="list-style-type: none">Two CEACs per operable CPC channel.Other CEAC remains operable.CPC uses last good PF from failed CEAC or current PF from operable CEAC, whichever is larger.One CPC channel in trip, three channel redundancy	<ul style="list-style-type: none">One CEAC Failed in all operable CPC channels, and one CPC channel in trip (RPS in a 1-out-of-2 coincidence logic).Other CPC channels remain operable with one CEAC in each channel.	Operation with a single CEAC failure in one or more channels addressed in LCO .3.3.3. 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.
3	Analog input module (PPS BP rack)	a) Failure of microprocessor common to all analog input channels	Component failure	<ul style="list-style-type: none">Scan and processing of analog input channels stopProcess 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.	<ul style="list-style-type: none">No loss of safety functionCoincidence 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	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		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.	<ul style="list-style-type: none">No loss of safety functionCoincidence 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.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (13 of 25)

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
3	Analog input module (PPS BP rack) (Continued)	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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
4	Digital input module (PPS BP rack)	a) Entire module (common portion) fails.	Component failure	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• CPCS trip inputs and ENFMS trouble (generates low DNBR and high 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
		b) Single channel fails ON (normal, untripped 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
		c) Single channel fails OFF (tripped state).	Component failure	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• LCL voting needs 2 safety channels to be tripped for coincidence.• A manual partial bypass can be entered for the failed input channel.	<ul style="list-style-type: none">• No loss of safety function• The resulting coincidence logic becomes 1-out-of-2 logic. If manual partial bypass entered, the resulting coincidence logic becomes 2-out-of-3 logic.	N/A
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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (14 of 25)

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
5	Bistable processor module (PPS BP rack) (Continued)	c) Processing section fails to scan input/output modules.	Component failure	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Corrupted I/O bus cycles are detected.Trouble alarm is actuated.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		d) Processing section fails to read from communication section.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected BPOp 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	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of BP processor updates detected by LCL via SDLLack of BP processor updates detected by MTP/ITP via SDNTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		e) Processor section fails to write to communication section.	Component failure	<ul style="list-style-type: none">No periodic updates transmitted to SDL from affected BP	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of BP processor updates detected by LCL via SDLTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		f) Communication section fails to receive SDL.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PMOp Bypass and VSP reset request data from MCR-CPM and RSR-CPM via SDL are lost to the BP bistable logic.	<ul style="list-style-type: none">Lack of CPM processor updates detected by BP via SDLTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		g) Communication section fails to transmit SDL.	Component failure	No periodic updates transmitted to SDL from affected PM	<ul style="list-style-type: none">Lack of BP processor updates detected by LCL via SDLTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		h) General failure of communication section	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDNNo periodic updates received from SDL by affected PMOp Bypass and VSP reset request data from MCR-CPM and RSR-CPM via SDL are lost to the BP bistable logic.	<ul style="list-style-type: none">PS detects lack of live signal handshaking and sets diagnostic alarm.Lack of BP processor updates detected by MTP/ITP via SDNLack of BP processor updates detected by LCL via SDLTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		i) PM locks (permanently) the backplane input/output network (BIOB)	Component failure	<ul style="list-style-type: none">Affected processor halts.All I/O functions are prevented including data exchange with SDN communication module.	<ul style="list-style-type: none">Lack of BIOB activity detected by BP diagnosticsLack of BP processor updates detected by LCL via SDLLack of BP processor updates detected by MTP/ITP via SDNTrouble alarm is actuated.	Partial trip/actuation selection logic in all LCLs use quality data from the redundant BP in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (15 of 25)

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	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.	<ul style="list-style-type: none">Lack of BP processor periodic updates detected by LCL SDLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence 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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Lack of CPM periodic updates is detected by BP via SDLTrouble alarm is actuated.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">No loss of safety function.Coincidence remains 2-out-of-3 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 divisions connected to failed BP detect loss of periodic updates.	<ul style="list-style-type: none">Lack of BP processor periodic updates detected by LCL SDLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
9	SDN communication module (PPS BP Rack)	a) Shared memory failure	Component failure	<ul style="list-style-type: none">BP halts.No PM periodic updates to all LCLs via SDL and on SDN network	<ul style="list-style-type: none">Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		b) Back Plane failure	Component failure	<ul style="list-style-type: none">BP halts.No PM periodic updates to all LCLs via SDL and on SDN network	<ul style="list-style-type: none">Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		c) SDN interface failure	Component failure	<ul style="list-style-type: none">BP halts.No PM periodic updates to all LCLs via SDL and on SDN network	<ul style="list-style-type: none">Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		d) Microprocessor failure	Component failure	<ul style="list-style-type: none">BP halts.No PM periodic updates to all LCLs via SDL and on SDN network	<ul style="list-style-type: none">Lack of BP processor periodic updates on SDN network detected by MTP/ITP and on SDL by LCLTrouble alarm is actuated.	BP selection logic in all the LCLs uses quality data from the redundant BP of the affected safety channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
				<ul style="list-style-type: none">Data storm.Spurious data is sent to the receiving processors	<ul style="list-style-type: none">Trip alarm is actuated.	Three-channel redundancy	<ul style="list-style-type: none">Coincidence remains as 1-out-of-2 logic.	N/A
10	LCL processor performing RT function (PPS LCL rack)	a) Processing section fails to execute program instructions.	Component failure	<ul style="list-style-type: none">Affected LCL halts and the WDT contact opens.No periodic updates transmitted to SDN from affected PMNo periodic updates received from SDL by affected PM	<ul style="list-style-type: none">Lack of LCL processor updates detected by MTP/ITP via SDNTrouble alarm is actuated.	Open WDT contact only affects one-half of the affected safety division RT initiation circuit.	Open WDT contact trips one-half of the safety division RT initiation circuit.	N/A
		b) Application program memory failure	Component failure	<ul style="list-style-type: none">Affected LCL halts and the WDT contact opens.No periodic updates transmitted to SDN from affected PMNo periodic updates received from SDL by affected PM	<ul style="list-style-type: none">CRC checks performed on memoryLack of LCL processor updates detected by MTP/ITP via SDNTrouble alarm is actuated.	Open WDT contact only affects one-half of the affected safety division RT initiation circuit.	Open WDT contact trips one-half of the safety division RT initiation circuit.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (16 of 25)

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	LCL processor performing RT function (PPS LCL rack) (Continued)	c) Processing section fails to scan input/output modules.	Component failure	<ul style="list-style-type: none">• LCL outputs (reactor trips) not updated periodically• Digital Output module sets outputs to default de-energized state.	<ul style="list-style-type: none">• Corrupted I/O bus cycles detected• Trouble alarm is actuated.	Digital output only affects one-half of the affected safety division RT initiation circuit.	Digital output trips one-half of the safety division RT initiation circuit.	N/A
		d) Processing section fails to read from communication section.	Component failure	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 division RT initiation circuit.	Open WDT contact trips one-half of the safety division 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
		h) General failure of communication section	Component failure	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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 division RT initiation circuit.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.• Open WDT contact trips one-half of the safety division RT initiation circuit.	N/A
		i) PM locks (permanently) the BIOB.	Component failure	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Lack of BIOB activity detected by PM diagnostics• Lack of LCL processor updates detected by MTP/ITP via SDN• Trouble alarm is actuated.	<ul style="list-style-type: none">• System level reactor trip provided by other three safety divisions.• Redundant LCL station available to provide RT function for affected division.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• System level reactor trip provided by other three safety divisions.• Redundant LCL station available to provide RT function for affected division.	<ul style="list-style-type: none">• No loss of safety function.• Coincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (17 of 25)

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	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	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">System level reactor trip provided by other three safety divisions.Redundant LCL station available to provide RT function for affected division.	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPartial actuation data to one ESF-CCS GC is lost.No periodic updates received from SDL by affected PM	<ul style="list-style-type: none">Lack of LCL processor updates detected by MTP/ITP via SDNLack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		b) Application program memory failure	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPartial actuation data to one ESF-CCS GC is lostNo periodic updates received from SDL by affected PM	<ul style="list-style-type: none">CRC checks performed on memoryLack of LCL processor updates detected by MTP/ITP via SDNLack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		c) Processing section fails to scan input/output modules.	Component failure	LCL outputs not updated periodically.	<ul style="list-style-type: none">Corrupted I/O bus cycles detectedTrouble alarm is actuated.	N/A	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		d) Processing section fails to read from communication section.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PMLack of CS/PS handshaking causes affected processor to haltNo periodic updates transmitted to SDL and SDN from affected PMPartial actuation data to one ESF-CCS GC is lost	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of LCL processor updates detected by MTP/ITP via SDNLack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		e) Processing section fails to write to communication section.	Component failure	<ul style="list-style-type: none">No periodic updates transmitted to SDL from affected PMPartial actuation data to one ESF-CCS GC is lost.	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety function occursCoincidence remains as 2-out-of-3 logic.	
		f) Communication section fails to receive SDL.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PMPartial trip/actuation data from two BPs (each from a separate channel) via SDL are lost to the LCL voting logic.	<ul style="list-style-type: none">Lack of BP processor updates detected by LCL via SDLTrouble 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.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		g) Communication section fails to transmit SDL.	Component failure	<ul style="list-style-type: none">No periodic updates transmitted to SDL from affected PMPartial actuation data to one ESF-CCS GC is lost.	<ul style="list-style-type: none">Lack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety function occursCoincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (18 of 25)

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	LCL processor module performing ESF actuation function (PPS LCL Rack) (Continued)	h) General failure of communication section	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPartial actuation data to one ESF-CCS GC is lost.No periodic updates received from SDL by affected PM	<ul style="list-style-type: none">PS detects lack of live signal handshaking and sets diagnostic alarm.Lack of LCL processor updates detected by MTP/ITP via SDNLack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety function occursCoincidence remains as 2-out-of-3 logic.	N/A
		i) PM locks (permanently) the BIOB.	Component failure	<ul style="list-style-type: none">Affected processor halts.All I/O functions are prevented including data exchange with SDN communication module.	<ul style="list-style-type: none">Lack of BIOB activity detected by PM diagnosticsLack of LCL processor updates detected by MTP/ITP via SDNLack of LCL processor updates detected by ESF-CCS GC via SDLTrouble alarm is actuated.	ESFAS actuations from redundant LCL station are provided to redundant ESF-CCS GC station.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
12	LCL processor module performing only COM function (PPS LCL rack)	a) Processor section fails to execute program instructions.	Component failure	<ul style="list-style-type: none">Affected processor halts.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.	<ul style="list-style-type: none">Lack of LCL processor updates detected by MTP/ITP via SDN.Trouble alarm is actuated.	Partial trip/actuation selection logic in ESF LCL and both RT LCLs of affected LCL process station will use good quality data from the redundant BP PM in affected channel.	<ul style="list-style-type: none">No loss of safety function.Coincidence remains 2-out-of-3 logic.	N/A
		b) Application program memory failure (mirror RAM)	Component failure.	<ul style="list-style-type: none">Affected processor halts.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.	<ul style="list-style-type: none">CRC checks performed on memory.Lack of LCL processor updates detected by MTP/ITP via SDN.Trouble alarm is actuated.	Partial trip/actuation selection logic in ESF LCL and both RT LCLs of affected LCL process station will use good quality data from the redundant BP PM in affected channel.	<ul style="list-style-type: none">No loss of safety function.Coincidence remains 2-out-of-3 logic.	N/A
		c) Processor section fails to scan input/output modules.	Component failure	<ul style="list-style-type: none">LCL COM PM does not access I/O modules.	N/A	N/A	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A
		d) Processor section fails to read from communication section.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PMPartial trip/actuation data from two BP PMs (each from a separate channel) via SDL are lost to the LCL voting logic.Lack of communication section/processing section handshaking causes affected processor to halt.No periodic updates transmitted to SDN from affected PM.	<ul style="list-style-type: none">Communication section 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 both RT LCLs of affected LCL process station will use good quality data from the redundant BP PM in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A
		e) Processor section fails to write to communication section.	Component failure	SDL transmits are not provided by this processor.	Communication section detects lack of handshaking and sets diagnostic alarm.	N/A	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (19 of 25)

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	LCL Processor module performing only COM function (PPS LCL rack) (Continued)	f) Communication section fails to receive SDL.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PM.Partial trip/actuation data from two BP PMs (each from a separate channel) via SDL are lost to the LCL voting logic.	<ul style="list-style-type: none">Lack of BP processor updates detected by LCL via SDLTrouble alarm is actuated	Partial trip/actuation selection logic in ESF LCL and both RT LCLs of affected LCL process station will use good quality data from the redundant BP PM in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 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	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A
		h) General failure of communication section	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDN from affected PMNo periodic updates received from SDL by affected PMPartial trip/actuation data from two BPs (each from a separate channel) via SDL are lost to the LCL voting logic.	<ul style="list-style-type: none">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 both RT LCLs of affected LCL process station will use good quality data from the redundant BP PM in affected channel.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A
		i) PM locks (permanently) the BIOB	Component failure	<ul style="list-style-type: none">Affected processor will halt.RT matrix associated with affected LCL station will prevent 1/2 leg trip.All I/O functions are prevented including data exchange via SDN.	<ul style="list-style-type: none">Lack of BIOB activity detected by PM diagnostics.Lack of LCL processor updates detected by MTP/ITP via SDN.Trouble alarm is actuated.	<ul style="list-style-type: none">System level reactor trip provided by other three safety channels.ESFAS actuations from redundant LCL station are provided to redundant ESFCCS GC station.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains 2-out-of-3 logic.	N/A
13	SDN communication module (PPS LCL rack)	a) Shared memory failure	Component failure	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Diagnostic alarms actuated upon failure of normal I/O functionsLack 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/ITPTrouble alarm is actuated.	<ul style="list-style-type: none">Other safety division cabinet RT initiation circuit half leg available to provide the safety division RT function.ESFAS initiations for the safety division with the affected LCL station will be received from the redundant LCL process station ESF PM.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		b) BIOB ASIC failure	Component failure	<ul style="list-style-type: none">All affected LCL station processors halt 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.	<ul style="list-style-type: none">Diagnostic alarms actuated upon failure of normal I/O functionsLack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCSLack of LCL station periodic updates on SDN network detected by MTP/ITPTrouble alarm is actuated.	<ul style="list-style-type: none">Other safety division cabinet RT initiation circuit half leg available to provide the safety division RT function.ESFAS initiations for the safety division with the affected LCL station will be received from the redundant LCL process station ESF PM.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
		c) SDN interface ASIC failure	Component failure	<ul style="list-style-type: none">All affected LCL station processors halt 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.	<ul style="list-style-type: none">Diagnostic alarms actuated upon failure of normal I/O functionsLack of affected ESF LCL processor periodic updates on SDL is detected by ESF-CCS.Lack of LCL processor periodic updates on SDN network detected by MTP/ITPTrouble alarm is actuated.	<ul style="list-style-type: none">Other safety division cabinet RT initiation circuit half leg available to provide the safety division RT function.ESFAS initiations for the safety division with the affected LCL station will be received from the redundant LCL process station ESF PM.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (20 of 25)

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
13	SDN communication module (PPS LCL Rack) (Continued)	d) Microprocessor failure	Component failure	<ul style="list-style-type: none">• All affected LCL station processors halt and the WDT times out.• ESFAS initiation signals to GC is not updated via SDL for affected LCL process station.• Affected LCL station causes half leg trip in the RT initiation circuit.	<ul style="list-style-type: none">• 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 processor periodic updates on SDN network is detected by MTP/ITP.• Trouble alarm is actuated.	<ul style="list-style-type: none">• Other safety division cabinet RT initiation circuit half leg available to provide the safety division RT function.• ESFAS initiations for the safety division with the affected LCL station will be received from the redundant LCL process station ESF PM.	<ul style="list-style-type: none">• 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 1-out-of-2 logic	N/A
14	DO Relay Output Module	a) Division (UV) contact does not open on command.	Component failure	Contact resistance remains near zero.	DO relay contacts are tested during surveillance test.	RT via UV interposing relay provided through other 3 RT LCL processors and corresponding 3 DO relay output modules.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
		b) Division (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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
		c) Common portion (BIOB) fails	Component failure	<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
15	Fiber-optic SDL link to GC Process Stations	Failure of fiber-optic modem	Component failure	<ul style="list-style-type: none">• Only failed fiber-optic modem does not transmit ESF initiations, from the connected LCL ESF PM, to one of the four GCs.• Other three fiber-optic modems transmit initiations to their connected GC.	GC detects loss of periodic updates and activates a diagnostic alarm.	<ul style="list-style-type: none">• Redundant GC process station receives valid communications from LCL ESF PM in redundant LCL station in opposite safety division cabinet.• 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.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A
16	Failure of LCL Process Station Backplane	Loss of power to one LCL station	Power supply wire termination failed	<ul style="list-style-type: none">• Contacts open on digital output modules removing one leg of the two powering both interposing relay coils for RT initiation for the safety division SDL.• The communication for ESFAS initiation to GC is lost.	Safety division ITP detects loss of LCL periodic updates on SDN network and alarm.	<ul style="list-style-type: none">• The digital output modules in the redundant LCL station of the safety division 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.• The LCL ESF processor in the redundant LCL station of the safety division continues to provide ESFAS initiations to the other ESF-CCS group controller.	<ul style="list-style-type: none">• No loss of safety function• Coincidence remains as 2-out-of-3 logic.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (21 of 25)

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
17	UV Relay (one/safety division)	a) Open or shorted coil	Component failure	<ul style="list-style-type: none">Energized UV relay drops out opening current path for TCB UV coil in safety division TCB opens.	<ul style="list-style-type: none">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 division TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.The safety division TCB UV coil is commanded to open.	N/A
		b) High resistance trip contact	Component failure	<ul style="list-style-type: none">RT contact on UV relay does not close when coil energized.TCB remains open.	<ul style="list-style-type: none">ITP provides breaker position and UV relay contact status signals to MTP for PPS screen display.	When four safety division TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.The safety division TCB UV coil is commanded to operate.	N/A
		c) Welded trip contact	Component failure	<ul style="list-style-type: none">RT contact on UV relay does not open when coil de-energized.TCB UV coil keeps TCB closed.	<ul style="list-style-type: none">UV relay function is verified during routine surveillance test.	When four safety division TCBs are wired in a 2-out-of-4 arrangement, a minimum of two open before an RT occurs.	<ul style="list-style-type: none">No loss of safety functionCoincidence remains as 2-out-of-3 logic.	N/A
18	ITP processor module	a) Functional processor section fails to execute program instructions.	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">Lack of ITP processor updates detected by MTP via SDNLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions	<ul style="list-style-type: none">No effect on PPS safety functionPPS status data processed by ITP for indication not updated for affected division.PPS status data transmitted to QIAS-N not updated for affected division.	N/A
		b) Application program memory failure (mirror RAM)	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">CRC checks performed on memoryLack of ITP processor updates detected by MTP via SDNLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions	<ul style="list-style-type: none">No effect on PPS safety functionPPS status data processed by ITP for indication not updated for affected division.PPS status data transmitted to QIAS-N not updated for affected division.	N/A
		c) Processor section fails to scan I/O modules.	Component failure	<ul style="list-style-type: none">ITP inputs (PPS status, ENFMS test requests) not updated periodically.ITP outputs (ENFMS test permissive, MTP Panel indications) not updated periodically.	<ul style="list-style-type: none">Corrupted I/O bus cycles detectedTrouble alarm is actuated.	ENFMS test capability provided by other divisions.	<ul style="list-style-type: none">No effect on PPS safety functionPPS status data processed by ITP for indication not updated for affected division.	N/A
		d) Processor section fails to read from communication section.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PMLack of CS/PS handshaking causes affected processor to haltNo periodic updates transmitted to SDL and SDN from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of ITP processor updates detected by MTP via SDNLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	<ul style="list-style-type: none">No effect on PPS safety functionPPS status data processed by ITP for indication not updated for affected division.PPS status data transmitted to QIAS-N not updated for affected division.	N/A
		e) Processor section fails to write to communication section.	Component failure	<ul style="list-style-type: none">No periodic updates transmitted to SDL from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">CS detects lack of live signal handshaking and sets diagnostic alarm.Lack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	No effect on PPS safety function	N/A

APR1400 DCD TIER 2

Table 7.2-7 (22 of 25)

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
18	ITP processor module (Continued)	f) Communication section fails to receive SDL.	Component failure	<ul style="list-style-type: none">No periodic updates received from SDL by affected PM	<ul style="list-style-type: none">Lack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	<ul style="list-style-type: none">No effect on PPS safety function	N/A
		g) Communication section fails to transmit SDL.	Component failure	<ul style="list-style-type: none">No periodic updates transmitted to SDL from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">Lack of ITP processor updates detected by other ITPs via SDLLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	<ul style="list-style-type: none">No effect on PPS safety function	N/A
		h) General failure of communication section.	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPPS status data from affected ITP are lost to the QIAS-N.	<ul style="list-style-type: none">Lack of ITP processor updates detected by MTP via SDNLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	<ul style="list-style-type: none">No effect on PPS safety function.PPS status data processed by ITP for indication not updated for affected division.PPS status data transmitted to QIAS-N not updated for affected division.	N/A
		i) PM locks (permanently) the BIOB.	Component failure	<ul style="list-style-type: none">Affected processor halts.No periodic updates transmitted to SDL and SDN from affected PMPPS status data from affected ITP are lost to the QIAS-N.All I/O functions are prevented including data exchange with SDN communication module.	<ul style="list-style-type: none">Lack of ITP processor updates detected by MTP via SDNLack of ITP processor updates detected by QIAS-N via SDLTrouble alarm is actuated.	ITPs operating in three other safety divisions.	<ul style="list-style-type: none">No effect on PPS safety function.PPS status data processed by ITP for indication not updated for affected division.PPS status data transmitted to QIAS-N not updated for affected division.	N/A
19	ITP fiber-optic modem	Transmitter fails	Component failure	<ul style="list-style-type: none">PPS status data transmitted to QIAS-N is not updated due to failed FOM for affected division.	Lack of ITP processor updates, due to failed FOM in affected division, detected by QIAS-N	None in ITP	No effect on PPS safety function.	N/A
20	MTP PC node box	General failure	Component failure	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">Data from the other three safety divisions are available to the non-safety system.Data through the OM safety display still available.	<ul style="list-style-type: none">No effect on PPS safety function.Data from this division is not available to the IPS.	N/A
21	MTP SDN communication module	General failure	Component failure	MTP display reacts normally, but data from division is stale.	ITP process station Monitors MTP health via SDN network; activates diagnostic alarm on loss of data update	<ul style="list-style-type: none">Data from the other three safety divisions 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.	<ul style="list-style-type: none">No effect on PPS safety function.Data from this division 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
22	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 divisions are available to the system IPS.	<ul style="list-style-type: none">No effect on PPS safety function.Data from this division is not available to the IPS.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (23 of 25)

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
23	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 division operator's module PPS screens are available to the operator.	<ul style="list-style-type: none">No effect on PPS safety function.Repair is performed before PPS safety division surveillance testing or software maintenance is available.	N/A
24	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	<ul style="list-style-type: none">No effect on PPS safety function.Keyboard is not required for any safety function.	N/A
25	PPS vital bus inverter	Off	Circuit breaker feed for PPS safety division opens.	<ul style="list-style-type: none">Loss of PPS safety divisionPPS safety division signals reactor trip breaker to open.SDLs to ESF-CCS group controllers do not update.	<ul style="list-style-type: none">LCL stations in other three safety divisions provide alarm loss of SDL updates from PPS safety division without power.ITP in safety division does not provide alarm.	<ul style="list-style-type: none">Three PPS safety divisions remain operable.A complete reactor trip requires two breakers to open.ESF-CCS group controllers take default action.	<ul style="list-style-type: none">No effect on PPS safety function.The resulting coincidence logic becomes 1-out-of-2 logic for RPS and the resulting coincidence logic becomes 2-out-of-2 logic for ESFAS.	N/A
26	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.	<ul style="list-style-type: none">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	<ul style="list-style-type: none">Loss of PPS safety division cabinetReactor 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 divisions provide alarm loss of SDL updates from PPS safety division cabinet without power.	<ul style="list-style-type: none">Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates.Redundant PPS safety division cabinet providing all signals necessary for safety functions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.	N/A
27	PPS surge suppressor	Open circuit (failure to provide surge suppression)	Device burned open	<ul style="list-style-type: none">Loss of PPS safety division cabinetPPS safety division has 1-out-of-2 legs for reactor trip open.PPS cabinet SDLs to ESF-CCS group controllers and SDN network do not update.	LCL stations in other three safety divisions provide alarm loss of SDL updates from PPS safety division cabinet without power.	<ul style="list-style-type: none">Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates.Redundant PPS safety division cabinet providing all signals necessary for safety functions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.	N/A
28	PPS EMI filter	a) Open (OFF); internal failure; short circuit	Device shorts internally	<ul style="list-style-type: none">Loss of PPS safety division cabinetPPS safety division has 1-out-of-2 legs for reactor trip open.PPS cabinet SDLs to ESF-CCS group controllers and SDN network do not update.	LCL stations in other three safety divisions provide alarm loss of SDL updates from PPS safety division cabinet without power.	<ul style="list-style-type: none">Receiving stations for failed PPS cabinet SDLs and SDN networks assign bad quality to updates.Redundant PPS safety division cabinet providing all signals necessary for safety functions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.	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.	<ul style="list-style-type: none">No effect on PPS safety function.No effect on the dc circuit functionality.	N/A
29	PPS cabinet power supplies	Overvoltage	Component failure	<ul style="list-style-type: none">Overvoltage device detects and removes voltage to the connected load.Lose BP and LCL stations.Results in safety division 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 division provide signals for safety functions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.Affected safety division has a half-leg reactor trip.	N/A

APR1400 DCD TIER 2

Table 7.2-7 (24 of 25)

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
30	PPS I/O power supplies	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.	N/A
31	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.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.No loss of DC circuit functionality.	N/A
32	PPS power supply auctioneering circuit applicable to 24 VDC cabinet power supply	Overvoltage	Over voltage protection device operates when voltage is in range.	<ul style="list-style-type: none">Overvoltage device detects and removes voltage to the connected load.Lose BP and LCL stationsResults in safety division 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 division provide signals for safety functions.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.Affected safety division has a half-leg reactor trip.	N/A
33	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.	<ul style="list-style-type: none">No effect on PPS safety function.Coincidence remains as 2-out-of-3 logic.	N/A
34	MTP / ITP cabinet input circuit breaker	a) Breaker is ON does not trip on overload.	Internal mechanical failure	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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 division due to redundant power feed.	No loss of safety function	N/A
35	MTP / ITP cabinet surge suppressor	Open circuit (failure to provide surge suppression).	Device burned open	<ul style="list-style-type: none">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
36	MTP / ITP cabinet EMI filter	a) Open (OFF); internal failure; short circuit.	Series component failure	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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
37	MTP / ITP cabinet power supplies: 24 VDC	Overvoltage	Component failure	<ul style="list-style-type: none">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 divisions operable.	<ul style="list-style-type: none">No loss of safety function.Some PPS screens on MTP and OM not updated.	N/A
38	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

APR1400 DCD TIER 2

Table 7.2-7 (25 of 25)

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
39	MTP / ITP cabinet power supply auctioneering circuit applicable to all cabinet power supplies: 24 VDC	a) Open diode	Overload, component failure	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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
40	MTP / ITP cabinet power supply auctioneering circuit applicable to 24 VDC cabinet power supply	Overvoltage	Component failure	<ul style="list-style-type: none">Overvoltage device detects and removes voltage to the connected load.Lose ITP stationNo SDL or SDN activity	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	ITP in other three safety divisions operable	<ul style="list-style-type: none">No loss of safety function.Some PPS screens on MTP and OM not updated.	N/A
41	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
42	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
43	MTP / ITP cabinet alternate ac feed breaker for MTP	Breaker opens while powering the MTP.	Component failure	<ul style="list-style-type: none">Alternate vital ac lost to MTPMTP 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 divisions.	Loss of MTP function with PPS in the safety division	N/A
44	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 divisions operating.	Lose MTP function with PPS in the safety division	N/A
45	Trip circuit breaker (TCB) of RTSG	1) Open	<ul style="list-style-type: none">Loss of 125Vdc control powerUnwanted energizing of UV coilMechanical failure of TCB	The RTSG opens.	<ul style="list-style-type: none">AlarmIndication on the MTP and OM in the MCR	The RTSGs in other divisions are not affected.	The resulting logic of RTSGs becomes 1-out-of-3.	
		2) Closed	<ul style="list-style-type: none">Mechanical failure of TCBFailure of UV coilShort contact of TCB	The RTSG cannot be opened.	Periodic test	The RTSGs in other divisions are not affected	The resulting logic of RTSGs becomes 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.
- (2) Pre-selected PF : Penalty factor which is selected to initiate plant trip for two CEACs fail condition
- (3) The output of the safety-related I&C system processors stay in a non-trip state when the processor is declared inoperable.
- (4) The "watchdog timer" or "WDT" described in Table 7.2-7 refers to the "window watchdog timer". See Section 5.2.1.3 of “Common Qualified Platform Topical Report” listed as Reference 77 in Subsection 7.1.5.

APR1400 DCD TIER 2

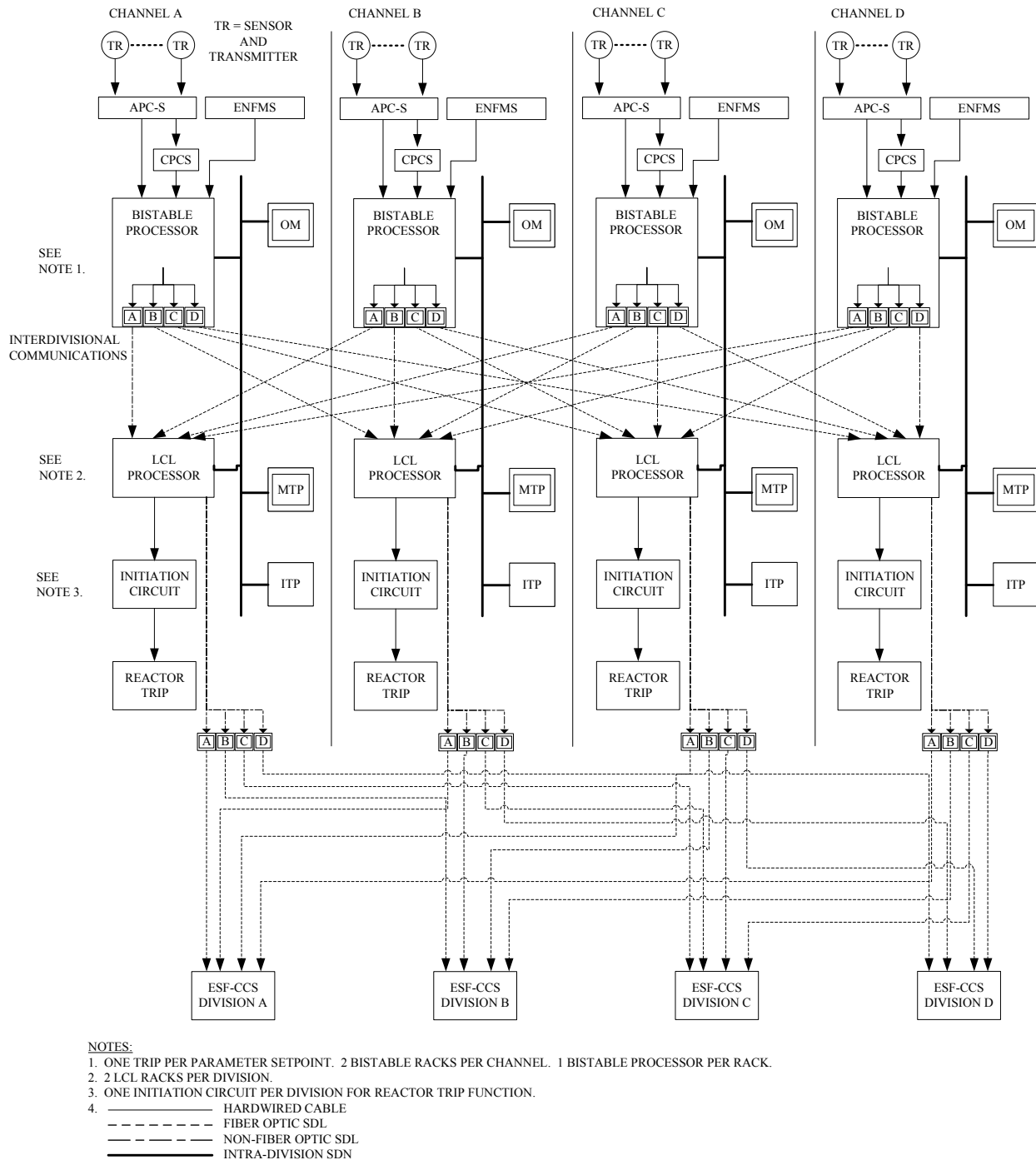


Figure 7.2-1 PPS Basic Block Diagram

APR1400 DCD TIER 2

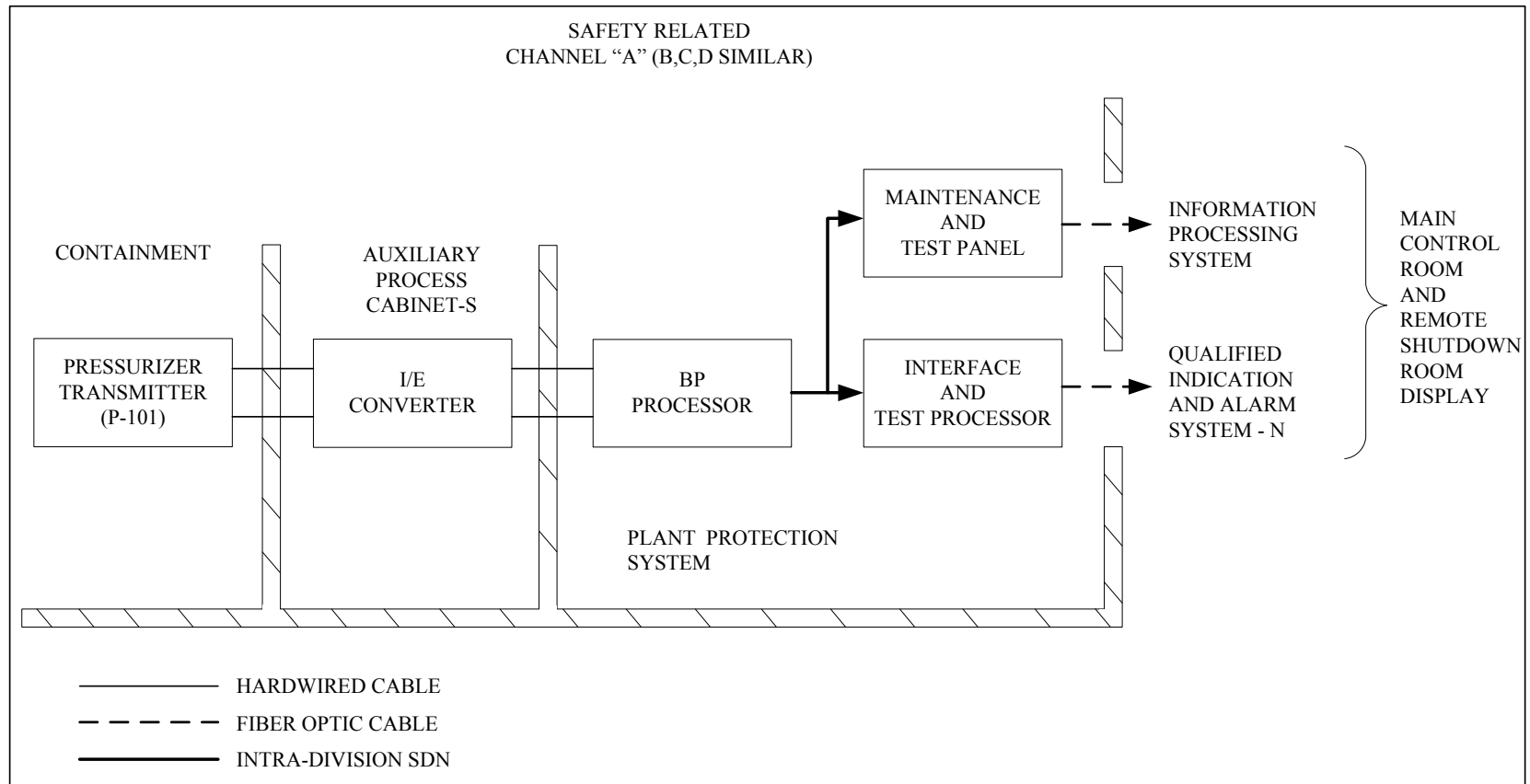


Figure 7.2-2 PPS Measurement Channel Functional Diagram (Pressurizer Pressure Narrow Range)

APR1400 DCD TIER 2

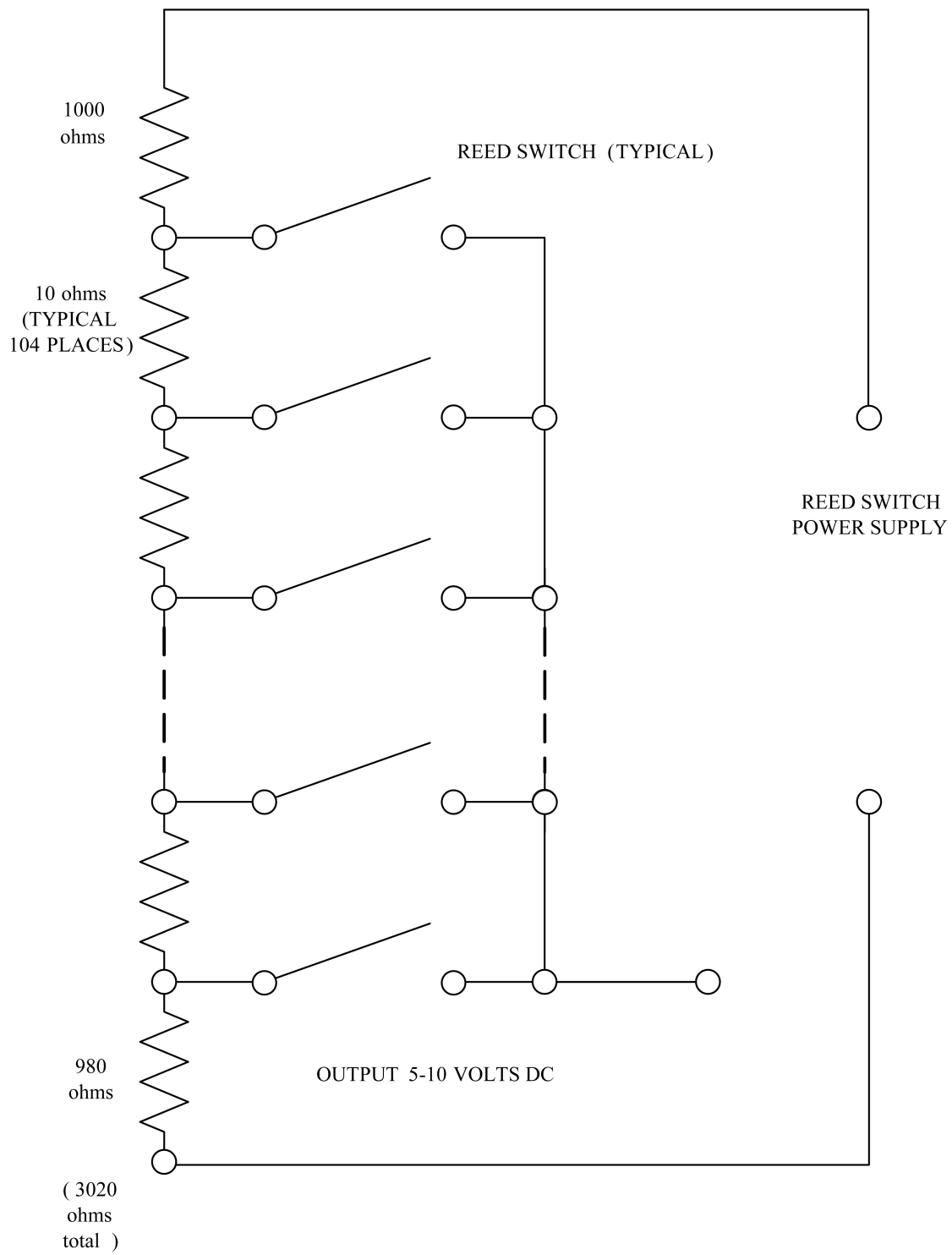


Figure 7.2-3 Reed Switch Position Transmitter Assembly Schematic

APR1400 DCD TIER 2

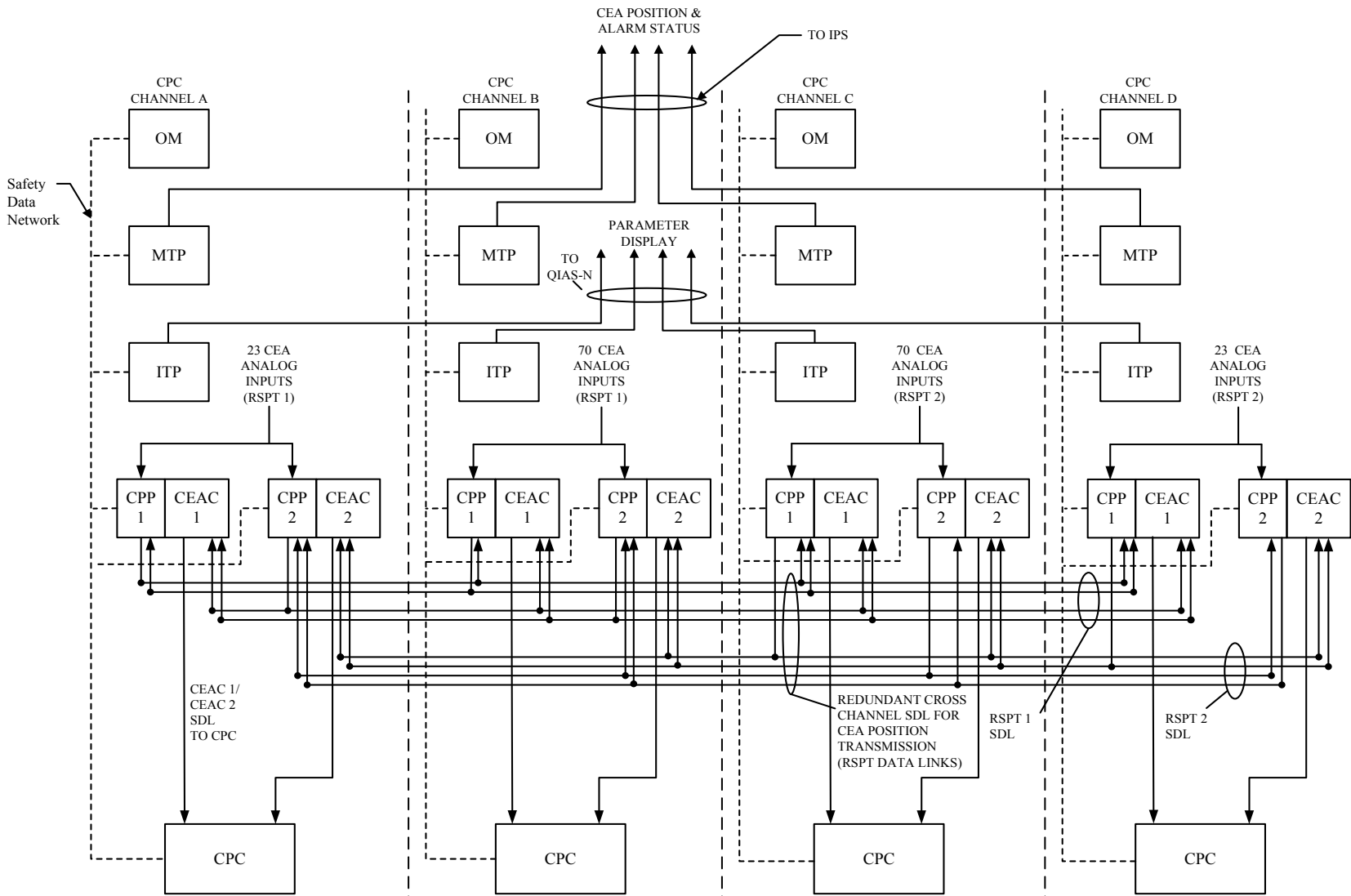


Figure 7.2-4 CEA Position Signal Flow for CPCS

APR1400 DCD TIER 2

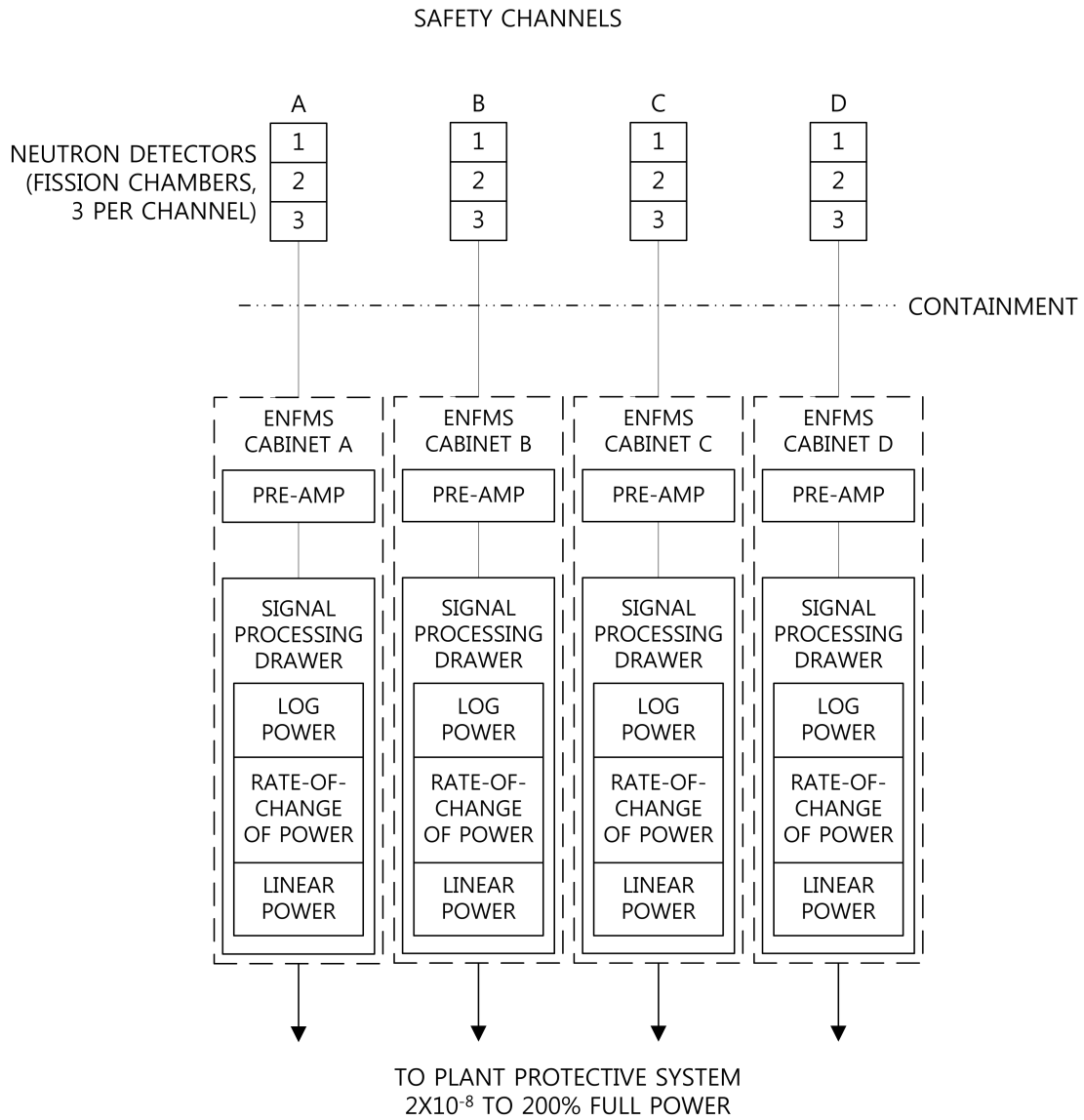


Figure 7.2-5 Ex-Core Neutron Monitoring System (Safety Channel)

APR1400 DCD TIER 2

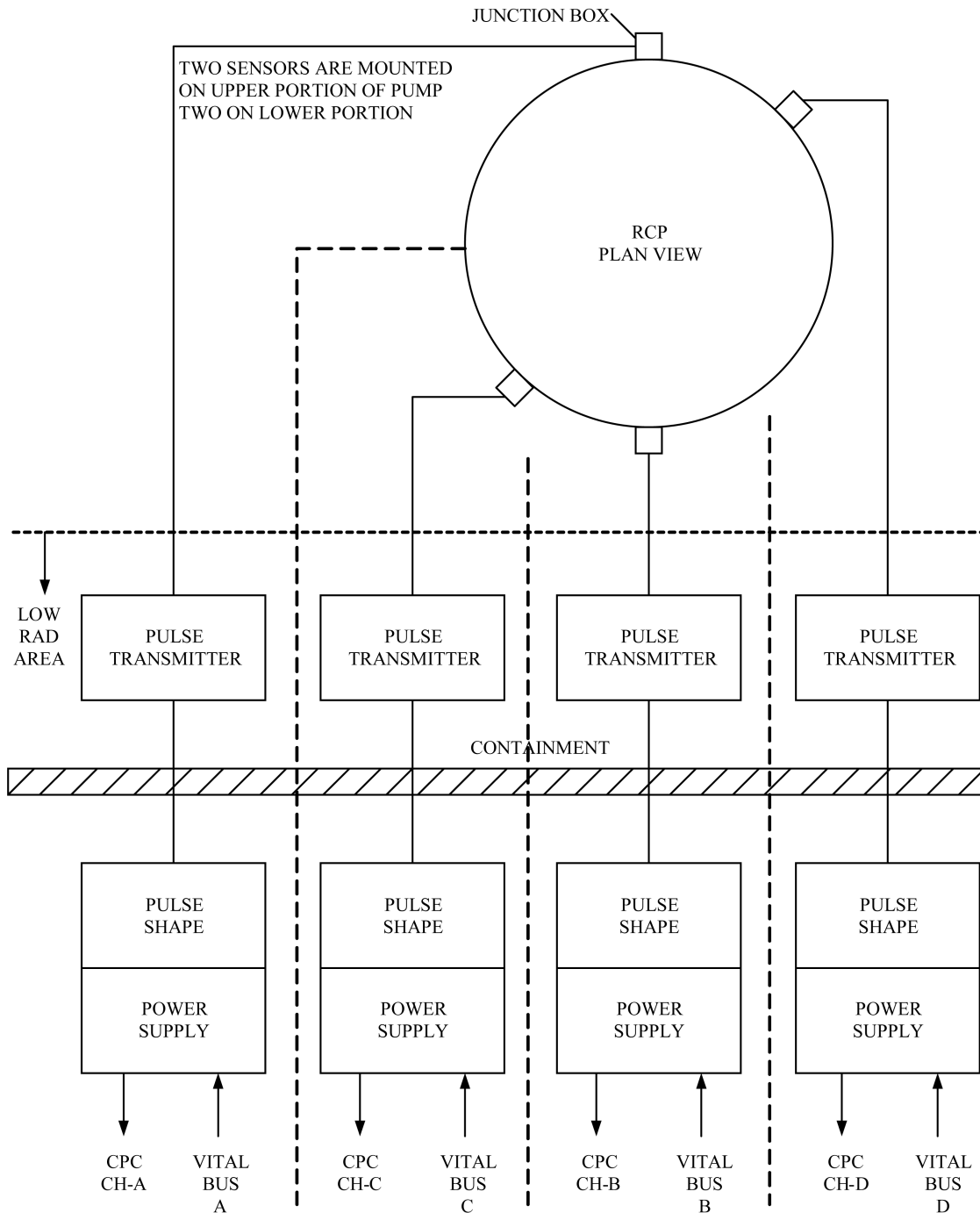


Figure 7.2-6 Reactor Coolant Pump Shaft Speed Sensing System

APR1400 DCD TIER 2

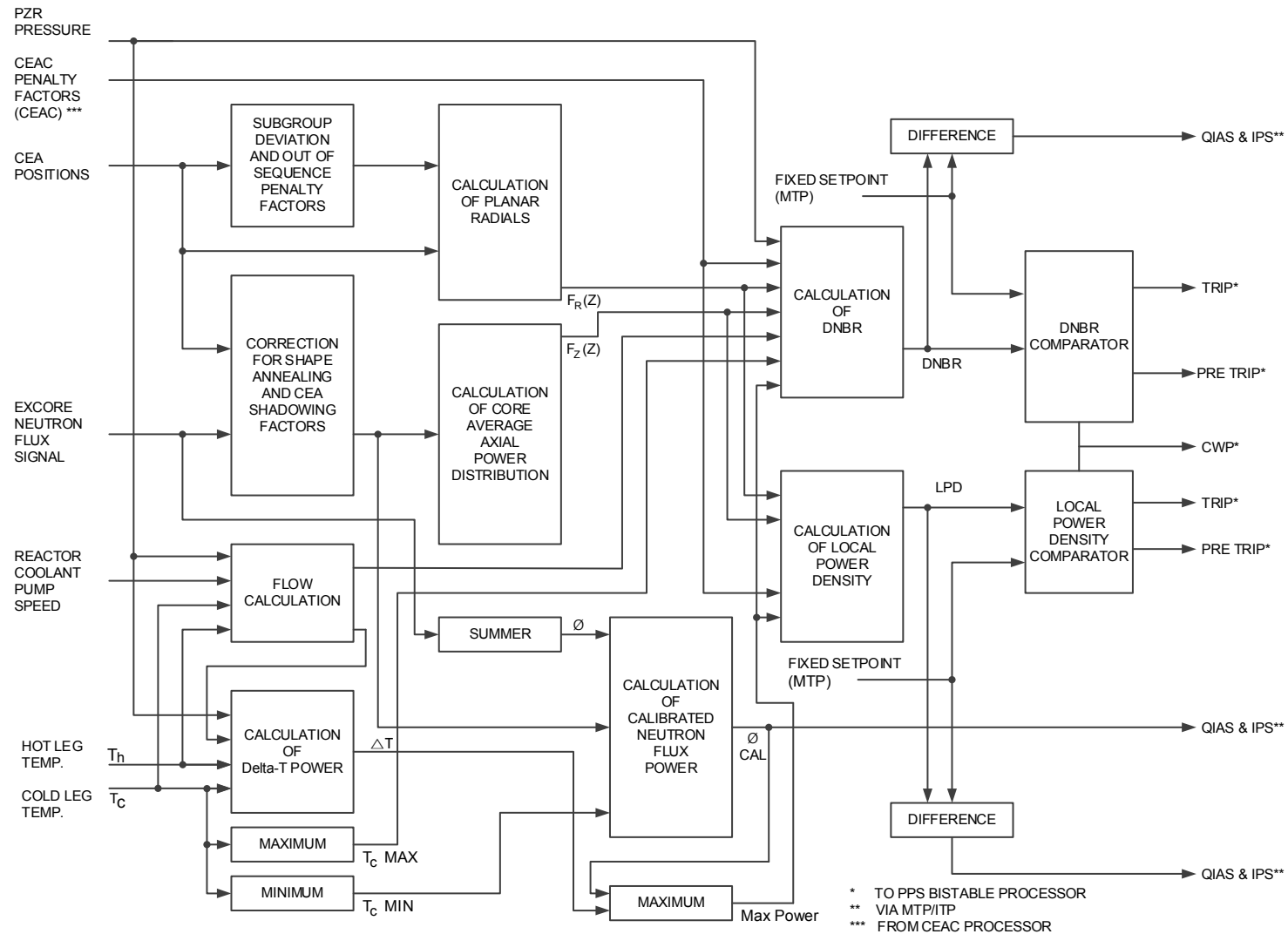


Figure 7.2-7 Core Protection Calculator Functional Block Diagram

APR1400 DCD TIER 2

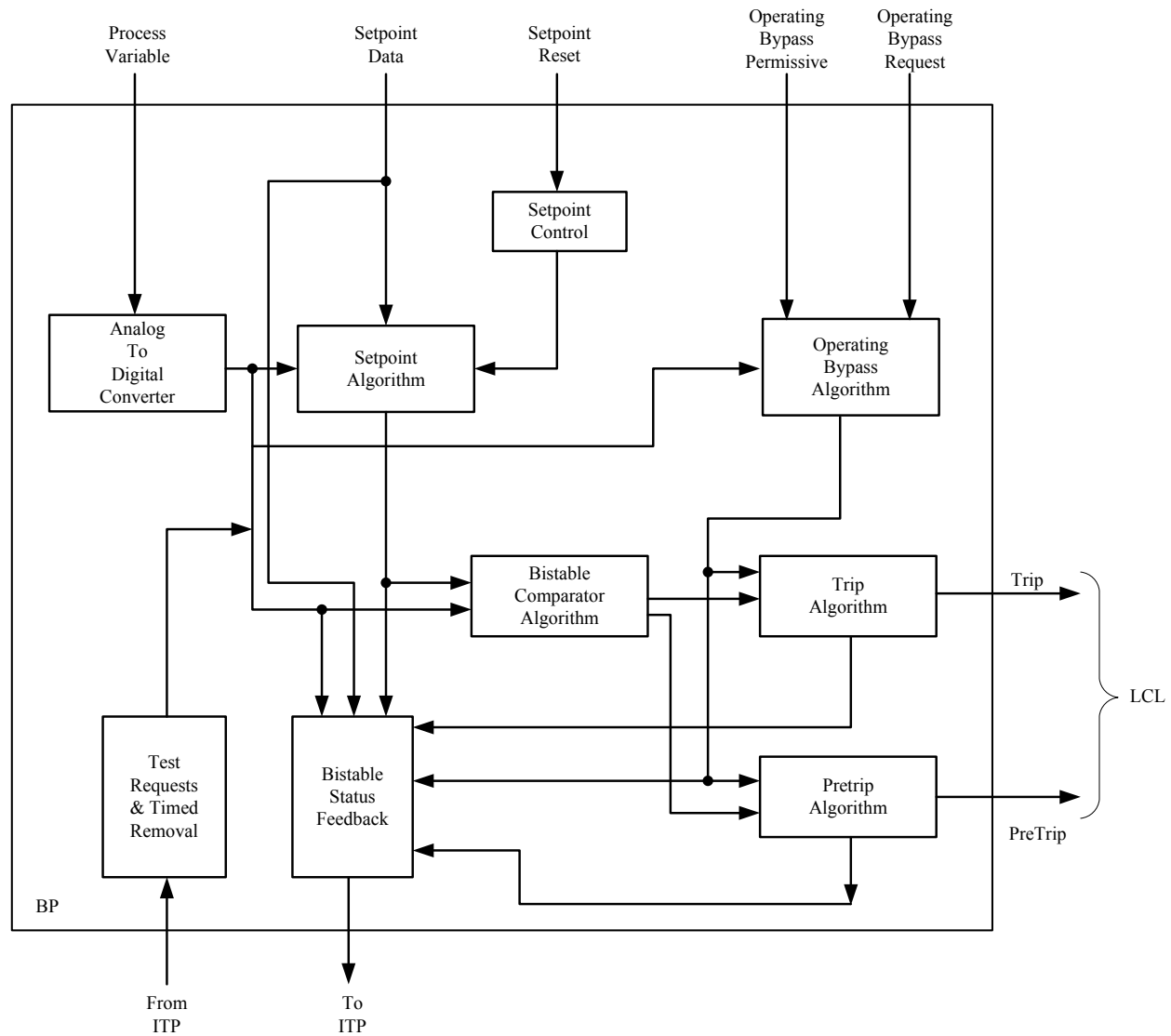
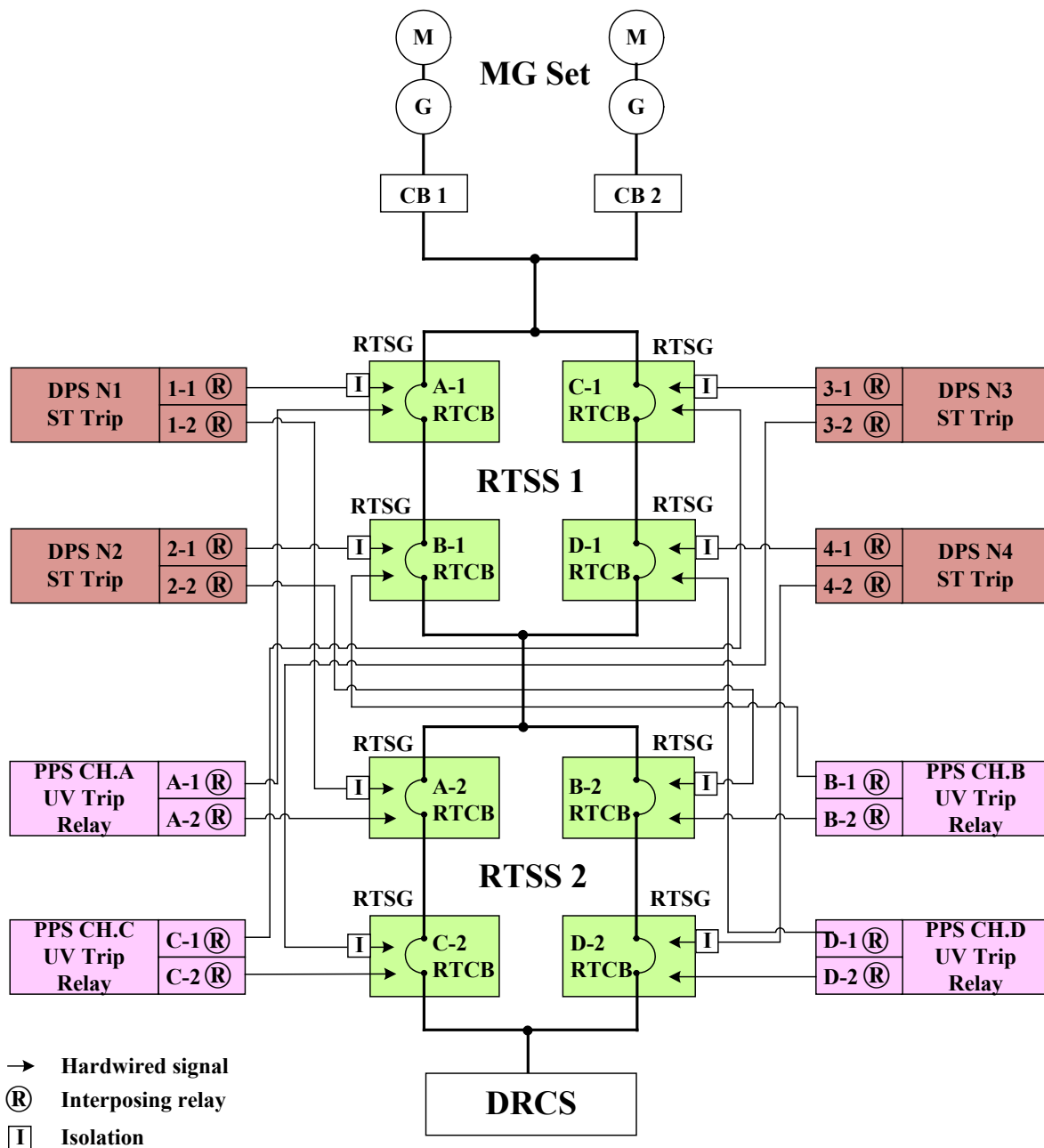


Figure 7.2-8 PPS Bistable Trip Logic Functional Block Diagram

APR1400 DCD TIER 2



CB : Circuit Breaker
DPS : Diverse Protection System
DRCS : Digital Rod Control System
UV : Under Voltage
ST : Shunt Trip

RTCB : Reactor Trip Circuit Breaker
RTSG : Reactor Trip Switchgear
RTSS : Reactor Trip Switchgear System

Figure 7.2-9 Reactor Trip Switchgear System Interface Diagram

APR1400 DCD TIER 2

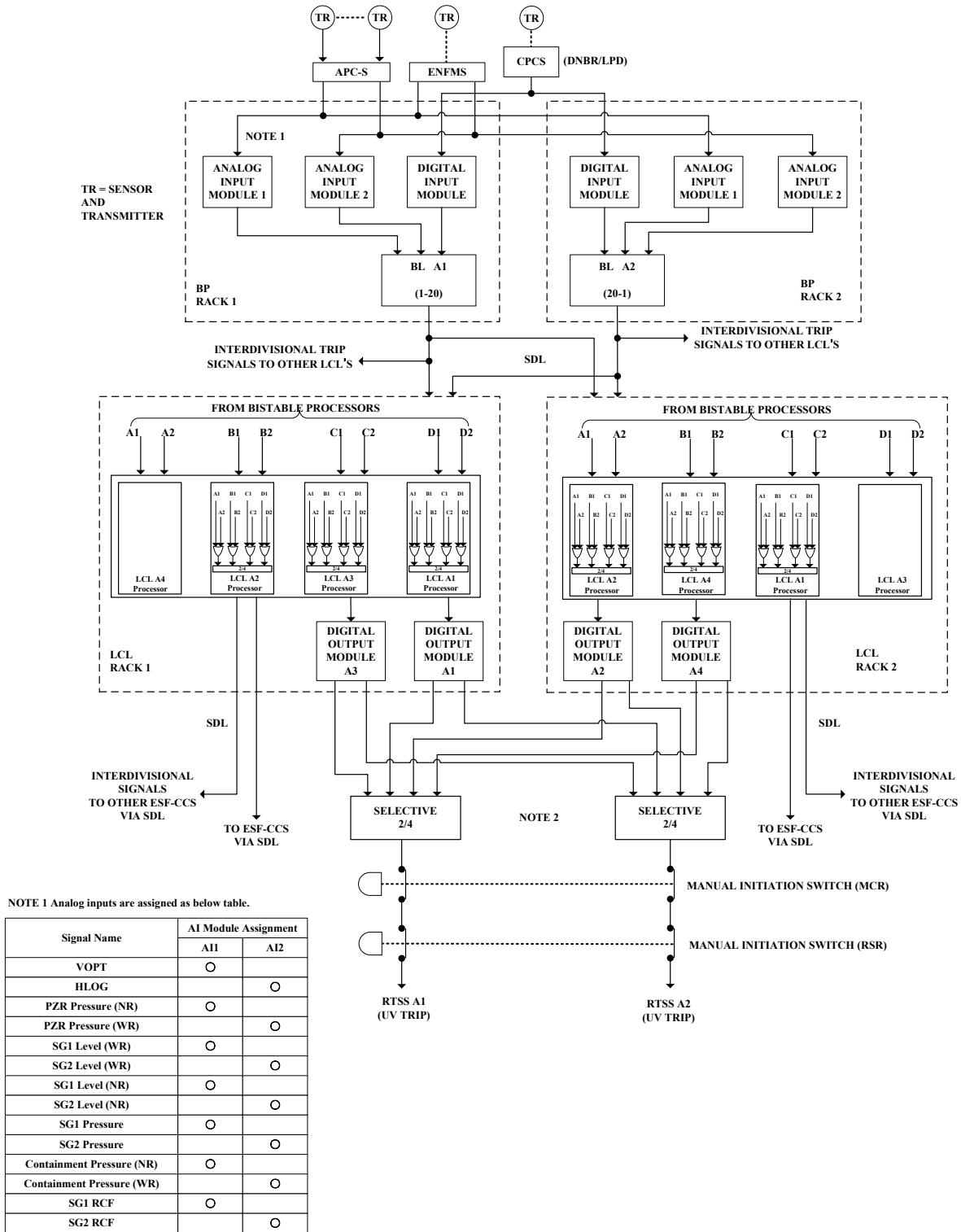
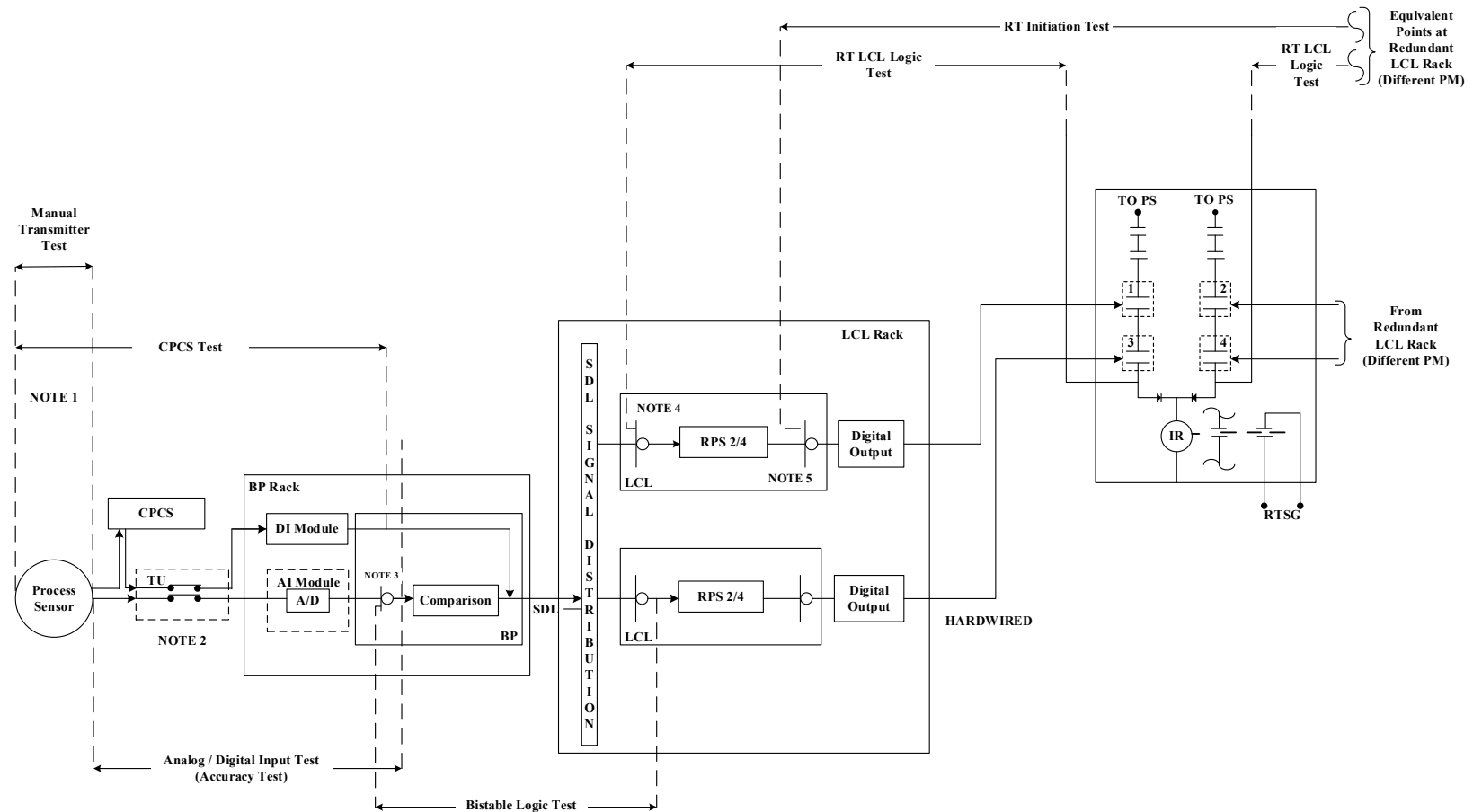


Figure 7.2-10 PPS Channel A Trip Path Diagram

APR1400 DCD TIER 2



NOTES:

1. EACH DASHED LINE INDICATES EITHER THE STARTING OR ENDING POINT OF TESTING.
2. A TERMINATION UNIT (TU) IS A DEVICE WHERE AN ACTUAL PROCESS SIGNAL OR A SIMULATED TEST INPUT SIGNAL, ANALOG OR DIGITAL, MAY BE SELECTED. AN ACCURACY TEST CAN BE PERFORMED BY SELECTING A SIMULATED ANALOG SIGNAL AS INPUT TO THE TU FOR PROCESSING BY THE BISTABLE PROCESSOR.
3. THE LOGICAL "OR" SYMBOL MEANS THAT THE DOWNSTREAM LOGIC PROCESSES EITHER THE ACTUAL PROCESS INPUT SIGNAL OR THE SIMULATED TEST INPUT SIGNAL.

Figure 7.2-11 RPS Testing Overlap

APR1400 DCD TIER 2

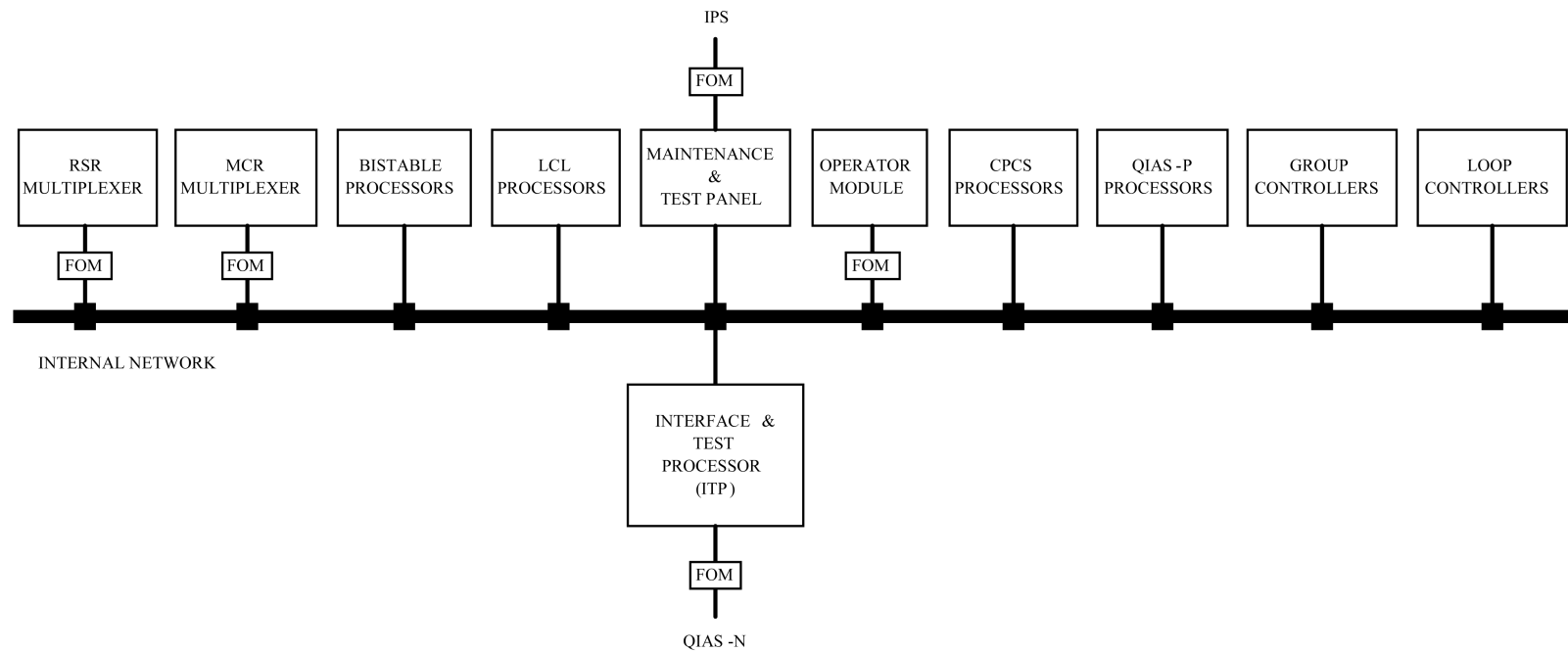


Figure 7.2-12 Interface and Test Processor Block Diagram

APR1400 DCD TIER 2

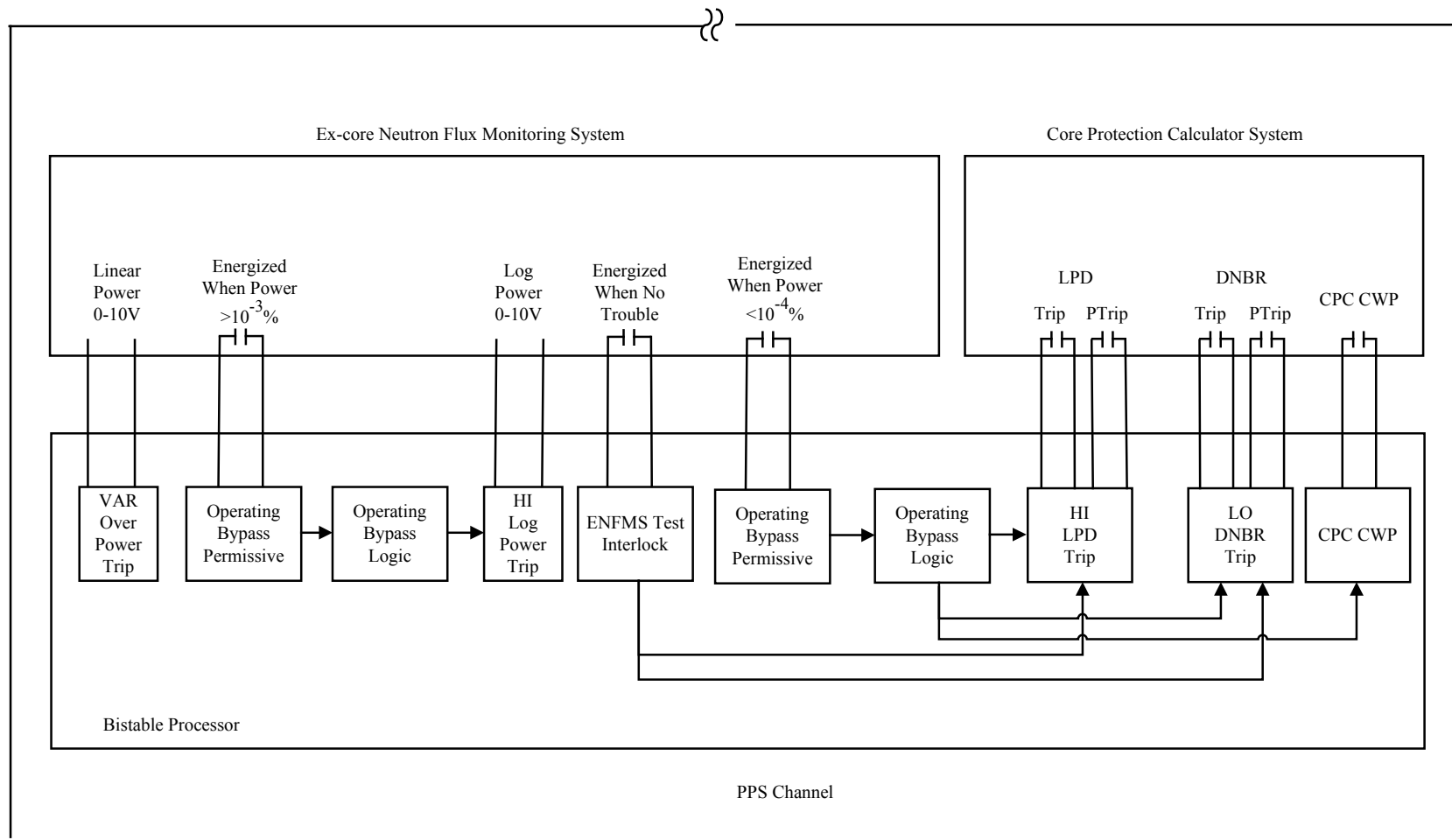


Figure 7.2-13 PPS Channel Contact Bistable Interface Diagram

APR1400 DCD TIER 2

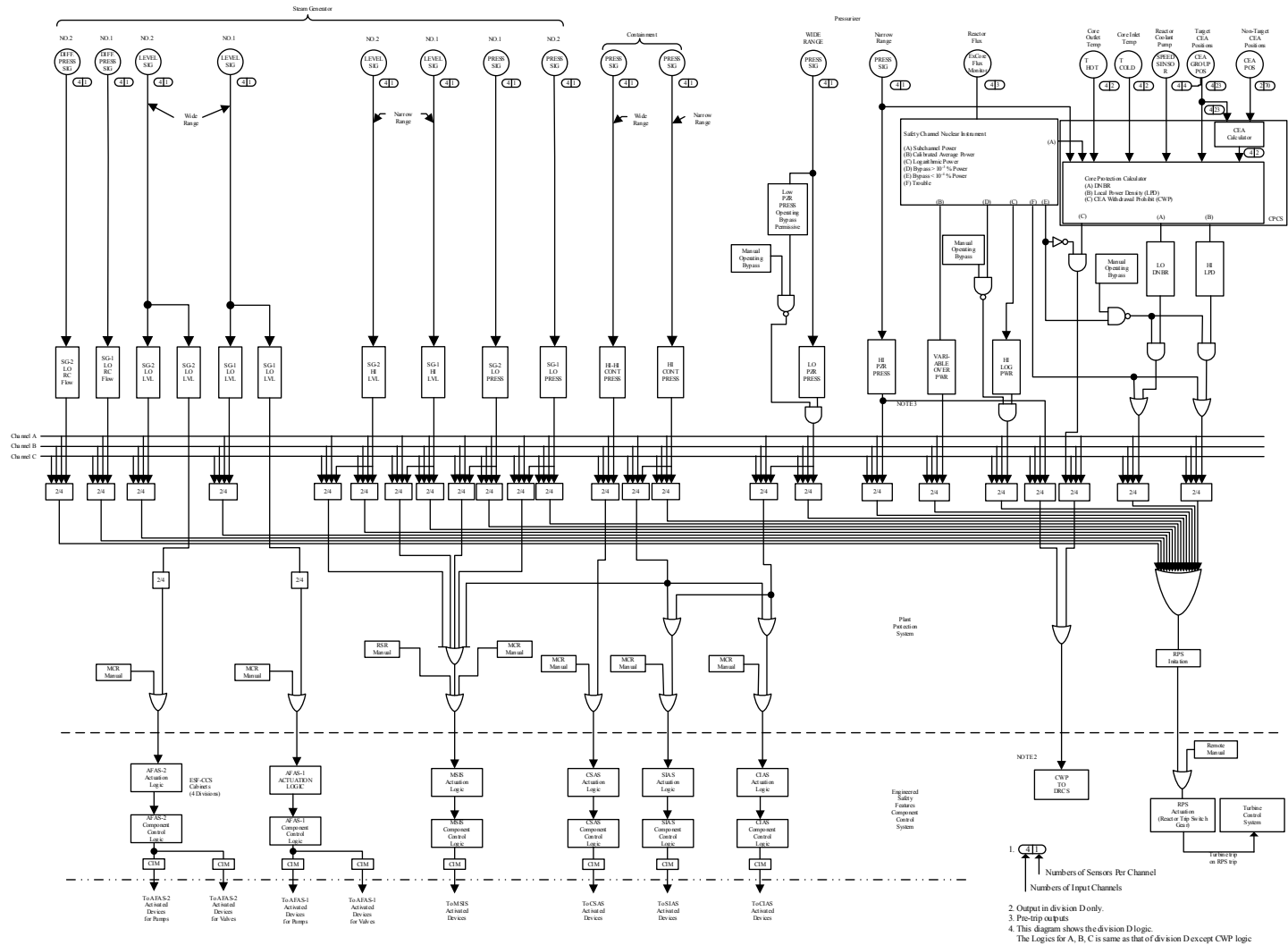
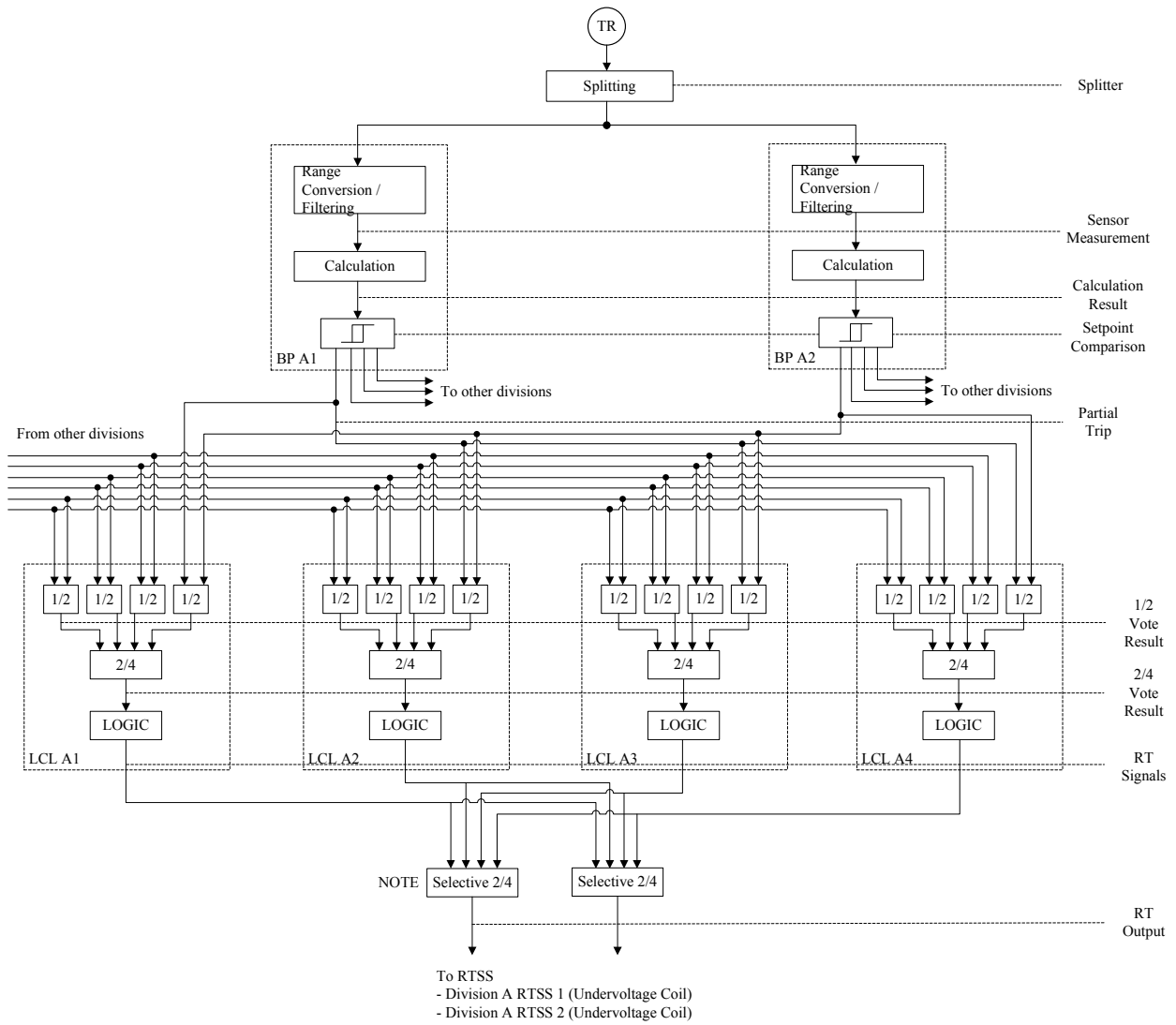


Figure 7.2-14 Plant Protection System Interface Logic Diagram for Division D

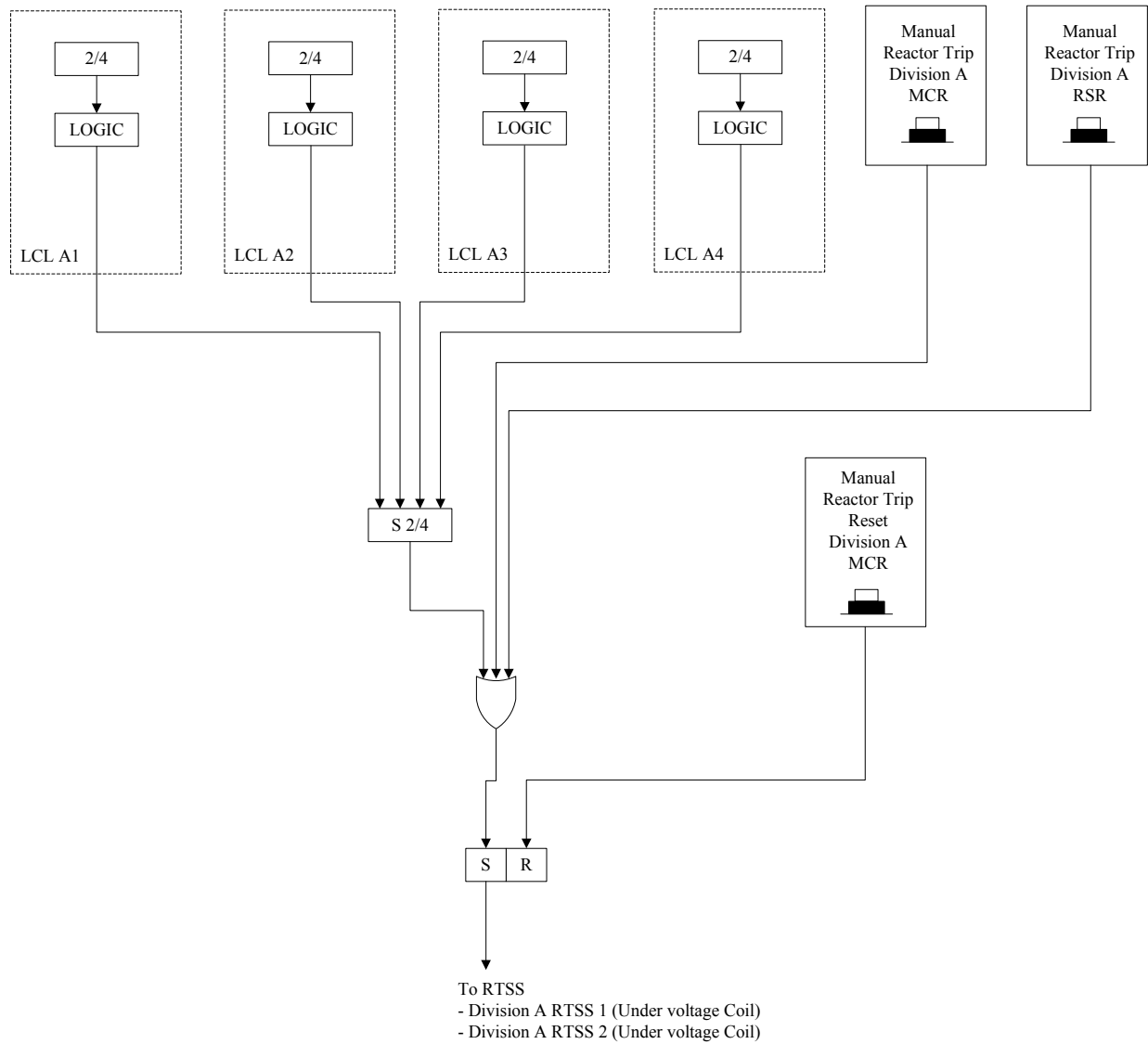
APR1400 DCD TIER 2



NOTE:
SELECTIVE 2/4 = (A1 OR A3) AND (A2 OR A4)

Figure 7.2-15 Reactor Trip Initiation Diagram

APR1400 DCD TIER 2



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

Figure 7.2-16 Manual Reactor Trip Initiation Diagram

APR1400 DCD TIER 2

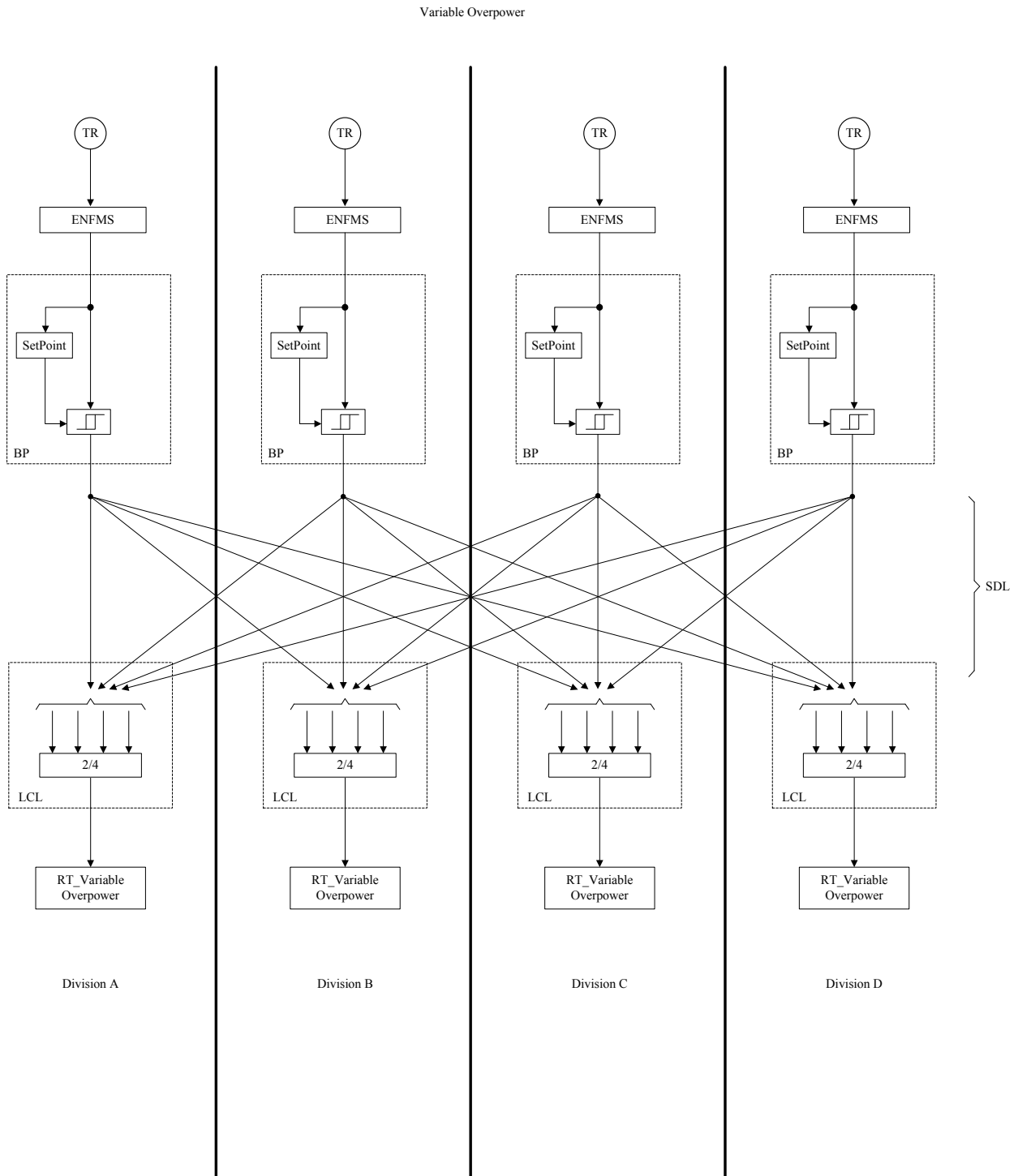


Figure 7.2-17 Functional Logic Diagram for Variable Overpower

APR1400 DCD TIER 2

High Logarithmic Power

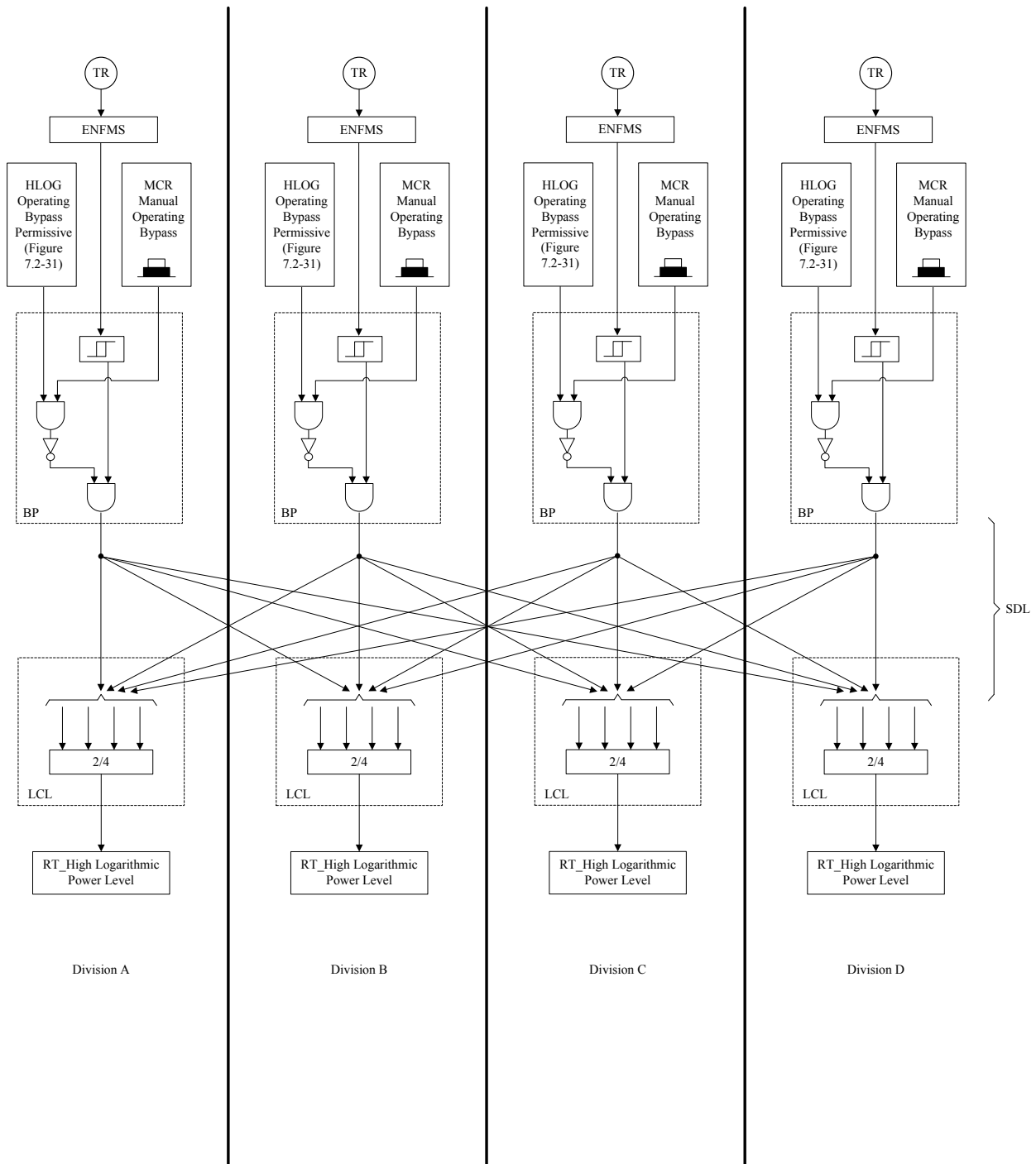


Figure 7.2-18 Functional Logic Diagram for High Logarithmic Power Level

APR1400 DCD TIER 2

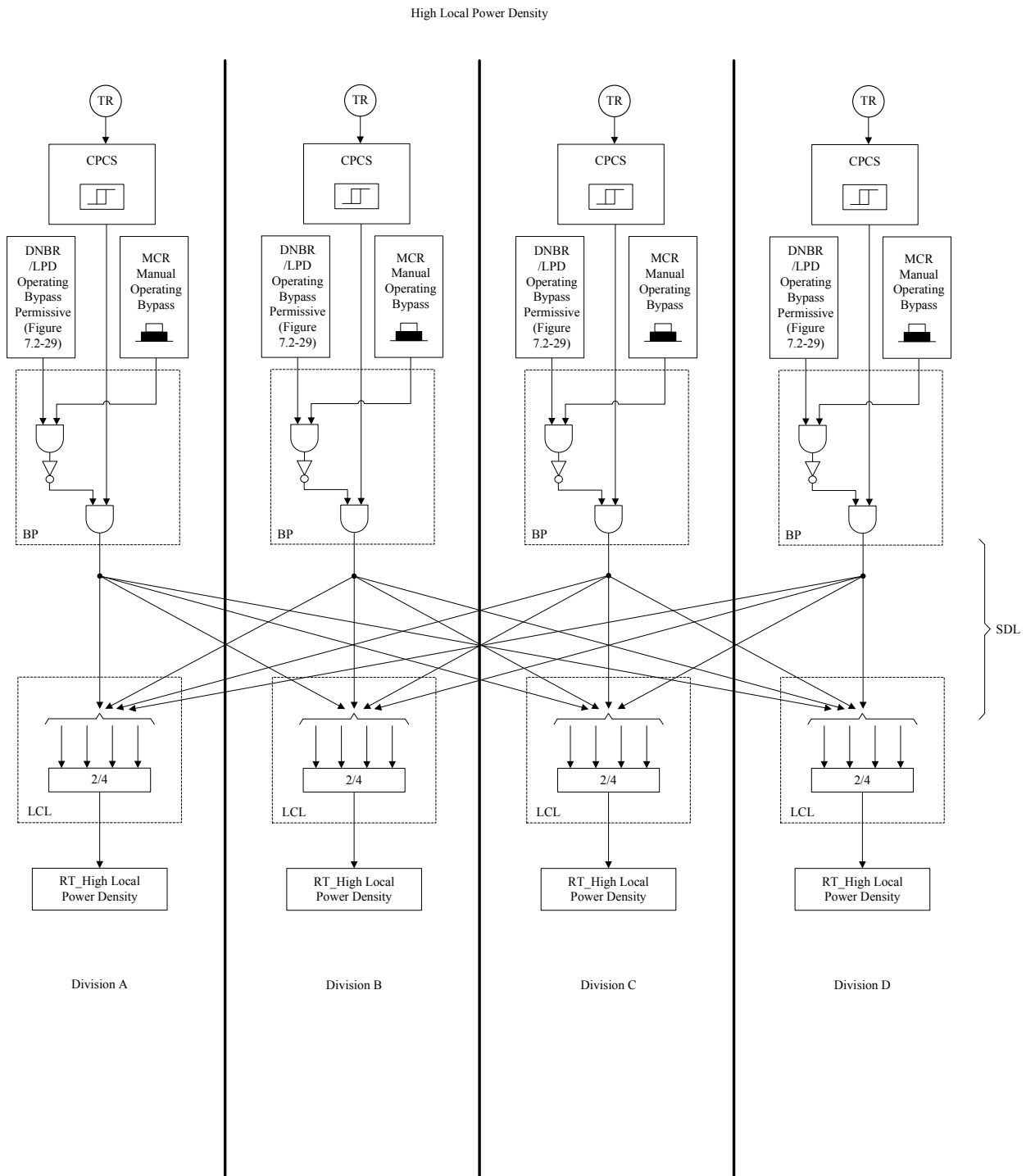


Figure 7.2-19 Functional Logic Diagram for High Local Power Density

APR1400 DCD TIER 2

Low Departure from Nucleate Boiling Ratio

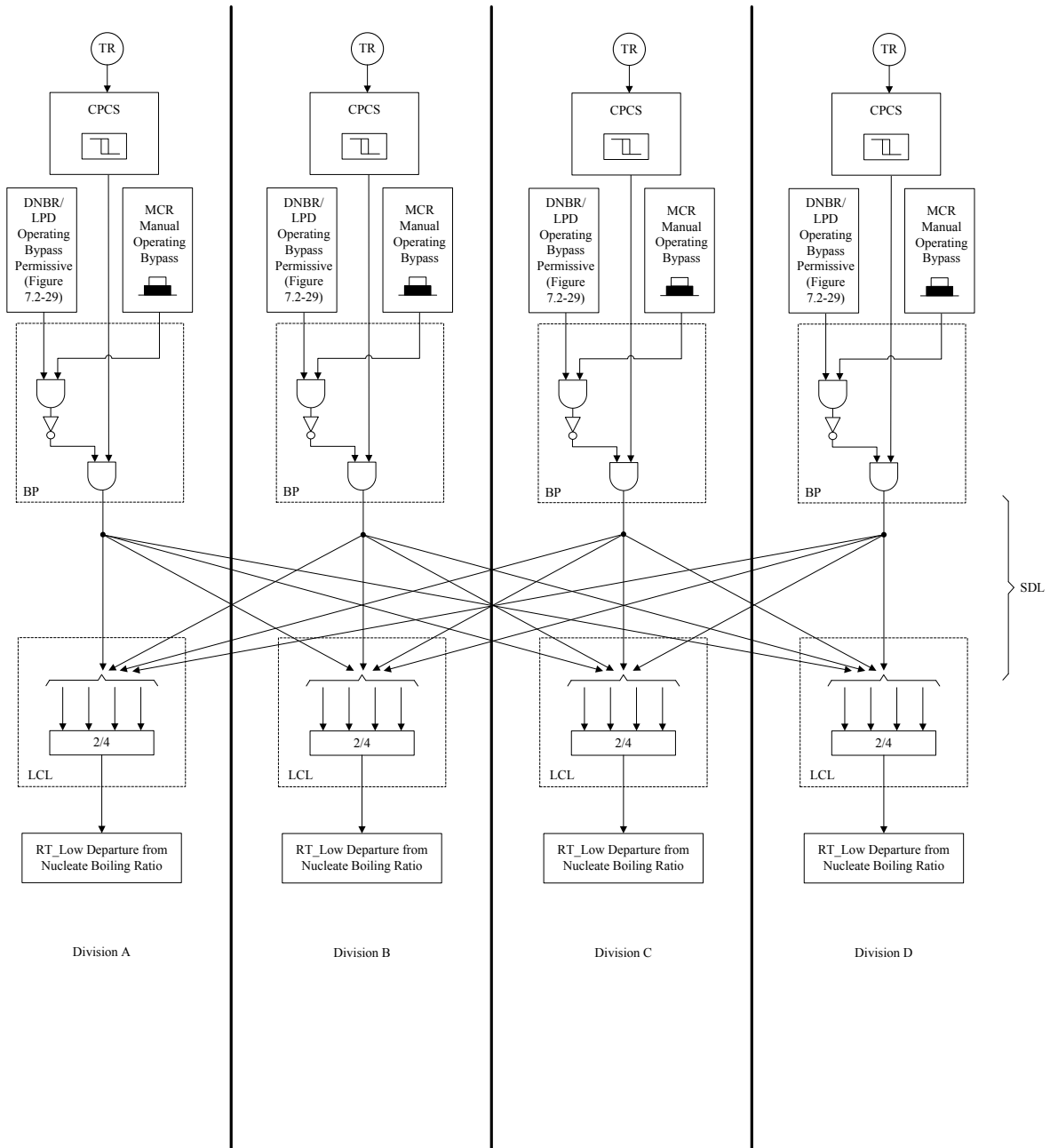


Figure 7.2-20 Functional Logic Diagram for Low Departure from Nucleate Boiling Ratio

APR1400 DCD TIER 2

High Pressurizer Pressure

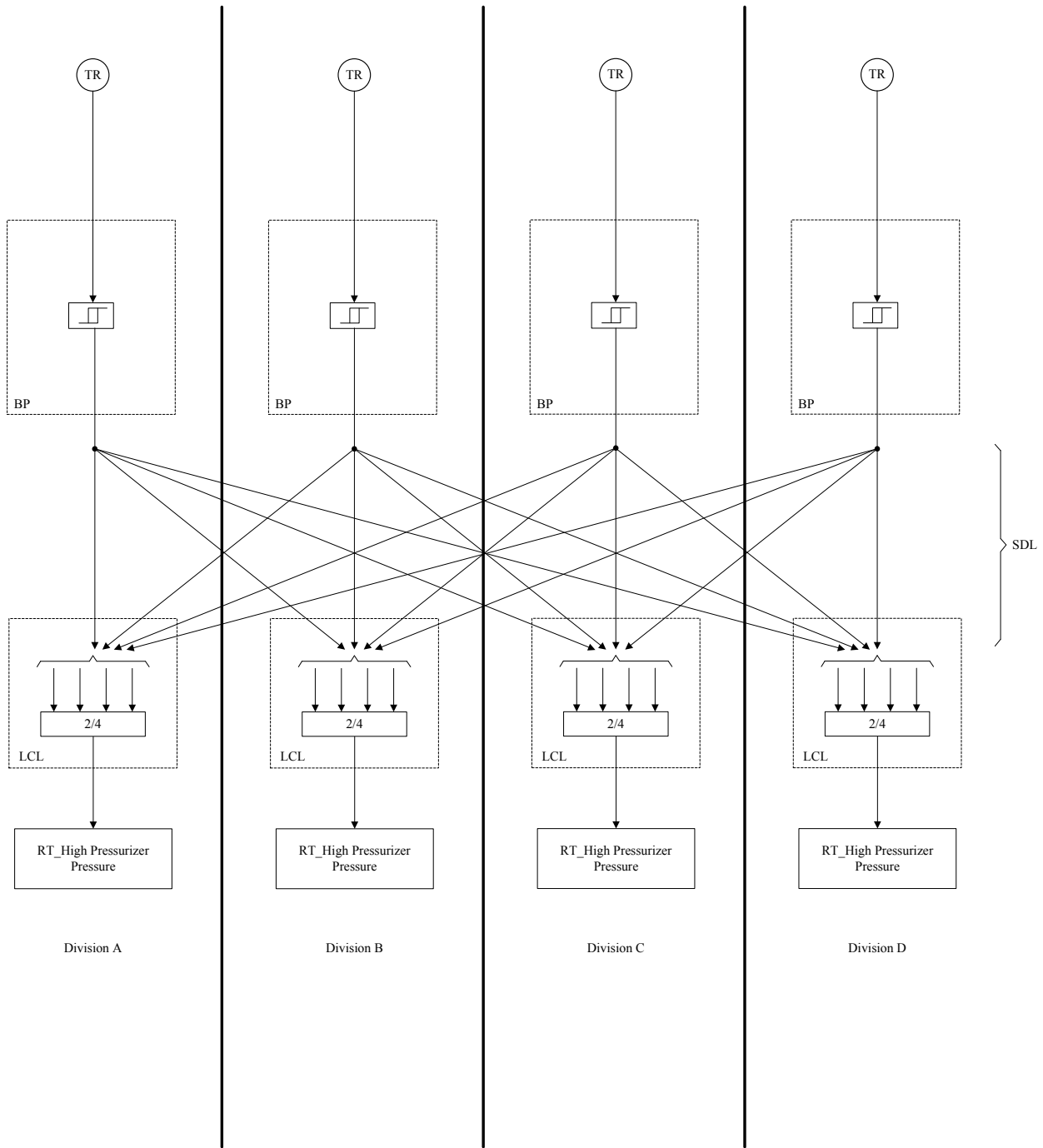


Figure 7.2-21 Functional Logic Diagram for High Pressurizer Pressure

APR1400 DCD TIER 2

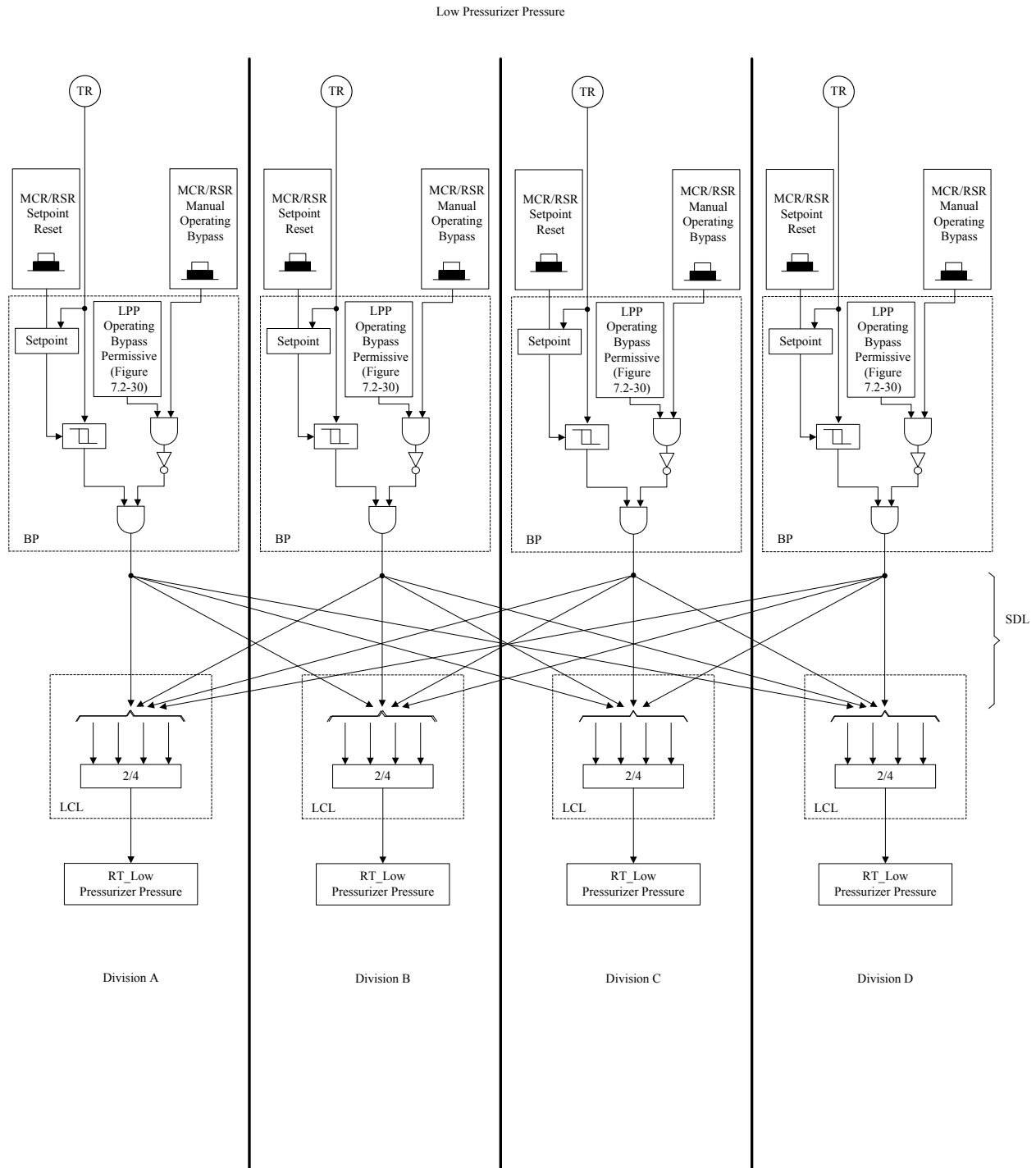
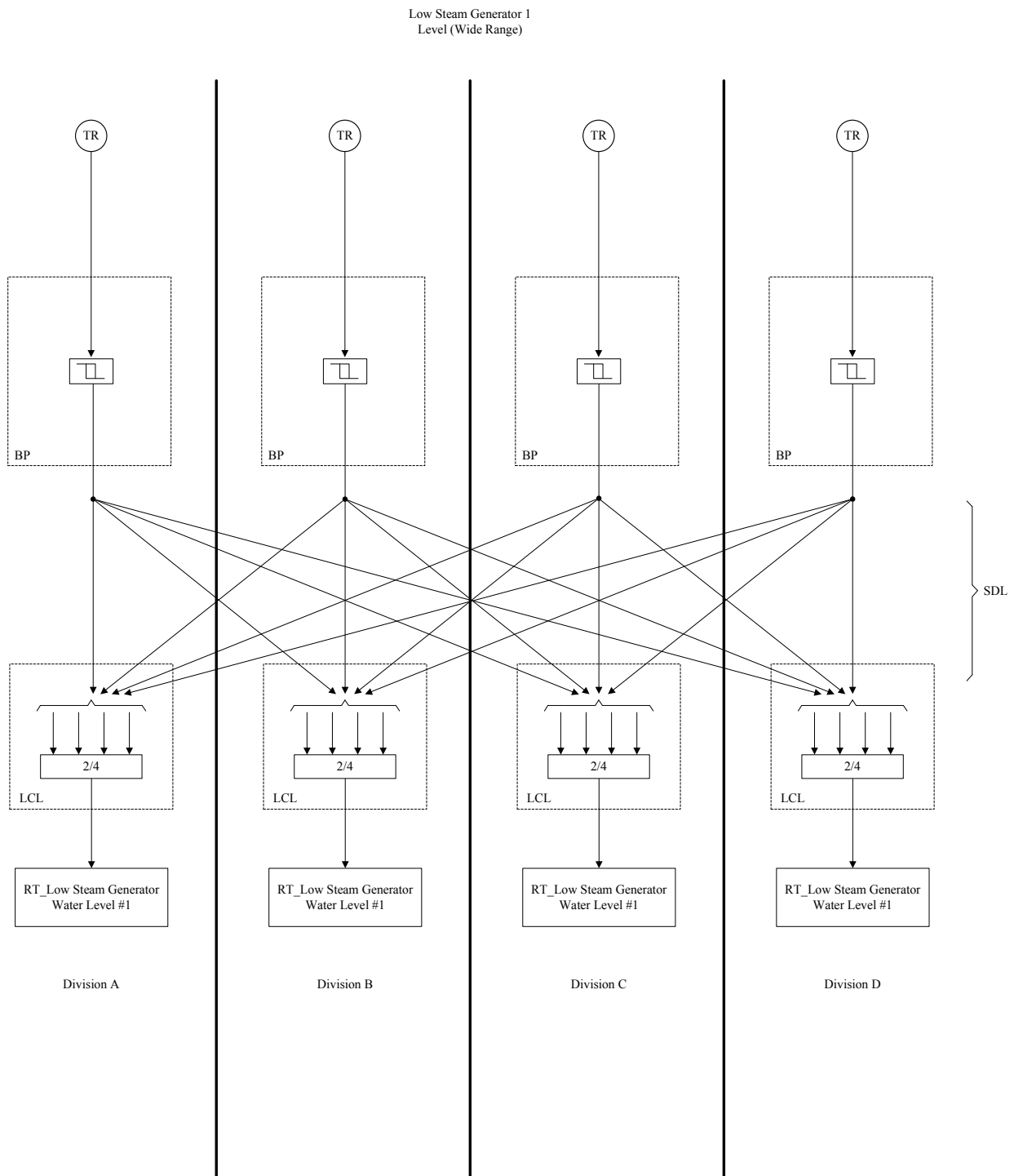


Figure 7.2-22 Functional Logic Diagram for Low Pressurizer Pressure

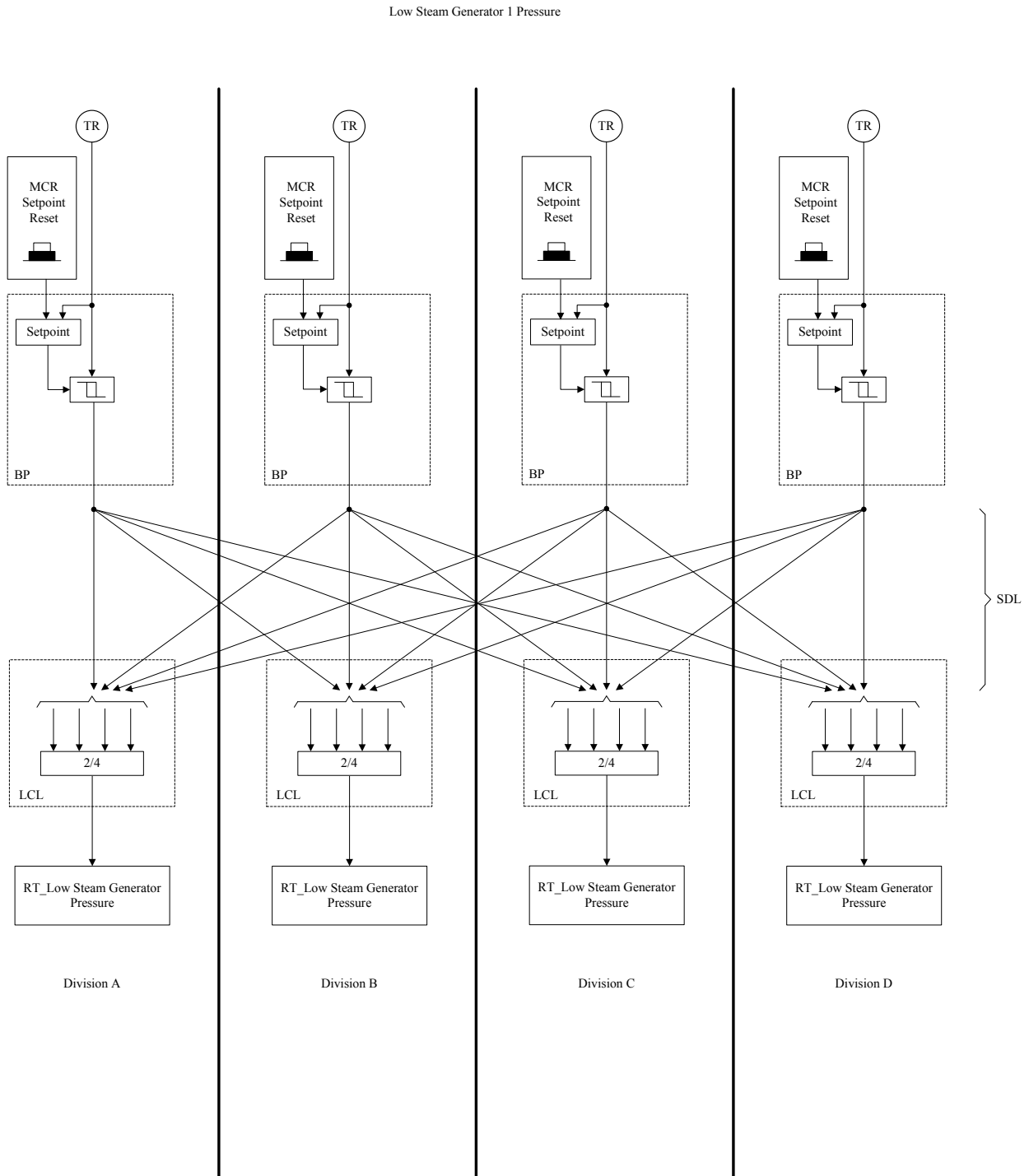
APR1400 DCD TIER 2



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



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

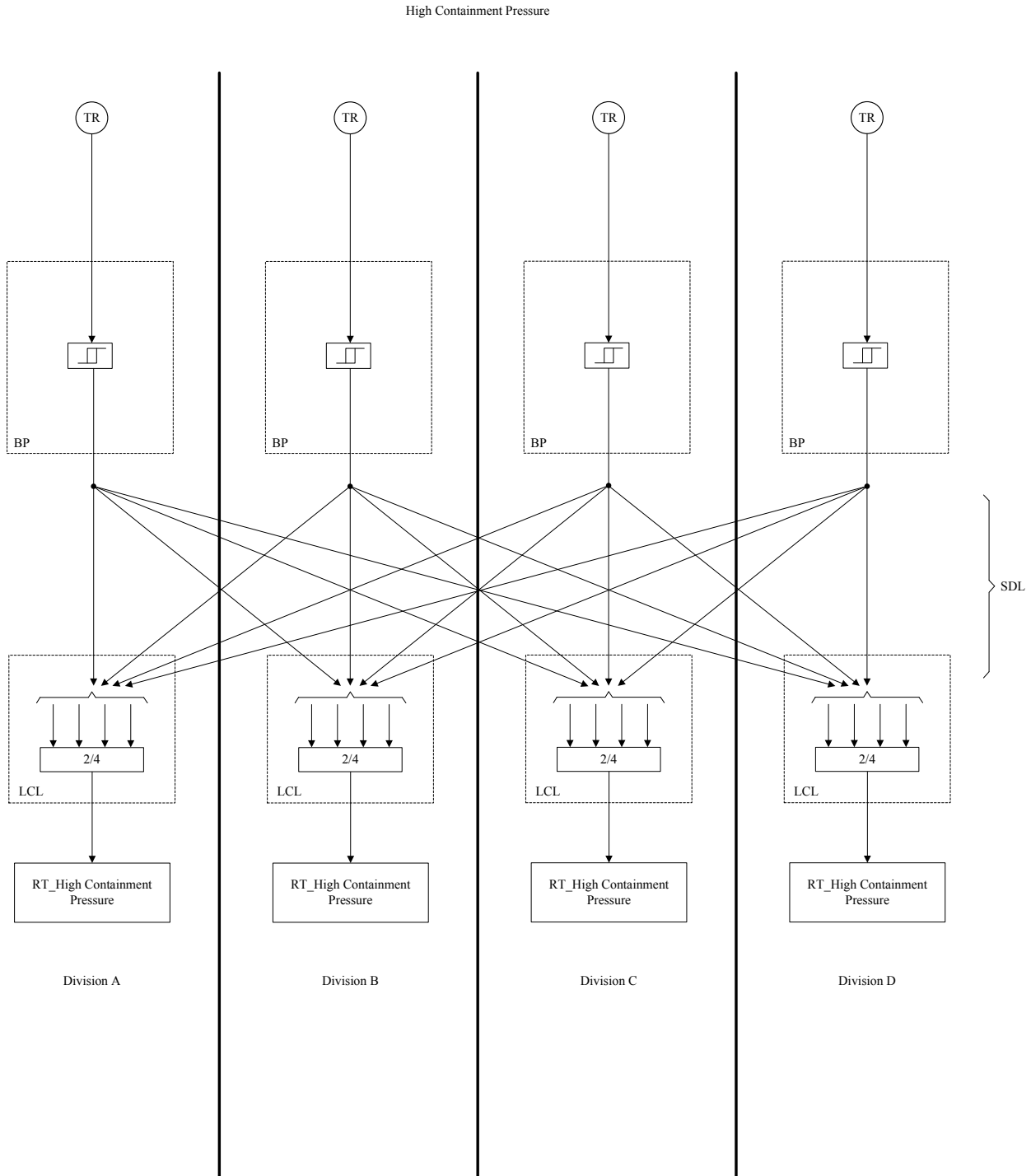
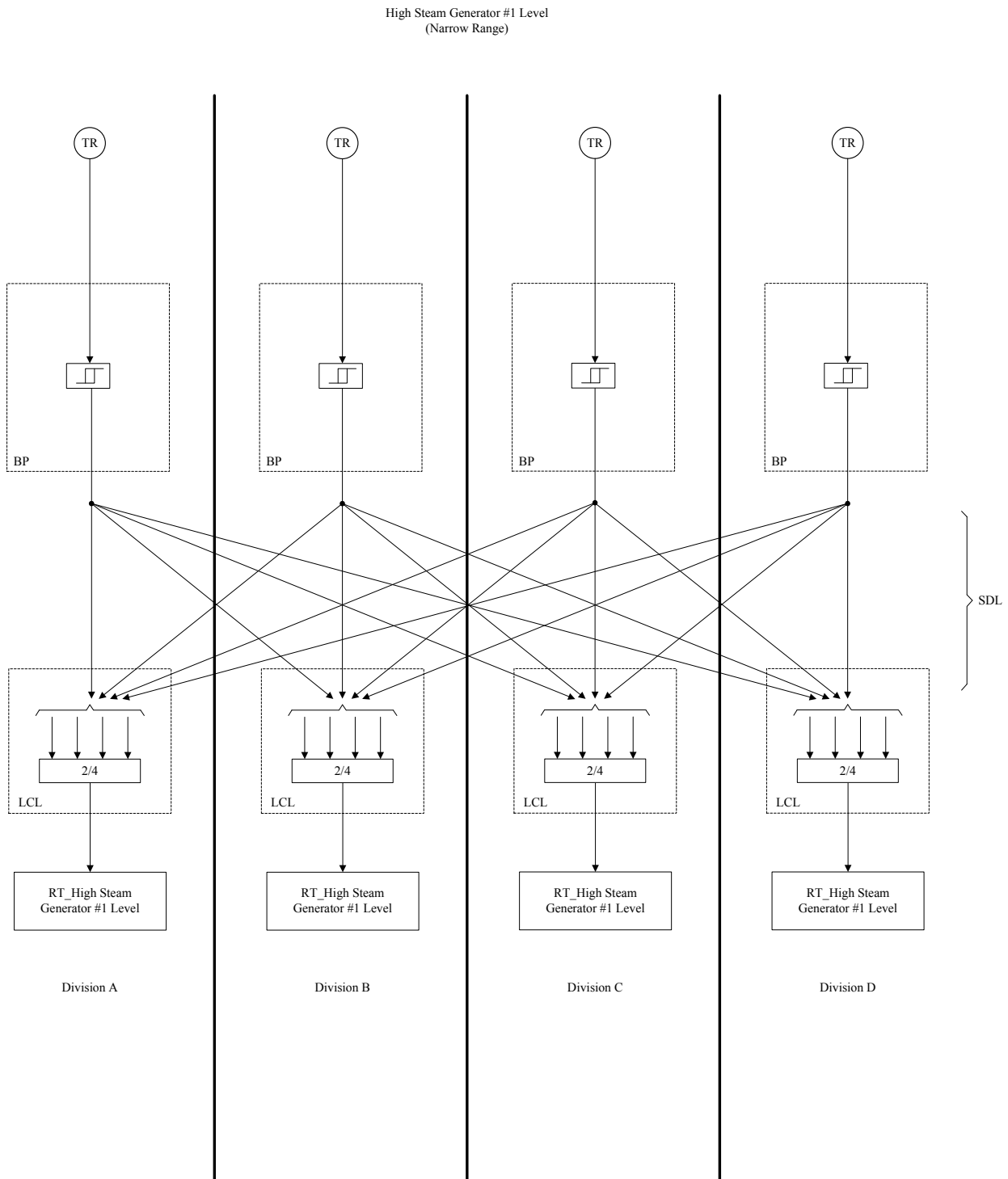


Figure 7.2-25 Functional Logic Diagram for High Containment Pressure

APR1400 DCD TIER 2

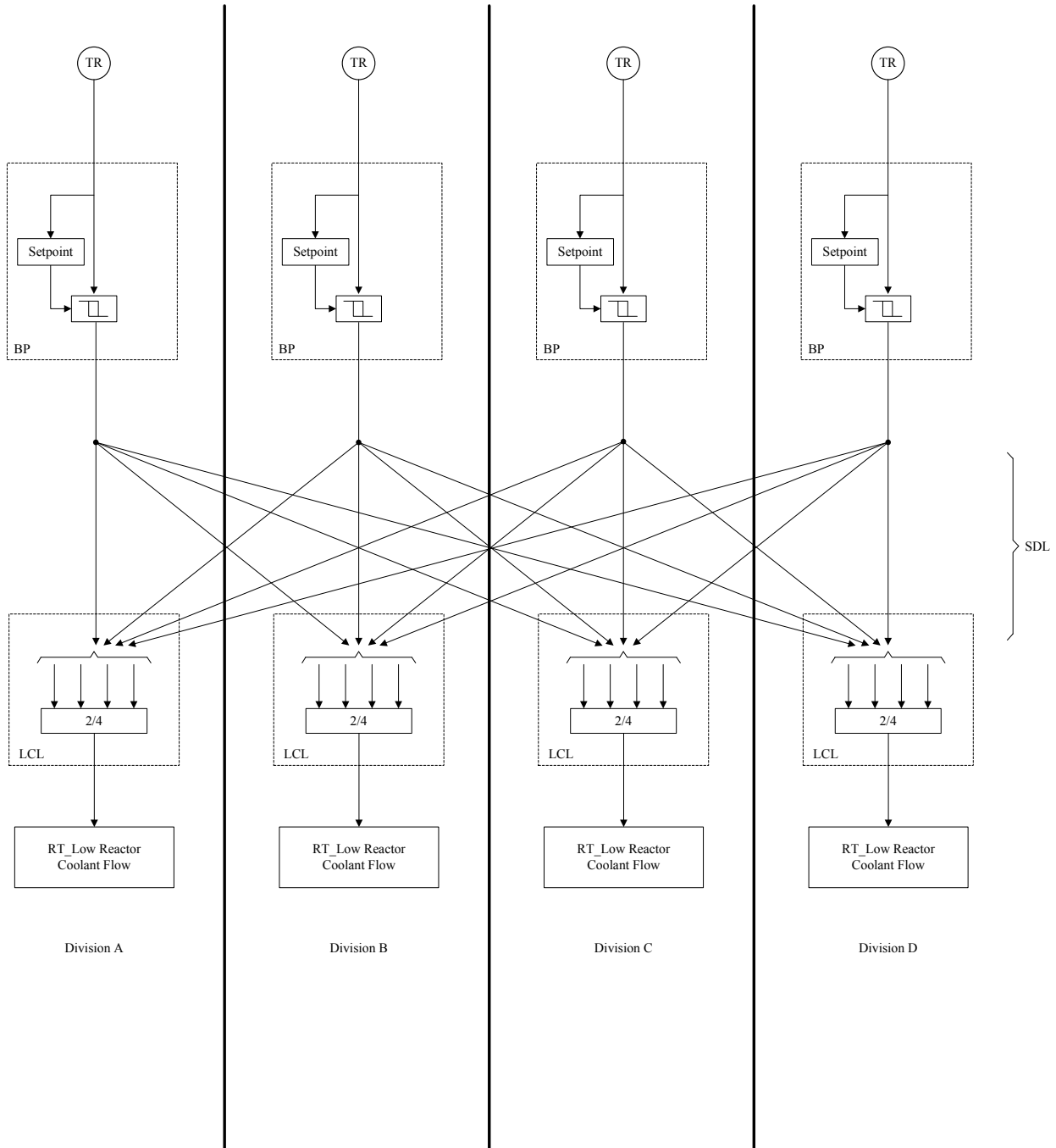


Note : High Steam Generator #2 Level Logic is same as that of High Steam Generator #1

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

APR1400 DCD TIER 2

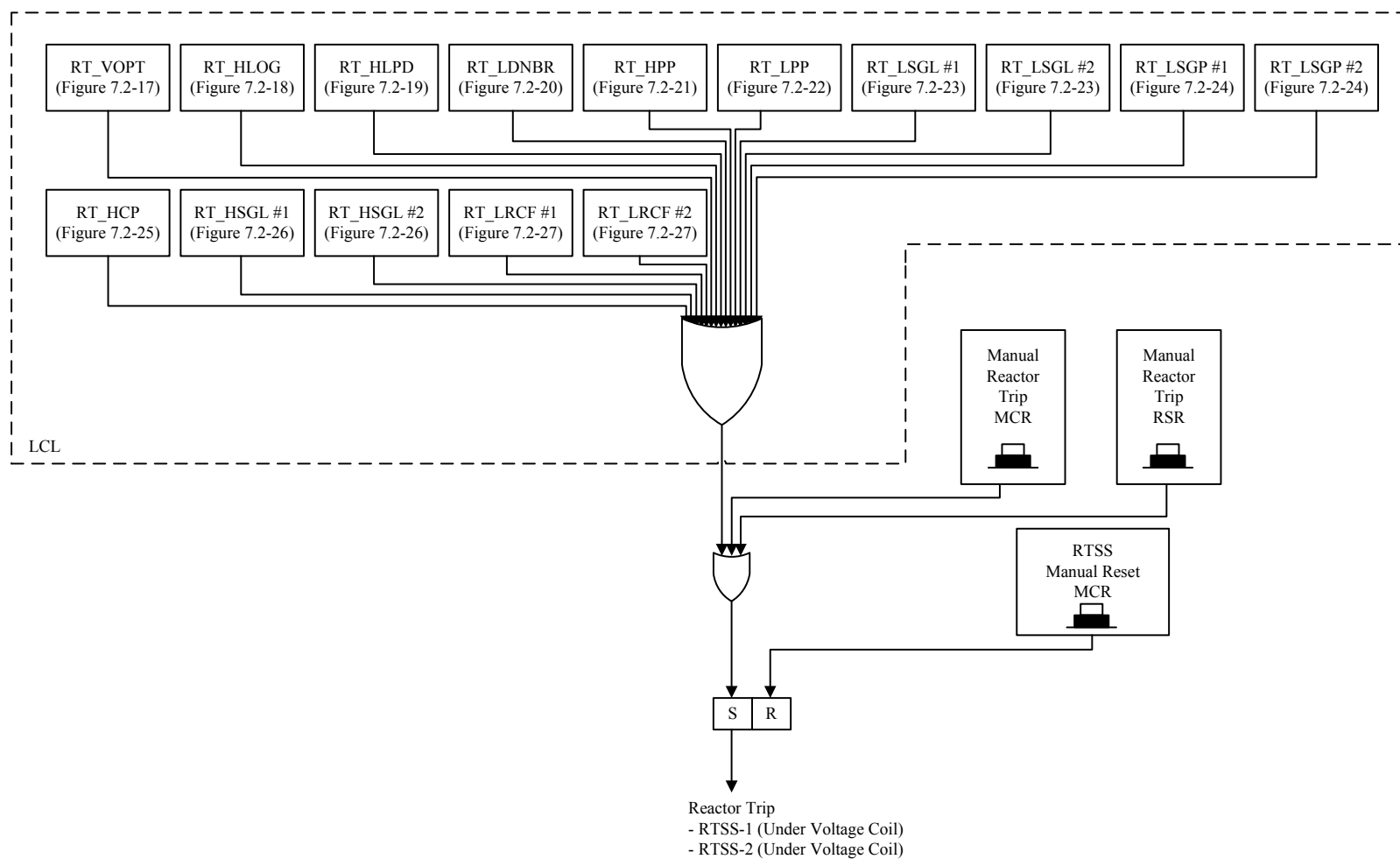
Low Reactor Coolant Flow #1



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



Note: The manual reactor trip switches in the RSR are provided only for divisions A and B

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

APR1400 DCD TIER 2

Ex-core Neutron Flux Power

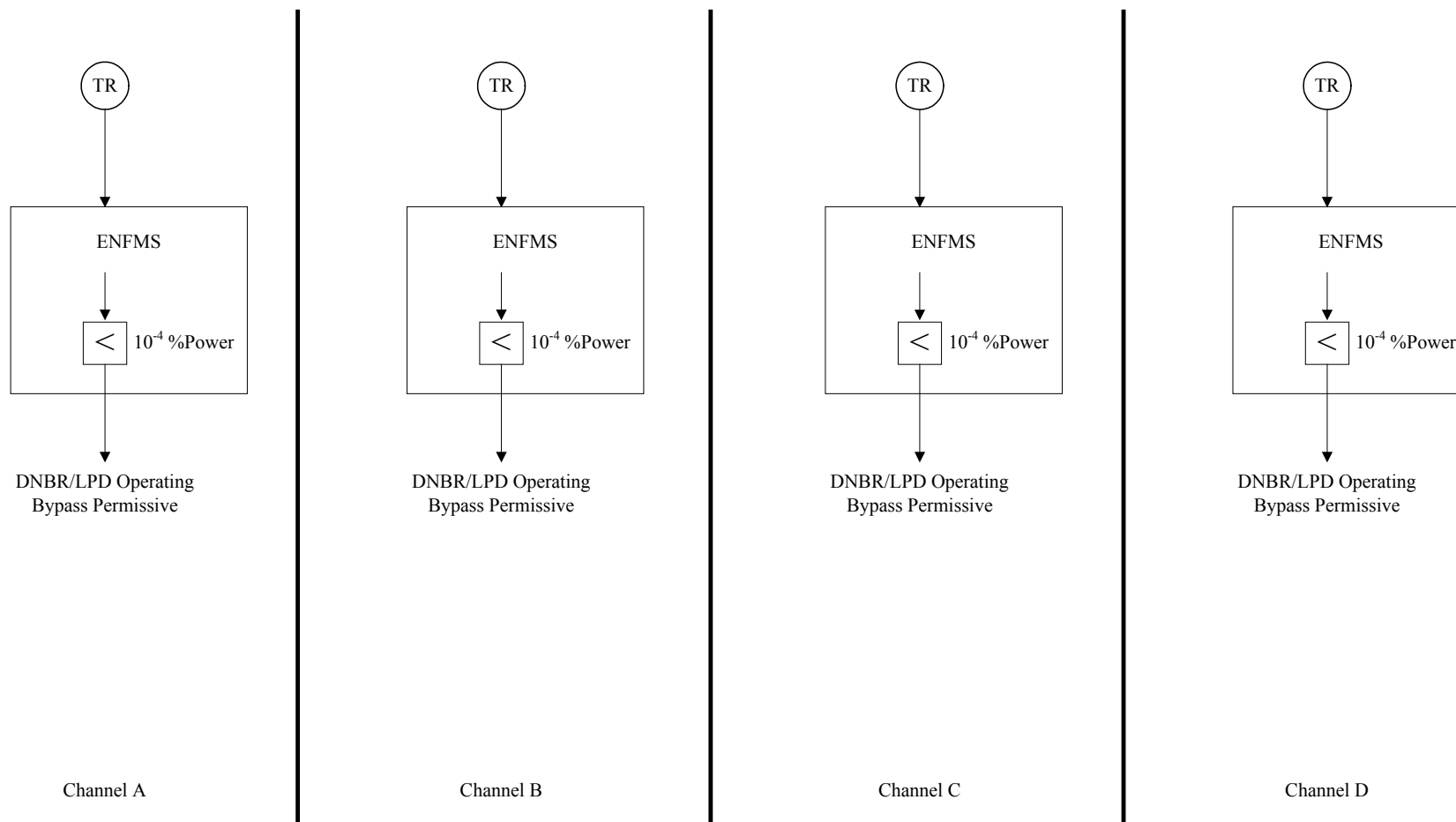


Figure 7.2-29 Functional Logic Diagram for DNBR/LPD Operating Bypass Permissive

APR1400 DCD TIER 2

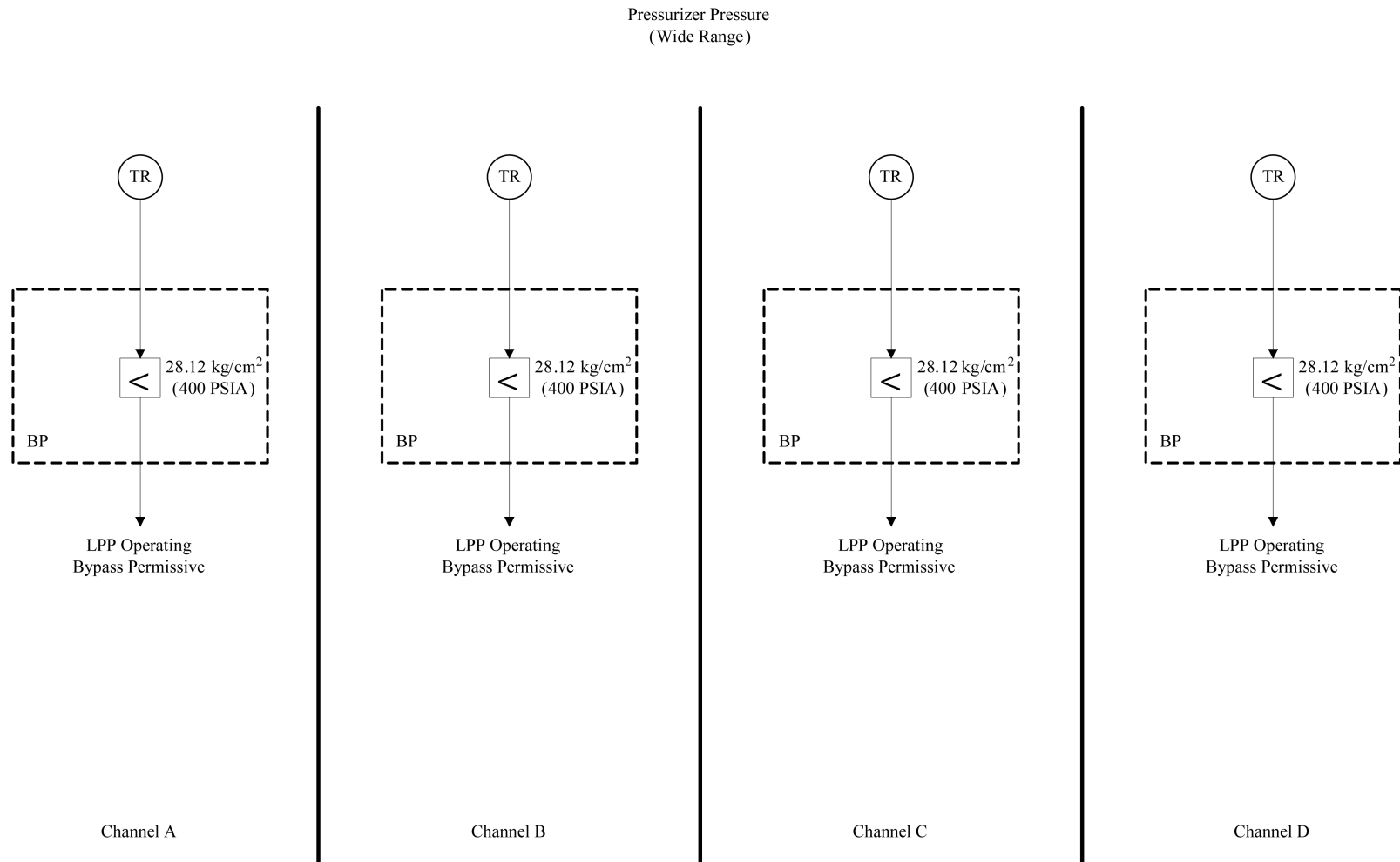


Figure 7.2-30 Functional Logic Diagram for Low Pressurizer Pressure Operating Bypass Permissive

APR1400 DCD TIER 2

Ex-core Neutron Flux Power

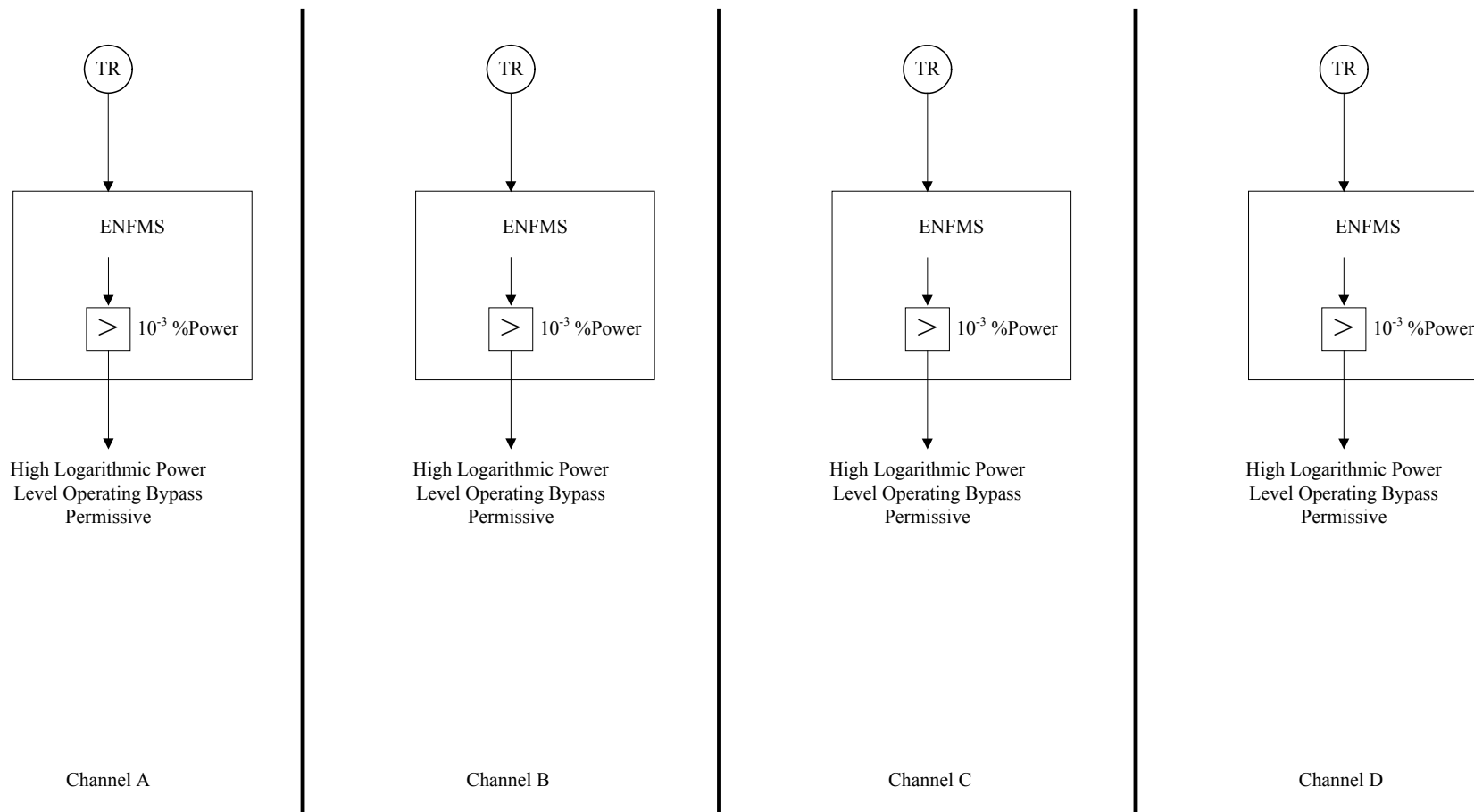


Figure 7.2-31 Functional Logic Diagram for High Logarithmic Power Level Operating Bypass Permissive

APR1400 DCD TIER 2

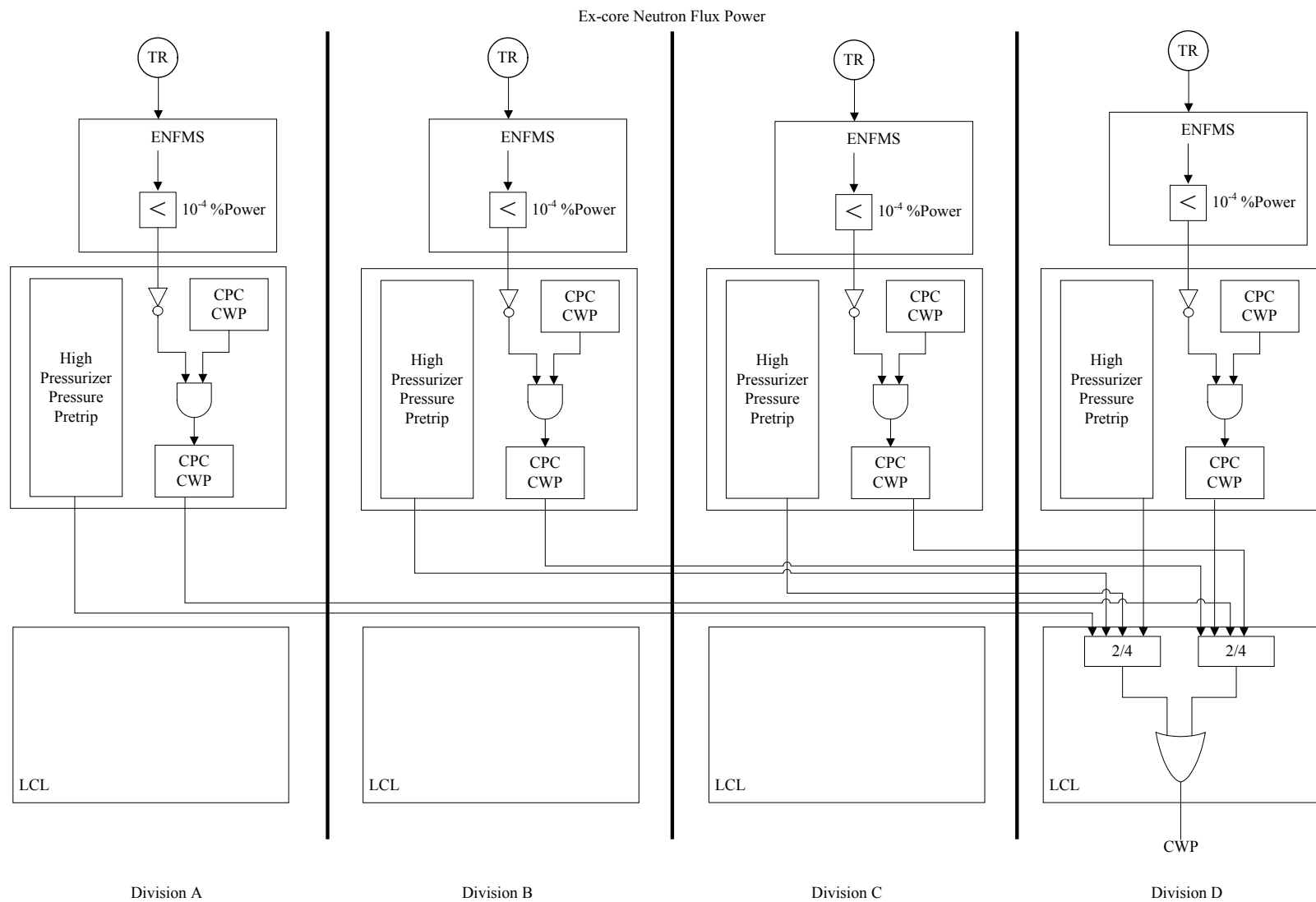


Figure 7.2-32 Functional Logic Diagram for CWP

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), four divisions of the engineered safety features actuation system (ESFAS) portion of the plant protection system (PPS), two divisions of the ESFAS portion of the radiation monitoring system (RMS), and four divisions of 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 (LCL), ESFAS initiation, and testing function.

The ESF-CCS receives ESFAS initiation signals from the PPS and RMS, electrical panel, or from the operators. The ESF-CCS generates ESF actuation signals to actuate the ESF system equipment. The ESF-CCS also generates emergency diesel generator (EDG) loading sequencer signals following loss of offsite power. The control circuitry for the components provides the proper sequencing and operation of ESF systems.

The ESF-CCS provides discrete and continuous control of safety systems as well as automatic or manual actuation of ESF systems. The 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. For modulating control in the ESF-CCS, the sensors and actuators for modulating control are directly interfaced to the analog input module and the analog output module in the ESF-CCS loop controller (LC). Any non-discrete components which require modulation are controlled via the analog output module in the ESF-CCS LC. The component interface module (CIM) is bypassed. The ESF actuation and component control logics are located in the ESF-CCS cabinets.

Upon receipt of ESFAS initiation signals, the ESF-CCS generates ESF actuation signals.

The simplified functional diagram and the block diagram of the ESF-CCS are shown in Figures 7.3-1 and 7.3-2, respectively.

APR1400 DCD TIER 2

a. ESF-CCS configuration

The ESF-CCS consists of four divisions 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 ESF actuation signals to the LC and supports the component control. The ESF functions are assigned to GCs within each ESF-CCS division. 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 information processing system (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 ESF actuation, ESF-CCS status, and ESFAS reset.

The ESF-CCS is designed based on a common 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 ESF actuation, component control logic, test logic, and EDG loading sequencer logic.

Each ESF-CCS GC performs selective 2-out-of-4 coincidence logic using ESFAS initiation signals from each division of the PPS.

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

The ESF-CCS provides interface and signal fan out capability for ESF actuation signals to the switchgear and motor control center (MCC) via the component control logic within the ESF-CCS. The logic produces digital output (DO) signals

APR1400 DCD TIER 2

to control the component through the component interface module (CIM), which performs signal prioritization. The CIM transmits signals to the final actuated device (e.g., switchgear, MCC, solenoids).

The ESF-CCS receives signals from the master transfer switches to disable all main control room (MCR) controls and enable remote shutdown room (RSR) controls.

7.3.1.1 Engineered Safety Features Actuation System Measurement Channels

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

The ESFAS measurement channels receive signals from the PPS and the safety-related divisionalized cabinet (SRDC) of the RMS. Detailed description of the RMS instrumentation is described in Section 11.5 and Subsection 12.3.4.

Undervoltage signals received from the electrical panel detect a loss of voltage on the Class 1E 4.16 kV buses.

A measurement channel for the PPS is shown in Figure 7.2-2. A measurement channel for the RMS is shown in Figure 7.3-23. The RMS measurement channel consists of a radiation element, a local unit, an SRDC processor, an RMS processor, and a fiber optic transmitter. The radiation element and the local unit are installed in the radiation monitor described in Subsections 11.5 and 12.3.4.1. The radiation element includes a radiation sensor and a signal transmitter. The local unit distributes the radiation signal to the safety-related SRDC processor and non-safety RMS processor. When the radiation signal exceeds the radiation setpoint value, the SRDC processor sends a BOP ESFAS initiation signal to the ESF-CCS GC. The radiation signal is displayed on the IPS and the QIAS-N in the MCR. The radiation signal originating from the safety-related radiation element that is transmitted to the non-safety RMS processor is electrically isolated using a Class 1E qualified isolator, at the local unit.

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

APR1400 DCD TIER 2

7.3.1.2 Engineered Safety Features Actuation System Initiation Logic

The BPs are in the PPS cabinet. The NSSS 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 NSSS ESFAS initiation there are two redundant BPs in each channel. The outputs of the BPs 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 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 the serial data link (SDL).

7.3.1.3 Actuation Logic

The ESFAS consists of 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-1 and AFAS-2)

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)

APR1400 DCD TIER 2

The ESF-CCS serves as an interface between the ESFAS portion of the PPS with the switchgear, solenoid, and MCC.

Each ESF-CCS division consists of redundant GC logic and redundant LC logic. Each ESF-CCS division receives NSSS ESFAS initiation signals from all four divisions of the PPS and performs an automatic initiation of the affected ESF system(s) when coincidence logic conditions are satisfied. The selective 2-out-of-4 coincidence logic is performed in the redundant GCs which independently receives NSSS ESFAS initiation signals from four PPS divisions (Divisions A, B, C, and D) and performs a selective 2-out-of-4 coincidence logic on the initiating signals. Valid ESF-CCS system-level initiation signals are latched and require a manual reset. Two redundant GCs are provided for improved GC availability within each ESF-CCS division.

The selective 2-out-of-4 coincidence logic in the GC processors enhances the fault tolerance to maintain system-level availability and minimize the consequences of single failures. A failure of a processor in the PPS or data communication between the PPS and ESF-CCS is tolerated by the signal quality checking logic and the coincidence logic in the GC.

The loss of (vital ac) electrical power to two PPS divisions causes the inputs from both PPS divisions to go to a failed (i.e., safe) state. The ESF-CCS recognizes the failed input signals as actuated states in the GCs. Accordingly, if the selective 2-out-of-4 coincidence logic in the ESF-CCS GC is met, the ESF-CCS GC generates the ESF actuation signals to the component control logic in the LC.

The redundant GCs provide ESF actuation signals to the redundant LCs in the respective division via SDLs. Each LC receives the ESF actuation signals from the GCs. There is no additional coincidence logic downstream of the GCs. See Figure 7.3-1 for a simplified functional diagram of the ESF-CCS.

All ESF actuation signals can be initiated using manual ESF system-level actuation switches on the safety console. In the ESF 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 7.3-3. Each ESF actuation signal, 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.

APR1400 DCD TIER 2

The BOP ESFAS receives process variable signals from the safety portion of the RMS, manual ESF system-level actuation switches, and manual channel bypass switches. The BOP ESFAS consists of 1-out-of-2 logics taken twice except the FHEVAS, which has one 1-out-of-2 logic.

The safety-related portion of the I&C system for the FHEVAS has the required redundancy to meet the single failure criteria of Clauses 5.1 in IEEE Std. 603. Having two divisions of initiating FHEVAS ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the other safety division will remain in service to perform the required ESFAS initiation.

The safety-related portion of the I&C system is designed as Class 1E, is seismic Category I, and remains functional during and following a safe shutdown earthquake. Controls, interlocks, sensors, and devices of the safety-related I&C system for FHEVAS are also functionally checked, adjusted, and tested to provide reasonable assurance of intended operation and performance as described in Section 9.4.2.4.

ESFAS Function

The ESFAS consists of six NSSS ESFAS signals and three BOP ESFAS signals. Manual ESF system-level actuation switches are provided on the safety console. The manual MSIS actuation switches are also provided on the remote shutdown console in the RSR.

a. SIAS

1) Input

Low pressurizer pressure, high containment pressure, or manual ESF system-level actuation switches located on the safety console in the MCR. The pressure signals are shared with the reactor protection system.

2) Function

The SIAS actuates the components necessary to inject borated water into the reactor coolant system and actuates components for emergency cooling. The SIAS also actuates the containment spray pumps. The SIAS is also initiated by a loss of power to two PPS divisions. The SIAS also actuates the EDG.

The functional logic for the SIAS is shown in Figure 7.3-4.

APR1400 DCD TIER 2

b. CSAS

1) Input

High-high containment pressure or manual ESF system-level actuation switches located on the safety console in the MCR.

2) Function

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

The functional logic for the CSAS is shown in Figure 7.3-5.

c. CIAS

1) Input

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

2) Function

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

The functional logic for the CIAS is shown in Figure 7.3-6.

d. MSIS

1) Input

Low pressure from each steam generator (SG), high containment pressure, high level from each SG, or manual ESF system-level actuation switches located on the safety console in the MCR.

2) Function

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

APR1400 DCD TIER 2

The functional logic for the MSIS is shown in Figure 7.3-7.

e. AFAS-1 and AFAS-2

1) Input

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

2) Function

The AFAS-1 or AFAS-2 actuates auxiliary feedwater on low water level of SG. The AFAS-1 or AFAS-2 is also initiated by a loss of power to two PPS divisions.

Actuation function AFAS-1 pertains to SG1, and AFAS-2 actuation function pertains to SG2.

The functional logic for the AFAS-1 and AFAS-2 is shown in Figure 7.3-8.

f. FHEVAS

1) Input

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

2) Function

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

The functional logic for the FHEVAS is shown in Figure 7.3-9.

g. CPIAS

1) Input

APR1400 DCD TIER 2

High radiation level sensed by containment upper operating area radiation monitors and containment operating area radiation monitors, or manual ESF system-level actuation switches located on the safety console in the MCR.

2) Function

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

The functional logic for the CPIAS is shown in Figure 7.3-10.

h. CREVAS

1) Input

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

2) Function

The CREVAS isolates normal makeup air path for the air handling unit (AHU) inlet, and the emergency makeup air cleaning unit (ACU) starts automatically to filter the outside makeup air and part of the recirculated air from the control room envelope.

The functional logic for the CREVAS is shown in Figure 7.3-11.

7.3.1.4 Component Control Logic

All ESF component control logics are located in the ESF-CCS LC. Each LC consists of a primary processor module (PM) and a standby PM. The primary and standby PMs exchange health status data with each other via the SDL. If the primary PM experiences a hardware failure, its health status is sensed by the standby PM, which initiates a failover, and the standby PM then becomes the “output active” PM. If a failure is detected in a GC, 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 LC provides discrete ESF component-level actuation signals to the associated CIM.

APR1400 DCD TIER 2

The ESF actuation signal is inputted to the component control logic to energize or de-energize the ESF component. When an ESF actuation signal occurs, all opposite command signals in the component control logic are blocked and the component proceeds and remains in the ESF commanded position until the ESF actuation signal is reset by the opposite command signals.

The redundant LCs receive the following control signals:

- a. Class 1E 4.16 kV switchgear undervoltage for the EDG loading sequencer, ESF-CCS GC output signals including ESF actuation signals, dedicated manual system-level ESF actuation switches, and minimum inventory (MI) switches
- b. Soft component-level controls from the ESF-CCS soft control module (ESCM) via the control channel gateway (CCG)
- c. Sensor input signals for component controls

The LC priority logic performs a prioritization between ESF actuation signals and component-level signal from the ESCM, and MI switches. The output of the LC priority logic is then inputted to the priority logic in the CIM.

The ESF actuation signal is latched until the ESFAS initiation signal is reset. The latched signal is transmitted to the LCs from the GCs. When an ESF actuation signal is maintained to complete protective action, the opposite signal is blocked to avoid blocking or overriding an ESF actuation.

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 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. Modulating component control
- f. Electro-hydraulic motor damper control

The ESF-CCS also provides continuous control and monitoring functions.

Solenoid-Operated Valve Control

- a. Two-state solenoid valve control

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 7.3-12 is a 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 ESF 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 (DO) module in the LC 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),

APR1400 DCD TIER 2

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.

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 7.3-13 is a CLD that shows 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 LC.

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 LC.

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

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. The MOV functional interface design is shown in Figure 7.3-14. 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 DO module in the LC 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 LC. This design allows the valve motor to stop by torque or limit switches without the 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/closed), component operation status deviation

APR1400 DCD TIER 2

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.

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 7.3-15 is a CLD that shows 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 ESF actuation signals, the control response to the ESF actuation signal is always full stroke. Figure 7.3-16 is a CLD that shows the generic design of a throttling motor-operated valve.

c. Thermal overload monitoring

The application of thermal overload protection devices in Class 1E MOV 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 CLD for the generic control design of a motor control is shown in Figure 7.3-17. 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

APR1400 DCD TIER 2

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

b. Control signal

The control logic uses the state-of-the-output relay and continuity monitoring circuit associated with the output. A DO module in the LC 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 7.3-18 is a CLD that shows the generic control logic necessary to energize the breaker closing circuit and energize the breaker trip circuit.

Modulating Component Control

A CLD showing the generic design of a modulating component is shown in Figure 7.3-19. 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) FO and FC position signals from the indicating limit switches interface with a DI module of the LC.
- 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 LC.

b. Component inoperable

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 Control

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 7.3-20 is a CLD that shows 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 DO module in the LC 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

APR1400 DCD TIER 2

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 operating bypass, as shown in Figure 7.3-4, is provided to allow plant depressurization without initiating protective actions when not desired. The operating bypass can be requested either from the MCR or from the RSR based on the master transfer switch status. 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.

There is no operating bypass for the BOP ESFAS logic.

b. Trip channel bypass

An all-bypass function for all ESFAS variables is provided to bypass all parameters in one channel. The channel bypasses are initiated manually and removed manually also. An administrative procedure permits only one channel bypass at a time. The alarms and indications for the channel bypasses are provided in the MCR.

For the NSSS ESFAS, a trip channel bypass prevents a bistable trip and results in a 2-out-of-3 coincidence logic in the LCL.

An individual trip channel bypass is possible on each MTP 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 divisions.

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

For the BOP ESFAS, double sets of two channels (A and B) are provided for measurement channels except the FHEVAS. If one channel is bypassed, the BOP

APR1400 DCD TIER 2

ESFAS 1-out-of-2 logic becomes modified 1-out-of-1 logic to perform single channel actuation. Other channels without a bypassed channel keep the 1-out-of-2 logic. The interval of maintenance bypasses should be shorten so that the failure probability of the remaining channel is acceptably low. Manual channel bypass switches are also located on the MTP.

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 hardwired cable between LCLs in all divisions. The purpose of the all-bypass function is to support testing and maintenance of the BP whereas the trip channel bypass is used against sensor failure.

There is no bypass interlocks for the BOP ESFAS logic.

b. Manual test interlock

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

7.3.1.7 Redundancy

The ESF-CCS consists of following redundant features:

- a. Four divisions of the GCs
- b. Four divisions of the LCs
- c. Four divisions of the 2-out-of-4 coincidence logic in the GCs for the NSSS ESFAS
- d. Two divisions of the 1-out-of-2 logic in the GCs for the BOP ESFAS
- e. Two 1-out-of-2 logics in each division for the BOP ESFAS except the FHEVAS

APR1400 DCD TIER 2

- f. Two GCs in each division
- g. Four redundant ac power supplies
- h. Four redundant dc power supplies

There are four redundant divisions for each parameter from the process sensors to the initiation logic in the PPS for the NSSS ESFAS.

There are two redundant divisions for each parameter from the process sensors to the actuation logic in the GC for the BOP ESFAS.

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

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

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

The SRDC is redundant, having divisions A and B.

7.3.1.8 Emergency Diesel Generator Loading Sequencer

Because of the large power requirements imposed on the EDGs by equipment that is connected to the Class 1E 4.16 kV buses, there is a need to sequentially load the equipment onto the bus.

The EDGs 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 EDG one at a time by the 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.

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

APR1400 DCD TIER 2

To minimize the EDG size and eliminate unnecessary equipment cycling but maintain plant safety, the EDG 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 offsite power is transferred rapidly 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 CLD for the EDG loading sequencer is shown in Figure 7.3-21.

a. EDG Loading 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 shedding (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 shedding signals and, upon receiving an indication that all of the breakers are open, generates a permissive to allow load sequencing to proceed. When the EDG 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 EDG 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 equipment loading sequence then begins loading the components onto the Class 1E 4.16 kV bus, which is powered by 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, and 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 Class 1E 4.16 kV buses. Receipt of an SIAS or a LOOP signal at the Class 1E 4.16 kV buses automatically initiates the loading sequencer. Following the LOOP signal, when the EDG reaches rated voltage and frequency, the EDG circuit breaker closes, and the loading 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 the SIAS, AFAS, or CSAS.

The EDG loading sequencer provides the following features:

- 1) The size of EDGs is minimized because each load group is always energized one at a time.
- 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.
- 5) When offsite power is lost at some point after the EDGs are up to rated voltage and speed and after the required ESF equipment is running ESF actuations, the response time assumed in the Chapter 15 safety analyses are met.

APR1400 DCD TIER 2

In the event that offsite power is unavailable and the EDGs are not yet up to rated voltage and speed when 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 for a listing of the ESF components that receive a load shedding signal, and the ESF components that are sequenced at each step.

7.3.1.9 Actuated Systems

The ESF systems are maintained in a standby mode during normal operations. ESF actuation 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 DBEs 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 the description of the containment isolation system (CIS). The actuation system is composed of redundant divisions A and B. The instrumentation and controls of the two divisions are physically and electrically separate and independent so that the loss of one division 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 CIVs listed in Table 6.2.4-1 are automatically actuated by CIAS, other ESFAS signals (SIAS, CSAS, MSIS, and AFAS), or process interlock signals such as high radiation actuation signal and tank level actuation signal. The process interlock signals are then entered in a logical “Or” with other ESFAS signals for CIVs actuation. The non-safety-related process interlock signals are sent hardwired to the ESF-CCS via fiber optic cable for electrical isolation. Remotely operated (automatic or manual) containment isolation valves (CIVs) are provided

APR1400 DCD TIER 2

with control and indication capability in the MCR. Additionally, a closed position signal of each valve inputs into the IPS, QIAS-P, and QIAS-N for critical function monitoring, which detects unisolated containment penetrations by monitoring the status of valves that are required to close upon 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 upon a CIAS.

b. Containment spray system

Subsection 6.5.2 contains the description of the containment spray system (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 divisions A and B. The instrumentation and controls of each division are physically and electrically separate and independent. Each division has 100 percent capacity. Therefore, the CSS can sustain the loss of an entire division 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.

Two containment spray pumps are assigned to divisions C and D independently, and they are actuated by CSAS or SIAS signals from the ESF-CCS LC via dedicated CIM. Two shutdown cooling pumps which are assigned to divisions A and B independently are aligned to perform the function of containment spray if the following three conditions are met at the same time:

APR1400 DCD TIER 2

- 1) CSAS actuation or SIAS actuation
 - 2) The containment spray pump is in trouble or disabled
 - 3) The cross-connection valves of the containment spray/shutdown cooling pumps are not fully closed
- c. Actuated systems on receipt of a main steam isolation signal

Section 10.3 contains the description of the main steam system (MSS). Subsection 10.4.7 contains the description of the feedwater system. Subsection 10.4.8 contains the description of the steam generator blowdown system (SGBS).

The actuation systems are composed of redundant divisions A and B. The instrumentation and controls of the valves in division A are physically and electrically separate and independent of the instrumentation and controls of the valves in division B. The separation and independence are such that a failure of one division 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 SG blowdown lines are actuated by an MSIS.

These valves effectively isolate the SGs from the MSS, feedwater system, and SGBS.

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

- d. Safety injection system

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

APR1400 DCD TIER 2

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

Subsection 10.4.9 contains the description of the auxiliary feedwater system (AFWS). The AFWS is actuated by an AFAS-1 for SG1 and an AFAS-2 for SG2. The AFWS is also actuated by the diverse protection system (DPS).

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

The auxiliary feedwater modulating valves are designed to fail open if control power is lost. In the unlikely event of such an occurrence, auxiliary feedwater isolation valves will be controlled by a cycling signal generated from the PPS. The cycling AFAS to the auxiliary feedwater isolation valves is not locked, while the latching AFAS signal to the pump is locked. The latching AFAS signal must be manually reset at the ESF-CCS cabinets. This is to allow the SG level to be automatically adjusted between the predetermined high and low levels.

When the SG water level reaches the predetermined high level, the cycling AFAS makes the auxiliary feedwater isolation valves for the affected SG close. When the SG water level drops to the low level again, the auxiliary feedwater isolation valves on the flow paths to the affected SG reopen. Opening and closing of the isolation valves continues to occur depending on the water level of the affected SG.

f. Fuel handling area HVAC system

Subsection 9.4.2 contains the description of the fuel handling area HVAC system. Two radioactivity detectors in the spent fuel pool area (one in division A and one in division B) provide radioactivity signals that produce signals for generation of a

APR1400 DCD TIER 2

FHEVAS. The fuel handling area emergency ventilation system automatically starts following a receipt of an FHEVAS.

g. Reactor containment building purge system

Subsection 9.4.6 contains the description of the reactor containment building purge system. Four radioactivity monitors (e.g., two for monitoring the containment operating area (one in division A and one in division B) and two for monitoring the containment upper operating area (one in division A and one in division B)) provide, upon detection of high radiation levels, signals to the bistable logic, which produces redundant CPIAS.

h. Control room HVAC system

Subsection 9.4.1 contains the description of the control room HVAC system. Four radioactivity detectors (two for monitoring the MCR outside supply air intake A and two for monitoring the MCR outside supply air intake B) provide radioactivity signals that produce signals for generation of a CREVAS.

The RMS detects high radiation signals from the two outside supply air intakes in each division 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.

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 system complies with ASME AG-1 (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.

APR1400 DCD TIER 2

7.3.1.11 Component Interface Module

The component interface module (CIM) is a qualified safety module that uses hardware logic devices to cope with a common-cause failure (CCF) of the digital protection and safety systems. The CIM receives component control signals from the ESF-CCS, DPS, diverse manual ESF actuation (DMA) switches, and front panel control (FPC) switch. The CIM combines these control signals through conventional hardware priority logic and then sends the resulting signal to the controlled component such as an MOV, pump motor, or solenoid-operated valve. The detailed design features of the CIM are described in the Component Interface Module Technical Report (Reference 5).

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 DBEs shown in Table 7.3-2. The ESF-CCS is designed to respond to those initiating signals to provide automatic actuation and manual control of the ESF plant components.

System compliance with the general design criteria (GDC) in 10 CFR Part 50, Appendix A (Reference 29), is described in the Safety I&C System Technical Report, and cross references to 10 CFR Part 50 (sections and the GDC in Appendix A) and sections of this APR1400 DCD are provided in Table 7.1-1.

7.3.2.1 Single Failure Criterion

The ESF system 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 division. 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 DBE.

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

The single failure of the initiation logic for the NSSS ESFAS in the PPS cabinet has no effect because selective 2-out-of-4 actuation logic is implemented in the 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 divisions is sufficient for the protective action.

APR1400 DCD TIER 2

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

Because the BOP ESFAS initiation signals are performed by 1-out-of-2 logic taken twice except for the FHEVAS, even if one of two radiation monitor in the same channel is placed in bypass for testing and the single failure of the different channel belonging to other division occurs at the same time under the radiation release accident, the 1-out-of-1 logic of the available division can be actuated by the remaining operating radiation monitor. The single failure criterion is met by changing the logic from 1-out-of-2 to 1-out-of-1 in the channel 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 except the FHEVAS. Even if one measurement channel is placed in test mode, the other measurement channel is available.

7.3.2.2 Quality of Components and Modules

The ESF system is 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 divisions 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 6) and NRC RG 1.151 (Reference 7). Cables for each division are physically separated. The I&C cables are routed separately from the power cables.

The ESFAS initiation logic is located in four PPS cabinets and two RMS cabinets, and the ESF actuation devices are controlled from four ESF-CCS cabinets. The geographical separation and electrical isolation between these cabinets reduces the possibility of a CCF.

APR1400 DCD TIER 2

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

The SRDC meets the independence requirement between safety systems and other systems of IEEE Std. 603.

7.3.2.4 Diversity and Defense-in-Depth

The diversity and defense-in-depth features for the ESF-CCS are implemented by the DPS and DMA switches. The control signals from the ESF-CCS, DPS, DMA switches, and FPC switch are input to the CIM, and the CIM prioritizes the control signals according to the priority logic as described in the Component Interface Module Technical Report.

According to BTP 7-19 (Reference 8) and Staff Requirements Memorandum (SRM) on SECY-93-087, Item II.Q, Position 4 (Reference 9), the event of a postulated CCF of both the PPS/ESF-CCS and a LOOP is evaluated.

Under the LOOP condition, the EDG is started to supply power into the safety buses. However, if a disabled condition is initiated by software CCF of the PPS and ESF-CCS, necessary power buses are supplied by the alternate alternating current gas turbine generator (AAC GTG) through manual action.

The EDG start/stop function can be accomplished through the manual operation of the local switches for the applicable breakers. The load shedding and the loading sequencer can be carried by the manual operation of the local switches for the applicable load.

The ESF system provides an echelon of defense, as described in the Diversity and Defense-in-Depth Technical Report (Reference 10).

7.3.2.5 System Testing and Inoperable Surveillance

The ESF system 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 11), which are endorsed by NRC RG 1.118 (Reference 12) and NRC RG 1.22 (Reference 13). The test intervals are specified in Chapter 16, Technical Specifications. The simplified test logic diagram for the ESF-CCS is shown in Figure 7.3-22.

APR1400 DCD TIER 2

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

Bypasses and the inoperable status of the safety system are displayed at the MTP and OM in accordance with NRC RG 1.47 (Reference 14).

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

Manual testing of the ESF system 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 logic 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. The trip path of 2-out-of-4 coincidence logic is tested for all input combination.

d. Initiation logic test

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

Testing of the BOP ESFAS initiation logic is accomplished using the test features within the RMS and ESF-CCS.

e. Actuation logic test

Actuation logic testing is performed manually. The trip path of selective 2-out-of-4 coincidence logic is tested for all input combinations. Trip paths of 1-out-of-2 logic are also tested for all input combinations.

APR1400 DCD TIER 2

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.

The selective group test of the ESF-CCS 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 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 7.3-21, 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 actuation input signal is received. In this manner, testing can be conducted without impeding required sequencer operation.

i. Component logic test

The component logic test is individually performed using manual control switches on the ESCM and minimum inventory switches on the safety console according to predetermined maintenance procedure as shown in Figure 7.3-24.

j. CIM test

The CIM is tested for interface test by inputting the signals to each connector or selecting FPC switch at the CIM according to predetermined maintenance procedure as shown in Figure 7.3-24.

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 Chapter 15 safety analysis.

When determining uncertainties, the worst environment considering ESF actuation is assumed for each different event. The methodology for calculating uncertainty is provided in the Uncertainty Methodology and Application for Instrumentation Technical Report (Reference 15).

The methodology for combining uncertainty in a division and determining the final actuation setpoint is provided in the Setpoint Methodology for Safety-Related Instrumentation Technical Report (Reference 16).

The setpoint methodology follows the methodology in ANSI/ISA S67.04 (Reference 17), as endorsed by NRC RG 1.105 (Reference 18).

The response time of the instrumentation division is a signal propagation time from the process sensor to the final actuation device. The response time for the ESF meets the response 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.

The methodology for calculating system response time is provided in the Response Time Analysis of Safety I&C System Technical Report (Reference 28).

7.3.2.8 Equipment Qualification

The ESF system is designed and tested in accordance with the requirements of IEEE Std. 323 (Reference 19) for environmental qualification and IEEE Std. 344 (Reference 20) for seismic qualification.

The ESF system is designed and tested to minimize both the emission and susceptibility of electromagnetic interference and radio-frequency interference in compliance with NRC RG 1.180 (Reference 21).

APR1400 DCD TIER 2

The ESF system is designed and tested to have immunity to electrostatic discharge and surge in accordance with IEC 61000-4-2 (Reference 22) and IEC 61000-4-5 (Reference 23), respectively.

7.3.2.9 System Drawings

The measurement channel functional diagram and functional logics are shown in Figures 7.2-2 and 7.3-3 through 7.3-11.

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 24) referred from IEEE Std. 603 (Reference 25), IEEE Std. 7-4.3.2 (Reference 26), and IEEE Std. 379 (Reference 27).

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 division redundancy.
- b. Any single failure is detected by diagnostic or periodic test.

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

7.3.3.2 Conformance with IEEE Std. 603

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

The SRDC will be supplied by a 10 CFR Part 50, Appendix B qualified supplier. The hardware of the SRDC will be designed and tested in accordance with the requirement of IEEE Std. 323.

APR1400 DCD TIER 2

7.3.3.3 Conformance with IEEE Std. 7-4.3.2

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

The software of the SRDC will meet the requirements of NRC RG 1.152 (Reference 30) and IEEE Std. 7-4.3.2.

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 divisions of safety cooling water, corresponding to the four divisions of safety ESF equipment. These four divisions are controlled by the ESF-CCS. Therefore, loss of a single division of cooling water does not prevent accomplishing the safety function.
- b. Loss of plant instrument air: There is no reliance on plant instrument air for any safety functions.
- c. Loss of power source: All of 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

Conformance of 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 ESF system is periodically tested to verify its operability. A division is completely tested without causing a system actuation and affecting system operability and availability. Testing is overlapped to provide reasonable assurance that the entire division is tested.

The response time test is performed during refueling outage.

7.3.4 Combined License Information

No combined license (COL) information is required with regard to Section 7.3.

APR1400 DCD TIER 2

7.3.5 References

1. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.
2. APR1400-Z-J-NR-14001-P, "Safety I&C System," Rev. 3, KEPCO & KHNP, May 2018.
3. ASME AG-1-2009, "Code on Nuclear Air and Gas Treatment," The American Society of Mechanical Engineers, 2009.
4. Regulatory Guide 1.52, "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," Rev. 4, U.S. Nuclear Regulatory Commission, September 2012.
5. APR1400-E-J-NR-14001-P, "Component Interface Module," Rev. 1, KEPCO & KHNP, March 2017.
6. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Rev. 3, U.S. Nuclear Regulatory Commission, February 2005.
7. Regulatory Guide 1.151, "Instrument Sensing Lines," Rev. 1, U.S. Nuclear Regulatory Commission, July 2010.
8. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," Rev. 6, U.S. Nuclear Regulatory Commission, July 2012.
9. Staff Requirements Memorandum on SECY-93-087, Item II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, July 21, 1993.
10. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
11. IEEE Std. 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems," Institute of Electrical and Electronics Engineers, 1987.

APR1400 DCD TIER 2

12. Regulatory Guide 1.118, “Periodic Testing of Electric Power and Protection Systems,” Rev. 3, U.S. Nuclear Regulatory Commission, April 1995.
13. Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions,” U.S. Nuclear Regulatory Commission, February 1972.
14. Regulatory Guide 1.47 “Bypassed and Inoperable Status indication for Nuclear Power Plant Safety Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, February 2010.
15. APR1400-Z-J-NR-14004-P, “Uncertainty Methodology and Application for Instrumentation,” Rev. 2, KEPCO & KHNP, January 2018.
16. APR1400-Z-J-NR-14005-P, “Setpoint Methodology for Safety-Related Instrumentation,” Rev. 2, KEPCO & KHNP, January 2018.
17. ANSI/ISA S67.04-1994, “Setpoints for Nuclear Safety-Related Instrumentation,” International Society of Automation, 1994.
18. Regulatory Guide 1.105, “Setpoints for Safety-Related Instrumentation,” Rev. 3, U.S. Nuclear Regulatory Commission, December 1999.
19. IEEE Std. 323-2003, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2003.
20. IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2005.
21. Regulatory Guide 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related instrumentation and Control Systems,” Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.
22. IEC 61000-4-2, “Electromagnetic Compatibility – Testing and Measurement Techniques – Electrostatic Discharge Immunity Test,” International Electrotechnical Commission, 1992.
23. IEC 61000-4-5, “Electromagnetic Compatibility-Testing and Measurement Techniques – Surge Immunity Test,” International Electrotechnical Commission.

APR1400 DCD TIER 2

24. IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 1987.
25. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.
26. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.
27. IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," Institute of Electrical and Electronics Engineers, 2000.
28. APR1400-Z-J-NR-14013-P, "Response Time Analysis of Safety I&C System," Rev. 2, KEPCO & KHNP, January 2018.
29. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
30. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.

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 division), 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.

APR1400 DCD TIER 2

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 POSRV 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 transmitter (wide range)	4 ⁽¹⁾	Pressurizer
Containment pressure (Hi-Hi)	Pressure transmitter (wide range)	4	Outside containment
Containment pressure (Hi)	Pressure transmitter (narrow range)	4 ⁽¹⁾	Outside containment
Steam generator pressure	Pressure transmitter	4/steam generator ⁽¹⁾	Steam generator
Steam generator level	Differential pressure transmitter (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	158.2 kg/cm ² A (2,250 psia)	156.4 to 159.9 kg/cm ² A (2,225 to 2,275 psia)	127.3 kg/cm ² A (1,810 psia ⁽¹⁾)	30.9 kg/cm ² A (440 psi)
High containment pressure	0 cmH ₂ O (0 psig)	0.0 to 63.3 cmH ₂ O (0.0 to 0.9 psig)	133.6 cmH ₂ O (1.9 psig)	133.6 cmH ₂ O (1.9 psig)
CSAS				
High-high containment pressure	0 cmH ₂ O (0 psig)	0.0 to 63.3 cmH ₂ O (0.0 to 0.9 psig)	1,408.3 cmH ₂ O (20.03 psig)	1,408.3 cmH ₂ O (20.03 psig)
MSIS				
Low steam generator pressure	70.3 kg/cm ² A (1,000 psia)	70.3 to 77.3 kg/cm ² A (1,000 to 1,100 psia)	60.1 kg/cm ² A (855 psia ⁽¹⁾)	10.2 kg/cm ² A (145 psia)
High containment pressure	0 cmH ₂ O (0 psig)	0.0 to 63.3 cmH ₂ O (0.0 to 0.9 psig)	133.6 cmH ₂ O (1.9 psig)	133.6 cmH ₂ O (1.9 psig)
High steam generator level	50 % NR	50 % NR	90.0 % NR	40.0 %
AFAS (PPS)				
Low steam generator level	77 % WR	77 % WR	25.0 % WR	52.0 %

(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 Margins 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	(1)	(1)
Containment operating area radiation level (during fuel handling operation)	0.02 mSv/hr	0.5 mSv/hr	(1)	(1)
FHEVAS				
Spent fuel pool area radiation level	0.02 mSv/hr	0.025 mSv/hr	(1)	(1)
CREVAS				
Control room air intake radiation level	Negligible	0.052 Bq/cc	0.52 Bq/cc	0.51 Bq/cc

(1) The COL applicant is to determine the setpoint (COL 12.3(6))

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)	158.2 kg/cm ² A (2,250 psia)	210.9 kg/cm ² A (3,000 psia)
Containment pressure	−400 cmH ₂ O (−5.7 psig)	0 cmH ₂ O (0 psia)	5,600 cmH ₂ O (79.5 psig)
Steam generator pressure	0 kg/cm ² A (0 psia)	70.3 kg/cm ² A (1,000 psia)	105.0 kg/cm ² A (1,494 psia)
Steam generator level (wide range)	0 %	77 %	100 %
Steam generator level (narrow range)	0 %	50 %	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
Control room air intake 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	
Spent fuel pool area radiation – High	
a. FHEVAS actuated isolation dampers	< 8.4 ^{(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. Class 1E 4.16 kV bus undervoltage (degraded voltage) loss of power 90 % system voltage	< 5 min ⁽⁷⁾
12. Class 1E 4.16 kV 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 EDG loading sequencer are included.

(5) Same as No. 3. In addition, delays of EDG loading sequencer 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 division 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.

APR1400 DCD TIER 2

Table 7.3-8 (1 of 21)

Failure Modes and Effects Analysis for the Engineered Safety Features-Component Control System

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
1	Processor module 1 (PM1) in the GC1 or GC2 of division A	a) Processor failures b) I/O addressing failures c) CRC run time error (OS or applications)	Component failure	<ul style="list-style-type: none"> The A and C ESFAS initiation signals from the PPS LCL are lost. The A (or C) coincidence logic performed by the PM1 is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM1 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The redundant GC receives ESFAS initiation signals from four divisions of redundant LCL and performs the selective 2-out-of-4 coincidence processing.
		a) Program failure b) Data memory failure	Component failure	<ul style="list-style-type: none"> The A and C ESFAS initiation signals from the LCL are lost. The A (or C) coincidence logic performed by the PM1 is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM1 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The redundant GC receives ESFAS initiation signals from four divisions of redundant LCL and performs the selective 2-out-of-4 coincidence processing.
		a) Communication failures on in division SDL (loss of SDL input from LCL division A or division C)	<ul style="list-style-type: none"> Cable failure Component failure Loose connection LCL fails to transmit data 	The division A (or division C), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> Trouble annunciation is generated by the GC. MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The PM1 in the GC detects lack of periodic SDL data transmission from the LCL and sets an SDL alarm.

APR1400 DCD TIER 2

Table 7.3-8 (2 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
1	PM1 in the GC1 or GC2 of division A (Continued)	a) Communication failure on external divisions SDL	<ul style="list-style-type: none"> • Component failure • Cable failure • Loose connection 	N/A	N/A	N/A	N/A	The PM1 does not generate an SDL output.
2	Fiber optic modem (FOM) transmitter in the GC1 or GC2 (from LCL division A or C)	a) Fails off	Component failure	The division A (or division C), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The PM in the GC detects lack of periodic SDL data transmission from the LCL rack and sets an SDL alarm.
3	FOM receiver in the GC1 or GC2 (from LCL division A or C)	a) Fails off	Component failure	The division A (or division C), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The PM in the GC detects lack of periodic SDL data transmission from the LCL and sets an SDL alarm.

APR1400 DCD TIER 2

Table 7.3-8 (3 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
4	PM2 in the GC1 or GC2 of division A	a) Processor failures b) I/O addressing failure c) CRC run time error (OS or applications)	Component failure	<ul style="list-style-type: none"> The B and D ESFAS initiation signals from the PPS LCL are lost. The B (or D) coincidence logic performed by the PM2 is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM2 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant B and D ESFAS initiation signals.	The redundant GC receives ESFAS initiation signals from four divisions of redundant LCL and performs the selective 2-out-of-4 coincidence processing.
		a) Program failure b) Data memory failure	Component Failure	<ul style="list-style-type: none"> The B and D ESFAS initiation signals from the LCL are lost. The B (or D) coincidence logic performed by the PM2 is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM2 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant B and D ESFAS initiation signals.	The redundant GC receives ESFAS initiation signals from four divisions of redundant LCL and performs the selective 2-out-of-4 coincidence processing.
		a) Communication failures on in-division SDL (loss of SDL input from LCL division B or division D)	<ul style="list-style-type: none"> Cable failure Component failure Loose connection LCL fails to transmit data 	The division B (or division D), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> Trouble annunciation is generated by the GC. MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant B and D ESFAS initiation signals.	The PM2 in the GC detects lack of periodic SDL data transmission from the LCL and sets an SDL alarm.
		a) Communication failure on external divisions SDL	<ul style="list-style-type: none"> Component failure Cable failure Loose connection. 	N/A	N/A	N/A	N/A	The PM2 does not generate an SDL output.

APR1400 DCD TIER 2

Table 7.3-8 (4 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
5	FOM transmitter in the GC1 or GC2 (from LCL division B or division D)	a) Fails off	Component failure	The division B (or division D), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant B and D ESFAS initiation signals.	The PM in the GC detects lack of periodic SDL data transmission from the LCL rack and sets an SDL alarm.
6	FOM receiver in the GC1 or GC2 (from LCL division B or division D)	a) Fails off	Component failure	The division B (or division D), ESF actuation signal from the LCL is not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant GC and redundant LCL ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC and redundant A and C ESFAS initiation signals.	The PM in the GC detects lack of periodic SDL data transmission from the LCL and sets an SDL alarm.

APR1400 DCD TIER 2

Table 7.3-8 (5 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
7	PM3 in the GC1 or GC2	a) Processor failure b) I/O addressing fails c) CRC run time error (OS or application)	Component failure	<ul style="list-style-type: none"> The MCR CPM signals are lost. The selective 2-out-of-4 coincidence logic performed by the PM3 is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM3 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC, redundant MCR CPM signals, and redundant ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. It also acquires redundant MCR and RSR CPM signals.
		a) Program Failure b) Data memory failure	Component failure	<ul style="list-style-type: none"> The MCR CPM signals are lost. The selective two-out-of-four coincidence logic performed by this PM is lost. The GC can no longer perform the ESF actuation logic for the division. 	<ul style="list-style-type: none"> The PM3 heart beat failure results in trouble annunciation. MTP and ITP provide status indication. 	Redundant GC, redundant MCR CPM signals, and redundant ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. It also acquires redundant MCR and RSR CPM signals.
		a) Communication failure on in division SDL (Loss of SDL input signal from MCR CPM)	<ul style="list-style-type: none"> Component failure Cable Failure Loose connection MCR CPM fails to transmit data 	The MCR CPM signals are not received by the GC.	<ul style="list-style-type: none"> Trouble annunciation is generated by the GC. MTP displays health status. 	Redundant MCR CPM signals are available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. It also acquires redundant MCR and RSR CPM signals.

APR1400 DCD TIER 2

Table 7.3-8 (6 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
7	PM3 in the GC1 or GC2 (Continued)	a) Communication failure on external division SDL	<ul style="list-style-type: none"> • Component failure • Cable Failure • Loose connection. 	MCR and RSR CPM signals are not received by the LC ESF actuation signals are not received by the LC	<ul style="list-style-type: none"> • Trouble annunciation is generated by the LC. • MTP displays health status. 	Redundant GC, redundant MCR CPM signals, and redundant ESFAS initiation signals are provided within the division.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	The LC uses the MCR and RSR CPM signals and the ESF actuation signals as provided by the redundant GC.
8.	FOM transmitter or receiver in the GC1 or GC2	a) Fails off	Component failure	The MCR CPM signals are not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant MCR CPM signals are available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> • The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. • It also acquires redundant MCR and RSR CPM signals.

APR1400 DCD TIER 2

Table 7.3-8 (7 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
9	PM4 in the GC1 or GC2	a) Processor failure b) I/O addressing fails c) CRC run time error (OS or application)	Component failure	The RSR CPM signals are lost.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant RSR CPM signal is available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> • The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. • It also acquires redundant MCR and RSR CPM signals.
		a) Program failure b) Data memory failure	Component failure	The RSR CPM signals are lost.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • MTP displays health status. 	Redundant RSR CPM signal is available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> • The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. • It also acquires redundant MCR and RSR CPM signals.
		a) Communication failure on in division SDL (loss of SDL input signal from RSR CPM)	<ul style="list-style-type: none"> • Cable failure • Component failure • Loose connection • RSR CPM fails to transmit data 	The RSR CPM signals are not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • The MTP displays health status. 	Redundant RSR CPM signal is available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> • The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. • It also acquires redundant MCR and RSR CPM signals.

APR1400 DCD TIER 2

Table 7.3-8 (8 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
10	FOM transmitter or receiver (from RSR CPM) in the GC1 or GC2	a) Fails off	Component failure	The RSR CPM signals are not received by the GC.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • The MTP displays health status. 	Redundant RSR CPM signal is available in the redundant GC.	Functionality is maintained within the division via use of redundant GC, redundant MCR and RSR CPM signals, and redundant ESFAS initiation signals.	<ul style="list-style-type: none"> • The redundant GC acquires four divisions of redundant LCL ESFAS initiation signals and performs the selective 2-out-of-4 coincidence processing. • It also acquires redundant MCR and RSR CPM signals.
11	CI module in the GC1 or GC2	a) Fails off	Component failure	Ability to communicate via SDN is lost, and global memory no longer available.	<ul style="list-style-type: none"> • SDN failure is detected by other stations on SDN network. • Trouble annunciation is shown on the MTP. 	Redundant GC which has access to SDN network and has an independent CI module	Functionality is maintained within the division via use of redundant GC.	Redundant GC has its own CI module which provides global memory and provides SDN access.
12	DI module in the GC1 or GC2	a) Entire module fails	Component failure	<ul style="list-style-type: none"> • Signal quality for DI input is set to BAD. • Internal cabinet status information is lost for the affected cabinet. 	<ul style="list-style-type: none"> • Failure detected by the PM in the GC. • The MTP displays health status. 	Redundant GC redundant ESFAS initiation signals are provided within the division.	<ul style="list-style-type: none"> • No safety function depends on these DI contact inputs; internal cabinet status information is lost for the affected cabinet. • Loss of local manual actuation in one GC in that division and redundant GC is still functional. 	Cabinet status information, such as cabinet door open, high cabinet temperature alarm, and power supply health is lost for the affected cabinet.
		a) Single point fails (erroneous state sensed)	Component failure	<ul style="list-style-type: none"> • Signal quality for DI input is set to BAD. • Internal cabinet status information is lost for the affected cabinet. 	<ul style="list-style-type: none"> • Failure is detected by the PM in the GC. • The MTP displays health status. 	Redundant GC redundant ESFAS initiation signals are provided within the division.	No safety function depends on these DI contact inputs; the affected cabinet status monitoring point is lost or a spurious cabinet alarm is activated.	

APR1400 DCD TIER 2

Table 7.3-8 (9 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
13	PM in control channel gateway ¹ (CCG1) of division A.	a) Processor fails b) I/O addressing fails c) CRC run time error (OS or application)	Component failure	The ability to manually manipulate individual ESF components within the division is lost for one set of four divisionalized ESCMs. (One set of the ESCMs in the MCR and one set of the ESCMs in the RSR can no longer manipulate individual ESF plant components within the affected division.)	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • The MTP displays health status. 	Redundant CCG is provided within the division which interfaces to the remaining set of ESCMs.	<ul style="list-style-type: none"> • Automatic ESF actuation, manual component-level controls by MI switches, and manual system-level ESF actuation are not impacted by the failure. • No safety impact. 	Redundant CCGs are provided within the division. One set of the ESCMs is interfaced to the CCG1 and the remaining other one set of the ESCMs is interfaced to the CCG2.
		a) Program failure b) Data memory failure	Component failure	The ability to manually manipulate individual ESF components within the division is lost for one set of the ESCMs. (One set of the ESCMs in the MCR and one set of the ESCMs in the RSR can no longer manipulate individual ESF plant components within the affected division.)	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • The MTP displays health status. 	Redundant CCG is provided within the division which interfaces to the remaining set of ESCMs.	<ul style="list-style-type: none"> • Automatic ESF actuation, manual component-level controls by MI switches, and manual system-level ESF actuation are not impacted by the failure. • No safety impact. 	Redundant CCGs are provided within the division. One set of ESCMs is interfaced to the CCG1, and the remaining set of ESCMs is interfaced to the CCG2.
		a) Communication failure on in division SDL (Loss of SDL input signal from MCR CPM or RSR CPM)	<ul style="list-style-type: none"> • Cable failure • Component failure • Loose connection • CPM fails to transmit data 	The ability to manually manipulate individual ESF components within the division is lost for one set of the ESCMs.	<ul style="list-style-type: none"> • Trouble annunciation is generated by the GC. • The MTP displays health status. 	Redundant CCG is provided within the division which interfaces to the remaining set of ESCMs.	<ul style="list-style-type: none"> • Automatic ESF actuation, manual component-level controls by MI switches, and manual system-level ESF actuation are not impacted by the failure. • No safety impact. 	Redundant CCGs are provided within the division. One set of ESCMs is interfaced to the CCG1, and the remaining set of ESCMs is interfaced to the CCG2.

APR1400 DCD TIER 2

Table 7.3-8 (10 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
14	CI module in the CCG1 or CCG2 (to interface with the LC)	a) Fails off	Component failure	<ul style="list-style-type: none"> Ability to transmit and receive manual component control actuation signals to the in division LC via the SDN is lost. Global memory is no longer available. The ability to manually manipulate individual ESF components within the division is lost for one set of the ESCMs. 	<ul style="list-style-type: none"> Data communication failure is detected by other stations on SDN. Trouble annunciation is shown on MTP. 	Redundant CCG is provided within the division which interfaces to the remaining set of ESCMs.	<ul style="list-style-type: none"> Automatic ESF actuation, manual component-level controls by MI switches, and manual system-level ESF actuation are not impacted by the failure. No safety impact. 	Redundant CCGs are provided within the division. One set of ESCMs are interfaced to the CCG1, and the remaining set of ESCMs are interfaced to the CCG2.
15	CI module in the CCG1 or CCG2(to interface with the ESCM)	a) Fails off	Component failure	The ability to transmit and receive ESF manual component control actuation requests from the ESCMs located in the MCR and RSR is lost on one SDN data communications.	<ul style="list-style-type: none"> Trouble annunciation is generated by the CCG. MTP displays health status. 	Redundant SDN network with redundant CI module.	Functionality is maintained within the division via use of redundant SDN network and redundant CI module.	The redundant SDN network and the redundant CI Module acquire the ESCM data.
16	DI module in the CCG	a) Entire module fails	Component failure	<ul style="list-style-type: none"> Signal quality for DI input is set to BAD. Status information is lost. 	<ul style="list-style-type: none"> Trouble annunciation is generated. MTP displays health status. 	None	No safety function depends on these DI contact inputs.	The DI module receives output from the transfer switches. When the transfer switches are switched to the RSC, all ESCM signals from the MCR are disabled and ESCM signals from the RSC are enabled by the CCG.

APR1400 DCD TIER 2

Table 7.3-8 (11 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
17	DI module in the CCG	a) Single point fails (erroneous status sensed)	Component failure	The affected monitoring status point is not activated or spurious activation indication is generated.	<ul style="list-style-type: none"> Periodic surveillance testing Presence of spurious alarm 	None	No safety function depends on these DI contact inputs.	The DI module receives output from the transfer switches. When the transfer switches are switched to RSC, all ESCM signals from MCR will be disabled and ESCM signals from RSC are enabled by the CCG.
18	DO module in the CCG	a) Entire module fails	Component failure	<ul style="list-style-type: none"> Signal quality for DO inputs is set to BAD. Status information is lost. 	<ul style="list-style-type: none"> Trouble annunciation is generated. MTP displays health status. 	None	No ESF-CCS safety function depends on DO output.	The DO module transmits the Transfer Switch status to the PPS. The effect on PPS would be evaluated in the PPS FMEA.

APR1400 DCD TIER 2

Table 7.3-8 (12 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
19	PM1 in the GC3	a) Processor fails b) I/O addressing fails c) CRC run time error (OS or applications)	Component failure	The failed PM1 no longer provides the required logic for actuation of BOP ESFAS or EDG loading sequencer.	<ul style="list-style-type: none"> ITP detects lack of PM1 heartbeat signal. MTP displays system health status and system alarms. 	Redundant GC3 PM2 provides the logic for actuation of BOP ESFAS and EDG loading sequencer.	Functionality is maintained within the division via use of redundant GC3 PM2 and redundant SDL.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and EDG loading sequencer logic and transmits the corresponding initiation signals.
		a) Program failure b) Data memory failure	Component failure	The failure no longer provides the required logic for actuation of BOP ESFAS or EDG loading sequencer.	<ul style="list-style-type: none"> ITP detects lack of PM1 heartbeat signal. MTP displays system health status and system alarms. 	Redundant GC3 PM2 provides the logic for actuation of BOP ESFAS and EDG loading sequencer.	Functionality is maintained within the division via use of redundant GC3 PM2 and redundant SDL data link.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and EDG loading sequencer logic and transmits the corresponding initiation signals.
		a) Communication failure on external division SDL	<ul style="list-style-type: none"> Cable failure Component failure Loose connection GC1 fails to transmit data 	The PM1 is no longer able to provide BOP ESFAS or EDG loading sequencer initiation output signals.	<ul style="list-style-type: none"> SDL trouble alarm is generated by the GC1. ITP detects lack of PM1 heartbeat signal. MTP displays system health status. 	Redundant GC3 PM2 and redundant GC3 SDL provide the BOP ESFAS and EDG loading sequencer initiation output signals	Functionality is maintained within the division via use of redundant GC3 PM2 and redundant GC3 SDL.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and EDG loading sequencer logic and transmits the corresponding initiation signals via the redundant SDL.

APR1400 DCD TIER 2

Table 7.3-8 (13 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
20	PM2 in the GC3	a) Processor fails b) I/O addressing fails c) CRC run time error(OS or applications)	Component failure	The failed PM2 no longer provides the required logic for actuation of BOP ESFAS or EDG loading sequencer.	<ul style="list-style-type: none"> ITP detects lack of PM2 heartbeat signal. MTP displays system health status and system alarms. 	Redundant GC3 PM1 provides the logic for actuation of BOP ESFAS and EDG loading sequencer.	Functionality is maintained within the division via use of redundant GC3 PM1 and redundant SDL.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and loading sequencer logic and EDG transmits the corresponding initiation signals.
		a) Program failure b) Data memory failure	Component failure	The failure no longer provides the required logic for actuation of BOP ESFAS or EDG loading sequencer.	<ul style="list-style-type: none"> ITP detects lack of PM2 heartbeat signal. MTP displays system health status and system alarms. 	Redundant GC3 PM1 provides the logic for actuation of BOP ESFAS and EDG loading sequencer.	Functionality is maintained within the division via use of redundant GC3 PM1 and redundant SDL data link.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and EDG loading sequencer logic and transmits the corresponding initiation signals.
		a) Communication failure on external division SDL	<ul style="list-style-type: none"> Cable failure Component failure Loose connection GC1 fails to transmit data 	The PM2 is no longer able to provide BOP ESFAS or EDG loading sequencer initiation output signals	<ul style="list-style-type: none"> SDL trouble alarm is generated by GC1. ITP detects lack of PM2 heartbeat signal. MTP displays system health status. 	Redundant GC3 PM1 and redundant GC3 SDL provide the BOP ESFAS and EDG loading sequencer initiation output signals.	Functionality is maintained within the division via use of redundant GC3 PM1 and redundant GC3 SDL.	The redundant PM acquires the RMS and loss of offsite power input signals, performs the BOP ESFAS and EDG loading sequencer logic and transmits the corresponding initiation signals via the redundant SDL.

APR1400 DCD TIER 2

Table 7.3-8 (14 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
21	Hot standby redundancy SDL in the GC3	a) Fails off	<ul style="list-style-type: none"> Cable failure Component failure Loose connection 	Health status data cannot be exchanged between PM 1 and PM2.	<ul style="list-style-type: none"> Loss of SDL communications is detected by both PM1 and PM2. MTP annunciates alarm. 	None	<ul style="list-style-type: none"> Loss of PM failover capability in GC3. The BOP ESFAS functions (FHEVAS, CPIAS, and CREVAS) generated from the RMS signal are not affected due to redundancy in divisions A and B. The EDG loading sequencer functions generated from the loss of offsite power input signal are not affected due to redundancy in divisions A, B, C, and D. 	None
22	CI module in the GC3	a) Fails off	Component failure	The global memory provided by the CI module is lost to the chassis.	<ul style="list-style-type: none"> PM modules detect failure to access global memory and set alarm. MTP displays health status. 	Redundant CI module provides redundant global memory for the chassis.	Functionality is maintained within the division via use of redundant CI module.	CI module 1 and CI module 2 are dedicated solely to providing redundant global memory for the chassis.

APR1400 DCD TIER 2

Table 7.3-8 (15 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
23	SDL in the GC3	a) Fails off	<ul style="list-style-type: none"> Cable failure Component failure Loose connection 	The RMS and loss of offsite power input signals from the LC are lost on the failed cable.	<ul style="list-style-type: none"> Data communication failure is detected by other station on SDL. Trouble annunciation is shown on MTP. 	Redundant SDL cables are provided.	Functionality is maintained via redundant SDL cable.	The GC3 is configured to have same SDL output data from both PMs and is therefore functionally redundant.
24	DI module in the GC3	a) Entire module fails	Component failure	<ul style="list-style-type: none"> Signal quality for DI inputs is set to BAD. Internal cabinet status information is lost for the affected cabinet. 	<ul style="list-style-type: none"> GC3 PM module detects failure. MTP displays system health status and system alarms. 	Redundant BOP ESFAS and EDG loading sequencer processing capability is provided via ESF-CCS division A, B, C and D.	<ul style="list-style-type: none"> Loss of BOP ESFAS and sequencing within the division. Redundant BOP ESFAS and EDG loading sequencer processing capability is provided via ESF-CCS divisions A, B, C, and D. 	<ul style="list-style-type: none"> Redundant GC3s are provided via ESF-CCS divisions A, B, C, and D. The redundant GC3 maintains the function.
		a) Single point fails(erroneous state sensed)	Component failure	The affected monitoring status point is not activated or spurious activation indication is generated.	<ul style="list-style-type: none"> Periodic surveillance testing Presence of spurious alarm 	Redundant BOP ESFAS and EDG loading sequencer processing capability is provided via ESF-CCS division A, B, C and D.	<ul style="list-style-type: none"> Loss of BOP ESFAS and EDG loading sequencer within the division. Redundant BOP ESFAS and EDG loading sequencer processing capability is provided via ESF-CCS divisions A,B,C, and D. 	<ul style="list-style-type: none"> Redundant GC3s are provided via ESF-CCS division A, B, C, and D. The redundant GC3 maintains the function.

APR1400 DCD TIER 2

Table 7.3-8 (16 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
25	PM1 in the LC1	a) Processor fails b) I/O addressing fails c) CRC run time error(OS or application)	Component failure	<ul style="list-style-type: none"> The input signals from the GC1 are lost. The failed PM1 no longer provides LC output for actuation of ESF components. 	<ul style="list-style-type: none"> ITP detects lack of PM1 heartbeat signal. MTP displays health status. 	Redundant PM2 in the LC, which interfaces with the redundant GC2, is available.	Functionality is maintained within the division via use of redundant PM2 in the LC and redundant GC.	The redundant PM2 in the LC acquires the ESF system-level and component-level actuation signals from redundant GC and provides the actuation outputs for ESF components.
		a) Program failure b) Data memory failure	Component failure	<ul style="list-style-type: none"> The input signals from the GC1 are lost. The failed PM1 no longer provides LC output for actuation of ESF components. 	<ul style="list-style-type: none"> ITP detects lack of PM1 heartbeat signal. MTP displays health status. 	Redundant PM2 in the LC, which interfaces with the redundant GC2, is available.	Functionality is maintained within the division via use of redundant PM2 in the LC and redundant GC.	The redundant PM2 in the LC acquires the ESF system-level and component-level actuation signals from redundant GC and provides the actuation outputs for ESF components.
		a) Communication failure on in division SDL (loss of SDL input from the GC1)	<ul style="list-style-type: none"> Cable failure Component failure Loose connection GC1 fails to transmit data 	<ul style="list-style-type: none"> The input signals from the GC1 are not received by the PM1. The PM1 is no longer able to provide LC output for actuation of ESF components. 	<ul style="list-style-type: none"> Trouble annunciation is generated by the LC. MTP displays health status. 	Redundant GC signal is available via the redundant PM2 in the LC.	Functionality is maintained within the division via use of redundant PM2 in the LC and redundant GC.	The redundant PM2 in the LC acquires the ESF system-level and component-level actuation signals from redundant GC and PM2 continues to provide the actuation outputs for ESF components.

APR1400 DCD TIER 2

Table 7.3-8 (17 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
26	PM2 in the LC1	a) Processor fails b) I/O addressing fails c) CRC run time error (OS or application)	Component failure	<ul style="list-style-type: none"> The input signals from the GC2 are lost. The failed PM2 no longer provides LC output for actuation of ESF components. 	<ul style="list-style-type: none"> ITP detects lack of PM2 heartbeat signal. MTP displays health status. 	Redundant PM1 in the LC, which interfaces with the redundant GC1, is available.	Functionality is maintained within the division via use of redundant PM1 in the LC and redundant GC.	The redundant LC PM1 acquires the ESF system-level and component-level actuation signals from redundant GC and provides the actuation outputs for ESF components.
		a) Program failure b) Data memory failure	Component failure	<ul style="list-style-type: none"> The input signals from the GC2 are lost. The failed PM2 no longer provides LC output for actuation of ESF components. 	<ul style="list-style-type: none"> ITP detects lack of PM2 heartbeat signal. MTP displays health status. 	Redundant PM1 in the LC, which interfaces with the redundant GC1, is available.	Functionality is maintained within the division via use of redundant PM1 in the LC and redundant GC.	The redundant LC PM1 acquires the ESF system-level and component-level actuation signals from redundant GC and provides the actuation outputs for ESF components.
		a) Communication failure on in division SDL (loss of SDL input from the GC2)	<ul style="list-style-type: none"> Cable failure Component failure Loose connection GC2 fails to transmit data 	<ul style="list-style-type: none"> The input signals from the GC2 are not received by the PM2. The PM2 is no longer able to provide LC output for actuation of ESF components. 	<ul style="list-style-type: none"> Trouble annunciation is generated by the LC. MTP displays health status. 	Redundant GC signal is available via the redundant PM1 in the LC.	Functionality is maintained within the division via use of redundant PM1 in the LC and redundant GC.	The redundant LC PM1 acquires the ESF system-level and component-level actuation signals from redundant GC and PM1 continues to provide the actuation outputs for ESF components.

APR1400 DCD TIER 2

Table 7.3-8 (18 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
27	FOM transmitter and receiver in the LC1 (from the GC)	a) Fails off	Component failure	<ul style="list-style-type: none"> The input signals from the GC1 are not received by the PM1. The PM1 is no longer able to provide LC output for actuation of ESF components. 	<ul style="list-style-type: none"> Trouble annunciation is generated by the LC. MTP displays health status. 	Redundant GC signal is available via the redundant PM2 in the LC1.	Functionality is maintained within the division via use of redundant PM2 in the LC1 and redundant GC2.	The redundant PM2 in the LC1 acquires the ESF system-level the component-level actuation signals from redundant GC2 and provides the actuation output for ESF components.
28	Hot standby redundancy SDL in the LC1	a) Fails off	<ul style="list-style-type: none"> Cable failure Component failure Loose connection 	Health status data cannot be exchanged between the PM1 and PM2.	<ul style="list-style-type: none"> Loss of SDL communications is detected by both PM1 and PM2. MTP annunciates alarm. 	None	<ul style="list-style-type: none"> Loss of PM failover capability in LC if a health problem occurs with the primary PM. The LC actuates the BOP ESFAS equipment on the RMS signals and the loading sequencer equipment on loss of offsite power signals. 	<ul style="list-style-type: none"> Impact is limited to the LC that experiences the failure. Other LCs are not affected.
29	CI module in the LC1	a) Fails off	Cable fault	Ability to communicate over redundant communications is lost for that CI module.	<ul style="list-style-type: none"> PM annunciates a CI module failure. Trouble annunciation is shown on MTP. 	Redundant CI module provides the communications.	No loss of functionality.	CI module 1 and CI module 2 are dedicated solely to providing redundant communications.

APR1400 DCD TIER 2

Table 7.3-8 (19 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
30	CI module in the LC1	a) Fails off	Component failure (memory)	The global memory provided by the CI module is lost to the chassis.	<ul style="list-style-type: none"> PM modules detect failure to access global memory and set alarm. MTP displays health status. 	Redundant CI module provides redundant global memory for the chassis.	Functionality is maintained within the division via use of redundant CI module.	CI module 1 and CI module 2 are dedicated solely to providing redundant global memory for the chassis.
		a) Fails off	Component failure (SDN)	Ability to communicate on SDN is lost.	<ul style="list-style-type: none"> Data network communication failure detected by other stations on SDN network. Trouble annunciation is shown on MTP. 	None	Loss of component feedback to MTP/ITP, ESCM and MI switches.	Loss of component feedback is limited to the single LC cabinet.

APR1400 DCD TIER 2

Table 7.3-8 (20 of 21)

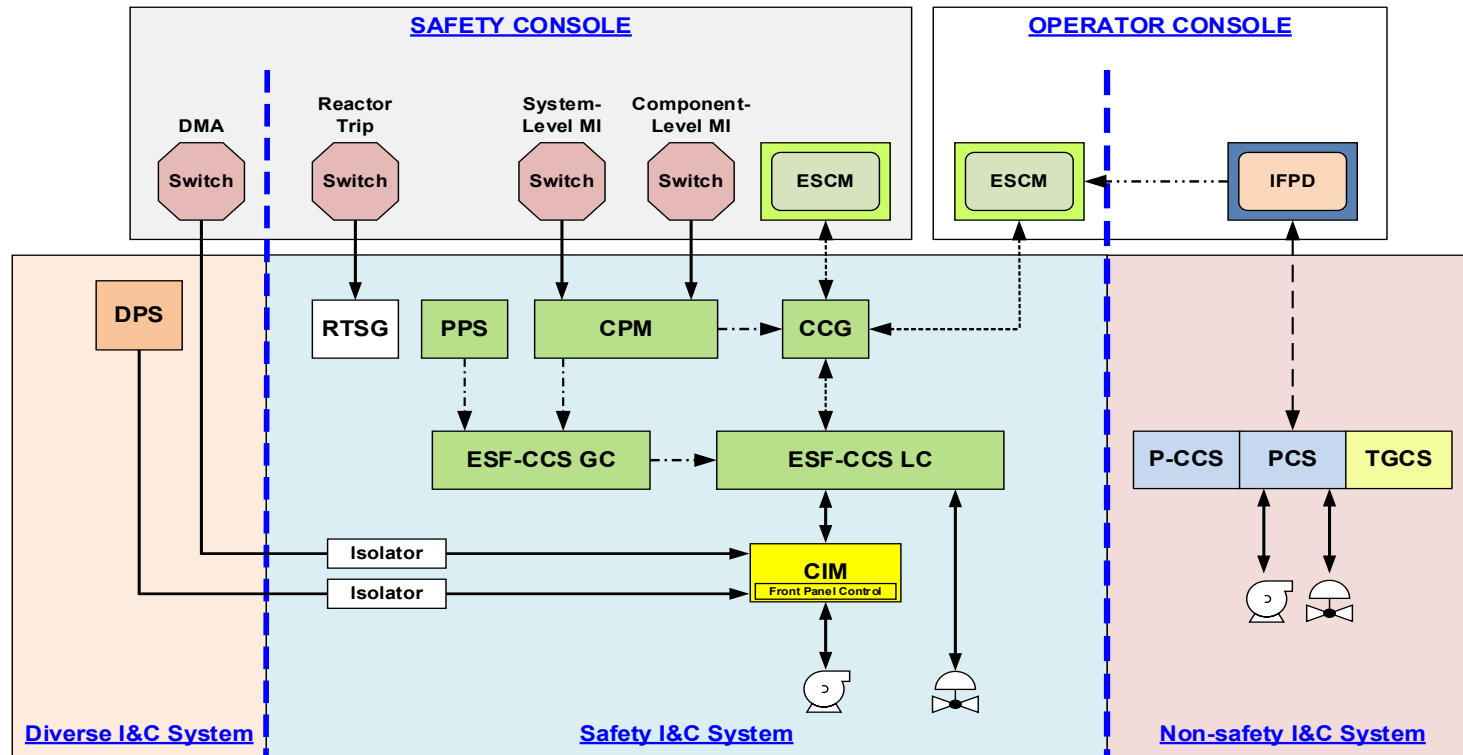
No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
31	MTP/ITP	a) General failure	Component failure	MTP display becomes “frozen” and does not update or respond to technician inputs; for ITP failure, many displays are marked “BAD” quality.	<ul style="list-style-type: none"> ITP process station monitors MTP health via redundant SDN. ITP activates diagnostic alarm on loss of data update. 	Four ESF divisions provide redundancy.	No safety function provided by the MTP/ITP.	<ul style="list-style-type: none"> The MTP process station is located in the same cabinet at the ITP process stations. It provides local display of the division status, and provides the means to conduct surveillance testing of the division (done during plant shutdown) as well as software maintenance of the various processors within the division.
32	MCR power supply 120 Vac	a) Off or output too low	<ul style="list-style-type: none"> Inverter failure Tripped circuit breaker Open fuse 	All components in the console are de-energized.	Annunciation, ITP detects loss of heartbeat signal from the affected division.	Four ESF divisions provide redundancy for system-level ESF actuations.	One of the four operator consoles loses its monitoring and/control functions.	The 120 Vac is on the vital bus power supply system.

APR1400 DCD TIER 2

Table 7.3-8 (21 of 21)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on System	Remarks and Other Effects
33	RSR power supply 120 Vac	a) Off or output too low	<ul style="list-style-type: none"> • Inverter failure • Tripped circuit breaker • Open fuse 	All components in the console will be de-energized.	Annunciation; ITP detects loss of heartbeat signal from the affected division.	Four ESF divisions provide redundancy for ESF system-level actuations.	One of the four consoles loses its monitoring and/control functions.	The 120 Vac is on the vital bus power supply system.
34	ESCM FPD	a) Off or incorrect display	Component failure	No display or incorrect display.	<ul style="list-style-type: none"> • Trouble and disable alarm signals from ESF-CCS control status feedback. • Visual inspection by operator on ESCM FPD. 	Redundant ESCM at every console in the MCR and RSR.	ESFAS signals from the PPS and manual ESF system-level actuation switches override ESCM signals at all times.	The ESCMs receive component and process control selection commands from the IFPD via isolated fiber optic Ethernet connections.

APR1400 DCD TIER 2



ABBREVIATIONS AND LEGENDS

CCG: Control Channel Gateway
 CIM: Component Interface Module
 CPM: Control Panel Multiplexer
 DMA: Diverse Manual ESF Actuation
 DPS: Diverse Protection System
 ESCM: ESF-CCS Soft Control Module
 ESF-CCS: Engineered Safety Features-Component Control System
 FLC: Field Programmable Gate Array (FPGA)-based Logic Controller
 IFPD: Information Flat Panel Display
 MI: Minimum Inventory
 P-CCS: Process-Component Control System
 PCS: Power Control System
 PPS: Plant Protection System
 RTSG: Reactor Trip Switchgear
 TGCS: Turbine/Generator Control System

NOTE

The DPS outputs that are to execute safety injection actuation function and auxiliary feedwater actuation function are hardwired to the CIMs.
 The DMA switches that are related to the components for safe shutdown are hardwired to the CIMs.

Figure 7.3-1 Simplified Functional Diagram of the ESF-CCS

APR1400 DCD TIER 2

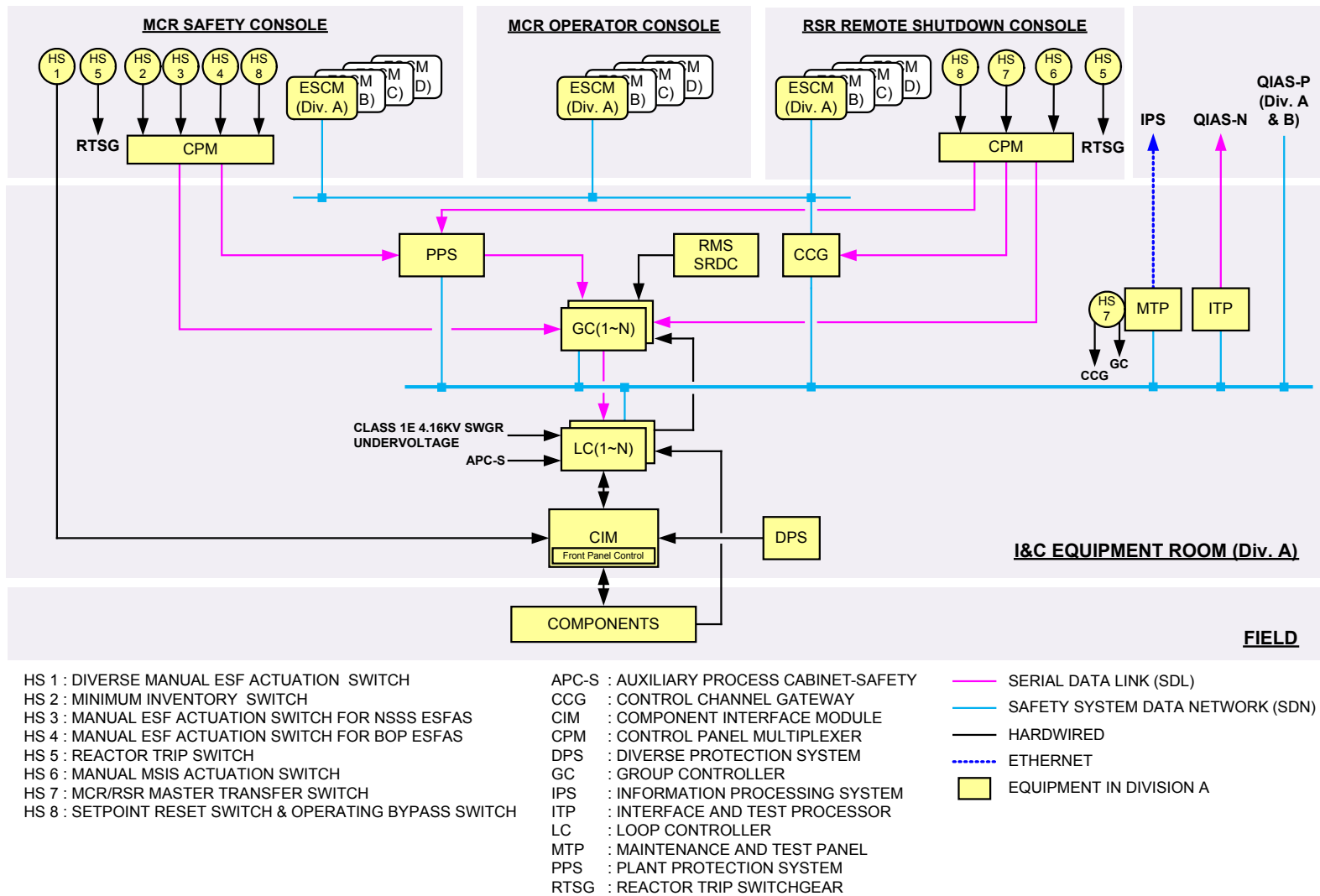


Figure 7.3-2 Block Diagram of the ESF-CCS

APR1400 DCD TIER 2

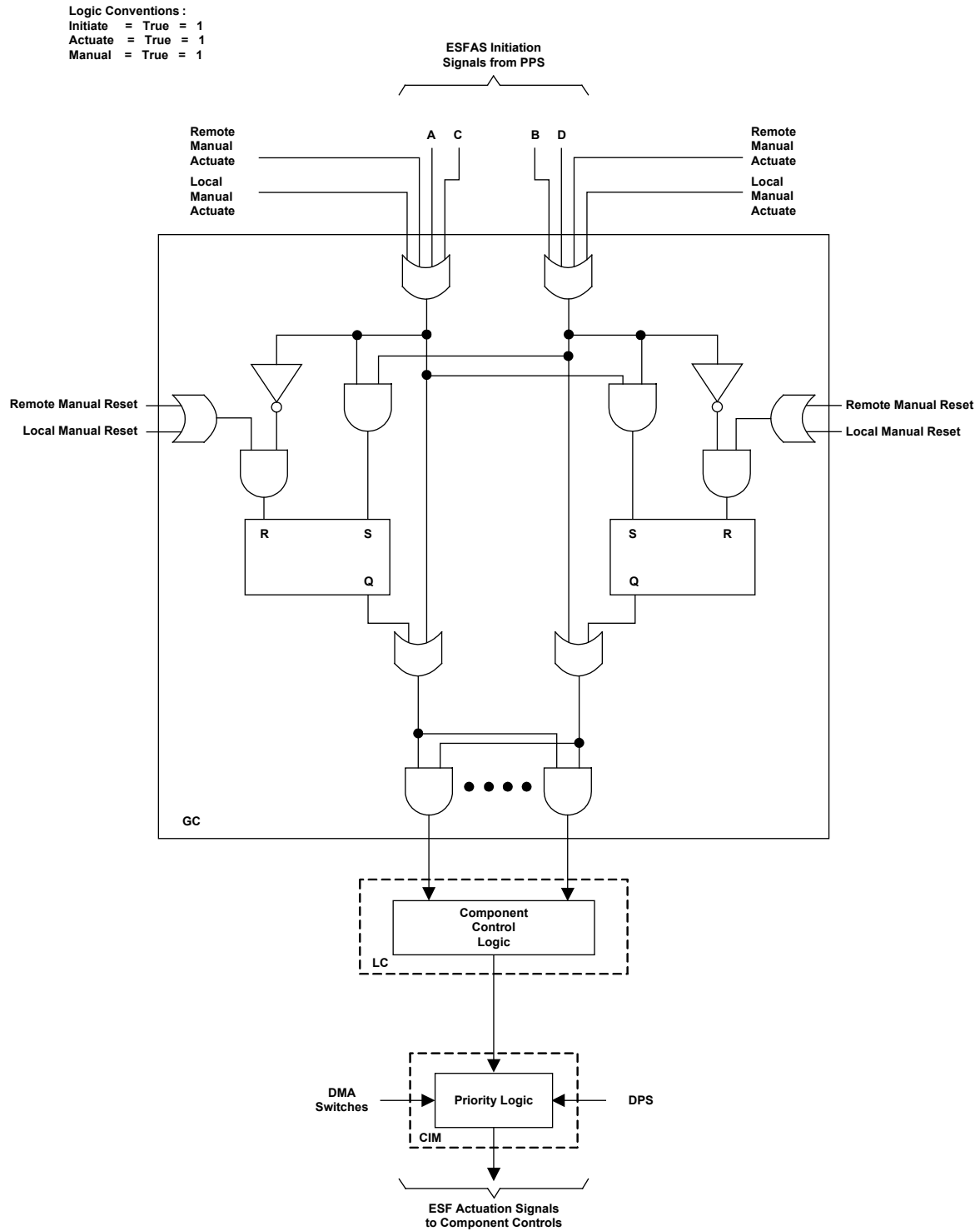


Figure 7.3-3 ESF-CCS Simplified Logic Diagram for 2-out-of-4 Actuation

APR1400 DCD TIER 2

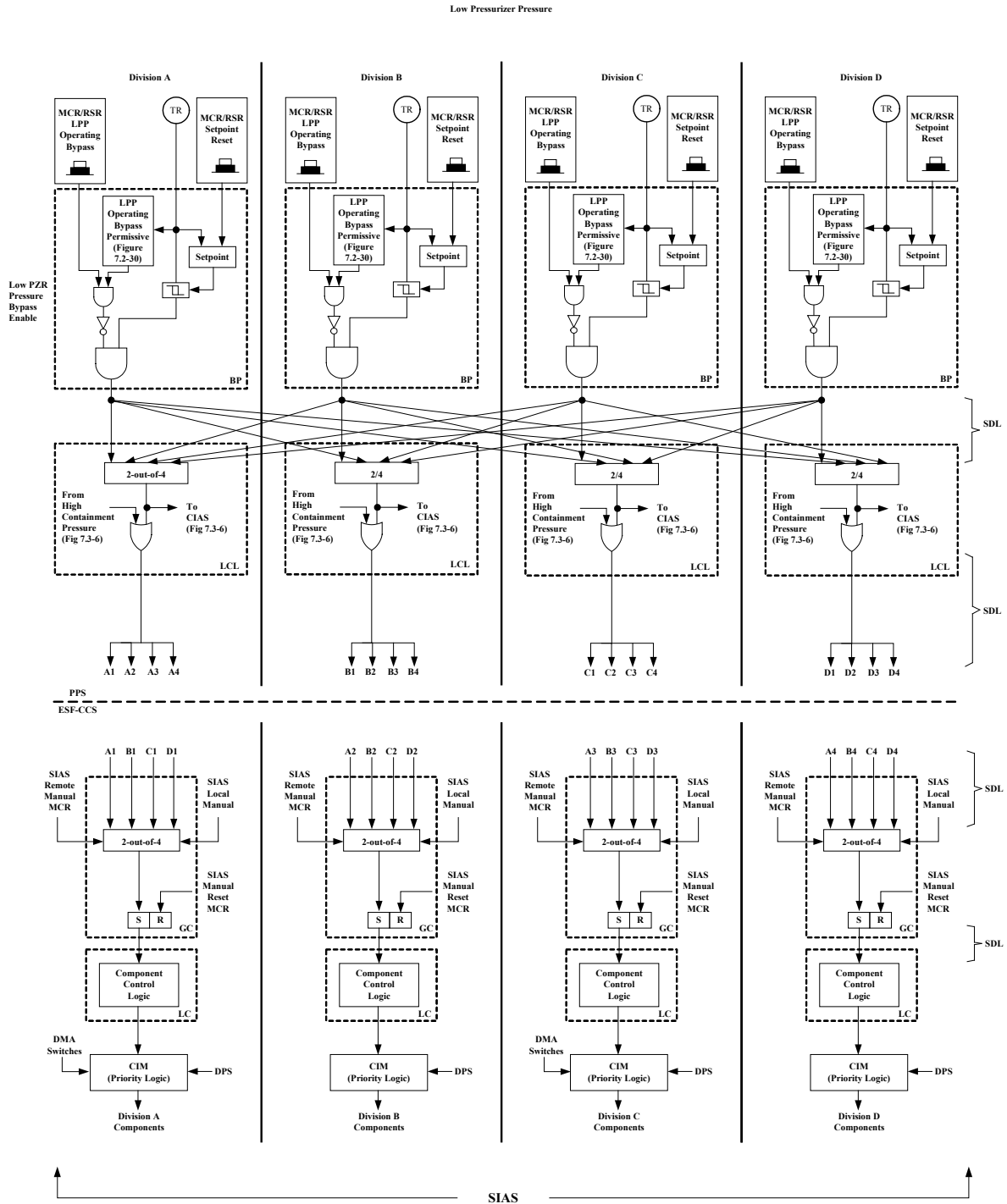


Figure 7.3-4 ESFAS Functional Logic (SIAS)

APR1400 DCD TIER 2

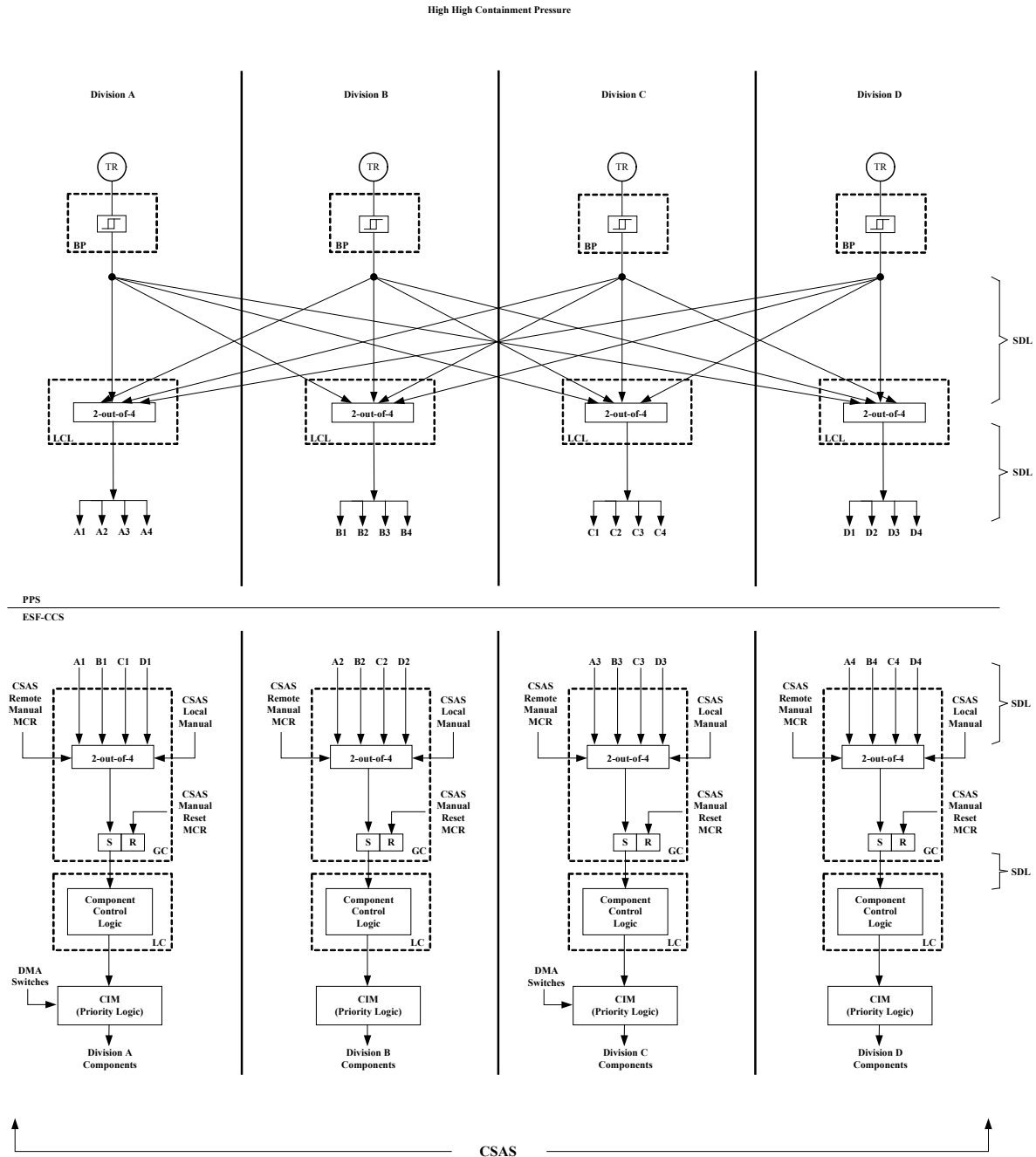


Figure 7.3-5 ESFAS Functional Logic (CSAS)

APR1400 DCD TIER 2

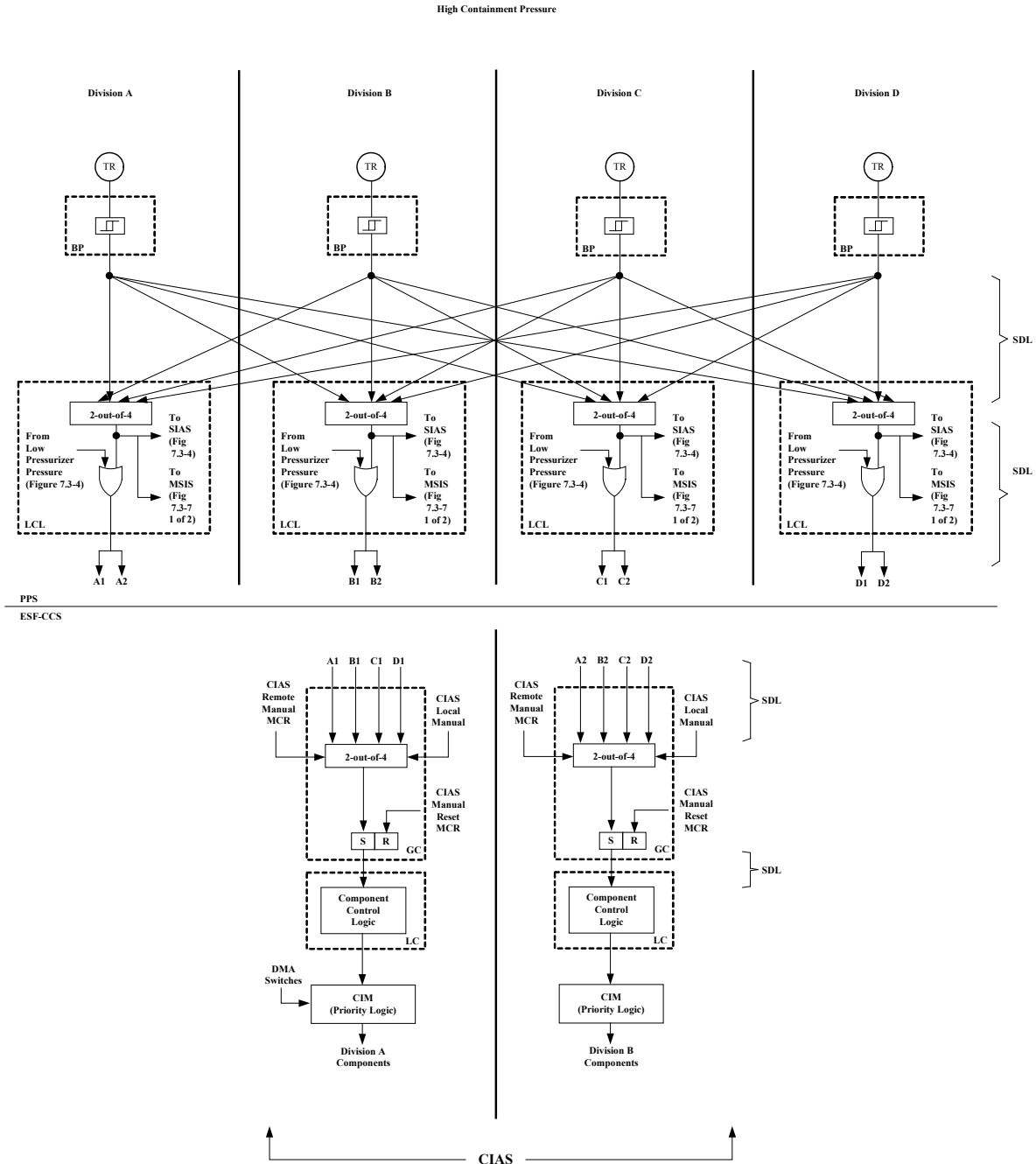


Figure 7.3-6 ESFAS Functional Logic (CIAS)

APR1400 DCD TIER 2

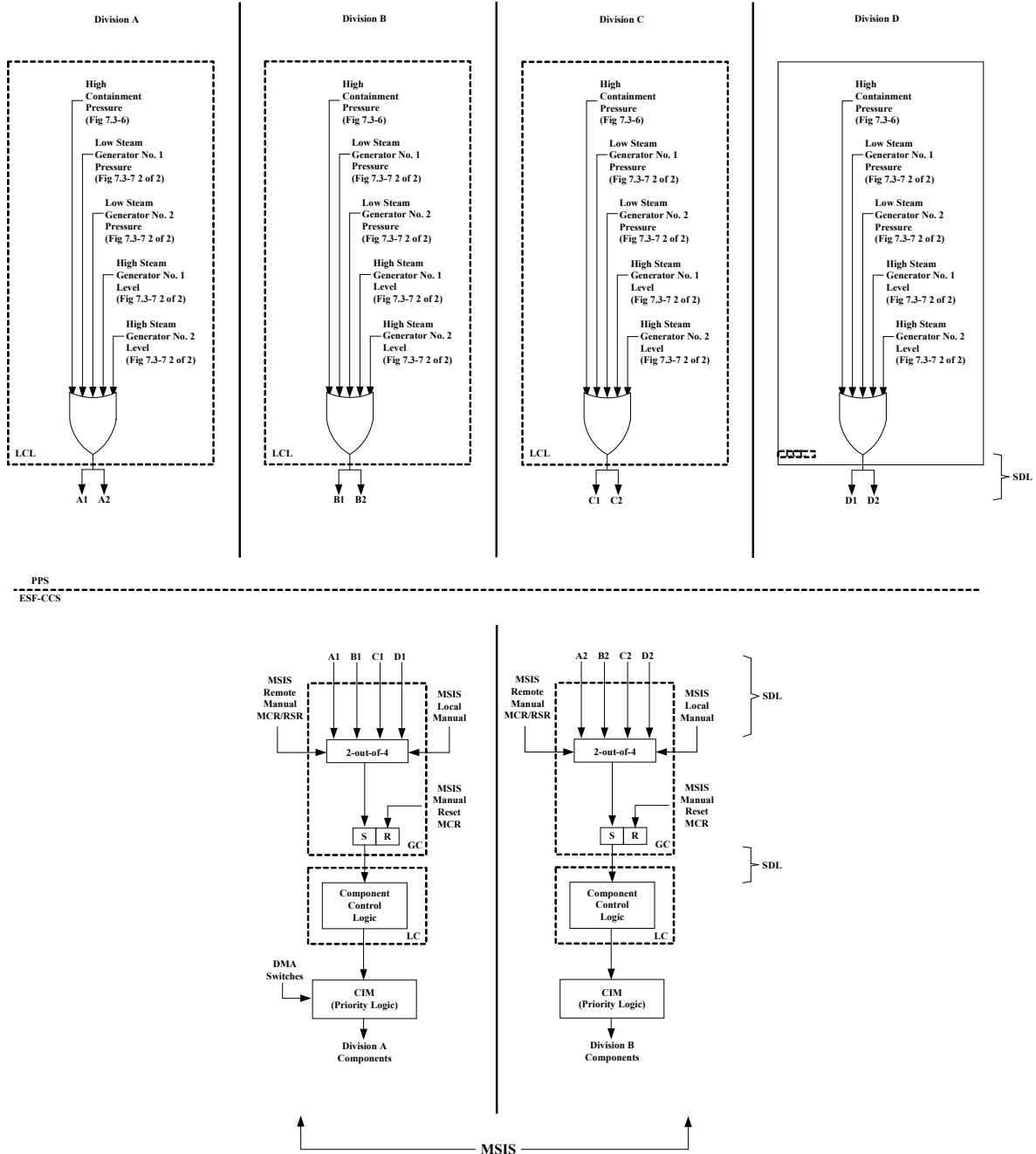
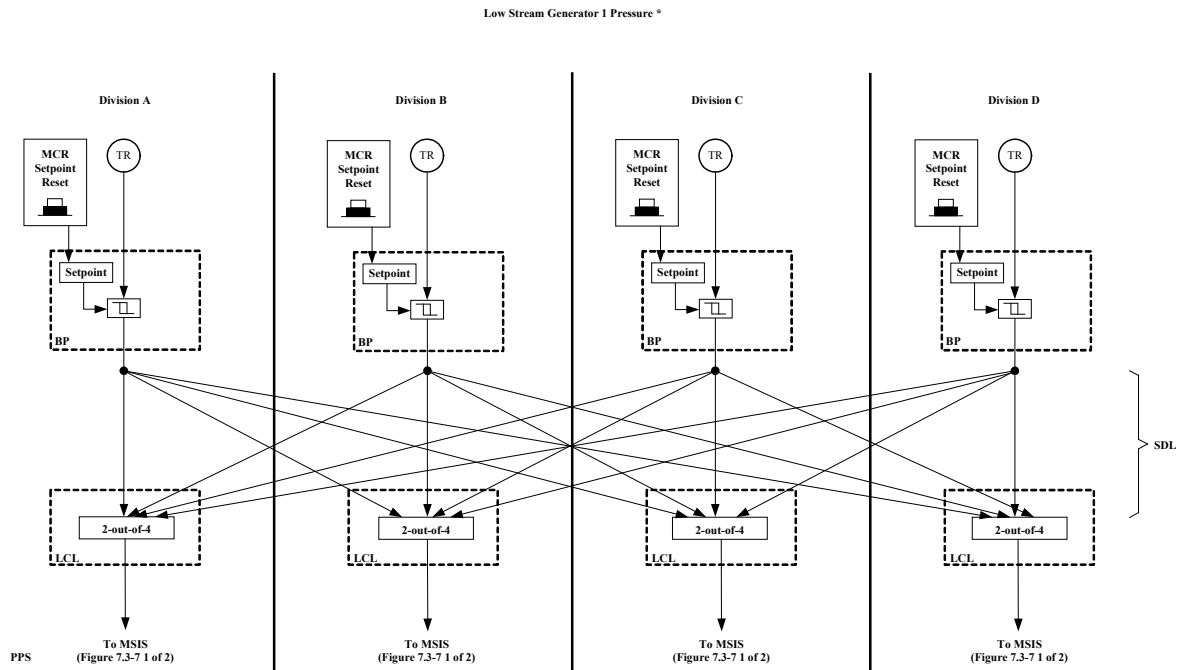
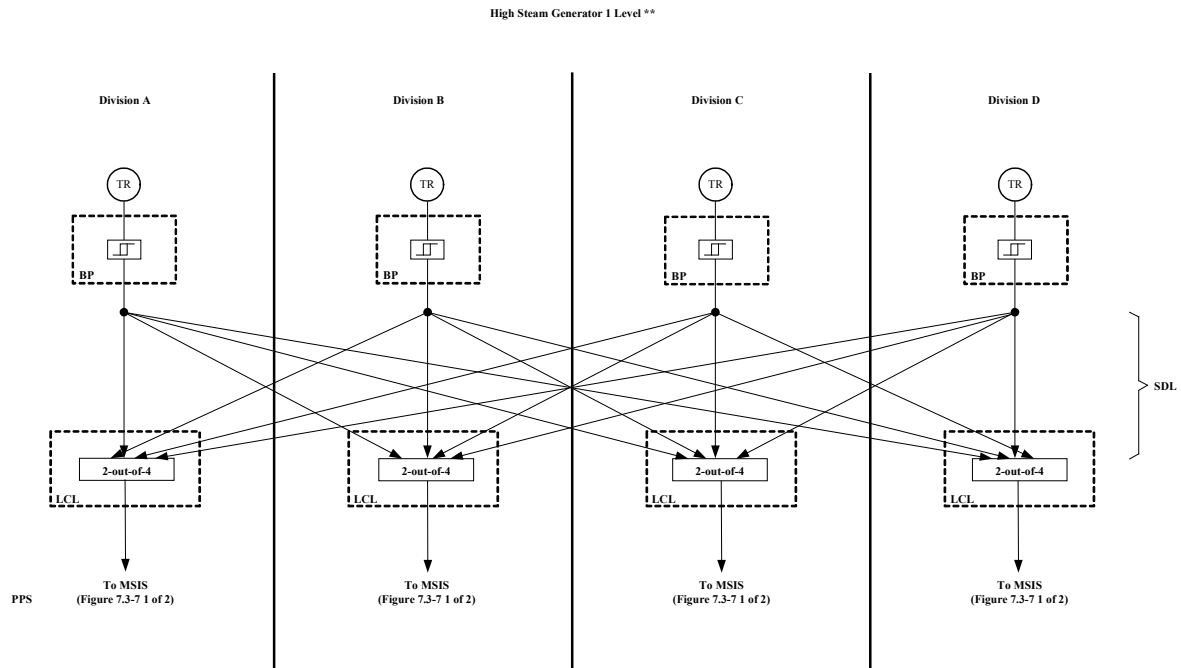


Figure 7.3-7 ESFAS Functional Logic (MSIS) (1 of 2)

APR1400 DCD TIER 2



* LSGP 2 Logic is same as LSGP 1 Logic



** HSLG 2 Logic is same as HSLG 1 Logic

Figure 7.3-7 ESFAS Functional Logic (MSIS) (2 of 2)

Low Stream Generator 1 Level



APR1400 DCD TIER 2

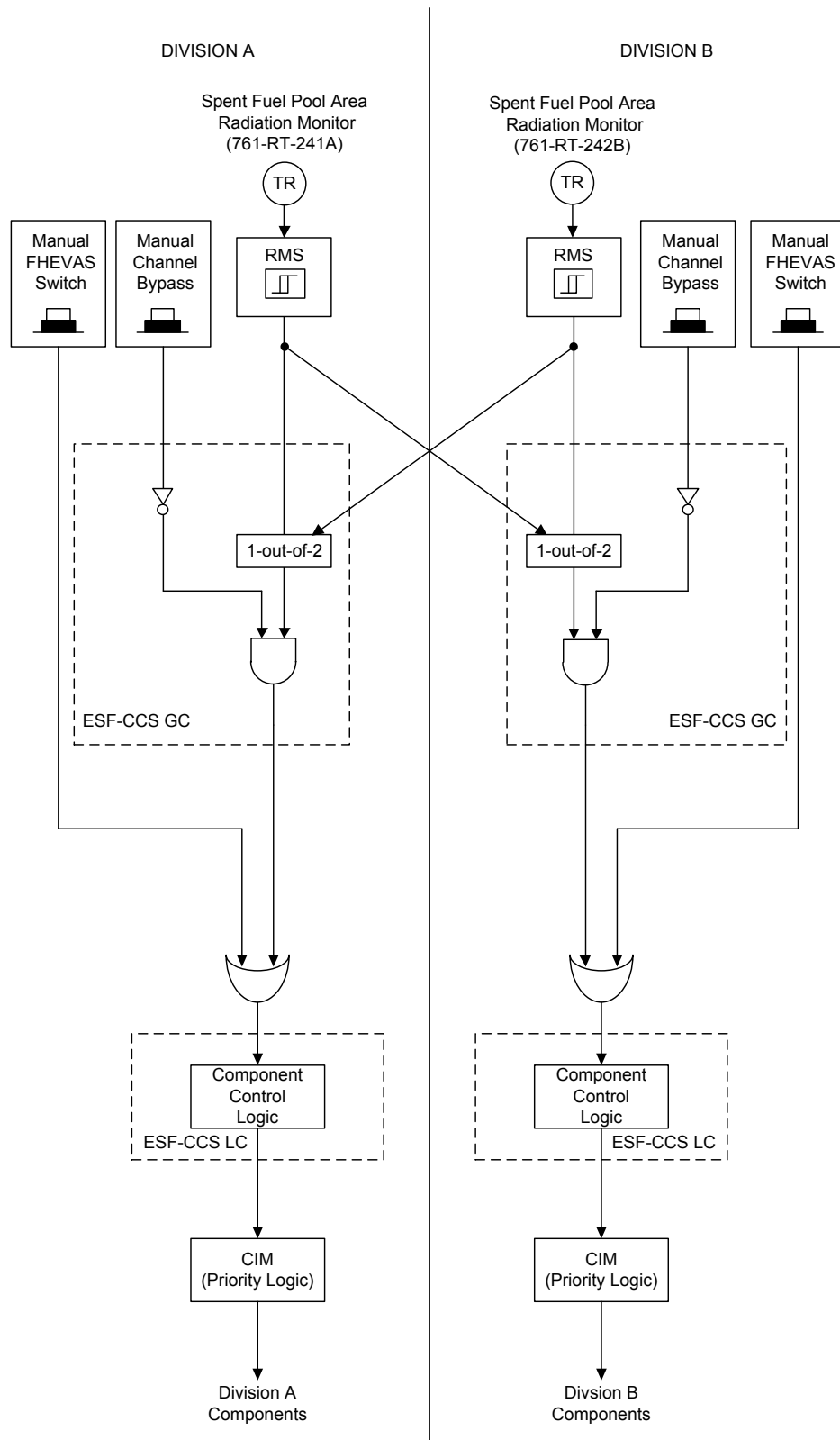


Figure 7.3-9 ESFAS Functional Logic (FHEVAS)

APR1400 DCD TIER 2

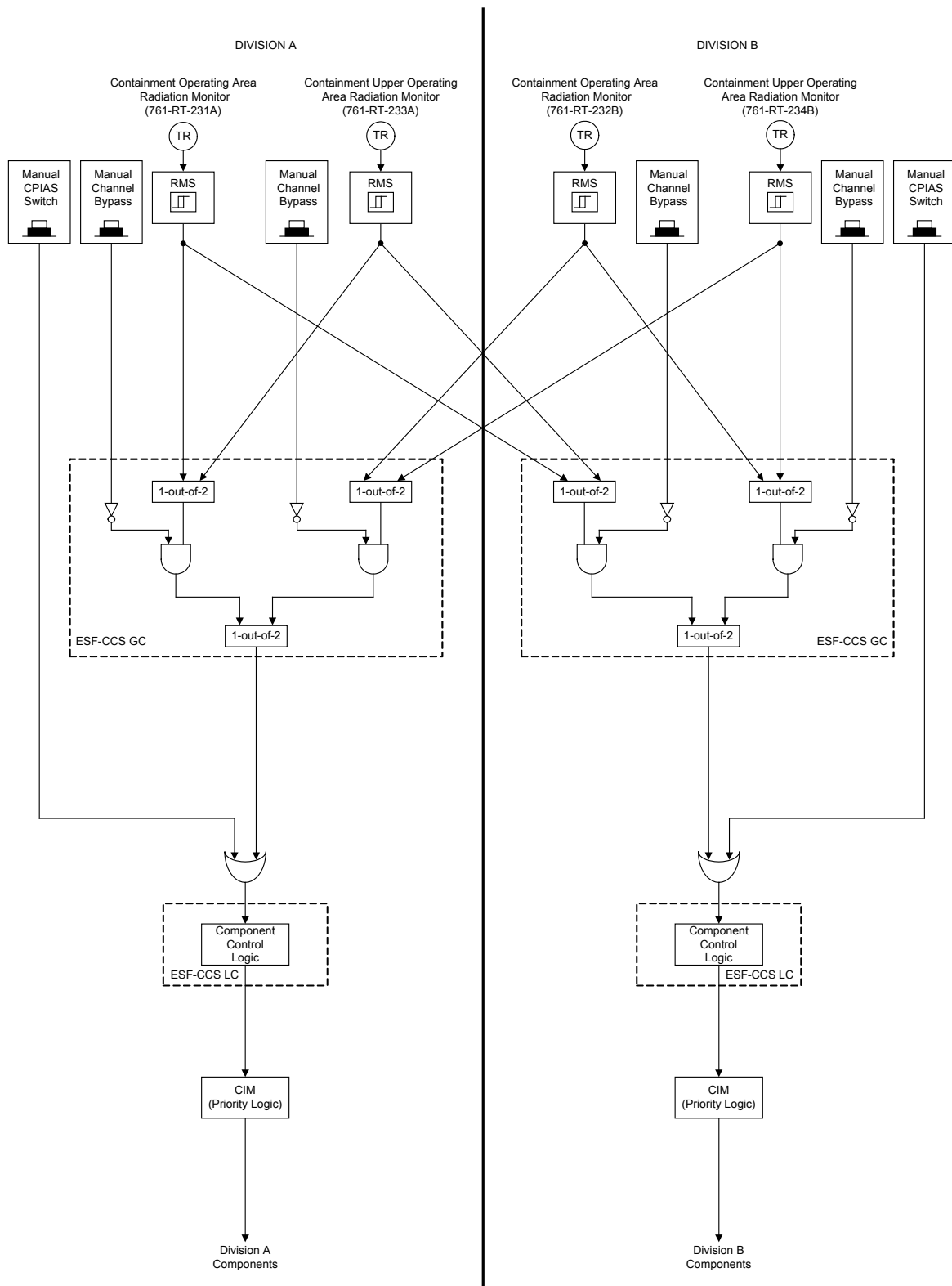


Figure 7.3-10 ESFAS Functional Logic (CPIAS)

APR1400 DCD TIER 2

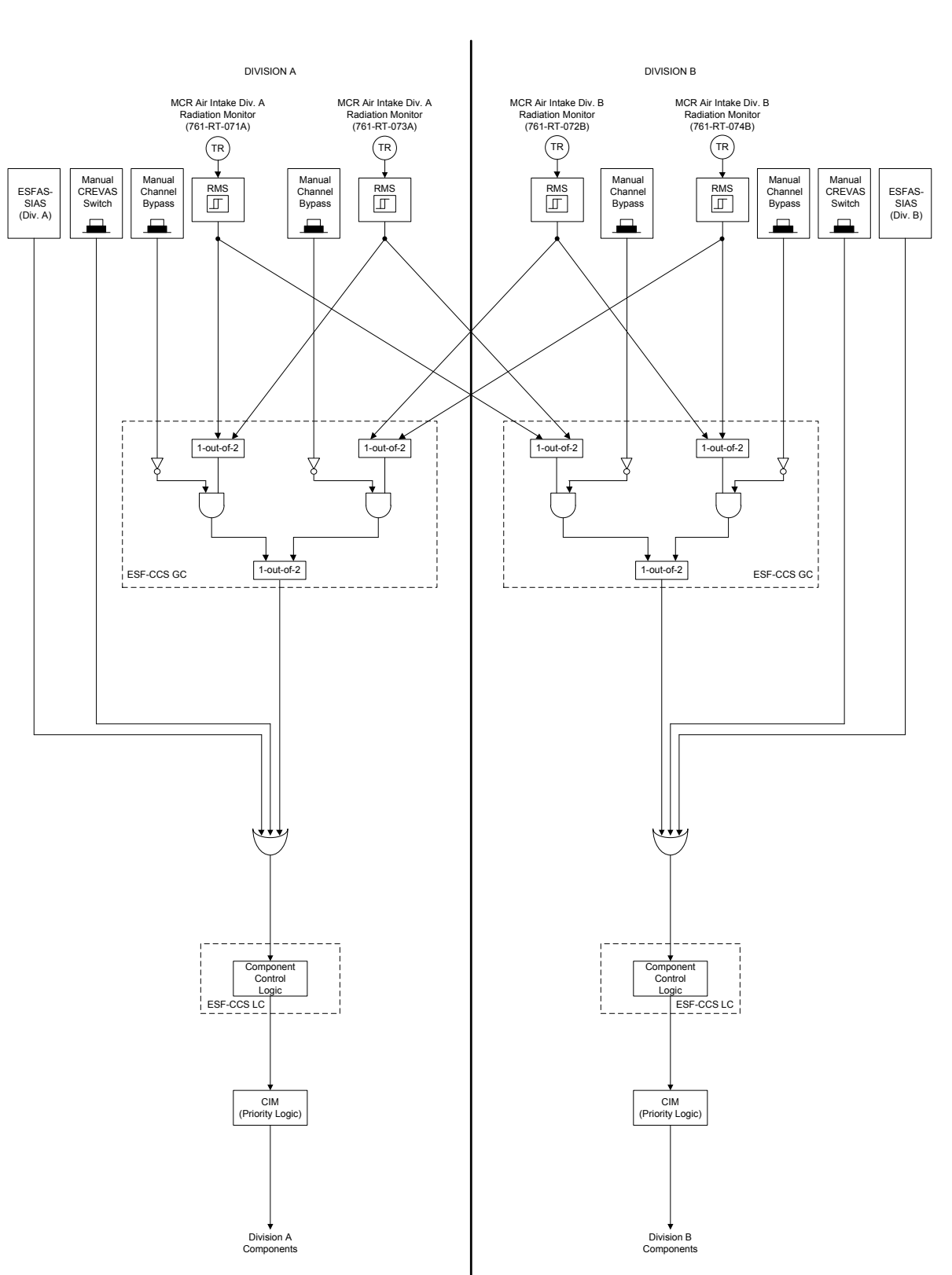


Figure 7.3-11 ESFAS Functional Logic (CREVAS)

APR1400 DCD TIER 2

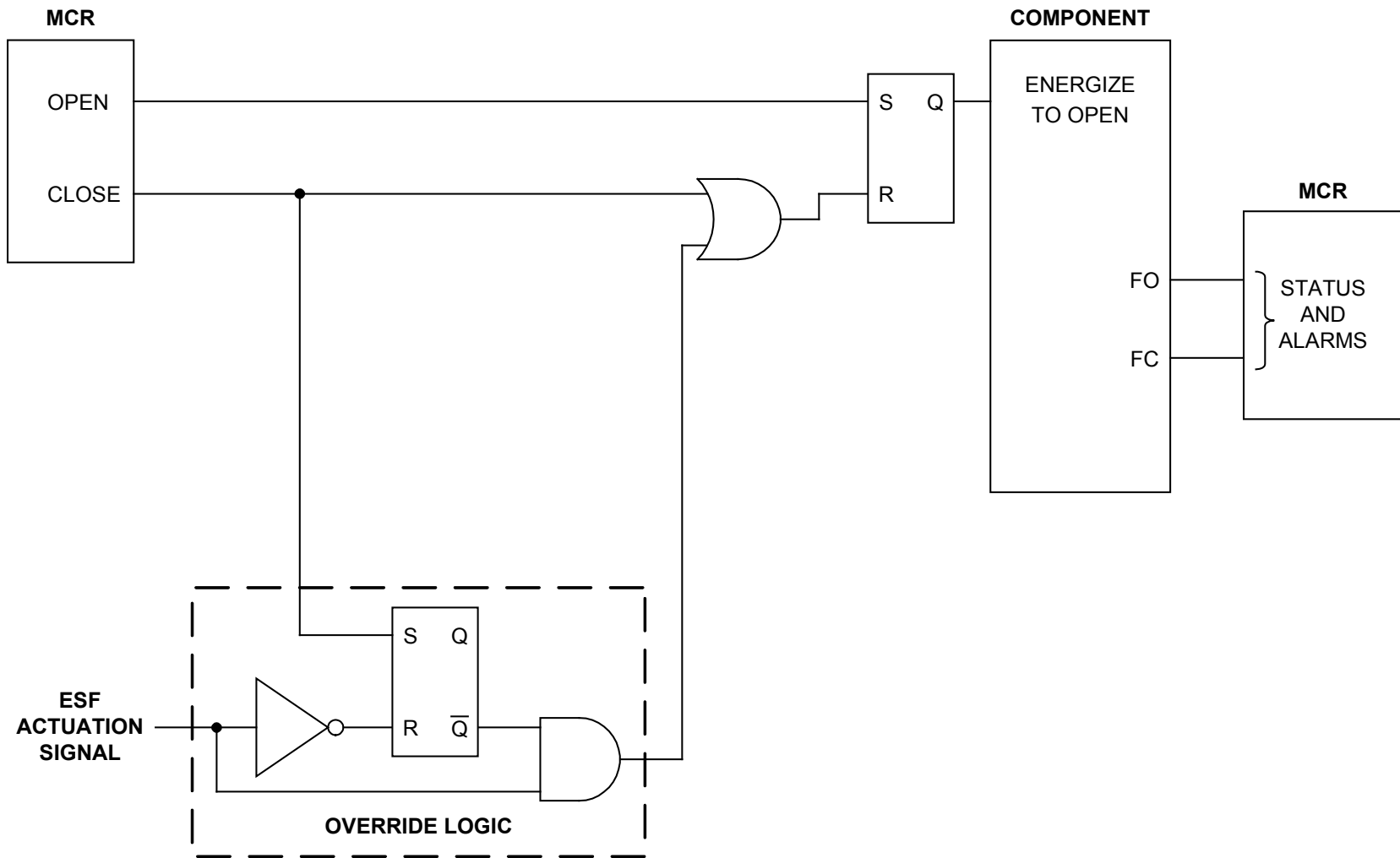


Figure 7.3-12 CLD for a Solenoid-Operated Valve

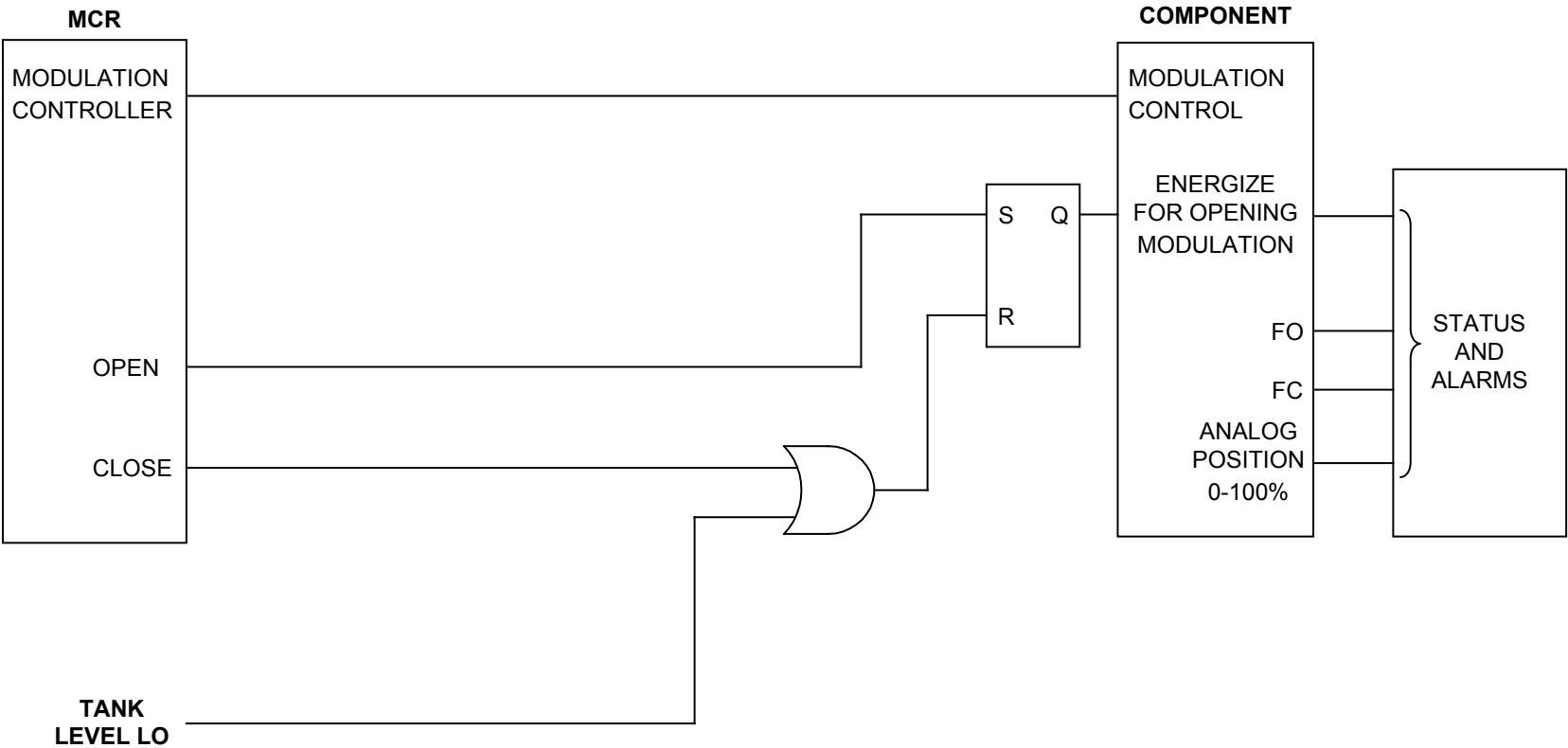


Figure 7.3-13 CLD for a Modulating Valve with Solenoid Operator

APR1400 DCD TIER 2

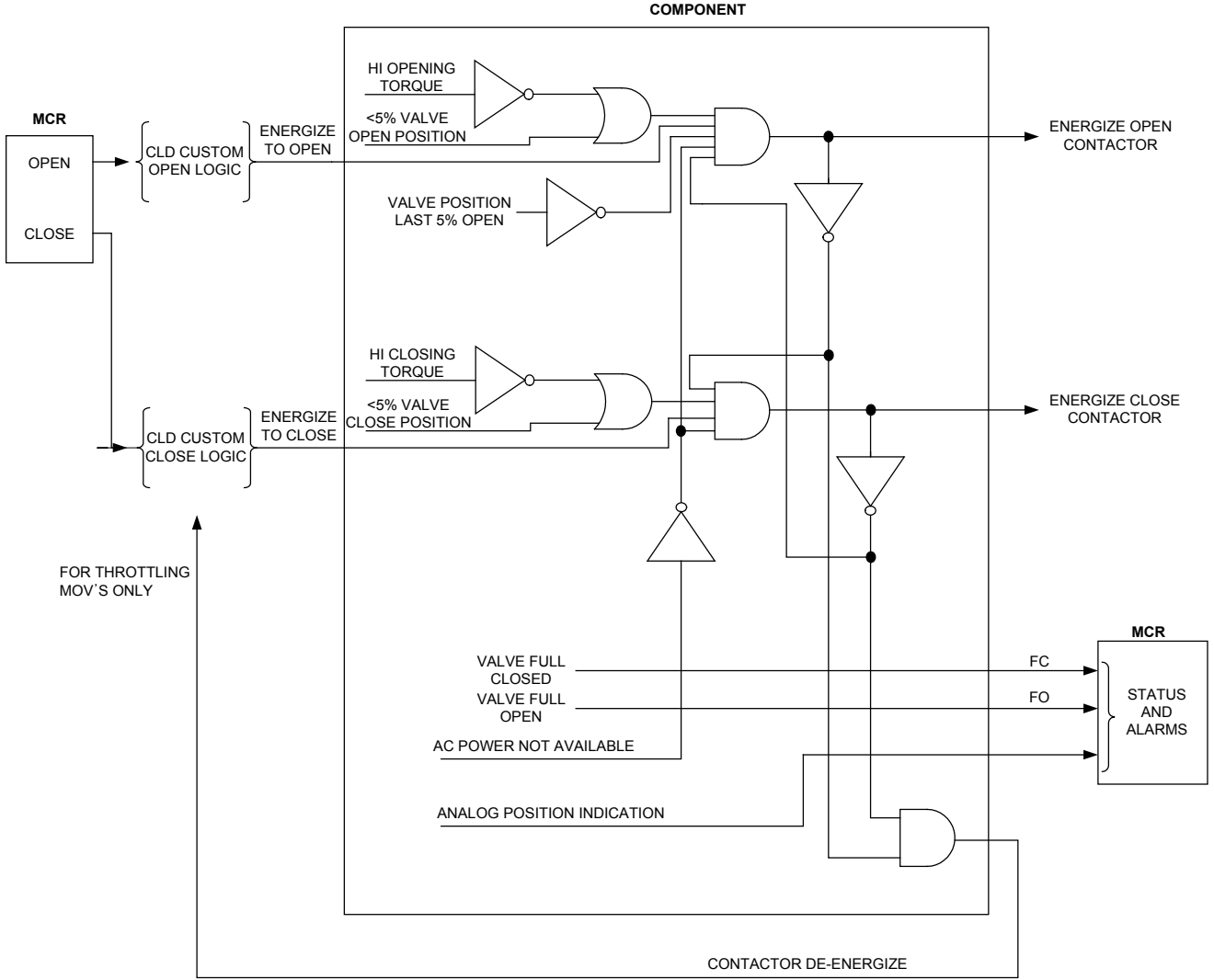


Figure 7.3-14 Motor-Operated Valve Functional Interface Design

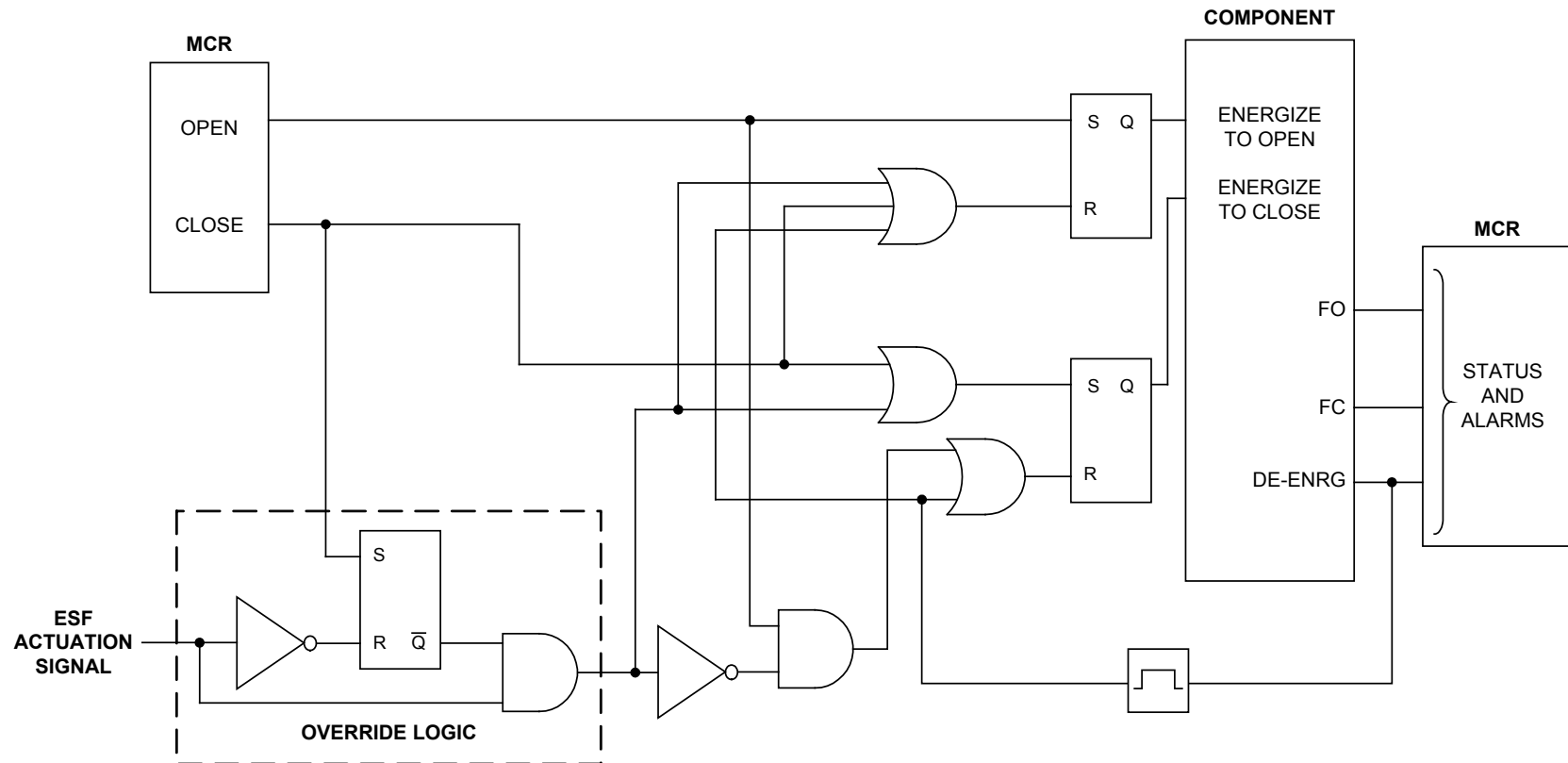


Figure 7.3-15 CLD for a Full Stroke Motor-Operated Valve

APR1400 DCD TIER 2

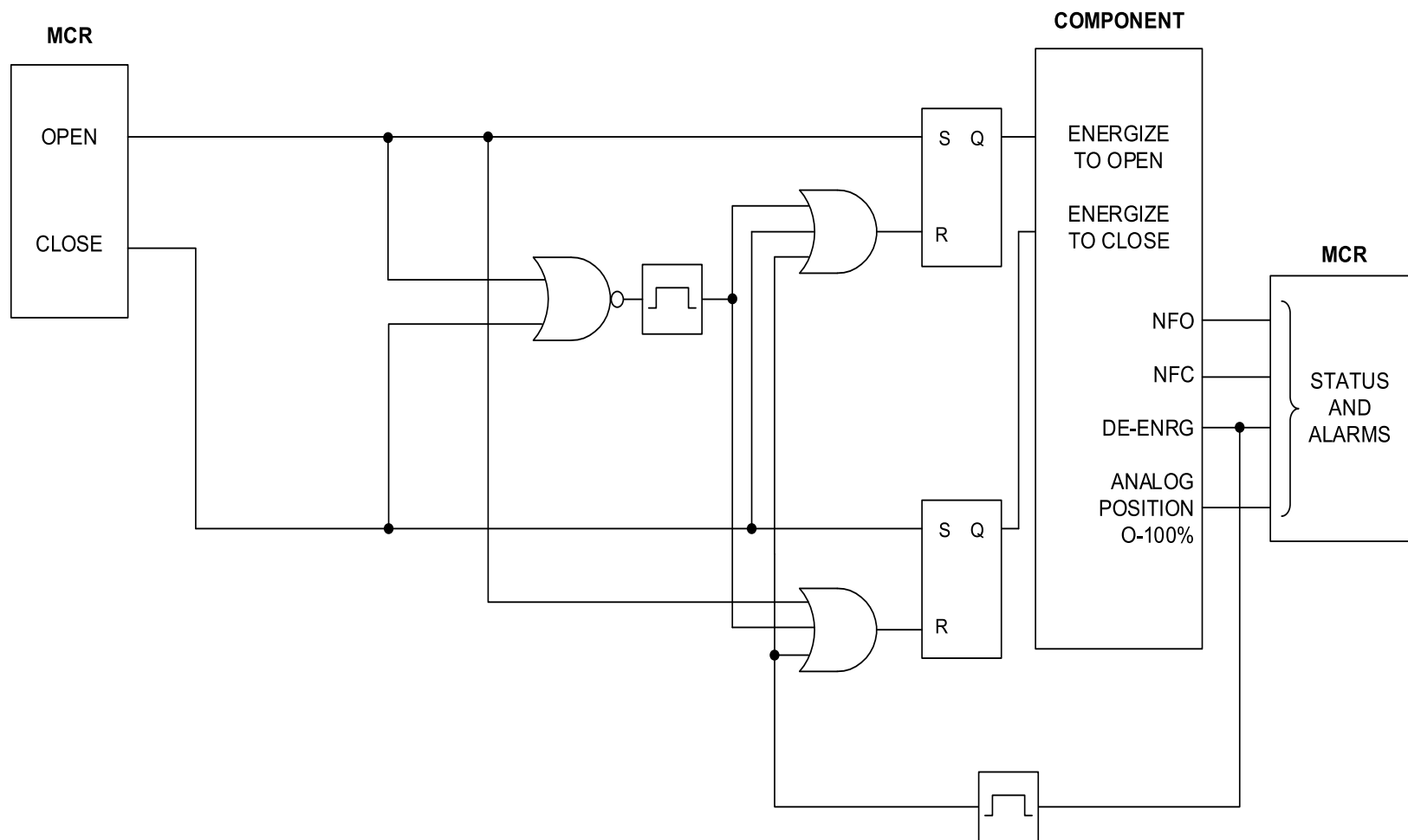


Figure 7.3-16 CLD for a Throttling Motor-Operated Valve

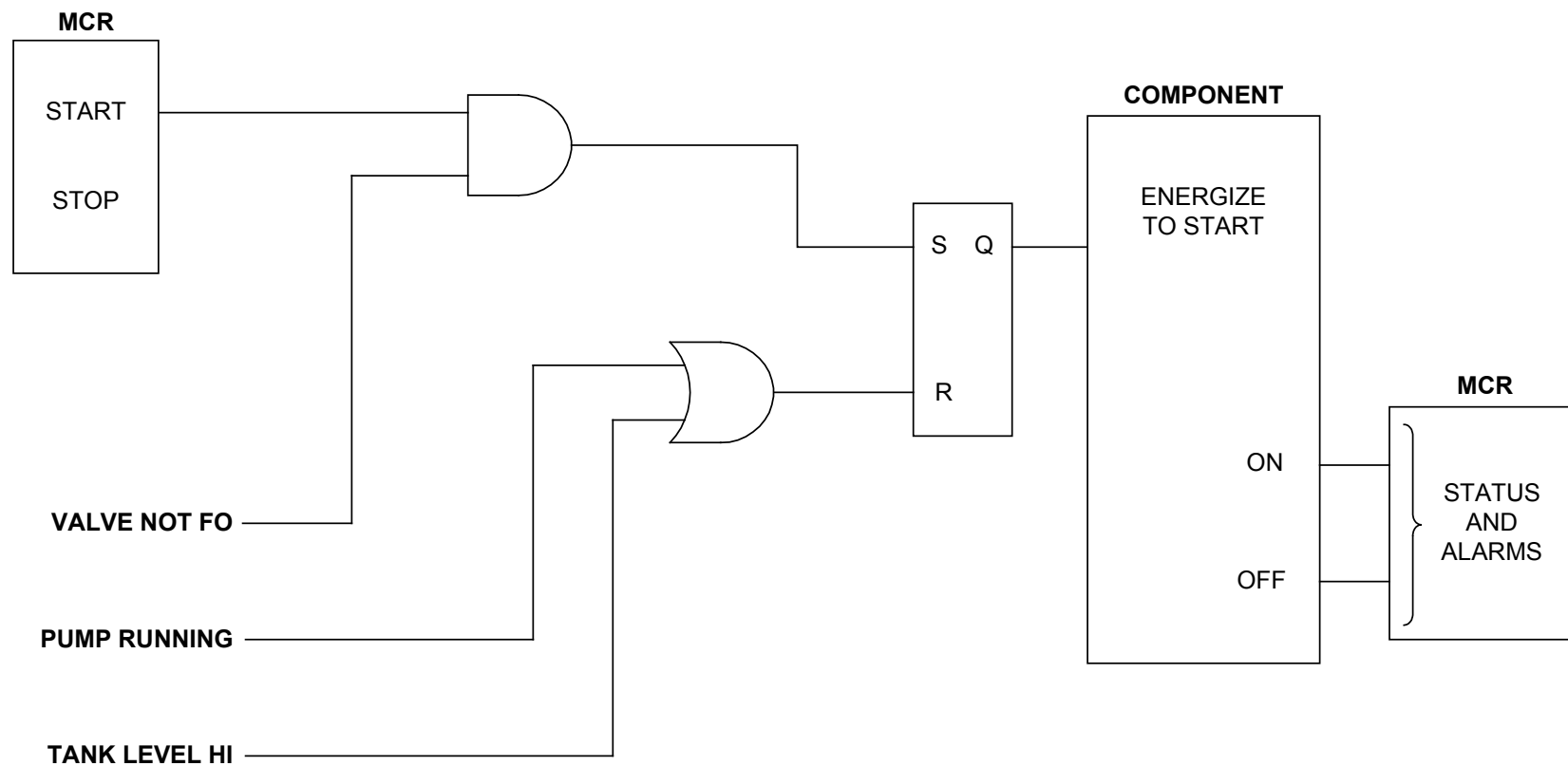


Figure 7.3-17 CLD for a Non-reversing Motor Starter Operated Component

APR1400 DCD TIER 2

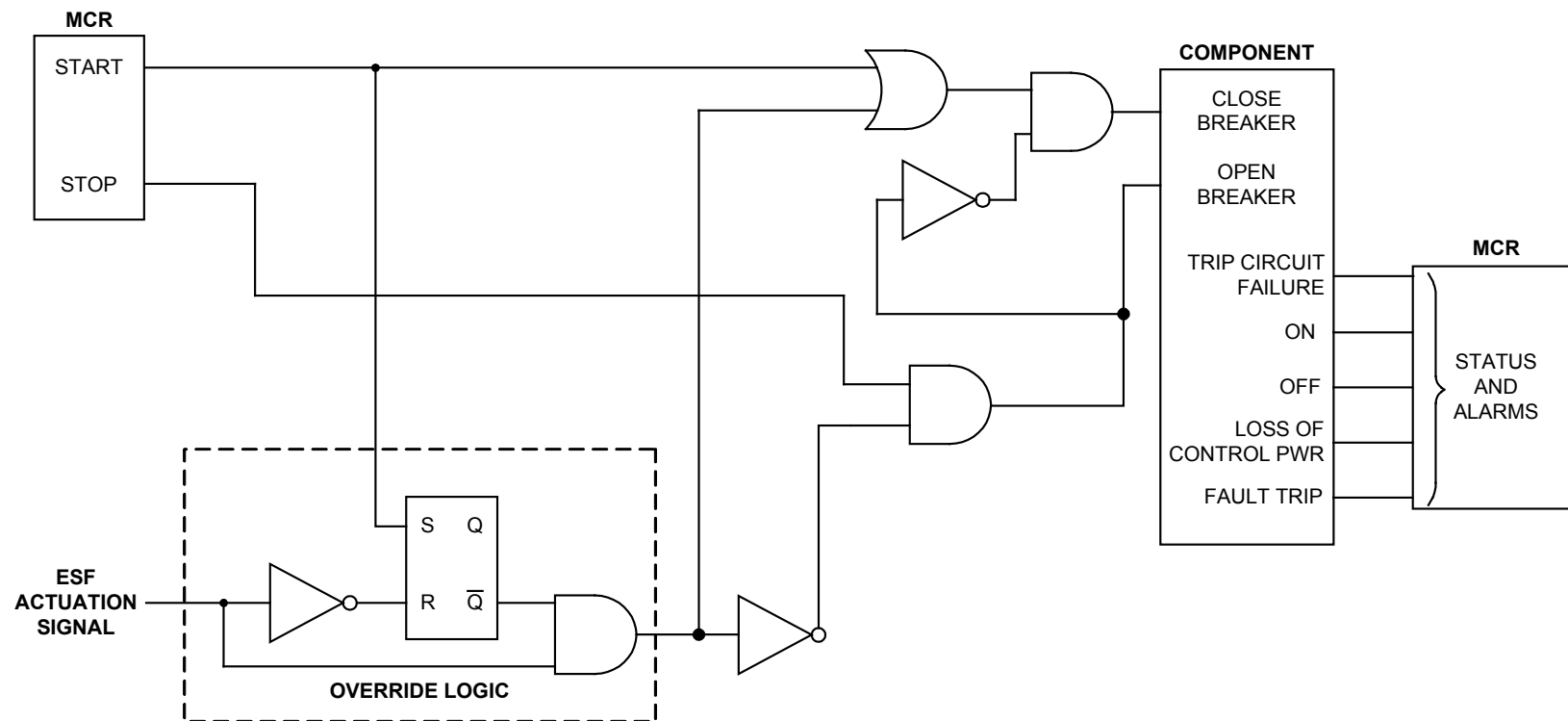


Figure 7.3-18 CLD for a Circuit Breaker Operated Component

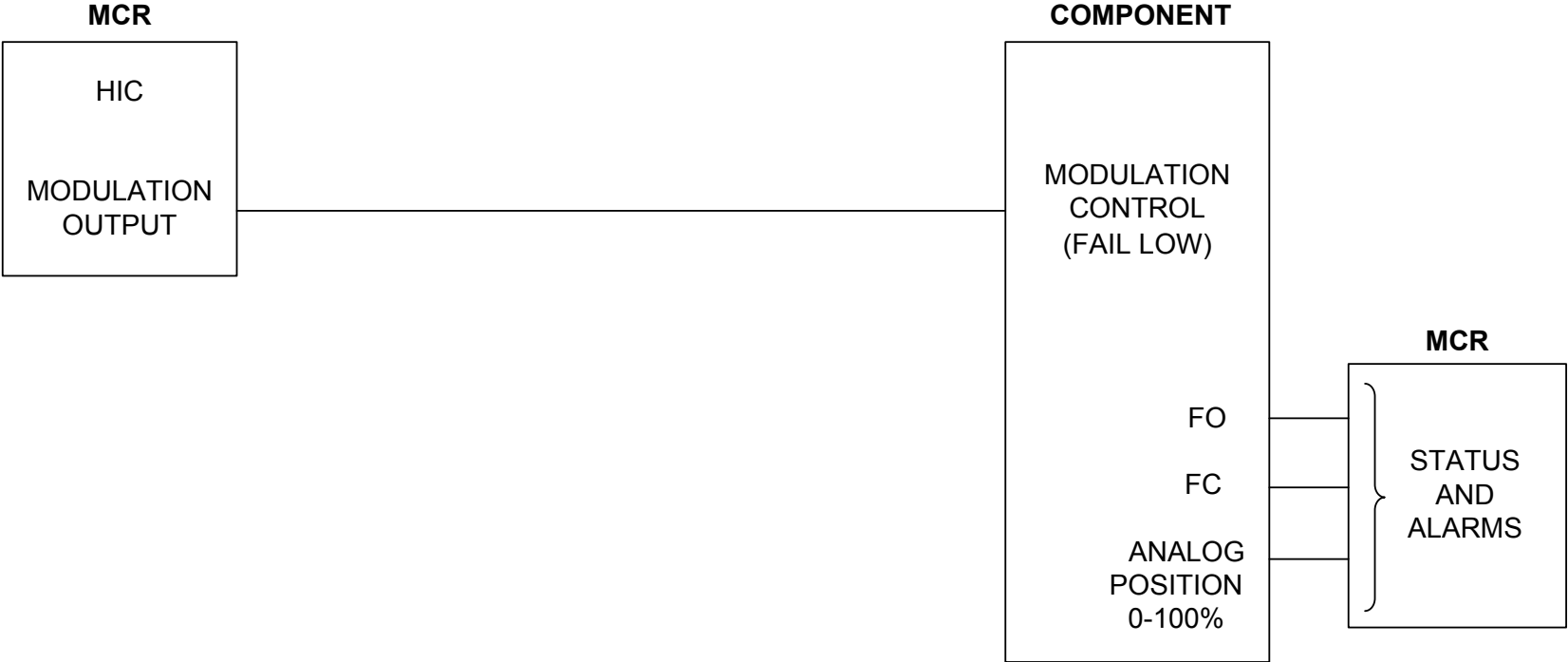


Figure 7.3-19 CLD for a Modulating Component

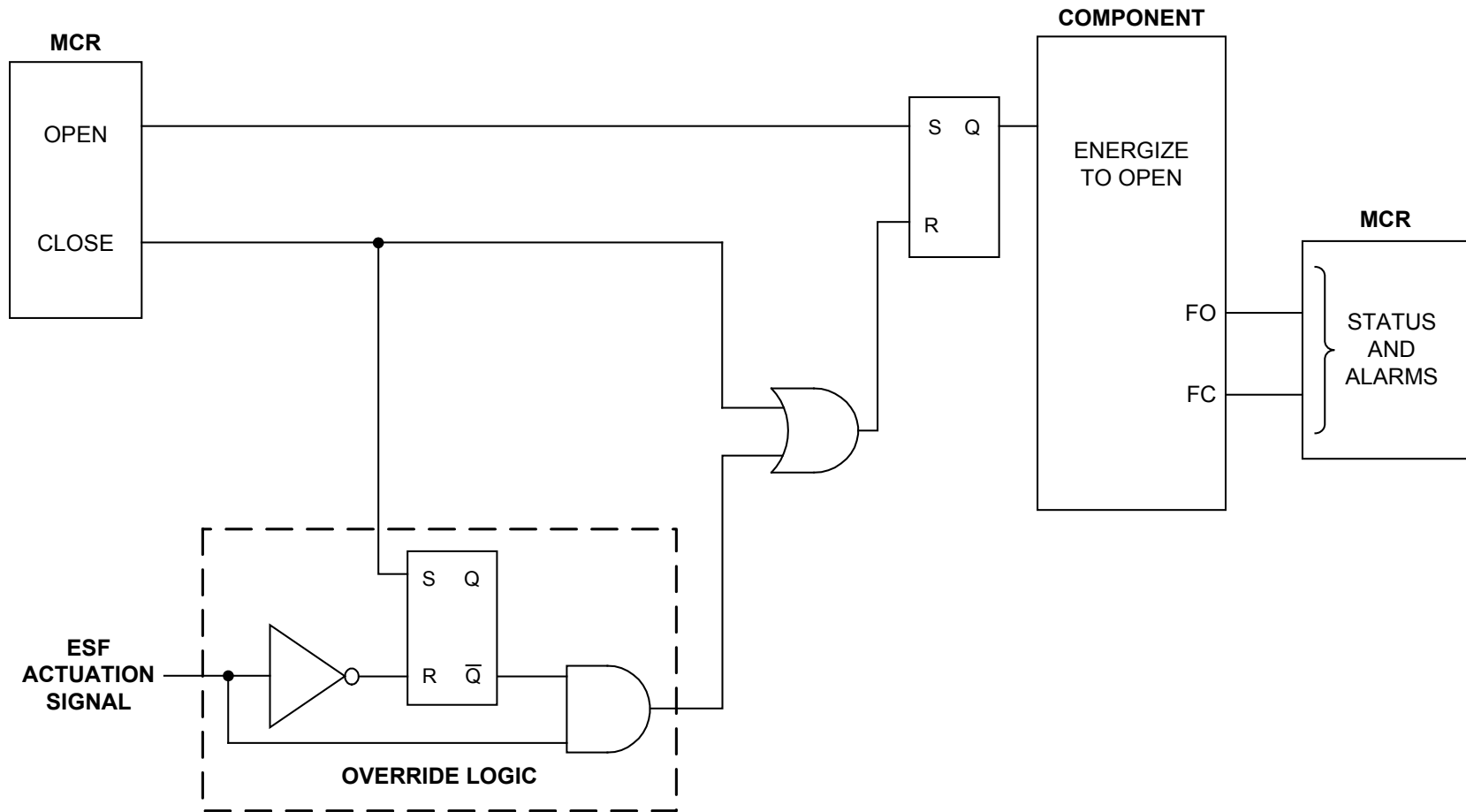


Figure 7.3-20 CLD for a Electro-Hydraulic Motor Damper

APR1400 DCD TIER 2

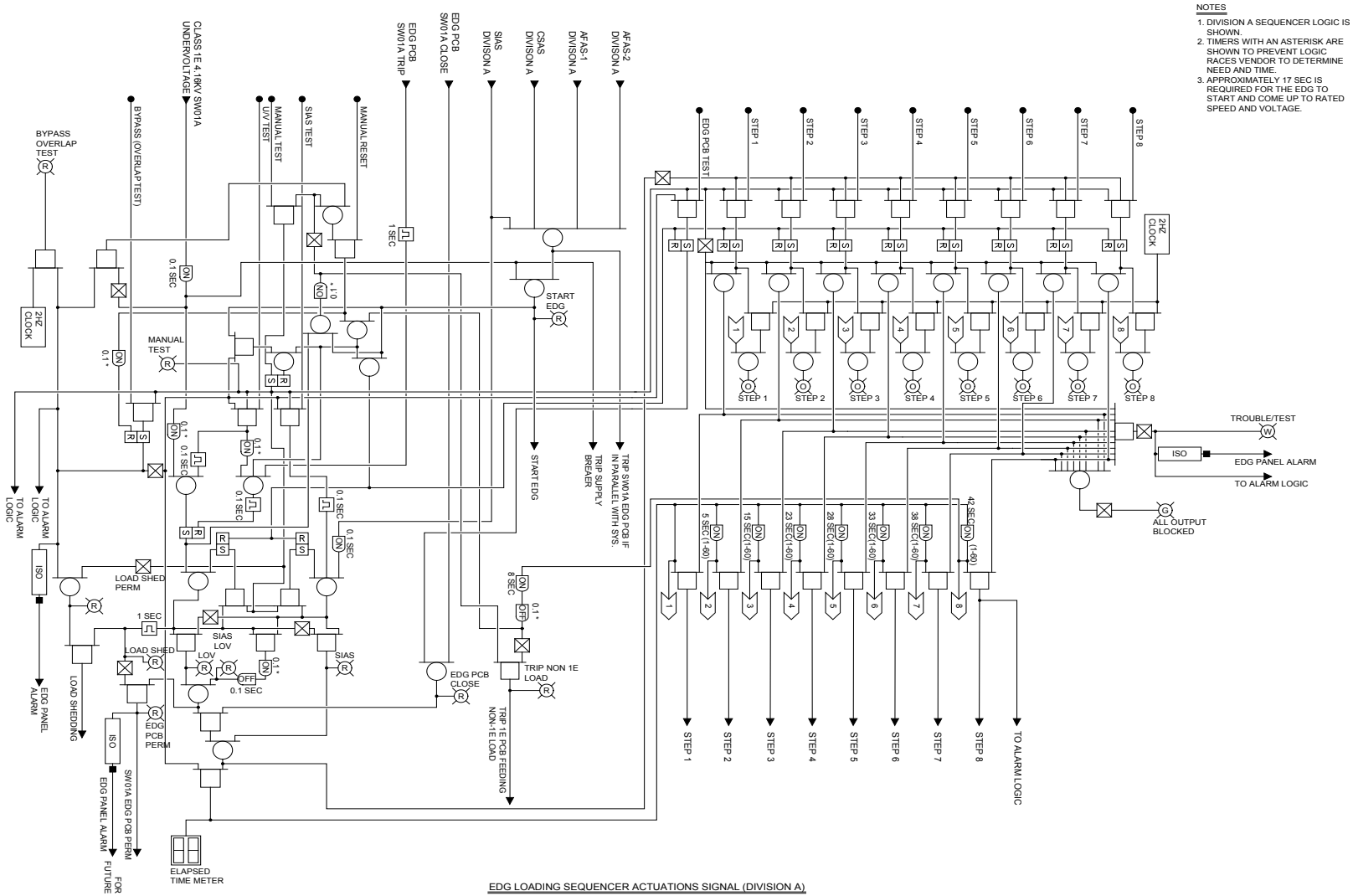


Figure 7.3-21 EDG Loading Sequencer – Control Logic Diagram (1 of 4)

APR1400 DCD TIER 2

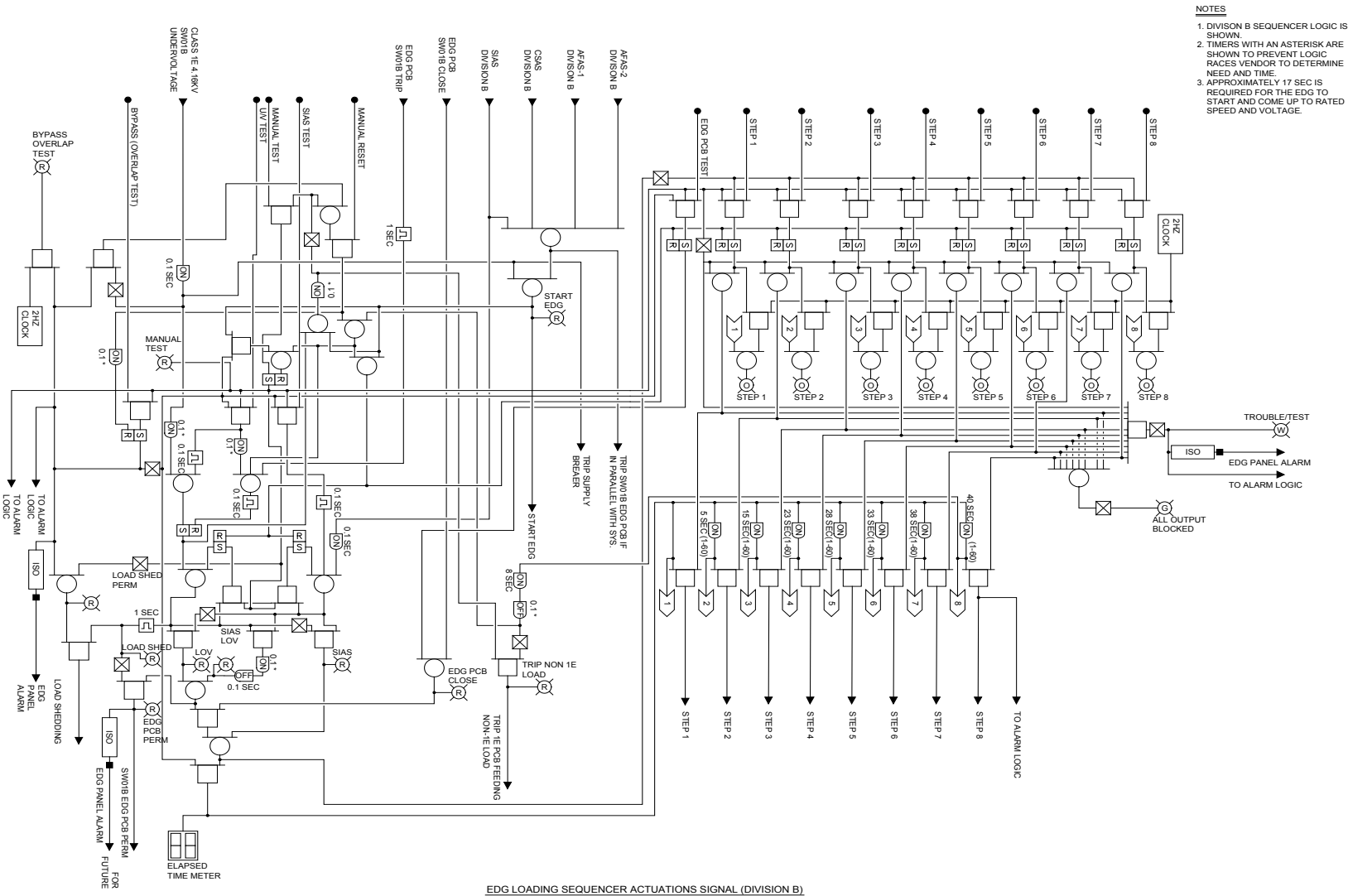


Figure 7.3-21 EDG Loading Sequencer – Control Logic Diagram (2 of 4)

APR1400 DCD TIER 2

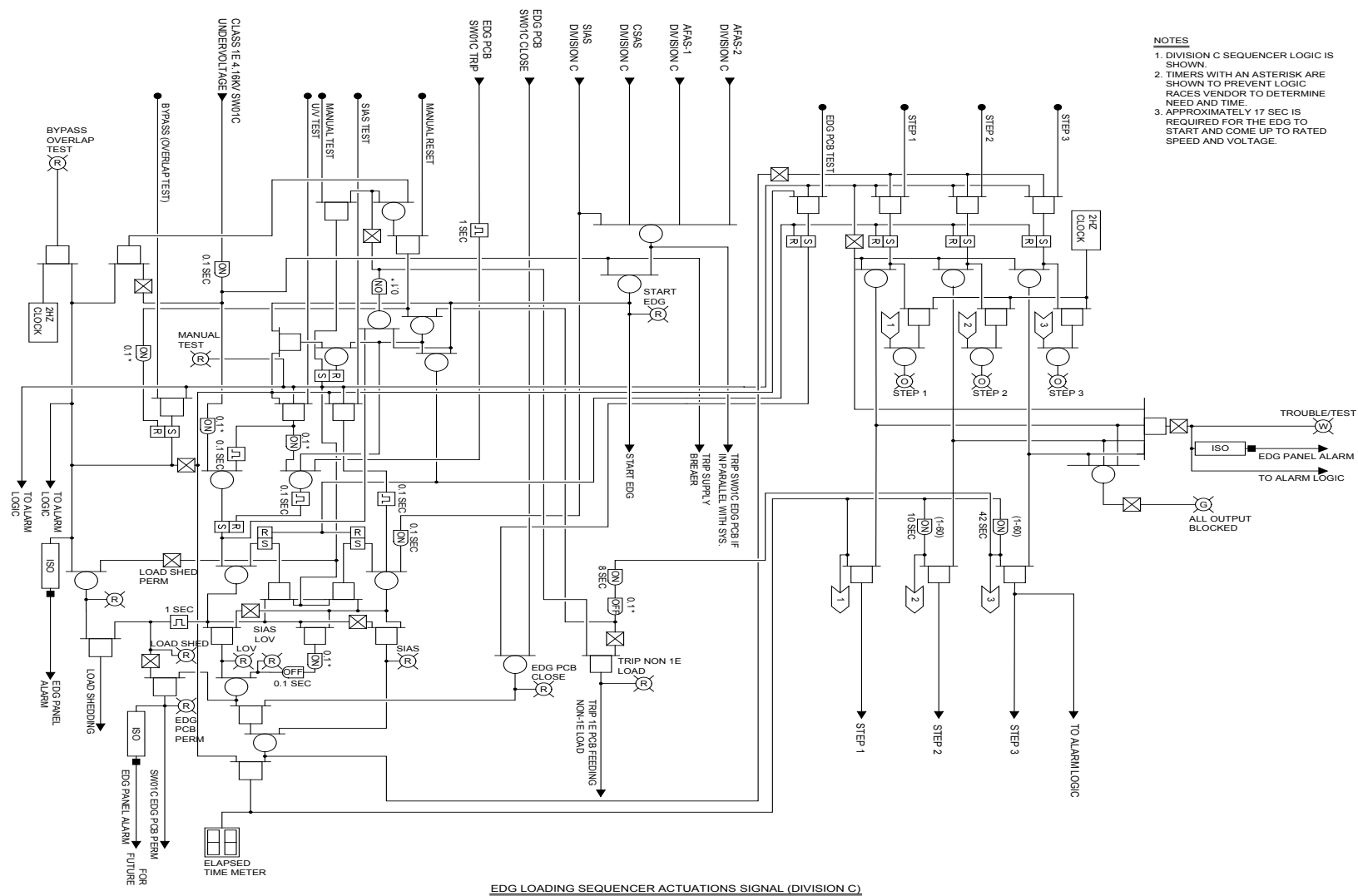


Figure 7.3-21 EDG Loading Sequencer – Control Logic Diagram (3 of 4)

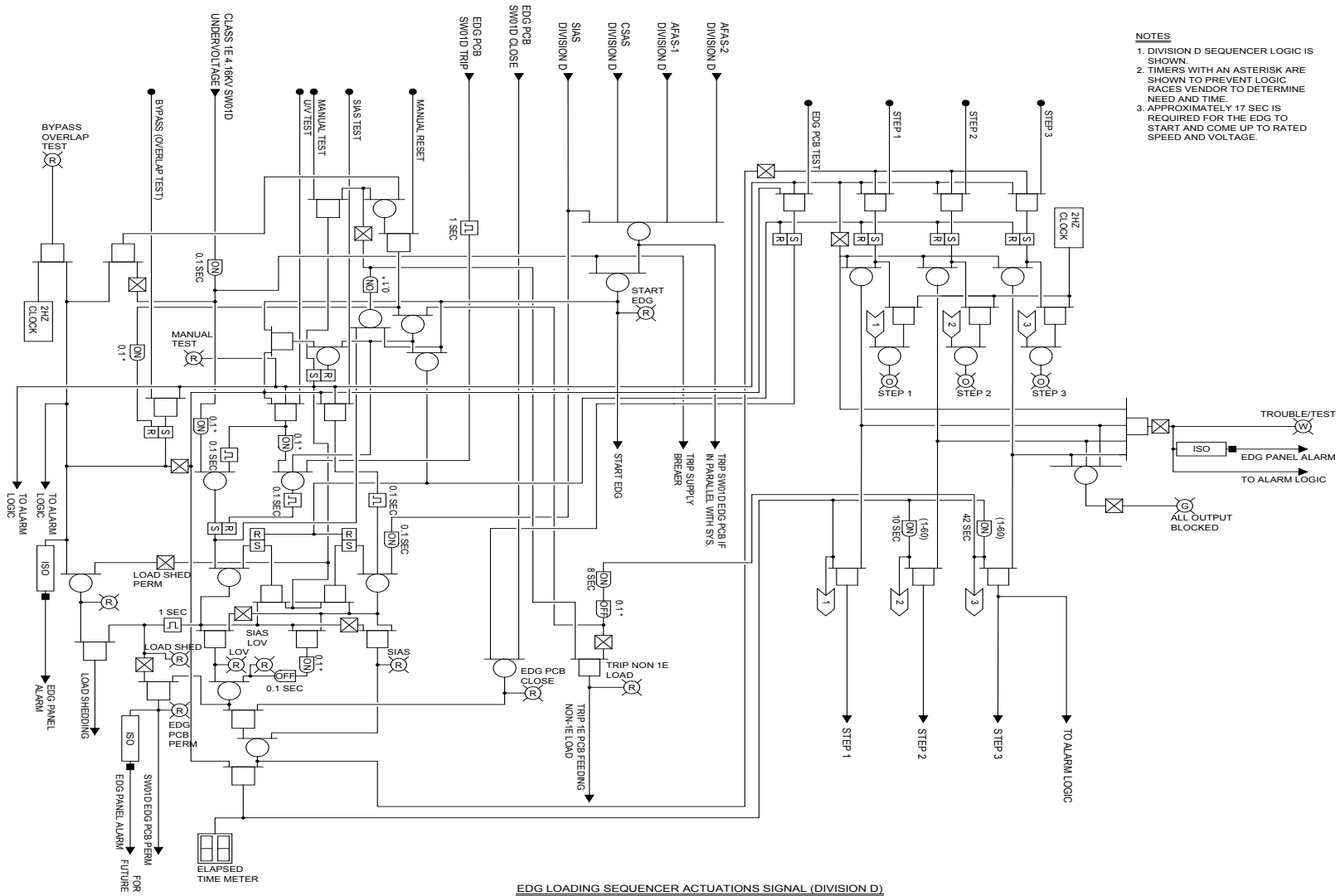


Figure 7.3-21 EDG Loading Sequencer – Control Logic Diagram (4 of 4)

APR1400 DCD TIER 2

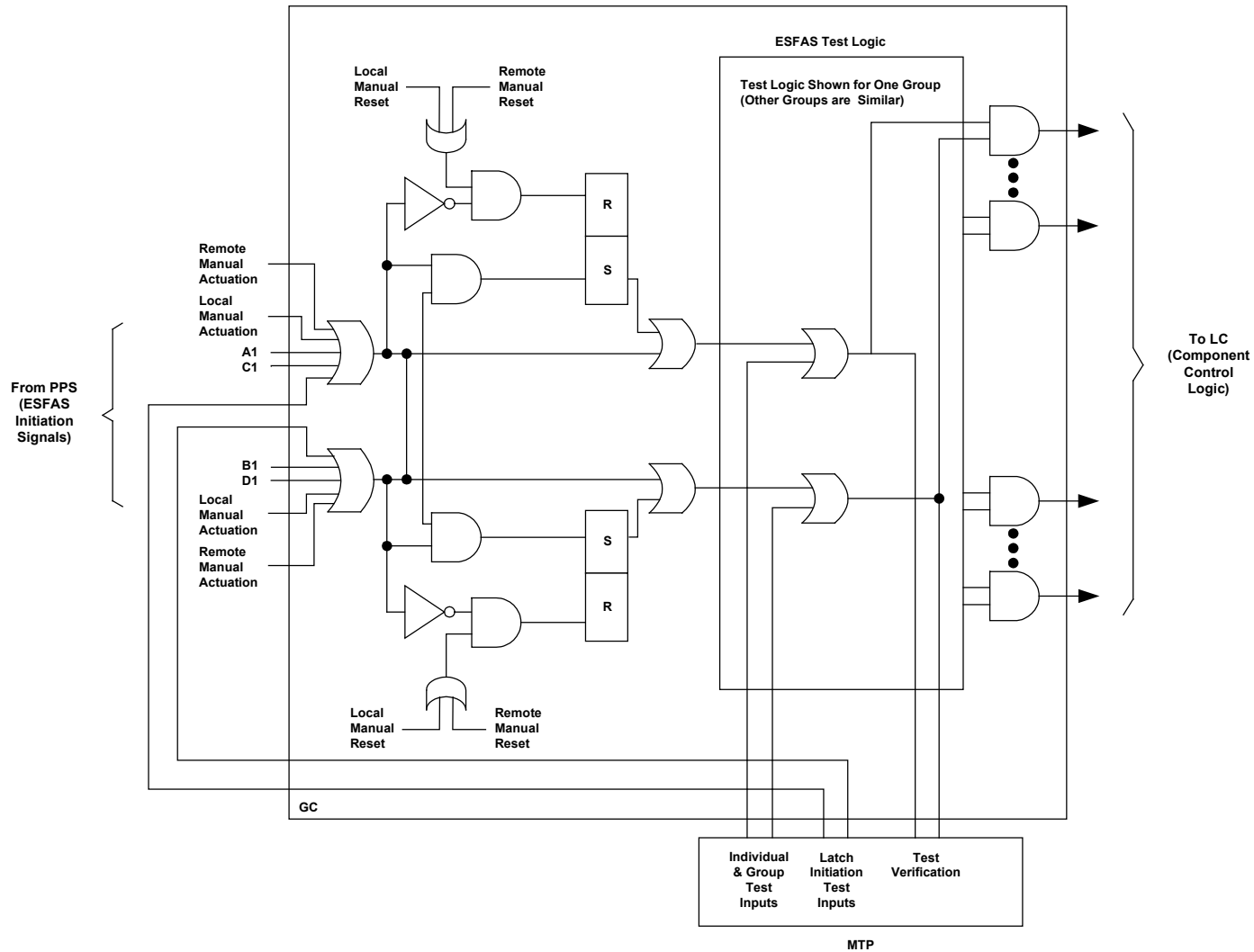
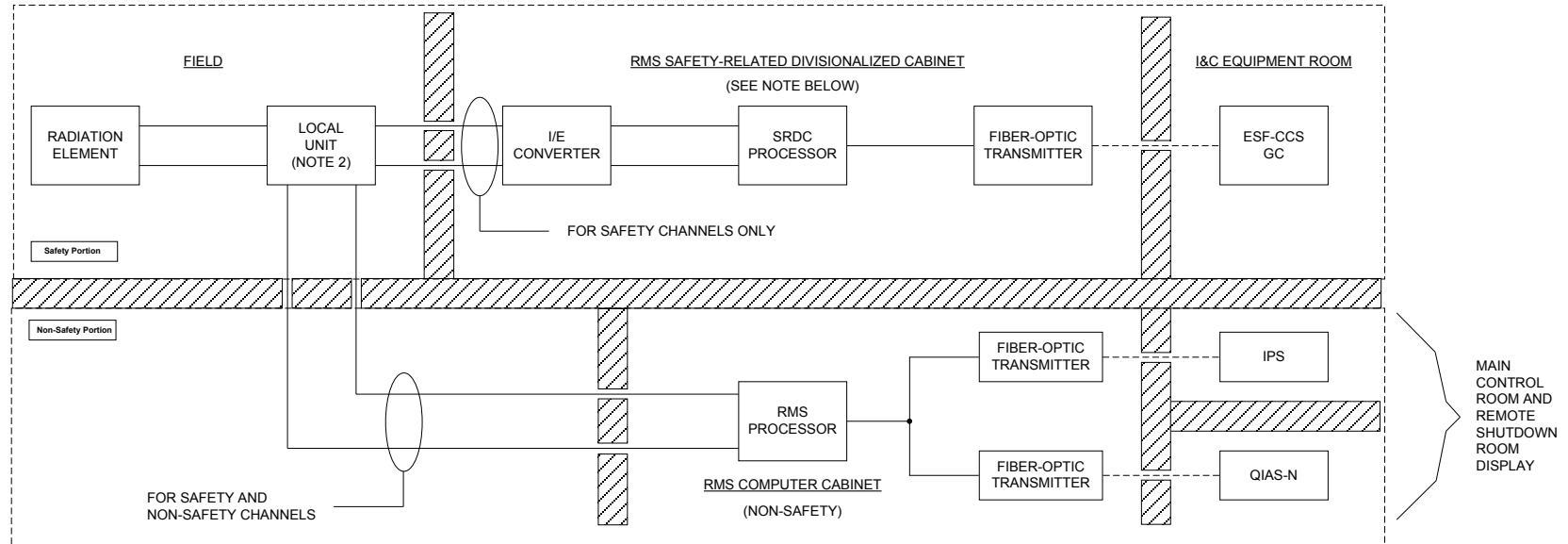


Figure 7.3-22 ESF-CCS Simplified Test Logic Diagram

APR1400 DCD TIER 2



ACRONYMS

ESF-CCS : Engineered Safety Features-Component Control System
 GC : Group Controller
 IPS : Information Processing System
 LC : Loop Controller
 QIAS-N : Qualified Indication and Alarm System - Non-safety
 RMS : Radiation Monitoring System
 SRDC : Safety-Related Divisionalized Cabinet

LEGENDS

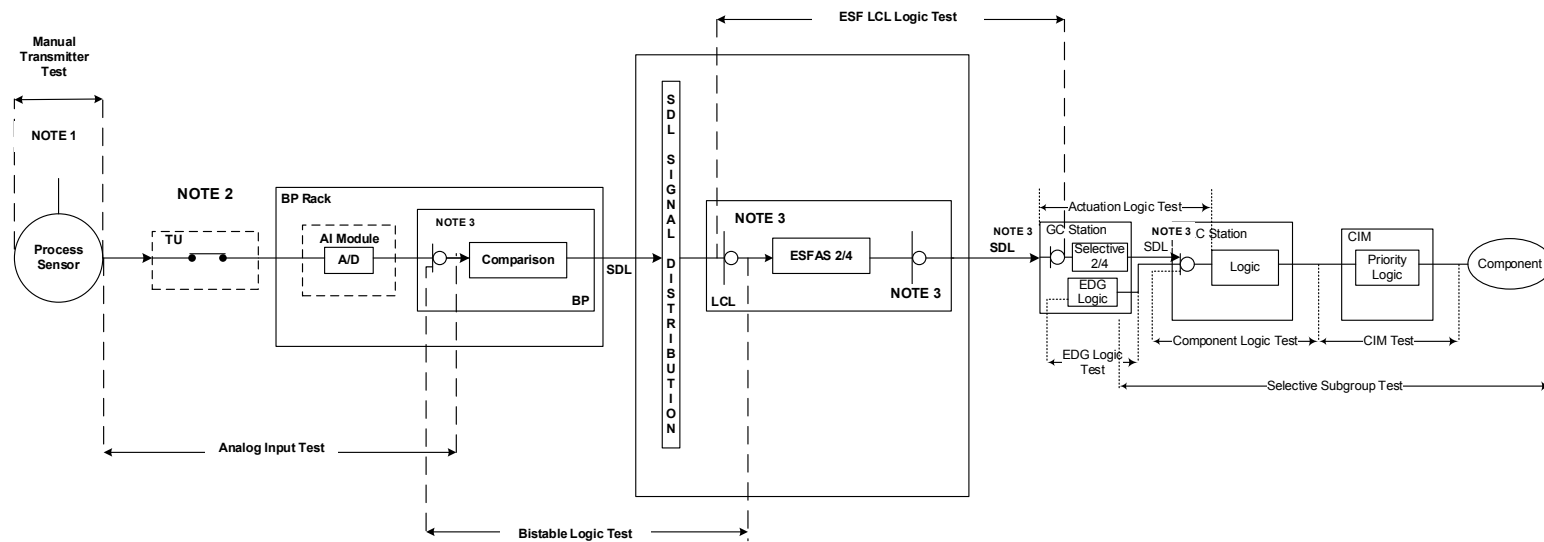
———— : Hardwired cable
 - - - - - : Fiber-optic cable

NOTE

1. THE SRDC CABINET IS REDUNDANT, HAVING DIVISION A AND B.
2. ISOLATORS ARE INCLUDED.

Figure 7.3-23 Radiation Monitoring System Measurement Channel Functional Diagram

APR1400 DCD TIER 2



NOTES:

1. EACH DASHED LINE INDICATES EITHER THE STARTING OR ENDING POINT OF TESTING.
2. A TERMINATION UNIT (TU) IS A DEVICE WHERE AN ACTUAL PROCESS SIGNAL OR A SIMULATED TEST INPUT SIGNAL, ANALOG OR DIGITAL, MAY BE SELECTED. AN ACCURACY TEST CAN BE PERFORMED BY SELECTING A SIMULATED ANALOG SIGNAL AS INPUT TO THE TU FOR PROCESSING BY THE BISTABLE PROCESSOR.
* THERE IS NO DIGITAL INPUT RELATED THE ESFAS.
3. THE LOGICAL "OR" SYMBOL MEANS THAT THE DOWNSTREAM LOGIC PROCESSES EITHER THE ACTUAL PROCESS INPUT SIGNAL OR THE SIMULATED TEST INPUT SIGNAL.

Figure 7.3-24 ESF-CCS Actuation Test Logic Diagram

7.4 Systems Required for Safe Shutdown

This section describes the instrumentation and control (I&C) systems 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, 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 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 normal 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.

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. Manual actuation of pressurizer pilot operated safety relief valve (POS RVs)
- f. Reactor coolant gas vent system (RCGVS)

The following auxiliary support systems are also required to achieve a safe shutdown of the reactor:

- a. Essential service water system (ESWS)

APR1400 DCD TIER 2

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

Discrete control and modulation control functions for these auxiliary support systems are implemented in the engineered safety features-component control system (ESF-CCS) loop controller (LC).

The manual component control of these auxiliary support systems is performed by divisionalized ESF-CCS soft control modules (ESCMs) which are located on the operator consoles and the safety console, or by the minimum inventory switches, which are located on the safety console. Also, the automatic control function is provided for these auxiliary support systems to ensure adequate auxiliary supporting features for the safety function. All components of the auxiliary support systems that are required for a safety function receive the ESF actuation signal from the ESF-CCS group controller (GC) for automatic actuation.

To meet the requirements of Clause 5.6, “Independence” of IEEE Std. 603, the physical separation and electrical isolation of the divisions within the auxiliary support systems are provided. In general, the component in one division of the auxiliary support system does not receive an interlock signal from another division.

7.4.1 System Description

The instrumentation, information displays, and controls of the auxiliary support system for safe shutdown are provided in the main control room (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 I&C for the AFWS are described in Subsections 10.4.9.2.4 and 10.4.9.5.

APR1400 DCD TIER 2

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.

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 controls necessary to achieve and maintain cold shutdown are described below. The flow diagrams for SCS are shown in Figure 5.4.7-3 and Figure 6.3.2-1.

The SCS is designed to be manually initiated upon the attainment of the required reactor coolant system (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 SCS 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.

APR1400 DCD TIER 2

The SCS has two 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 division configuration such that a single failure will not cause loss of shutdown cooling nor spuriously actuate it.

d. Safety injection system

Boron addition via the safety injection system (SIS) is used for the safe shutdown processes. The SIS I&C to achieve cold shutdown is described below.

The SIS logic and piping are provided in Section 7.3 and Figure 6.3.2-1.

1) Initiating circuits and logic

To aid in achieving cold shutdown, the required SIS component actuation steps are as follows:

- a) Coordinated control of the safety injection (SI) pumps and SI pump discharge valves to adjust and maintain the correct pressurizer water level.
- b) 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 pressurizer level control system (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.

2) Interlocks, sequencing, and bypasses

The interlocks, sequence of operation, and bypasses of the SIS are described in Subsection 6.3.1.

APR1400 DCD TIER 2

3) Redundancy and diversity

The SIS uses multiple signals as described in Section 6.3.

4) 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 pilot operated safety relief valve (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.

f. Reactor coolant gas vent system

The RCGV function 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 the ESWS are described in Subsection 9.2.1.

h. Component cooling water system

The instrumentation and controls for the CCWS are described in Subsection 9.2.2.

i. Class 1E EDG system

Four independent, 100 percent capacity emergency diesel generators (EDGs) (one per division) 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

APR1400 DCD TIER 2

sequentially load essential components onto the Class 1E 4.16 kV 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 Class 1E 4.16 kV 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.

- 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 MCR

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 from the remote shutdown room (RSR), controls and indications are available through the soft controls and displays on the information flat panel display (IFPD) on the remote shutdown console (RSC). The IFPDs in the RSR are operation ready, but control is normally blocked. 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.

APR1400 DCD TIER 2

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 facility (ERF) 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.

MCR/RSR master transfer switches are located in the maintenance and test panel (MTP) in the I&C equipment rooms and RSR. One MCR/RSR master transfer switch is provided for each division of the ESF-CCS and each division of the P-CCS, respectively. Interface diagrams of the MCR/RSR master transfer switches are provided in Figures 7.4-1 and 7.4-2.

When the MCR/RSR master 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 ESF-CCS soft control module (ESCM) 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 division 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 MCR/RSR master transfer switches, as shown in Figure 7.4-3.

APR1400 DCD TIER 2

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 division to the operator that the MCR/RSR master transfer logic has transferred the controls to the RSC. The component controls within each division also report the component group transfer status to the information processing system (IPS). The transfer status is also indicated on the MCR/RSR master 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 MCR/RSR master transfer switches maintains isolation between the ESF-CCS divisions and between the P-CCS divisions. No direct electrical connection exists between the switches and the ESF-CCS, the P-CCS, or the consoles.

The MCR/RSR master transfer switch implementation for one division of the ESF-CCS is shown in Figure 7.4-1. Input to the MCR/RSR master transfer logic for division A is provided from two locations: at the RSC and the MTP division A. The logic transfers the operator interface for ESF components controlled by ESF-CCS division A. The interfaces for manual initiation of reactor trip and main steam isolation signal (MSIS) are not transferred because it can be performed from either the MCR or the RSR at any time.

The MCR/RSR master transfer switch implementation for one division of the P-CCS is shown in Figure 7.4-2.

m. Hot shutdown

If the MCR becomes uninhabitable, sufficient indications and controls are provided in the RSR to achieve and maintain hot shutdown 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 are assumed other than an MCR fire and MCR evacuation occur (i.e., events proceed as if following a reactor trip).

APR1400 DCD TIER 2

Table 7.4-1 lists the indications and controls provided in the RSR that are necessary to achieve and maintain hot shutdown.

n. Cold shutdown

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.

o. 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.

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" [II.G.1] (Reference 5)
- b. 10 CFR 50.55a(h), "Codes and Standards, Protection and Safety Systems" (Reference 6)
- c. 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records" (Reference 7)
- d. 10 CFR Part 50, Appendix A, GDC 2, "Design Bases for Protection against Natural Phenomena" (Reference 8)
- e. 10 CFR Part 50, Appendix A, GDC 4, "Environmental and Dynamic Effect Design Bases" (Reference 9)
- f. 10 CFR Part 50, Appendix A, GDC 13, "Instrumentation and Control" (Reference 10)

APR1400 DCD TIER 2

- g. 10 CFR Part 50, Appendix A, GDC 19, “Control Room” (Reference 11)
- h. 10 CFR Part 50, Appendix A, GDC 24, “Separation of Protection and Control Systems” (Reference 12)
- i. 10 CFR Part 50, Appendix A, GDC 34, “Residual Heat Removal” (Reference 13)
- j. 10 CFR Part 50, Appendix A, GDC 35, “Emergency Core Cooling” (Reference 14)
- k. 10 CFR Part 50, Appendix A, GDC 38, “Containment Heat Removal” (Reference 15)
- l. NRC RG 1.189, Rev. 2, “Fire Protection for Nuclear Power Plants” April 2009 (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.

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 quality assurance (QA) program described in Chapter 17.

7.4.2.3 Independence

The safe shutdown I&C independence is achieved by electrical and physical separation. The independence precludes a single event causing multiple division 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 pressurizer POSRVs. All automatic and manual actuation devices are capable of being tested to verify their operability. MCR/RSR master transfer switches are also tested

APR1400 DCD TIER 2

periodically. Periodic testing is described further in Section 13.5 and the Technical Specifications.

7.4.2.5 Use of Digital Systems

The reactor protection system (RPS) and engineered safety features actuation system (ESFAS) functions rely on digital systems with the exception of the manual RT and ESF 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

Conformance with IEEE Std. 603 (Reference 2) and IEEE Std. 7-4.3.2 (Reference 3) is described in the Safety I&C System Technical Report (Reference 4).

7.4.3.2 Conformance with General Design Criterion 19

Conformance 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.

APR1400 DCD TIER 2

7.4.3.3.2 Loss of Cooling Water to Vital Equipment

Loss of cooling water to vital equipment does not affect the safe shutdown function because the safety-related component cooling water system has two separate divisions of cooling water systems. Therefore, the loss of a single division does not hinder the safe shutdown function.

7.4.3.3.3 Loss of safety-related HVAC system

The safety-related HVAC systems connected to I&C equipment rooms or remote multiplexer rooms of each division maintain the mild (non-harsh) environments to meet the cabinet environmental design requirements.

A long-term loss of safety-related HVAC system may result in a loss of safety-related I&C equipment. However, divisional redundancy ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the second safety division will remain in service to perform the required safety function.

7.4.3.3.4 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.

7.4.3.3.5 Multiple Setpoints

Multiple setpoints comply with the restrictive setpoint requirement of IEEE Std. 603, as described in Reference 4.

7.4.4 Combined License Information

No combined license (COL) information is required with regard to Section 7.4.

7.4.5 References

1. Regulatory Guide 1.189, "Fire Protection for Nuclear Power Plants," Rev. 2, U.S. Nuclear Regulatory Commission, April 2009.

APR1400 DCD TIER 2

2. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.
3. IEEE Std. 7-4.3.2-2003, "IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.
4. APR1400-Z-J-NR-14001-P, "Safety I&C System," Rev. 3, KEPCO & KHNP, May 2018.
5. 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves," [II.G.1], U.S. Nuclear Regulatory Commission.
6. 10 CFR 50.55a(h), "Codes and Standards, Protection and Safety Systems," U.S. Nuclear Regulatory Commission.
7. 10 CFR Part 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," U.S. Nuclear Regulatory Commission.
8. 10 CFR Part 50, Appendix A, General Design Criterion 2, "Design Bases for Protection Against Natural Phenomena," U.S. Nuclear Regulatory Commission.
9. 10 CFR Part 50, Appendix A, General Design Criterion 4, "Environmental and Dynamic Effect Design Bases," U.S. Nuclear Regulatory Commission.
10. 10 CFR Part 50, Appendix A, General Design Criterion 13, "Instrumentation and Control," U.S. Nuclear Regulatory Commission.
11. 10 CFR Part 50, Appendix A, General Design Criterion 19, "Control Room," U.S. Nuclear Regulatory Commission.
12. 10 CFR Part 50, Appendix A, General Design Criterion 24, "Separation of Protection and Control Systems," U.S. Nuclear Regulatory Commission.
13. 10 CFR Part 50, Appendix A, General Design Criterion 34, "Residual Heat Removal," U.S. Nuclear Regulatory Commission.
14. 10 CFR Part 50, Appendix A, General Design Criterion 35, "Emergency Core Cooling," U.S. Nuclear Regulatory Commission.

APR1400 DCD TIER 2

15. 10 CFR Part 50, Appendix A, General Design Criterion 38, “Containment Heat Removal,” U.S. Nuclear Regulatory Commission.

APR1400 DCD TIER 2

Table 7.4-1 (1 of 4)

Remote Shutdown Console Instrumentation and Controls for Hot Shutdown

No.	Function
NSSS Instrumentation	
1	Neutron Logarithmic Power
2	Hot/Cold Leg Temperature
3	Pressurizer Pressure
4	Pressurizer Level
5	RCGV Valve Position
6	Steam Generator No. 1 Pressure
7	Steam Generator No. 1 Level
8	Steam Generator No. 2 Pressure
9	Steam Generator No. 2 Level
10	CVCS Charging Flow ⁽¹⁾
11	CVCS Charging Pressure ⁽¹⁾
12	Boric Acid Storage Tank Level ⁽¹⁾
13	In-containment Refueling Water Storage Tank (IRWST) Level
14	AFW Motor-Driven Pump 1 Discharge Pressure
15	AFW Motor-Driven Pump 2 Discharge Pressure
16	AFW Turbine-Driven Pump 1 Discharge Pressure
17	AFW Turbine-Driven Pump 2 Discharge Pressure
18	AFW Motor-Driven Pump 1 Suction Pressure and Low Pressure Alarm
19	AFW Motor-Driven Pump 2 Suction Pressure and Low Pressure Alarm
20	AFW Turbine-Driven Pump 1 Suction Pressure and Low Pressure Alarm
21	AFW Turbine-Driven Pump 2 Suction Pressure and Low Pressure Alarm
22	AFW Turbine-Driven Pump Turbine 1 Inlet Pressure
23	AFW Turbine-Driven Pump Turbine 2 Inlet Pressure
24	AFW Motor-Driven Pump 1 Flow
25	AFW Motor-Driven Pump 2 Flow
26	AFW Turbine-Driven Pump 1 Flow
27	AFW Turbine-Driven Pump 2 Flow

APR1400 DCD TIER 2

Table 7.4-1 (2 of 4)

No.	Function
28	AFW Motor-Driven Pump 1 Recirculation Flow
29	AFW Motor-Driven Pump 2 Recirculation Flow
30	AFW Turbine-Driven Pump 1 Recirculation Flow
31	AFW Turbine-Driven Pump 2 Recirculation Flow
32	AFW Storage Tank 1 Level and Low Alarm
33	AFW Storage Tank 2 Level and Low Alarm
34	AFW Steam-Driven Pump 1 Turbine Speed
35	AFW Steam-Driven Pump 2 Turbine Speed
36	AFW Turbine Trip and Throttle (Stop) Valves 1 & 2 Open Position and Close Position Alarm
37	SIS Pump Discharge Pressure P-308, P-309
38	SIT Wide Range Pressure P-311D, P-321B, P-331C, P-341A
39	Shutdown Cooling Inlet/Outlet Temperature (Loop1) T-300A, T-301A
40	Shutdown Cooling Inlet/Outlet Temperature (Loop2) T-303B, T-304B
41	Shutdown Cooling Pump Flow F-302A, F-305B
42	Safety Injection Pump Flow F-321B, F-341A
Balance of Plant Instrumentation	
43	Essential Component Coolant Pump and Service Water Pump Status Indication ⁽²⁾
44	Emergency Diesel Generator Status Indication
NSSS Control ⁽³⁾	
45	Reactor Coolant Pump Trip Pushbuttons
46	Pressurizer Backup Heater Groups 1 and 2 Controls
47	Atmospheric Steam Dump Valve and Atmospheric Dump Block Valves
48	Pressurizer Auxiliary Spray Valve ⁽¹⁾
49	RCGV Valves RG-410, RG-411, RG-412, RG-413, RG-414, RG-415, RG-416, RG-417, RG-419, RG-420
50	Charging Pump ⁽¹⁾
51	Letdown Isolation Valve ⁽¹⁾
52	Reactor Coolant Pump Seal Controlled Bleed off Valve
53	MSIS Actuation Switches

APR1400 DCD TIER 2

Table 7.4-1 (3 of 4)

No.	Function
54	Manual Reactor Trip Switches
55	AFW Motor Driven Pump 1
56	AFW Motor Driven Pump 2
57	AFW Turbine Driven Pump 1
58	AFW Turbine Driven Pump 2
59	AFW Steam Generator Isolation Valves AF-100, AF-101, AF-102, AF-103
60	AFW Flow Control Valves AF-104, AF-105, AF-106, AF-107
61	AFW Steam Supply Bypass Valves AF-112, AF-113
62	AFW Steam Supply Isolation Valves AF-108, AF-109
63	AFW Turbine Trip and Throttle (Stop) Valves 1 & 2 Trip/Reset
64	AFW Turbine 1 & 2 Speed
65	Shutdown Cooling System Warmup Line Isolation Valve SI-690, SI-691
66	Shutdown Cooling System Suction Line Isolation Valve SI-651, SI-652, SI-653, SI-654, SI-655, SI-656
67	In-Containment Refueling Water Storage Tank (IRWST) Isolation Valve SI-304, SI-305
68	Shutdown Cooling System Test Return Line Isolation Valve (Throttle) SI-314, SI-315
69	Shutdown Cooling System Test Return Line Isolation Valve SI-688, SI-693
70	Containment Spray Pump/Shutdown Cooling Pump Suction Cross-Connection Valve SI-340, SI-342
71	IRWST Return Line Isolation Valve SI-300, SI-301
72	Shutdown Cooling Heat Exchanger Bypass Flow Control Valve SI-312, SI-313
73	Shutdown Cooling Heat Exchanger Isolation and Throttle Valve SI-310, SI-311
74	Safety Injection Low-Flow Control Bypass Valve SI-602, SI-603
75	Safety Injection Tank Atmospheric Vent Valve SI-605, SI-606, SI-607, SI-608, SI-613, SI-623, SI-633, SI-643
76	Safety Injection Tank Isolation Valve SI-614, SI-624, SI-634, SI-644
77	Shutdown Cooling System Direct Injection Isolation Valve SI-600, SI-601
78	Safety Injection Line Isolation Valve SI-626, SI-646

APR1400 DCD TIER 2

Table 7.4-1 (4 of 4)

No.	Function
79	Safety Injection Pump/Shutdown Cooling Pump Suction Cross-Connection Valve SI-344, SI-346
80	Safety Injection Pump SIP 1, SIP 2
81	Shutdown Cooling Pump SCP 1, SCP 2
Balance of Plant Control	
82	Essential Component Coolant Pump and Service Water Pump Control ⁽²⁾
83	EDG Power Circuit Breaker (PCB) Controls
84	Reactor Containment Building Fan Cooler Controls
85	Area Cooling Fan Controls
86	Master Transfer Switches

- (1) These are not required to achieve or maintain hot shutdown, 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 shutdown.
- (3) Status indication for essential equipment (e.g., valve position, pump on/off status) is provided on the RSC.

APR1400 DCD TIER 2

Table 7.4-2

Remote Shutdown Console Instrumentation and Controls for Cold Shutdown

No.	Function
Instrumentation	
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	Shutdown Cooling Pump Flow
6	Shutdown Cooling 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

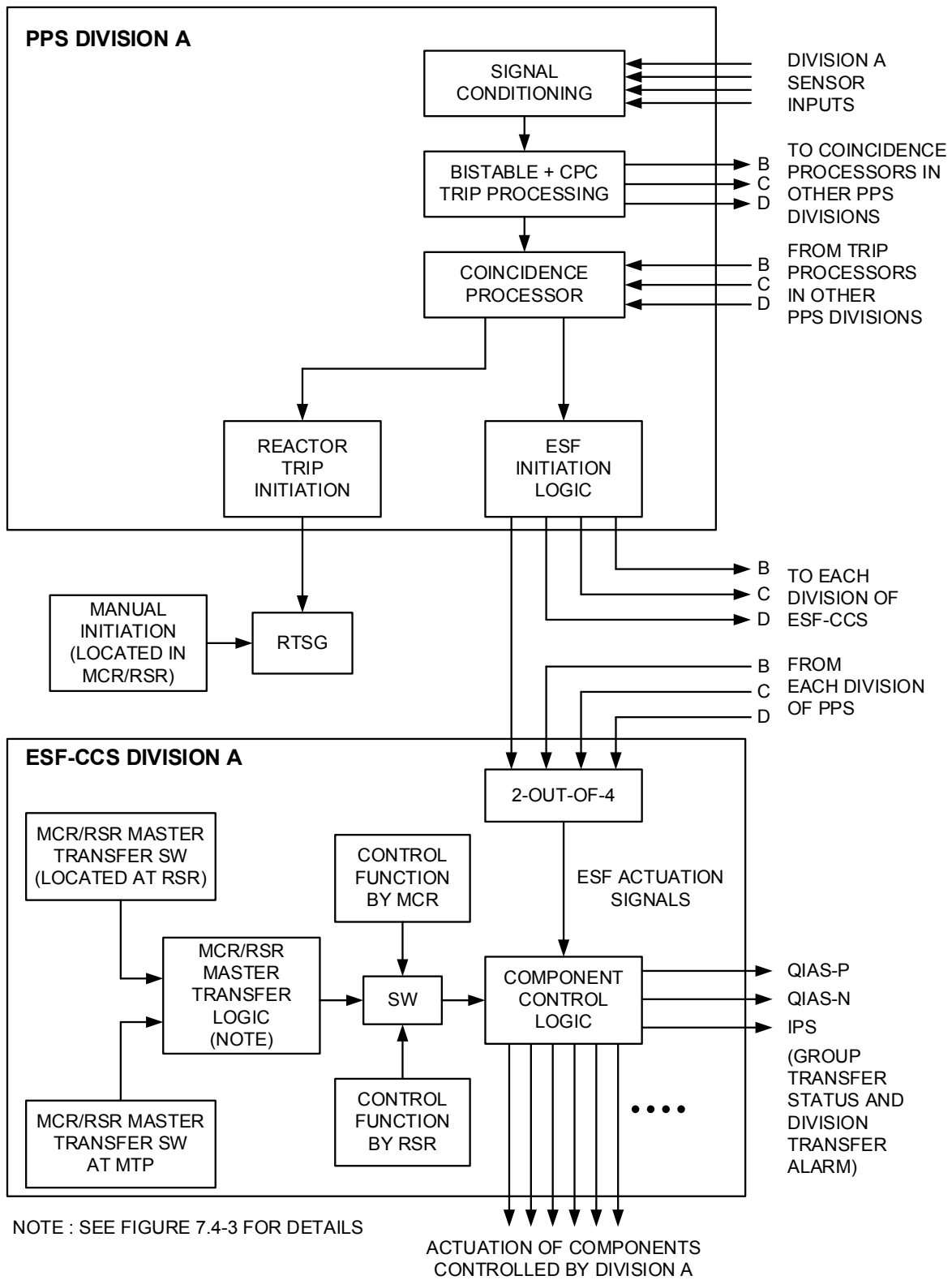


Figure 7.4-1 Interface Diagram for Division A MCR/RSR master transfer switches

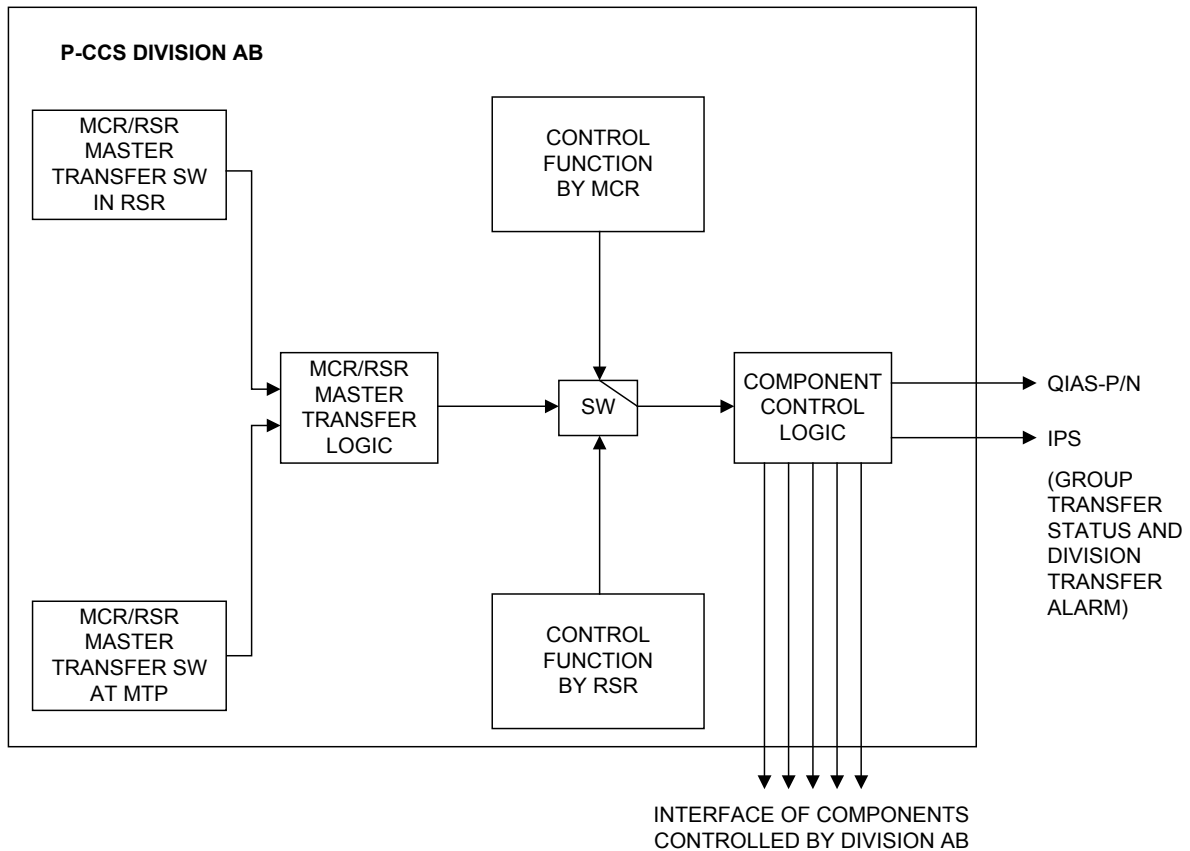


Figure 7.4-2 Interface Diagram for Division AB MCR/RSR master transfer switches

APR1400 DCD TIER 2

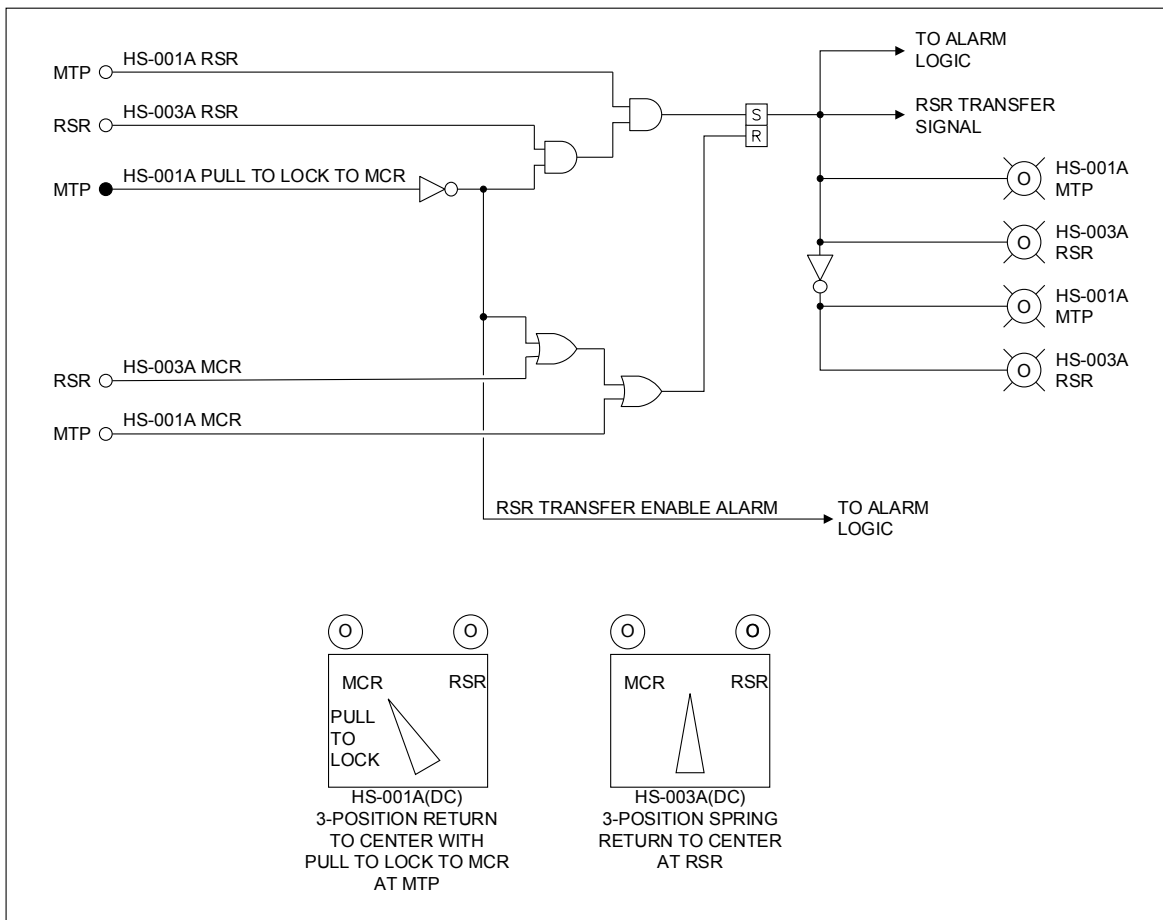


Figure 7.4-3 MCR/RSR Master Transfer Logic (Division A)

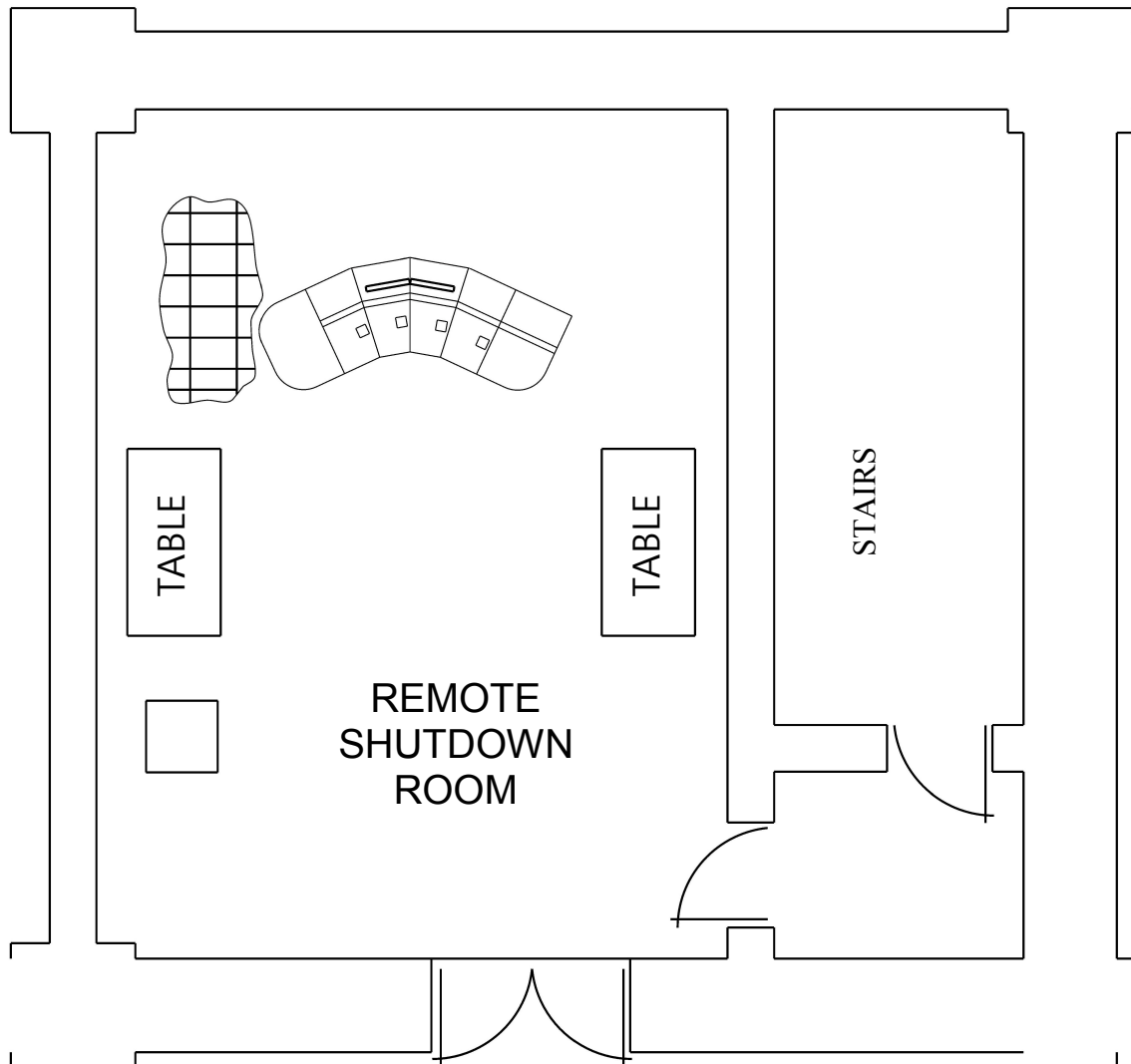


Figure 7.4-4 Layout of Remote Shutdown Room

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 operations facility (EOF)

APR1400 DCD TIER 2

7.5.1.1 Accident Monitoring Instrumentation

The 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 meet the guidance of NRC Regulatory Guide (RG) 1.97 (Reference 1), as depicted in Figure 7.5-1 and as follows:

- a. The qualified indication and alarm system - P (QIAS-P) is dedicated to continuously monitor and display AMI Type A, B and C variables. The QIAS-P in each division (A or B) has one flat panel display, which is mounted on a safety console in the MCR.
- 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 AMI Type A, B, C, and selected sets of Type D and E variables.
- c. The IPS provides displays for all AMI variables. The IPS also has a historical data storage, retrieval, and trending capability.

The combined license (COL) applicant is to provide a description of the site-specific AMI variables such as wind direction, wind speed, and atmosphere stability temperature difference (COL 7.5(1)).

Basis and Analysis to Select AMI Variables

The Table 7.5-2 provides basis and analysis of selection for AMI variables. AMI variables are selected in accordance with IEEE Std. 497, which is endorsed by NRC RG 1.97, Rev. 4.

The basis and analysis for selecting each AMI variable are described as follows:

Type A

Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

APR1400 DCD TIER 2

- a. Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
- b. Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

Type B

Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions.

Any plant critical safety functions addressed in the emergency operation guidelines (EOGs) that are in addition to those identified above are also included.

In order to select Type B variables for meeting the requirements in IEEE Std. 497 (endorsed by NRC RG 1.97, Rev. 4), the EOGs are reviewed. The plant critical safety functions described in the EOGs include those of IEEE Std. 497. EOGs provide the plant critical safety functions to be verified for each event and the criteria for deciding the plant critical safety functions.

The plant critical safety functions described in the EOG are as follows:

- Reactivity control
- Maintenance of vital auxiliaries
- Reactor coolant system (RCS) inventory control
- RCS pressure control
- Core heat removal
- RCS heat removal
- Containment isolation
- Containment temperature and pressure control
- Containment combustible gas control

APR1400 DCD TIER 2

Type C

Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach, or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

The selection of these variables represents a minimum set of plant variables that provide the most direct indication of the integrity of the three fission product barriers and provide the capability for monitoring beyond the normal operating range.

Type D

Type D variables are those variables that are required in procedures and licensing basis documentation to:

- Indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events (DBEs).
- Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
- Verify safety system status.

The Type D variables are based upon the plant accident analysis licensing basis and those necessary to implement the EOGs.

The resource tree of the EOG functional recovery guides describes the systems, including instruments and components, that are required for recovering the plant critical safety functions. Those instruments and components, as well as the variables required for verifying the system-base safety function performance, were selected as Type D variables.

Type E

Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The selection of these variables includes, but are not limited to the following:

APR1400 DCD TIER 2

- Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).
- Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).
- Monitor radiation levels and radioactivity in the plant environs.
- Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

Qualified Indication and Alarm System – P

The QIAS-P provides the continuous display of AMI 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 the 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

The QIAS-P provides an unambiguous indication of ICC and advanced warning of the approach of ICC.

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 controls the power for the HJTC heaters. The heater power control devices are located in the QIAS-P cabinet. Heater control for the HJTC is manually switched from the QIAS-P channel A only to the diverse indication system (DIS) via DIS switch on safety console. The QIAS-P also calculates the reactor vessel level based on the HJTC signals.

APR1400 DCD TIER 2

The QIAS-P provides backup displays for the ICC variables. The primary displays for ICC variables are implemented in the safety parameter display and evaluation system + (SPADES+) within the IPS.

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 safety system data network (SDN) and auxiliary process cabinet - safety (APC-S) and process instrumentation via a hardwired connection.

The QIAS-P has divisionalized cabinets for divisions A and B. The QIAS-P cabinets for each division are physically located in divisionalized I&C equipment rooms to meet the requirements of IEEE Std. 603 (Reference 3).

The QIAS-P generates alarms and sends them to the QIAS-N and IPS.

Qualified Indication and Alarm System – Non-Safety

The QIAS-N displays the safety parameters and key operating parameters to be used by the operators during both normal operation and accidents. The QIAS-N displays parameter values and alarms using signal validation, alarm filtering, alarm suppression, and alarm prioritization.

The QIAS-N consists of the following equipment:

- a. QIAS-N redundant processors
- b. QIAS-N redundant networks
- c. QIAS-N redundant servers
- d. QIAS-N redundant display networks
- e. QIAS-N MTP
- f. QIAS-N flat panel displays (FPDs)
- g. Mini-large display panels (LDPs)
- h. Shutdown overview display panels (SODPs)

APR1400 DCD TIER 2

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 QIAS-N FPDs and mini-LDPs in the MCR and the SODPs in the RSR. The QIAS-N processor receives safety system signals via the ITP. The QIAS-N MTP receives non-safety system signals via the multi-channel gateway. Isolation devices are used between the ITP and QIAS-N processor, and between the multi-channel gateway and QIAS-N MTP. The QIAS-N processor performs applicable calculations based on the data received from the safety systems and non-safety systems. The QIAS-N MTP provides maintenance and testing means of the QIAS-N, and a gateway function with the multi-channel gateway to provide communication from the non-safety P-CCS. The QIAS-N server contains the process database, updates the values and status of the database records, executes the alarm processing function, and functions as a gateway between the QIAS-N network and QIAS-N display network. The data from the QIAS-N processor (safety system signals) and the data from the QIAS-N MTP (non-safety system signals) are broadcasted on the QIAS-N network. The QIAS-N server captures the data from the QIAS-N network and updates the QIAS-N process database. The QIAS-N server broadcasts them on the QIAS-N display network for indication on the QIAS-N displays (QIAS-N FPDs, mini-LDPs, and SODPs).

In addition, the QIAS-N server provides system diagnostic functions as follows:

- a. Monitor the QIAS-N MTP, QIAS-N processor, QIAS-N network, QIAS-N display network.
- b. Detect QIAS-N trouble and generate QIAS-N trouble status signals.
- c. Transfer the QIAS-N trouble status to the non-safety IPS for alarm purpose.
- d. Transfer the QIAS-N trouble status to the QIAS-N MTP via QIAS-N network for indication on the QIAS-N MTP displays.
- e. Transfer the QIAS-N trouble status to the QIAS-N FPDs, mini-LDPs, and SODPs via QIAS-N display network.

The operator controls the plant utilizing four ESCMs, four IFPDs, and the associated mouse on the operator console. An operator console is considered inoperable when one of the following occurs: 1) Three IFPDs and each mouse are unavailable, 2) Three ESCMs are unavailable, or 3) The workstation disable switch is switched to “disable mode.”

APR1400 DCD TIER 2

The detailed information of workstation disable switch is provided in Subsection 7.7.1.2.

The QIAS-N is physically separated and electrically isolated from the IPS and QIAS-P so that the failure of QIAS-N does not cause a loss of the IPS or QIAS-P.

The QIAS-N is seismically qualified for physical and functional integrity to enhance information availability.

The block diagram for the QIAS-N is shown in Figure 7.5-2.

Information Processing System (IPS)

The IPS displays all AMI variables on the information flat panel display (IFPD) 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. The IPS also displays AMI information on the IFPD and LDP. 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 to meet the requirements of 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.

APR1400 DCD TIER 2

SPADES+ is designed to meet the criteria for SPDS set forth in NUREG-0696 (Reference 4) and NUREG-0737, Supplement No. 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

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/RV upper head saturation margin – the lower value of either the RCS saturation margin or RV 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 following the guidance of the Style Guide (Reference 6).

The QIAS-P displays are designed as follows:

- 1) To provide display of ICC variables

APR1400 DCD TIER 2

- 2) To provide 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:

- 1) RCS/RV 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

The bypass and inoperable status indication (BISI) is a non-safety system because it is not required to operate during design basis accident (DBA) conditions to mitigate the accidents.

System-level automatic bypass indication is provided based on the guidance of NRC RG 1.47 (Reference 7). Compliance with 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

APR1400 DCD TIER 2

- b. Trip channel bypasses
- c. ESF components inoperable

There are no system-level bypasses for the RPS or ESFAS.

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 resulting trip logic becomes 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 as follows:

- a. Safety injection system

APR1400 DCD TIER 2

- b. Shutdown cooling system
- c. Chemical and volume control system
- 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

The BISI design for the EDGs is described in Subsection 8.3.1.2.4.

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:

APR1400 DCD TIER 2

- a. Alerting the operators to off-normal conditions that require the operator to take action
- b. Guiding the operators to the appropriate response
- 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:

- a. 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 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.
- b. The IPS is configured by diverse hardware and software from the QIAS-N.
- c. The IPS performs online diagnostics for continuous self-health monitoring. The QIAS-N also includes automatic online diagnostics.
- d. 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.

APR1400 DCD TIER 2

7.5.1.6 Information Systems Associated with the Emergency Response Facility and Emergency Response Data System

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). The IPS associated with the ERF provides 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 following the guidance of 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

1) Single failure

The QIAS-P consists of two divisions that are electrically and physically isolated from each other so that 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.

2) 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

APR1400 DCD TIER 2

while the IPS is implemented using a distributed control system (DCS)-based platform.

3) 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.

4) Isolation

The QIAS-P is isolated from the QIAS-N and the IPS. The isolation device meets the requirements of IEEE Std. 384 (Reference 9).

5) Information ambiguity

To resolve the information ambiguity, additional variables are provided as listed in Table 7.5-1.

6) 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.

7) 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 following the guidance of IEEE Std. 497 and NRC RG 1.97. 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

APR1400 DCD TIER 2

outside the containment so the devices can be accessed for maintenance during accident conditions.

8) Direct measurement

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

AMI Type A, B and C variables are continuously displayed on the dedicated QIAS-P. AMI Type A, B, C, and selected Type D and E variables are also displayed on the QIAS-N. AMI Type A, B, C, D, and E variables are displayed on the IPS.

Recording is provided for at least one division of AMI Type A, B and C variables. Recording on the IPS is also provided for AMI 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 are identified as AMI variables with a characteristic designation to discern information intended for use under accident conditions.

e. Performance criteria

1) 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 divisions for each range.

APR1400 DCD TIER 2

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.

2) Accuracy

The required accuracy of AMI is established based on the assigned function.

The instrumentation uncertainties used in determining the emergency operating procedure (EOP) action points for AMI variables are derived from final design data conforming to NRC RG 1.105 (Reference 17).

3) Response Time

AMI is designed to provide real-time and timely information. AMI signals are transmitted from sensors to the QIAS-P, QIAS-N, and IPS. The response time between detection and indication is approximately 1 to 3 seconds. The update frequency is less than 1 second.

The COL applicant is to provide the bases document accounting for measurement uncertainties for the EOP action points (COL 7.5(3)).

7.5.2.2 Inadequate Core Cooling Monitoring

The ICC monitoring is designed to meet the requirements of 10 CFR 50.34(f)(2)(xviii) (Reference 10) and NUREG-0737, Item II.F.2.

7.5.2.3 Bypassed and Inoperable Status Indication

The BISI is designed to meet the requirements of 10 CFR 50.34(f)(2)(v) (Reference 11) and NRC RG 1.47.

7.5.2.4 Alarm System

The alarm system is designed to meet the requirements of the Staff Requirements Memorandum (SRM) on SECY-93-087, Item II.T (Reference 12).

APR1400 DCD TIER 2

7.5.2.5 Safety Parameter Display System

The SPDS is designed to meet the requirements of 10 CFR 50.34(f)(2)(iv) (Reference 13), regarding the SPDS console, and NUREG-0737, Supplement No. 1.

7.5.2.6 Information Systems Associated with the Emergency Response Facility and Emergency Response Data System

The ERF is designed to include EOF that provides sufficient information near the site to meet the requirements of 10 CFR 50.34(f)(2)(xxv) (Reference 14).

7.5.3 Analysis

Conformance with IEEE Std. 603 and IEEE Std. 7-4.3.2 (Reference 15) is described in the Safety I&C System Technical Report (Reference 16).

The safety analysis shows that the APR1400 remains safe although required manual safety functions are delayed 30 minutes after a PA 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 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

COL 7.5(3) The COL applicant is to provide the bases document accounting for measurement uncertainties for the EOP action points.

7.5.5 References

1. Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Rev. 4, U.S. Nuclear Regulatory Commission, June 2006.
2. NUREG-0737, "Clarification of TMI Action Plan Requirements," TMI Action Plan Item II.F.2, "Instrumentation for Detection of Inadequate Core Cooling," U.S. Nuclear Regulatory Commission, 1980.
3. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.
4. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, February 1981.
5. NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements" U.S. Nuclear Regulatory Commission, 1983.
6. APR1400-E-I-NR-14012-P, "Style Guide," Rev. 2, KEPCO & KHNP, January 2018.
7. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Rev. 1, U.S. Nuclear Regulatory Commission, February 2010.
8. IEEE Std. 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2002.
9. IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers, 1992.
10. 10 CFR 50.34(f)(2)(xviii), "Instrumentation for Detection of Inadequate Core Cooling," [II.F.2], U.S. Nuclear Regulatory Commission.
11. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3], U.S. Nuclear Regulatory Commission.

APR1400 DCD TIER 2

12. Staff Requirements Memorandum on SECY-93-087, Item II.T, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advance Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, July 21, 1993.
13. 10 CFR 50.34(f)(2)(iv), “Safety Parameter Display Console” [I.D.2] U.S. Nuclear Regulatory Commission.
14. 10 CFR 50.34 (f)(2)(xxv), “Additional TMI-related Requirements,” [III.A.1.2], U.S. Nuclear Regulatory Commission.
15. IEEE Std. 7-4.3.2-2003, “IEEE Standard Design for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2003.
16. APR1400-Z-J-NR-14001-P, “Safety I&C System,” Rev. 3, KEPCO & KHNP, May 2018.
17. Regulatory Guide 1.105, “ Setpoint for Safety-Related Instrumentation,” Rev. 3, U.S. Nuclear Regulatory Commission, December 1999.

APR1400 DCD TIER 2

Table 7.5-1 (1 of 6)

Accident Monitoring Instrumentation Variables

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
Pressurizer Pressure (Wide Range)	0 to 210.9 kg/cm ² A (0 to 3,000 psia)	Pressurizer	2	A, B	C,D (PPS OM)
Pressurizer Level	0 to 100 % (0 to 562.15 in)	Pressurizer	2	A, B, D	A, B (IPS)
Hot Leg Temperature (Wide Range)	0 to 400 °C (32 to 752 °F)	RCS	2/loop	A, B, D	Hot Leg Temperature (Narrow Range) A, B, C, D (PPS OM)
Cold Leg Temperature (Wide Range)	0 to 400 °C (32 to 752 °F)	RCS	2/loop	A, B, D	Cold Leg Temperature (Narrow Range) A, B, C,D (PPS OM)
Steam Generator Pressure	0 to 105 kg/cm ² A (0 to 1,494 psia)	Steam Generator	2/SG	A, B, D	C,D (PPS OM)
Steam Generator Level (Wide Range)	0 to 100 % (0 to 1117.6 cm (0 to 440 in tap span)	Steam Generator	2/SG	A, B, D	C,D (PPS OM)
Core Exit Temperature	0 to 1260 °C (32 to 2,300 °F)	Inadequate Core Cooling	2	B, C	Validation (QIAS-P)
RCS Saturation Margin	Temp. Margin : -399 to 358.3 °C Press. Margin : -225.5 to 210.9 kg/cm ²	Inadequate Core Cooling	2	A, B	Validation (QIAS-P)
CET Saturation Margin	Temp. Margin : -1,260 to 368.3 °C Press. Margin : -225.5 to 210.9 kg/cm ²	Inadequate Core Cooling	2	A, B	Validation (QIAS-P)
RV Upper Head Saturation Margin	Temp. Margin : -1,260 to 368.3 °C Press. Margin : -225.5 to 210.9 kg/cm ²	Inadequate Core Cooling	2	B	Validation (QIAS-P)
Reactor Vessel Level (RV closure head level/RV plenum level)	0 to 100 %	RCS	2	B	Validation (QIAS-P)
Hydrogen Concentration	0 to 15 %	Combustible gas control	2	B	A, B (IPS)

APR1400 DCD TIER 2

Table 7.5-1 (2 of 6)

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
RCS Pressure	0 to 281.2 kg/cm ² G (0 to 4,000 psig)	RCS	2	C, D	Pressurizer Pressure A, B, C, D (PPS OM)
IRWST Level	0 to 100 %	IRWST	2	B, D	C,D (ESCM)
IRWST Temperature	10 to 177 °C (50 to 350 °F)	IRWST	2	B, D	C,D (ESCM)
Holdup Volume Tank Level	0 to 100 %	IRWST	2	B	C,D (ESCM)
Containment Water Level	0 to 100 %	Containment monitoring system	2	B	A, B (IPS)
Containment Pressure (Wide Range)	-400 to 5,600 cmH ₂ O (-5.7 to 79.5 psig)	Maintaining containment integrity	2	B, D	C,D (PPS OM)
Reactor Cavity Level	0 to 100%	Maintaining containment integrity	2	B	C,D (ESCM)
Containment Isolation Valve Position	N/A	Maintaining containment integrity	1 pair/ valve	B, D	Validation (QIAS-P)
Logarithmic Reactor Power (neutron flux)	2×10 ⁻⁸ to 200 % power	Reactor power	2	A, B	C,D (PPS OM)
CEA Position	0 to 381 cm (0 to 150 in)	Reactivity control	1/rod	D	N/A
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 (For Fuel Handling Accident)	Refer to range information for Tag No. RE-231A and RE-232B in Table 12.3-7.	Monitoring fueling handling accident	2	C	A, B (IPS)
Spent Fuel Pool radiation	Refer to range information for Tag No. RE-241A and RE-242B in Table 12.3-7.	Monitoring fueling handling accident	2	C	A, B (IPS)

APR1400 DCD TIER 2

Table 7.5-1 (3 of 6)

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
Containment Upper Operating Area Radiation	Refer to range information for Tag No. RE-233A and RE-234B in Table 12.3-7.	Monitoring LOCA	2	C	A, B (IPS)
MS ADV Position	N/A	Monitoring position of MS ADV actuation	2	B, D	C, D (ESCM)
Auxiliary Feedwater Flow	0 to 3,600 lpm (0 to 950 gpm)	Monitoring auxiliary feedwater flow	2	B, D	C, D (ESCM)
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	1	D	N/A
Containment Atmosphere Temperature	4.44 to 204.44 °C (40 to 400 °F)	Monitoring accomplishment of cooling	2	B, D	C, D (ESCM)
SI Hot Leg Injection Flow Rate	0 to 5,678 lpm (0 to 1,500 gpm)	Monitoring the operating status for a safety system	1	D	N/A
Safety Injection Tank Level	0 to 100 % (402 inch full scale)	Monitoring a boron injection potential	1/Tank	D	N/A
Safety Injection Tank Pressure	0 to 53 kg/cm ² g (0 to 750 psig)	Monitoring a boron injection potential	1/Tank	D	N/A
Emergency Ventilation Damper Position	N/A	Prevention of radiation effluent release	1 pair/damper	D	N/A
Auxiliary Feedwater Storage Tank Level	0 to 100%	Monitoring level of auxiliary feedwater storage tank	1	D	N/A
DC Bus Voltage	0 to 150 Vdc	Electrical power supplies for safety system and safe shutdown system	2	B, D	C, D (ESCM)
Instrument Power Bus Voltage	0 to 150 Vac	Electrical power supplies for safety system and safe shutdown system	2	B, D	C, D (ESCM)
CREACS Emergency ACU flow	0 to 13,592 cmh (0 to 8,000 cfm)	Verifying the status of a safety system	1	D	N/A

APR1400 DCD TIER 2

Table 7.5-1 (4 of 6)

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
ABCAEES Emergency ACU flow	0 to 5,097 cmh (0 to 3,000 cfm)	Verifying the status of a safety system	1	D	N/A
FHAEES Emergency ACU flow	0 to 8,495 cmh (0 to 5,000 cfm)	Verifying the status of a safety system	1	D	N/A
Emergency Diesel Generator Voltage	0 to 5,250 Vac	Electrical power supplies for safety system and safe shutdown system	1	D	N/A
Emergency Diesel Generator Current	0 to 2,000 Amps	Electrical power supplies for safety system and safe shutdown system	1	D	N/A
4.16 kV Switchgear Voltage	0 to 5,250 Vac	Electrical power supplies for safety system and safe shutdown system	2	B, D	C, D (ESCM)
4.16 kV Switchgear Current	0 to 2,000 Amps	Electrical power supplies for safety system and safe shutdown system	1	D	N/A
480 V L/C Voltage	0 to 600 Vac	Electrical power supplies for safety system and safe shutdown system	1	D	N/A
480 V L/C Current	0 to 3,000 Amps	Electrical power supplies for safety system and safe shutdown system	1	D	N/A
CCW Temperature	0 to 100 °C (32 to 212 °F)	Monitoring CCWS operation	1	D	N/A
CCW Flow	0 to 110% design flow	Monitoring CCWS operation	1	D	N/A
ESW Temperature	0 to 50 °C (32 to 122 °F)	Monitoring ESW operation	1	D	N/A
ESW Flow	0 to 120% design flow	Monitoring ESW operation	1	D	N/A
Charging Line Flow	0 to 750 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 G (0 to 3,129 psig)	Monitoring the status of boric acid flow to RCS	1	D	N/A

APR1400 DCD TIER 2

Table 7.5-1 (5 of 6)

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
Shutdown Cooling Heat Exchange Outlet Temperature	0 to 200°C (40 to 392°F)	Monitor the operating status for a safety system	1	D	N/A
Shutdown Cooling Pump Flow Rate	0 to 25,000 lpm (0 to 6,604 gpm)	Monitor the operating status for a safety system	1	D	N/A
SIT Discharge Isolation	N/A	Monitor the operating status for a safety system	1	D	N/A
SIP DVI Flow Rate	0 to 5,678 lpm (0 to 1,500 gpm)	Monitor the operating status for a safety system	4	B, D	A, B, C, D (ESCM)
Containment Purge Effluent	Refer to range information for Tag No. RE-037 in Table 11.5-1.	Monitoring gaseous effluent in containment building	1	E	N/A
Auxiliary Building Controlled Area HVAC Effluent	Refer to range information for Tag No. RE-015, 016, 019, and 020 in Table 11.5-1.	Monitoring gaseous effluent of controlled area in AUX. building	1	E	N/A
Compound Building HVAC Effluent	Refer to range information for Tag No. RE-082 in Table 11.5-1.	Monitoring gaseous effluent in compound building	1	E	N/A
Condenser Vacuum Vent Effluent Radiation	Refer to range information for Tag No. RE-063 in Table 11.5-1.	Monitoring SG tube leakage	1	E	N/A
MCR and TSC Area Radiation	Refer to range information for Tag No. RE-275 and RE-279 in Table 12.3-7.	Monitoring area radiation level	1	E	N/A
Normal Primary Sample Room Area Radiation	Refer to range information for Tag No. RE-285 in Table 12.3-7.	Monitoring area radiation level	1	E	N/A
Radiochemistry Lab. Area Radiation	Refer to range information for Tag No. RE-257 in Table 12.3-7.	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

APR1400 DCD TIER 2

Table 7.5-1 (6 of 6)

Variable	Range	Monitored Function or System ⁽¹⁾	Required Channels	Type	Ambiguity (Division)
Atmosphere Stability Temperature Difference	-22.78 to -7.78°C (-9 to +18°F) Delta-T	Release assessment	1	E	N/A
Main Steam Line Radiation	Refer to range information for Tag No's. RE-217 through RE-220 in Table 11.5-1.	Monitoring leakage of steam generator	1	E	N/A
High Energy Line Break Area ACU Inlet Radiation	Refer to range information for Tag No. Re-007 in Table 11.5-1.	Monitoring gaseous effluent of high-energy line break area in AUX building	1	E	N/A
Auxiliary Building Controlled Area (I,II) HVAC Normal/Emergency Exhaust ACU Inlet Radiation	Refer to range information for Tag No. RE-013, 014, 017, and 018 in Table 11.5-1.	Monitoring gaseous effluent of controlled area in AUX. building	1	E	N/A
Containment Air Radiation	Refer to range information for Tag No. RE-039A and 40B in Table 11.5-1.	Monitoring the unidentified leakage from RCS	1	E	N/A
Fuel Handling Area HVAC Effluent Radiation	Refer to range information for Tag No. RE-043 in Table 11.5-1.	Monitoring gaseous effluent of fuel handling area in AUX. building	1	E	N/A
Compound Building Hot Machine Shop Radiation	Refer to range information for Tag No. RE-293 in Table 12.3-7.	Monitoring gaseous effluent of hot machine shop in compound building	1	E	N/A
Steam Generator Blowdown Radiation	Refer to range information for Tag No. RE-104 in Table 11.5-2.	Monitoring SG tube leakage	1	E	N/A
Post-accident Primary Sample Room Radiation	Refer to range information for Tag No. RE-205 in Table 12.3-7.	Monitoring area radiation level	1	E	N/A

- (1) Parameters to monitor critical safety functions in SPADES+ as described in Section 7.7 are confirmed by functional requirements analysis as described in Section 18.3

APR1400 DCD TIER 2

Table 7.5-2 (1 of 8)

Basis and Analysis of Selection for AMI Variables

Variable	Type	Basis and analysis
Pressurizer Pressure (Wide Range)	A, B	Pressurizer Pressure (Wide Range) is required for manual operator action based on the Accident Analyses. (Type A) Pressurizer Pressure (Wide Range) is a primary variable for monitoring critical safety function. (Type B)
Pressurizer Level	A, B, D	Pressurizer Level is required for manual operator action based on the Accident Analyses. (Type A) Pressurizer Level is a primary variable for monitoring critical safety function. (Type B) Pressurizer Level verifies the status of a safety system. (Type D)
Hot Leg Temperature (Wide Range)	A, B, D	Hot Leg Temperature (Wide Range) is required for manual operator action based on the Accident Analyses. (Type A) Hot Leg Temperature (Wide Range) is a primary variable for monitoring critical safety function. (Type B) Hot Leg Temperature (Wide Range) verifies the status of a safety system. (Type D)
Cold Leg Temperature (Wide Range)	A, B, D	Cold Leg Temperature (Wide Range) is required for manual operator action based on the Accident Analyses. (Type A) Cold Leg Temperature (Wide Range) is a primary variable for monitoring critical safety function. (Type B) Cold Leg Temperature (Wide Range) verifies the status of a safety system. (Type D)
Steam Generator Pressure	A, B, D	Steam Generator Pressure is required for manual operator action based on the Accident Analyses. (Type A) Steam Generator Pressure is a primary variable for monitoring critical safety function. (Type B) Steam Generator Pressure verifies the status of a safety system. (Type D)
Steam Generator Level (Wide Range)	A, B, D	Steam Generator Level (Wide Range) is required for manual operator action based on the Accident Analyses. (Type A) Steam Generator Level (Wide Range) is a primary variable for monitoring critical safety function. (Type B) Steam Generator Level (Wide Range) verifies the status of a safety system. (Type D)
RCS Saturation Margin	A, B	RCS Saturation Margin is required for manual operator action based on the Accident Analyses. (Type A) RCS Saturation Margin is a primary variable for monitoring critical safety function. (Type B)

APR1400 DCD TIER 2

Table 7.5-2 (2 of 8)

Variable	Type	Basis and analysis
CET Saturation Margin	A, B	CET Saturation Margin is required for manual operator action based on the Accident Analyses. (Type A) CET Saturation Margin is a primary variable for monitoring critical safety function. (Type B)
RV Upper Head Saturation Margin	B	RV Upper Head Saturation Margin is a primary variable for monitoring critical safety function. (Type B)
Hydrogen Concentration	B	Hydrogen Concentration is a primary variable to support containment combustible gas control of critical safety function. (Type B)
Core Exit Temperature (CET)	B, C	Core Exit Temperature (CET) is a primary variable for monitoring critical safety function. (Type B) Core Exit Temperature (CET) is an indicator for probable breach of cladding. (Type C)
Reactor Vessel Level (RV Closure Head Level /RV plenum Level)	B	Reactor Vessel Level (RV Closure Head Level/RV plenum Level) is a primary variable for monitoring critical safety function. (Type B)
RCS Pressure	C, D	RCS Pressure is a primary variable for monitoring RCPB integrity and breach of the RCPB. (Type C) RCS Pressure verifies the status of a safety system. (Type D)
Holdup Volume Tank Level	B	Holdup volume tank level is a variable to monitor RCS pressure control, inventory control and RCS heat removal. RCS pressure control, inventory control and RCS heat removal are included in the critical safety functions. (Type B)
Containment Water Level	B	Containment water level is a variable to monitor RCS pressure control, inventory control and RCS heat removal. RCS pressure control, inventory control and RCS heat removal are included in the critical safety functions. (Type B)
Containment Pressure (Wide Range)	B, D	Containment Pressure (Wide Range) is a primary variable for monitoring critical safety function. (Type B) Containment Pressure (Wide Range) is a primary variable for monitoring the operating status for a safety system. (Type D)
Reactor Cavity Level	B	Reactor cavity level is a variable to monitor RCS pressure control, inventory control and RCS heat removal. RCS pressure control, inventory control and RCS heat removal are included in the critical safety functions. (Type B)

APR1400 DCD TIER 2

Table 7.5-2 (3 of 8)

Variable	Type	Basis and analysis
Containment Isolation Valve Position	B, D	Containment Isolation Valve Position is a primary variable for monitoring critical safety function. (Type B) Containment isolation valves are variables to monitor the containment integrity status. (Type D)
Logarithmic Reactor Power (Neutron Flux)	A, B	Logarithmic Reactor Power (Neutron Flux) is required for manual operator action based on the Accident Analyses. (Type A) Logarithmic Reactor Power (Neutron Flux) is a primary variable for monitoring critical safety function. (Type B)
CEA Position	D	These variables monitor the performance of CEDMs that affect the core reactivity. (Type D)
Containment Pressure (Extended Wide Range)	C	Containment Pressure is a primary variable for monitoring the integrity of protection barrier against fission product release. (Type C)
Containment Operating Area Radiation (For Fuel Handling Accident)	C	Containment operating area radiation is a variable for monitoring fueling handling accident during refueling operation inside containment. A breach of fuel cladding is detected by this variable. (Type C)
Spent Fuel Pool Radiation	C	Spent fuel pool radiation is a variable for monitoring fueling handling accident. A breach of fuel cladding is detected by this variable. (Type C)
Containment Upper Operating Area Radiation	C	Containment upper operating area radiation is a variable to monitor loss of coolant accident (LOCA). A breach of RCPB is detected by this variable. (Type C)
IRWST Level	B, D	IRWST is the borated water source of safety injection system (SIS) and containment spray system (CSS) during the accident. IRWST level is a variable to monitor RCS pressure control, inventory control and RCS heat removal. (Type B) IRWST level is a monitoring variable for indicating the performance of SIS and CSS necessary for the mitigation of DBEs. (Type D)
IRWST Temperature	B, D	IRWST is the borated water source of SIS and CSS during the accident. IRWST temperature is a variable to monitor RCS pressure control, inventory control and RCS heat removal. (Type B) IRWST temperature is a monitoring variable for indicating the performance of SIS and CSS necessary for the mitigation of DBEs. (Type D)

APR1400 DCD TIER 2

Table 7.5-2 (4 of 8)

Variable	Type	Basis and analysis
Main Steam Automatic Depressurization Valve (MS ADV) Position	B, D	MS ADV position is a monitoring variable for verifying the RCS heat removal. Therefore, this variable meets the criteria for the selection of Type B variable in IEEE Std. 497. (Type B) MS ADV position is the monitoring variable to verify safety system status. (Type D)
Auxiliary Feedwater Flow	B, D	Auxiliary feedwater flow meters are designed as safety-related and seismic Category I. It is an important parameter for monitoring the cooling capability of the RCS which is a critical safety function. Therefore, this variable meets the criteria for the selection of Type B variable in IEEE Std. 497. (Type B) Auxiliary feedwater flow is the monitoring variable of safety system to achieve a safety shutdown condition. (Type D)
POSRV Position	D	POSRV Position verifies the status of a safety system. (Type D)
CS Flow	D	Containment spray flow is a variable for monitoring containment spray operation. Containment spray flow indicates the performance of CSS necessary for the mitigation of DBEs. (Type D)
Containment Atmosphere Temperature	B, D	Containment atmosphere temperature is a variable to monitor containment atmospheric conditions. (Type B) Containment atmosphere temperature is a variable for monitoring accomplishment of cooling. This variable is used to monitor the performance of safety systems for the mitigation of DBEs. (Type D)
SI Hot Leg Injection Flow Rate	D	SI hot leg injection flow rate is a variable that monitors the operation status of safety injection pump (hot leg injection) in case of an accident. It is an indicator to monitor the operating status for a safety system. This variable is included in EOG functional recovery guide. (Type D)
Safety Injection Tank (SIT) Level	D	Safety Injection Tank (SIT) Level is a primary variable for monitoring the operating status for a safety system. (Type D)
Safety Injection Tank (SIT) Pressure	D	Safety Injection Tank (SIT) Pressure is a primary variable for monitoring the operating status for a safety system. (Type D)
Emergency Ventilation Damper Position	D	Emergency ventilation damper position is used to monitor the performance of safety systems for the mitigation of design basis events. (Type D)

APR1400 DCD TIER 2

Table 7.5-2 (5 of 8)

Variable	Type	Basis and analysis
Auxiliary Feedwater Storage Tank Level	D	The auxiliary feedwater storage tanks are designed to have sufficient feedwater to allow an orderly plant cooldown to shutdown cooling initiation without additional makeup. During normal plant operation, the main purpose of this variable is to confirm sufficient inventory of auxiliary feedwater for accident conditions. If an accident occurs, it is not necessary to monitor water level for additional makeup to the auxiliary feedwater storage tanks. Therefore, this variable meets the criteria for the selection of Type D variable in IEEE Std. 497. (Type D)
DC Bus Voltage	B, D	DC bus voltage is a primary variable to monitor maintenance of vital auxiliaries. Maintenance of vital auxiliaries is included in the critical safety functions. (Type B) DC bus voltage is variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
Instrument Power Bus Voltage	B, D	Instrument power bus voltage is a primary variable to monitor maintenance of vital auxiliaries. Maintenance of vital auxiliaries is included in the critical safety functions. (Type B) Instrument power bus voltage is variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
Emergency Diesel Generator Voltage	D	Emergency diesel generator voltage is variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
Emergency Diesel Generator Current	D	Emergency diesel generator current is a variable for monitoring Electrical Power supplies for safety systems and safe shutdown systems. (Type D)
4.16 kV Switchgear Voltage	B, D	4.16 kV switchgear voltage is a primary variable to monitor maintenance of vital auxiliaries. Maintenance of vital auxiliaries is included in the critical safety functions. (Type B) 4.16 kV switchgear voltage is a variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
4.16 kV Switchgear Current	D	4.16 kV switchgear current is a variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
480 V L/C Voltage	D	480 V L/C voltage is a variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)
480 V L/C Current	D	480 V L/C current is a variable for monitoring electrical power supplies for safety systems and safe shutdown systems. (Type D)

APR1400 DCD TIER 2

Table 7.5-2 (6 of 8)

Variable	Type	Basis and analysis
CCW Temperature	D	Component cooling water (CCW) system removes heat from all safety-related components necessary for the safe shutdown and the mitigation of DBEs. CCW temperature is a variable for monitoring CCW operation. This variable indicates the performance of the CCW system necessary for the safe shutdown and the mitigation of DBEs. (Type D)
CCW Flow	D	CCW system removes heat from all safety-related components necessary for the safe shutdown and the mitigation of DBEs. CCW flow is a variable for monitoring CCW operation. This variable indicates the performance of the CCW system necessary for the safe shutdown and the mitigation of DBEs. (Type D)
ESW Temperature	D	Essential service water (ESW) system removes heat from the CCW heat exchangers and transfers to the UHS. ESW temperature is a variable for monitoring ESW operation. This variable indicates the performance of the ESW system necessary for the safe shutdown and the mitigation of DBEs. (Type D)
ESW Flow	D	ESW system removes heat from the CCW heat exchangers and transfers to the UHS. ESW Flow is a variable for monitoring ESW operation. This variable indicates the performance of the ESW system necessary for the safe shutdown and the mitigation of DBEs. (Type D)
Charging Line Flow	D	Charging Line Flow is a primary variable for monitoring the status of boric acid flow to the RCS. (Type D)
Charging Line Pressure	D	Charging Line Pressure is a primary variable for monitoring the operating status for a safety system. (Type D)
Shutdown Cooling Heat Exchange Outlet Temperature	D	Shutdown Cooling Heat Exchange Outlet Temperature is a primary variable for monitoring the operating status for a safety system. (Type D)
Shutdown Cooling Pump Flow Rate	D	Shutdown Cooling Pump Flow Rate is a primary variable for monitoring the operating status for a safety system. (Type D)
SIT Discharge Isolation	D	SIT Discharge Isolation provides information of operating status for a safety system. (Type D)
CREACS Emergency ACU flow	D	CREACS Emergency ACU flow verifies the status of a safety system. (Type D)
ABCAEES Emergency ACU flow	D	ABCAEES Emergency ACU flow verifies the status of a safety system. (Type D)
FHAEES Emergency ACU flow	D	FHAEES Emergency ACU flow verifies the status of a safety system. (Type D)

APR1400 DCD TIER 2

Table 7.5-2 (7 of 8)

Variable	Type	Basis and analysis
SIP DVI Flow Rate	B, D	SIP DVI is a primary variable for monitoring critical safety function. (Type B) SIP DVI is a primary variable for monitoring the operating status for a safety system. (Type D)
Containment Purge Effluent	E	Containment purge effluent is used to monitor gaseous effluent in containment building. This variable is required to monitor releases of radioactive materials through identified pathways. (Type E)
Auxiliary Building Controlled Area HVAC Effluent	E	Auxiliary building controlled area HVAC effluent is used to monitor gaseous effluent of controlled area in auxiliary building. This variable is required to monitor releases of radioactive materials through identified pathways. (Type E)
Compound Building HVAC Effluent	E	Compound building HVAC effluent is used to monitor gaseous effluent in compound building. This variable is required to monitor releases of radioactive materials through identified pathways. (Type E)
Condenser Vacuum Vent Effluent Radiation	E	Condenser vacuum vent effluent radiation is used to monitor SG tube leakage. This variable is required to monitor releases of radioactive materials through identified pathways. (Type E)
MCR and TSC Area Radiation	E	MCR and TSC area radiation is used to monitor radiation level and radioactivity in the control room. (Type E)
Normal primary sample Room Area Radiation	E	Normal primary sample room area radiation is used to monitor selected plant areas where access is required for plant recovery. (Type E)
Radiochemistry Lab. Area Radiation	E	Radiochemistry laboratory area radiation is used to monitor selected plant areas where access is required for plant recovery. (Type E)
Wind Direction	E	Wind direction is required to monitor environmental conditions used to determine the impact of releases of radioactive materials through identified pathways. (Type E)
Wind Speed	E	Wind speed is required to monitor environmental conditions used to determine the impact of releases of radioactive materials through identified pathways. (Type E)
Atmosphere Stability Temperature Difference	E	Atmosphere stability temperature difference is required to monitor environmental conditions used to determine the impact of releases of radioactive materials. (Type E)
Main Steam Line Radiation	E	Main steam line radiation is used to monitor the magnitude of releases of radioactive materials through identified pathways. (Type E)

APR1400 DCD TIER 2

Table 7.5-2 (8 of 8)

Variable	Type	Basis and analysis
High Energy Line Break Area ACU Inlet Radiation	E	High Energy Line Break Area ACU Inlet Radiation is used to monitor radiation releases from the breaks of high energy piping. (Type E)
Auxiliary Building Controlled Area (I,II) HVAC Normal/Emergency Exhaust ACU Inlet Radiation	E	Auxiliary Building Controlled Area (I,II) HVAC Normal/Emergency Exhaust ACU Inlet Radiation is used to monitor radiation leakage in the gaseous effluent from the controlled area. (Type E)
Containment Air Radiation	E	Containment Air Radiation is used to monitor the unidentified leakage from RCS. (Type E)
Fuel Handling Area HVAC Effluent Radiation	E	Fuel Handling Area HVAC Effluent Radiation is used to monitor the radioactivity in the HVAC effluents from the fueling handling area. (Type E)
Compound Building Hot Machine Shop Radiation	E	Compound Building Hot Machine Shop Radiation is used to monitor radioactive releases of identified pathways from the hot machine shop. (Type E)
Steam Generator Blowdown Radiation	E	Steam Generator Blowdown Radiation is used to monitor radioactive leakage of identified pathways from SG blowdown stream. (Type E)
Post-accident Primary Sample Room Radiation	E	Post-accident Primary Sample Room Radiation is used to monitor selected plant area where access is required for plant recovery. (Type E)

APR1400 DCD TIER 2

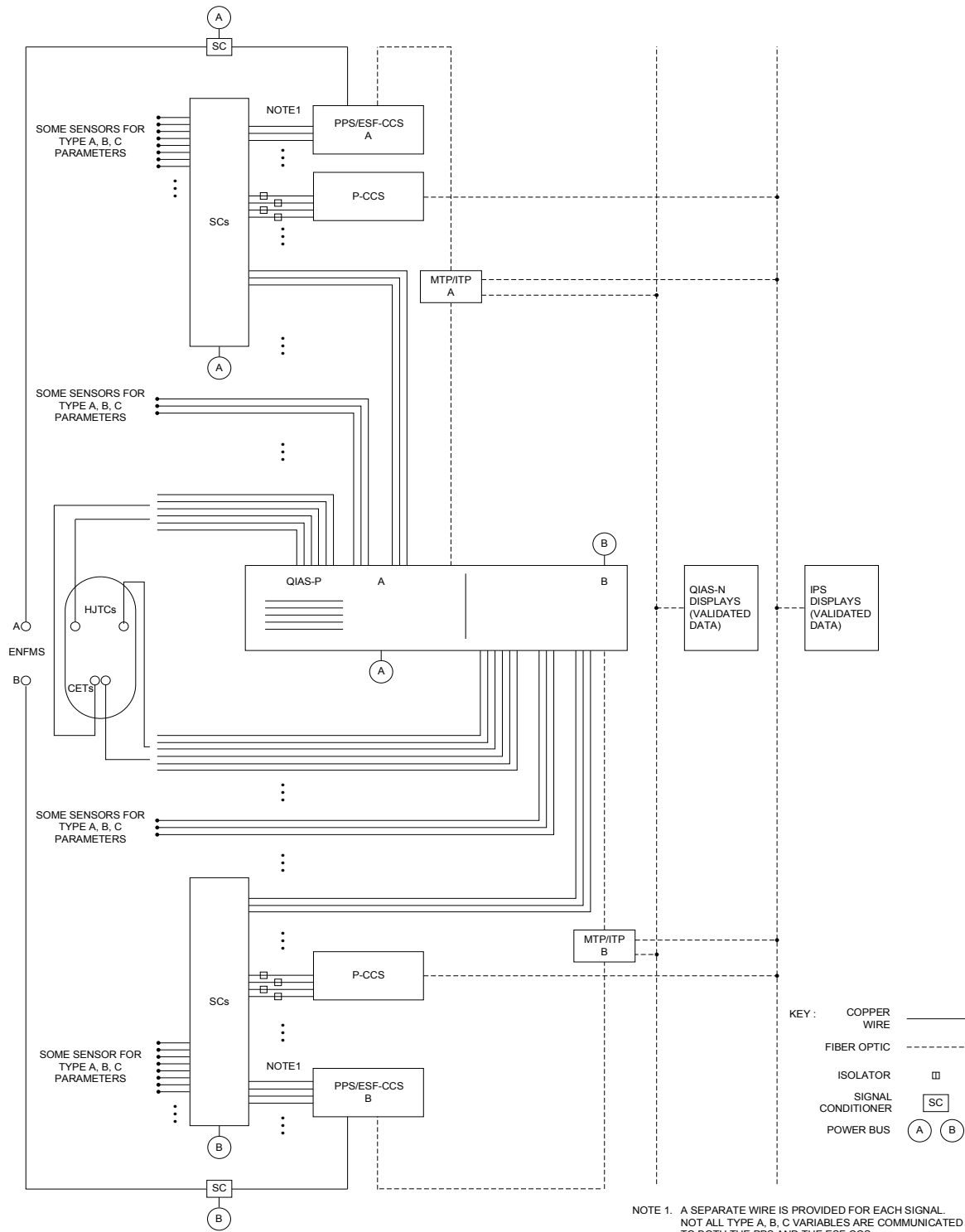
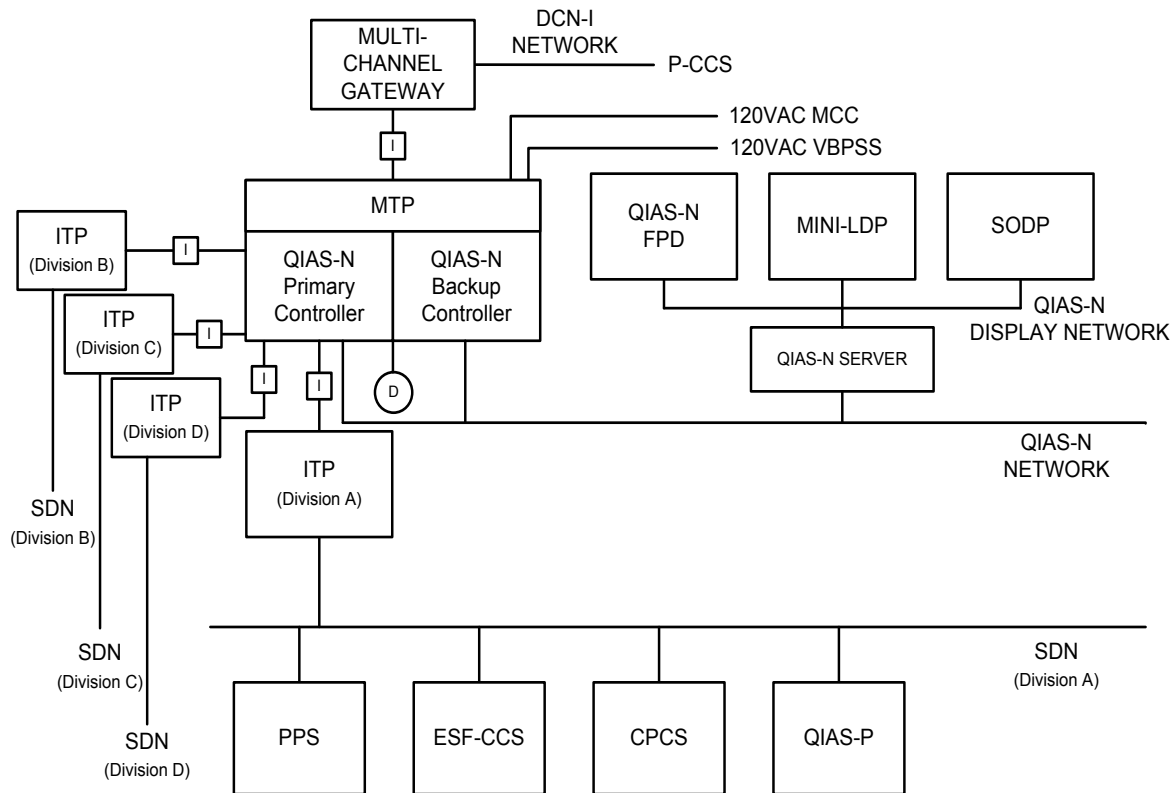


Figure 7.5-1 Diverse Display of Accident Monitoring Type A, B and C Variables

APR1400 DCD TIER 2



KEYS:

ISOLATION DEVICE



POWER SOURCE



LEGENDS:

CPCS : CORE PROTECTION CALCULATOR SYSTEM
 DCN-I : DATA COMMUNICATION NETWORK-INFORMATION
 ESF-CCS : ENGINEERED SAFETY FEATURES-COMPONENT CONTROL SYSTEM
 FPD : FLAT PANEL DISPLAY
 IPS : INFORMATION PROCESSING SYSTEM
 ITP : INTERFACE AND TEST PROCESSOR
 LDP : LARGE DISPLAY PANEL
 MCC : MOTOR CONTROL CENTER
 MTP : MAINTENANCE AND TEST PANEL
 P-CCS : PROCESS-COMPONENT CONTROL SYSTEM
 PPS : PLANT PROTECTION SYSTEM
 QIAS-N : QUALIFIED INDICATION AND ALARM SYSTEM-NON-SAFETY
 QIAS-P : QUALIFIED INDICATION AND ALARM SYSTEM-P
 SDN : SAFETY SYSTEM DATA NETWORK
 SODP : SHUTDOWN OVERVIEW DISPLAY PANEL
 VBSS : VITAL BUS POWER SUPPLY SYSTEM

Figure 7.5-2 QIAS-N Block Diagram

APR1400 DCD TIER 2

HSI Means		Normal Operation	Abnormal Condition (AOO)	DBA Condition	Beyond DBA (CCF)		MCR Evacuation	AIA &MCR Evacuation
OPERATOR CONSOLE	IFPD, LDP (1)							
	Safety Soft Control (ESCM) (2)							
SAFETY CONSOLE	Safety Soft Control (ESCM) (2)							
	Minimum Inventory Switch							
	QIAS-N FPD & Mini-LDP							
	QIAS-P FPD							
	Manual ESFAS Switch & Reactor Trip Switch							
	DMA Switch & DIS							
	RSR Console (IFPD, ESCM, SODP, Reactor Trip Switch)							
RCC	Remote Control Console (ESCM, Conventional Switch) (3)							

Primary Means

Backup Means

Primary Means

Backup Means

(1): Operator Console is used for primary means for the plant operation when the Operator Console is available

(2): ESCM can be used in all mode of operation condition except CCF condition of ESF-CCS.

(3): RCC provides manual control and monitoring means to achieve plant hot shutdown and maintain this condition.

Figure 7.5-3 HSI Primary and Backup Means

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 overpressurization of low-pressure systems.
- b. Prevent overpressurization 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. Provide reasonable assurance of the independence of each safety mechanical divisions of the CCW system.
- f. Provide reasonable assurance of the availability of interlocks for both shutdown cooling pumps and containment spray pumps.

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 Shutdown Cooling System 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 overpressurization

APR1400 DCD TIER 2

protection (LTOP) valve setpoint when the SCS is aligned to the RCS for normal shutdown cooling.

Each SCS suction line has independent, redundant motor-operated isolation valves to prevent overpressurization and provide isolation between the RCS and the SCS. See 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 Shutdown Cooling System 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).

APR1400 DCD TIER 2

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 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. See 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 Safety Injection Tank 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.

APR1400 DCD TIER 2

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.

The isolation valves are manually closed when RCS pressure drops below the setpoint in Table 7.6-1 so that the SITs cannot cause overpressurization of the SCS while the SITs are maintained above atmospheric pressure.

As RCS pressure increases, the valves automatically reopen at the set pressure in accordance with BTP 8-1 (Reference 12).

The opening of the SIT isolation valves provides reasonable assurance that the SITs are available for injection during plant startup.

Automatic opening of the SIT isolation valves when pressurizer pressure exceeds a determined value in Table 7.6-1 or SIAS is present is provided, as shown in Figure 7.6-2. The status indication and BISI of the SIT isolation valves are provided in the MCR.

If the isolation valves are closed and an SIAS is initiated, the isolation valves automatically open in accordance with BTP 8-1. 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 3.9.6.3.1 and 6.3.4 for valve tests.

7.6.1.4 Component Cooling Water Non-essential Supply and Return Header Isolation Valves 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.

APR1400 DCD TIER 2

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.

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 and Figure 7.6-4. 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 CCW Cross Connection Line Isolation Valve Interlocks

The CCW system consists of two independent and redundant closed loop safety divisions. There are two cross connection lines between the two separate divisions, and each cross connection line has two in series motor-operated isolation valves (CC-V-937 and CC-V-938 downstream of the CCW heat exchangers and CC-V-939 and CC-V-940 on the pump suction header).

The design of the CCW system is described in Subsection 9.2.2, and a flow diagram of the isolation valves (CC-V-937, 938, 939, and 940) is provided in Figure 9.2.2-1. The setpoint and function of CCW isolation valves are described in Table 7.6-2.

If one division fails, the isolation valves can be manually opened to supply CCW flow to the other division during normal operation. The valves are normally locked closed and

APR1400 DCD TIER 2

automatically close on a SIAS or low-low CCW surge tank level signal in the event of an accident or transient.

The interlocks provide reasonable assurance of the independence of each safety mechanical division of the CCW system, thereby providing cooling water to safety components required for mitigating an event.

The two series valves powered from different divisions provide reasonable assurance of isolation in the presence of a single failure. The interlocks provide reasonable assurance of the independence of each CCW safety division.

The interlocks for these valves are shown in Figure 7.6-3. The signal path for surge tank interlock is from local level transmitters to the ESF-CCS loop controller for control of these valves.

7.6.1.6 Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps

The containment spray primary function is achieved by two redundant and independent containment spray pumps (CSPs) of divisions C and D. Each CSP has 100% capability for the containment spray function.

The shutdown cooling pumps (SCPs) are designed as backups to the CSPs with 100% capability of the containment spray function if the CSPs are not available. The failure to start of the CSP in division C is used for actuation of the SCP in division A when an SIAS or a CSAS is present. Likewise, the failure to start of the CSP in division D is used for actuation of the SCP in division B.

One CSP is assigned to division C and one to division D independently and are actuated by CSAS or SIAS signals from the ESF-CCS LC via dedicated CIM. One SCP is assigned to division A and one to division B independently and are aligned to perform the function of containment spray if the following three conditions are met at the same time:

- a. CSAS actuation or SIAS actuation
- b. The containment spray pump is unavailable
- c. The cross-connect valves for the containment spray/shutdown cooling pumps are not fully closed.

APR1400 DCD TIER 2

The logic diagram of the interlocks for both the SCPs and CSPs are shown in Figure 7.6-5.

An SCP can only be automatically started on a SIAS/CSAS when the SCP/CSP cross-connect valves are manually aligned for the containment spray function and a CSP is inoperable. Therefore, a single failure of a spurious CSP actuation concurrent with an SCP actuation has no effect on the safety analysis.

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. Conformance with applicable GDC is described in Subsection 7.6.2.1, and conformance 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 are designed to comply with the following codes and regulations:

- a. 10 CFR 50.34(f)(2)(v), “Bypass and Inoperable Status Indication” (Reference 2)

The BISI described in Subsection 7.6.1 is designed in accordance with 10 CFR 50.34(f)(2)(v).

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(h)(3), “Codes and Standards, Safety Systems” (Reference 4)

The important-to-safety interlock systems described in Subsections 7.6.1.1, 7.6.1.3, 7.6.1.4, 7.6.1.5, and 7.6.1.6 are designed in accordance with 10 CFR 50.55a(h)(3) as follows:

The interlock systems important to safety consist of four independent divisions except the SCS suction line relief valves, SCPs, and CSPs, which consist of two divisions. The protection division is physically separated and electrically isolated from the other protection divisions. All equipment/components used for safety-

APR1400 DCD TIER 2

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 the SCS suction line relief valve interlock is available for display at the IPS display and operator module (OM) in the main control room (MCR).

- c. General Design Criterion (GDC) 1, “Quality Standards and Records.” The GDC is contained in 10 CFR Part 50, Appendix A (Reference 5).

The important-to-safety interlock systems discussed in Subsections 7.6.1.1 through 7.6.1.6 are designed in accordance with GDC 1 in conformance with IEEE Std. 603, Clause 5.3. Conformance with GDC 1 is described in Subsection 7.1.2.

- d. 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.

- e. 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.

- f. 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. Conformance with GDC 10 is described in Subsections 7.6.1.1 through 7.6.1.5.

- g. 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, 7.6.1.4, 7.6.1.5, and 7.6.1.6 and maintain interlock

APR1400 DCD TIER 2

variables within safe states by observing the setpoint or component conditions as depicted in Figures 7.6-1A through 7.6-4 and as shown in Tables 7.6-1 and 7.6-2.

h. GDC 15, “Reactor Coolant System Design”

The interlock systems important to safety to prevent overpressurization of the RCS are designed in conformance with GDC 15, as described in Subsections 7.6.1.1 and 7.6.1.2.

i. GDC 16, “Containment Design”

The leak-tightness of the containment system and short-term and long-term performance following a LOCA are designed in conformance with GDC 16, as described in Section 6.2.

j. 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 conformance with GDC 19 to be maintained in a safe condition under accident conditions (see Figures 7.6-1A through 7.6-4).

The SCS suction line relief valves are not required to comply with 10 CFR 50.34(f)(2)(xi) (Reference 6) addressing the TMI Action Plan, Item II.D.3 (Reference 11). 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 Item II.D.3 requirement of the TMI Action Plan.

k. GDC 24, “Separation of Protection and Control Systems”

Conformance with GDC 24 presents the characteristics described in IEEE Std. 603 as follows:

1) Single failure criterion

All interlocks important to safety are designed to comply with the single failure criterion.

APR1400 DCD TIER 2

2) Physical, electrical, and communications independence

Complete physical, electrical, and communication independence 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 prevent non-safety system interactions with safety systems.

4) Auxiliary features

Not applicable to Section 7.6.

5) Power sources

The divisions 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 divisions.

l. 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 the opening of the reactor trip switchgear system (RTSS) circuit breakers, which is described in Section 7.2.

m. 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.

n. 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.

APR1400 DCD TIER 2

o. GDC 34, “Residual Heat Removal”

The interlock systems important to safety are designed in conformance with GDC 34, as described in Subsections 7.6.1.1, 7.6.1.2, 7.6.1.4, 7.6.1.5, and 7.6.1.6.

p. GDC 35, “Emergency Core Cooling”

The interlock systems important to safety are designed in conformance with GDC 35, as described in Subsections 7.6.1.1 through 7.6.1.6.

q. GDC 38, “Containment Heat Removal”

The containment heat removal function implemented by the containment spray system (CSS), which is described in Subsections 6.2.2 and 6.5.2, is designed in conformance with GDC 38.

r. 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 conformance with GDC 41.

s. GDC 44, “Cooling Water”

The CCW non-essential supply and return header isolation valves interlocks, and CCW cross connection line isolation valve interlocks are designed in accordance with GDC 44. Conformance with GDC 44 is described in Subsection 7.6.1.4.

7.6.2.2 Conformance with IEEE Std. 603

This subsection describes the conformance of 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. The CCW non-essential supply and return header isolation valves and CCW cross connection line isolation valve are addressed in Subsection 9.2.2.2.2.4. The SCPs and CSPs are addressed in Subsection 5.4.7.2 and 6.2.2.2.

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 7.6.1.6.

APR1400 DCD TIER 2

b. Completion of Protective Action (Clauses 5.2 and 7.3)

This requirement is not applicable to Section 7.6.

c. Quality (Clause 5.3)

The sensors for the 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 7.6.1.6 are implemented using Class 1E qualified components. They are qualified to operate in the worst case environment to which they are exposed.

e. System Integrity (Clause 5.5)

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.

In the case of the CCW cross connection line isolation valve interlocks, failure of one interlock does not preclude the isolation of each division during accident conditions. In the case of the CCW non-essential supply and return header isolation valves interlocks, the failure of one interlock does not adversely affect the other division. In the case of the interlocks for both SCPs and CSPs, the failure of one interlock does not adversely affect the other division.

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 7.6.1.6.

The method for identifying power and signal cables and cable trays dedicated to the instrumentation, control, and electrical equipment associated with the isolation

APR1400 DCD TIER 2

valves is described in Subsection 7.3.2.3 and complies with NRC RG 1.75 (Reference 7), 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, SIT isolation valve interlocks, CCW non-essential supply and return header isolation valves interlocks, CCW cross connection line isolation valve interlocks, and interlocks for both CSP and SCP exist. The tests are performed in conjunction with inspection of the valves and pumps. 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 and pumps. 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 for the interlocks on the QIAS-N and IPS. For the interlocks, position indication of each valve and operating status of each pump are provided.

i. Control of Access (Clause 5.9)

Access is controlled by administrative procedures.

j. Repair (Clause 5.10)

Components are accessible for repair. One division can be placed out of service for maintenance without jeopardizing the isolation of the SCS, the availability of the SITs, the safety function of CCW, or the interlocks for both CSP and SCP.

k. Identification (Clause 5.11)

APR1400 DCD TIER 2

The instrumentation and cables associated with the interlocks are uniquely identified. The divisions are identified to distinguish between redundant divisions of safety-related equipment.

l. Auxiliary Features (Clause 5.12)

This requirement is not applicable to Section 7.6. Access to equipment rooms and cabinets is limited by the utility to the personnel who are allowed to have access.

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 in accordance with APR1400 human factor guidance described in Chapter 18 for both 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 according to the requirement for the ESF-CCS in which the interlocks important to safety are implemented.

p. Automatic Control (Clauses 6.1 and 7.1)

The SCS suction line isolation valve interlock and SCS suction line relief valve interlock are 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.

The CCW non-essential supply and return header isolation valves interlocks and the CCW cross connection line isolation valve interlocks are designed to close the valve automatically on the CCW surge tank low-low level signal or SIAS.

The interlocks for both SCPs and CSPs are not applicable to this requirement.

APR1400 DCD TIER 2

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 non-essential supply and return header isolation valves interlocks in the division I and the CCW cross connection line isolation valve interlocks cannot override the automatic close signal (SIAS) by a manual operation from the MCR. The CCW non-essential supply and return header isolation valves interlocks in the division II can override the automatic close signal (SIAS) by a manual operation from the MCR to cool the post-accident primary sample cooler rack, if necessary.

The interlocks for both SCPs and CSPs are not applicable to this requirement.

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, CCW non-essential supply and return header isolation valves interlocks, CCW cross connection line isolation valve interlocks, and interlocks for both SCPs and CSPs 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 non-essential supply and return header isolation valves interlocks, CCW cross connection line isolation valve interlocks.

The interlocks for both SCPs and CSPs are not applicable to this requirement.

APR1400 DCD TIER 2

t. Operating Bypasses and Maintenance Bypass (Clauses 6.6, 6.7, 7.4, and 7.5)

Removal of one division for testing does not degrade system reliability. Failure of one of the remaining divisions during a test outage does not generate an unacceptable situation because the valve position indication monitoring, with alarms and administrative controls, effectively precludes inadvertent opening or closing of the valves by the operator.

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.

Multiple setpoints are not required for the SCS suction line relief valve interlock, SIT isolation valve interlock, CCW non-essential supply and return header isolation valves interlocks, or CCW cross connection line isolation valve interlocks.

The interlocks for both SCPs and CSPs are not applicable to this requirement.

v. Power Source Requirements (Clause 8)

The divisions 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 3.9.6.2, 3.9.6.3.1, and 3.9.6.3.6.

System testing complies with the criteria of IEEE Std. 338 (Reference 8), which is endorsed by NRC RG 1.22 (Reference 9) and NRC RG 1.118 (Reference 10). Test intervals and their bases are included in the Technical Specifications (Chapter 16).

APR1400 DCD TIER 2

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 Overpressurization of Low-Pressure Systems

The SCS suction line isolation valve interlock is described in Subsection 7.6.1.1. The interlocks to prevent overpressurization of low-pressure systems meet the design bases in Subsection 7.6.2.

7.6.3.2 Interlocks to Prevent Overpressurization 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 control circuitry for SCS suction line relief valves because the valves are spring-loaded relief valves. The interlocks to prevent overpressurization 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 Safety Injection Tank 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 Component Cooling Water Non-essential Supply and Return Header Isolation Valves

The CCW non-essential supply and return header isolation valves 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.

APR1400 DCD TIER 2

7.6.3.5 Interlocks for Component Cooling Water Cross Connection Line Isolation Valves

The CCW cross connection line isolation valve interlocks are described in Subsection 7.6.1.5. The interlocks required to isolate each separated divisions meet the design bases in Subsection 7.6.2.

7.6.3.6 Interlocks for Both Shutdown Cooling Pumps and Containment Spray Pumps

The interlocks for both SCPs and CSPs are described in Subsection 7.6.1.6. The functionally interchangeable interlocks for both SCPs and CSPs meet the design bases in Subsection 7.6.2.

7.6.4 Combined License Information

No combined license (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, 1991.
2. 10 CFR 50.34(f)(2)(v), "Bypass and Inoperable Status Indication," [I.D.3], U.S. Nuclear Regulatory Commission.
3. ANSI/ANS 51.1-1983, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants," American Nuclear Society, 1983.
4. 10 CFR 50.55a(h)(3), "Codes and Standards, Safety Systems," U.S. Nuclear Regulatory Commission.
5. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
6. 10 CFR 50.34(f)(2)(xi), "Direct Indication of Relief and Safety Valve Position," [II.D.3], U.S. Nuclear Regulatory Commission.
7. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Rev. 3, U.S. Nuclear Regulatory Commission, February 2005.

APR1400 DCD TIER 2

8. IEEE Std. 338-1987, “IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generation Station Safety Systems,” Institute of Electrical and Electronics Engineers, 1987.
9. Regulatory Guide 1.22, “Periodic Testing of Protection System Actuation Functions,” U.S. Nuclear Regulatory Commission, February 1972.
10. Regulatory Guide 1.118, “Periodic Testing of Electric Power and Protection Systems,” Rev. 3, U.S. Nuclear Regulatory Commission, April 1995.
11. NUREG-0737, Item II.D.3, “Clarification of TMI Action Plan Requirements,” U.S. Nuclear Regulatory Commission, 1980.
12. NUREG-0800, Standard Review Plan, BTP 8-1, “Requirements on Motor-Operated Valves in the ECCS Accumulator Lines,” Rev. 3, U.S. Nuclear Regulatory Commission, March 2007.

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 6.3.2.1.1.
- (4) Refer to Figure 6.3.2-1 (Sheet 3 of 3) for the flow diagram of the valves.

APR1400 DCD TIER 2

Table 7.6-2

CCW Non-essential Supply and Return Header Isolation Valves and Cross Connection Line Isolation Valves

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⁾	Closes 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⁾	Isolates the nonessential return headers in the event of an accident
CCW Cross Connection Line Isolation Valves (CC-V-937, CC-V-938, CC-V-939, CC-V-940) ⁽³⁾	SIAS CCW Surge tank low-low level signal ⁽²⁾	Closes to terminate CCW flow to the other safety division 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 (SIAS) cannot be overridden by a manual operation from the MCR in the division I. The automatic close signal (SIAS) can be overridden by a manual operation from the MCR to cool the post-accident primary sample cooler rack in the division II, if necessary. The interlock valves are listed in Table 9.2.2-5. Refer to Figure 9.2.2-1 for a flow diagram of the valves.
- (2) Refer to Subsection 9.2.2.5.4.
- (3) 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 cannot be overridden by a manual operation from the MCR. The interlock valves are listed in Table 9.2.2-5. Refer to Figure 9.2.2-1 for a flow diagram of the valves.

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

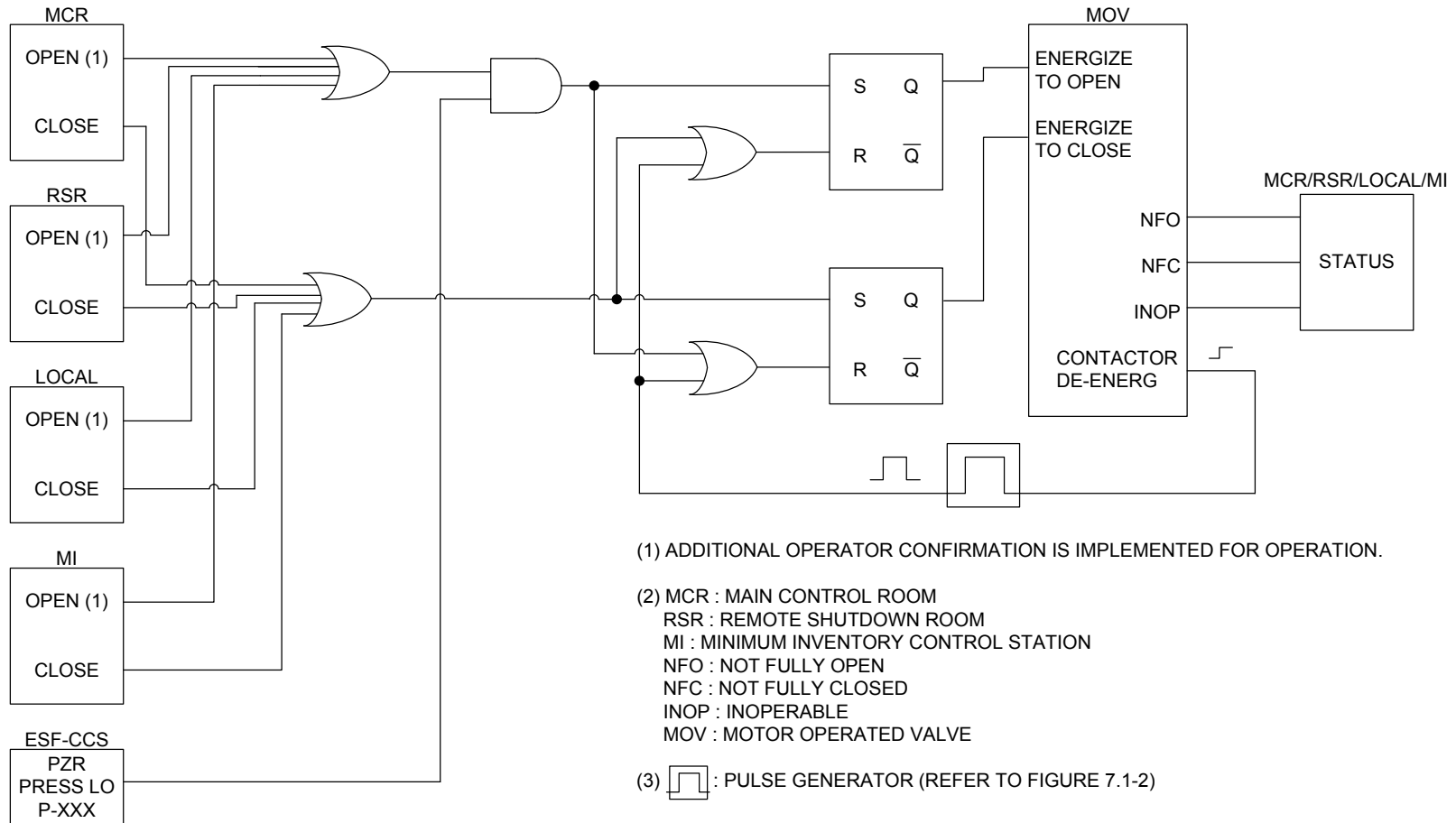


Figure 7.6-1A Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

TAG NO.	DESCRIPTION	CHANNEL	COMPONENT	PZR PRESS
SI-651	SHUTDOWN COOLING SYSTEM SUCTION LINE ISOLATION VALVE	A	MOV (FULL THROW)	P-103A
SI-652	SHUTDOWN COOLING SYSTEM SUCTION LINE ISOLATION VALVE	B	MOV (FULL THROW)	P-104B

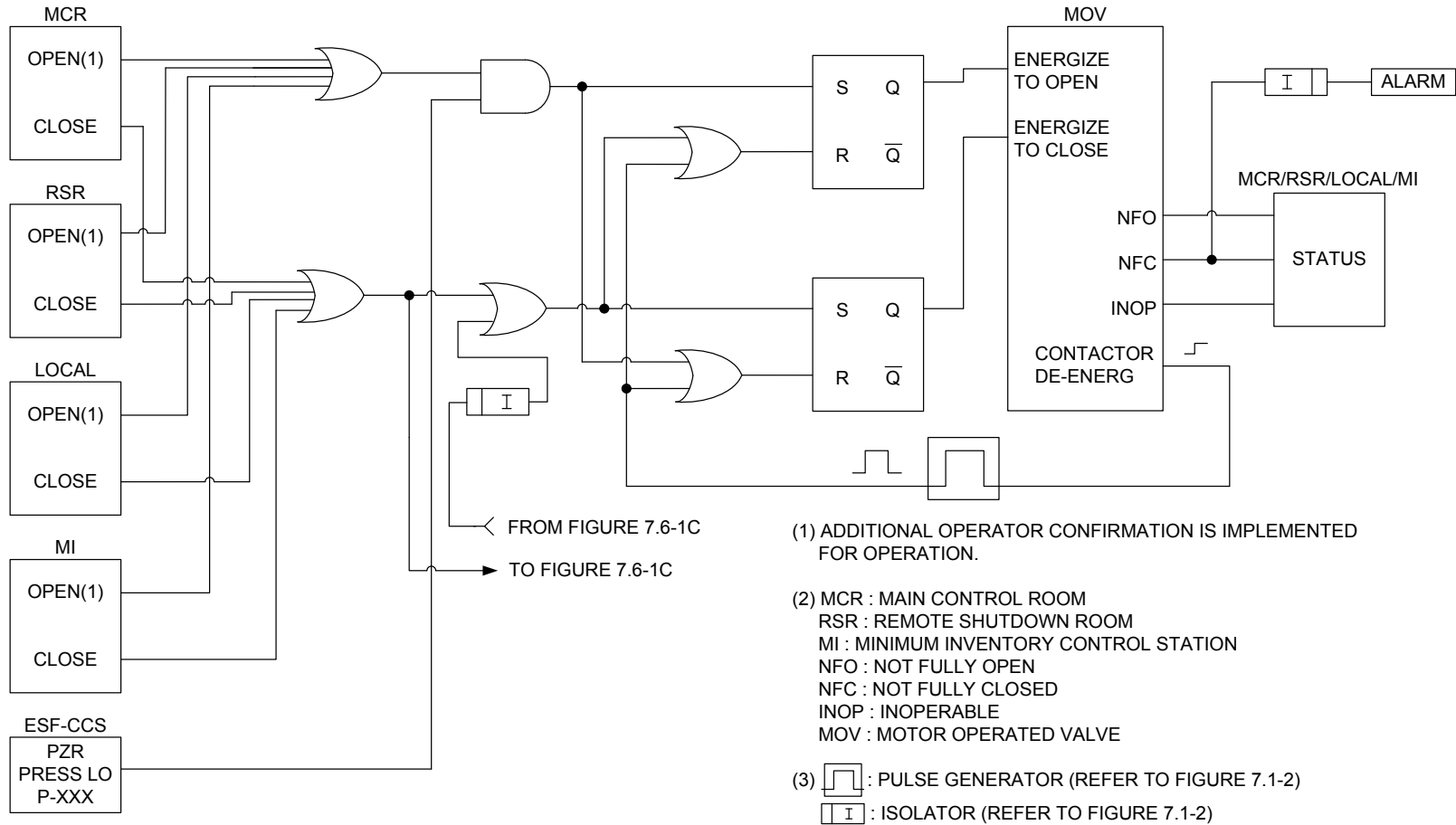


Figure 7.6-1B Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

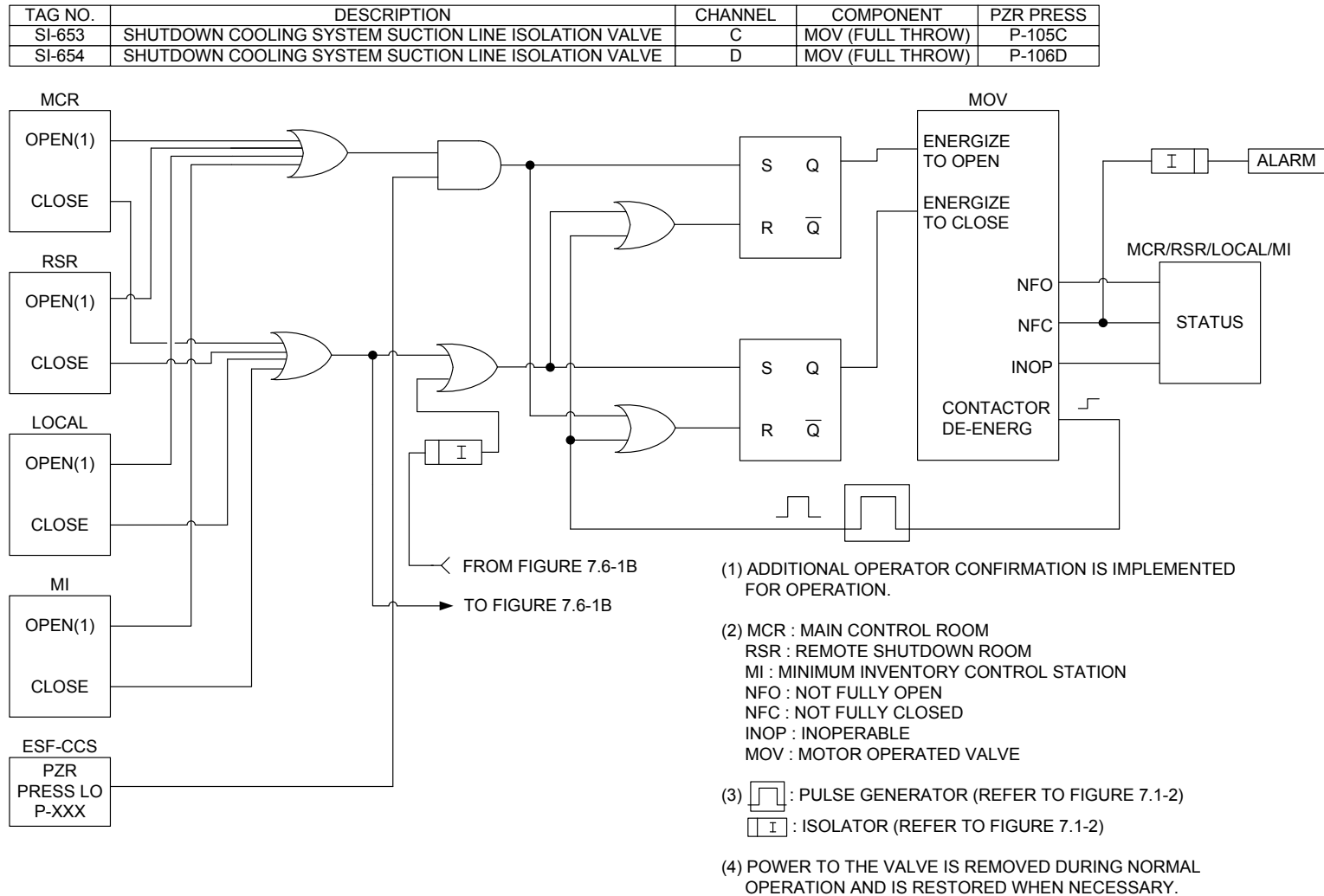


Figure 7.6-1C Interlocks for Shutdown Cooling System Suction Line Isolation Valve

APR1400 DCD TIER 2

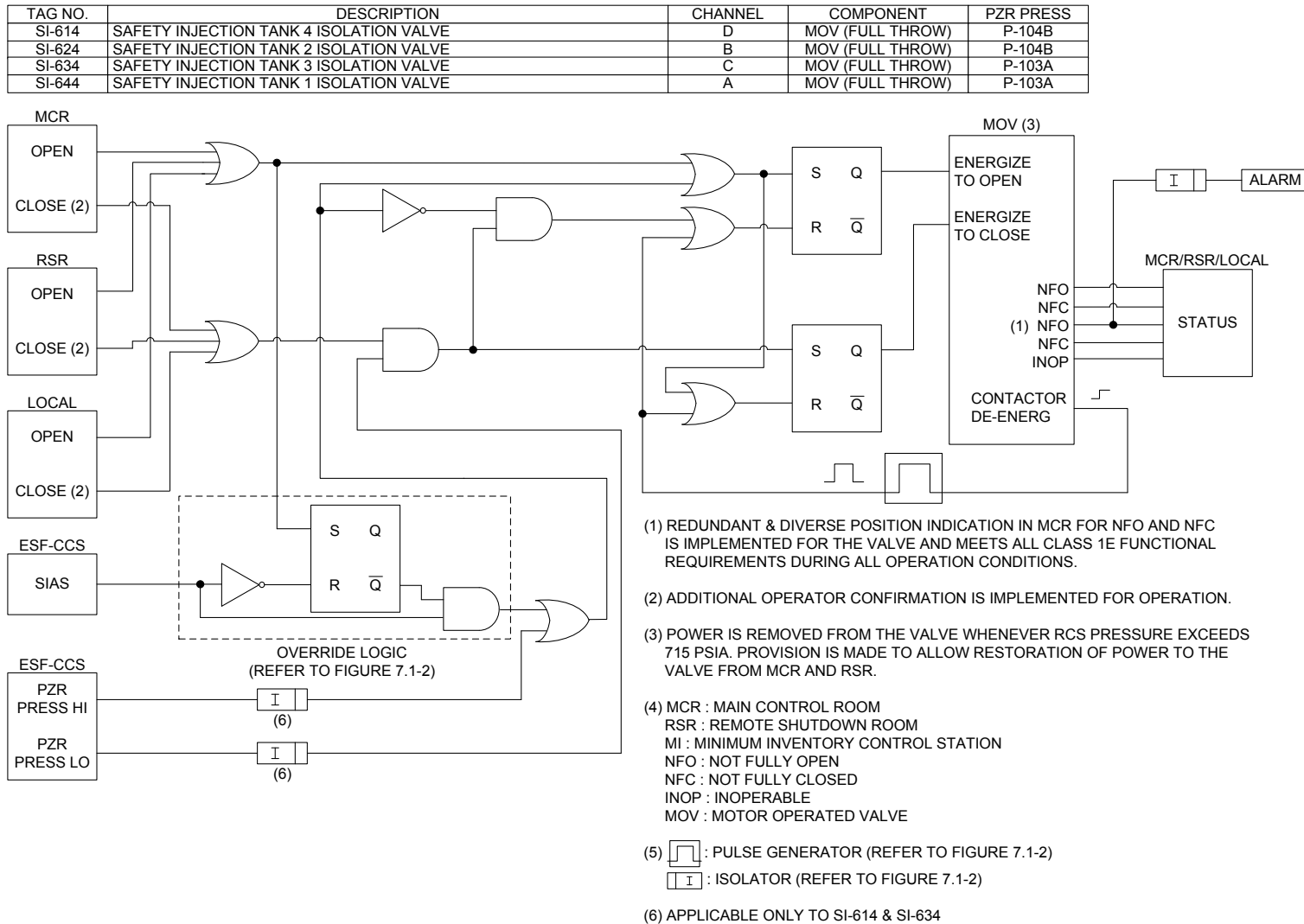


Figure 7.6-2 Interlocks for Safety Injection Tank Isolation Valve

APR1400 DCD TIER 2

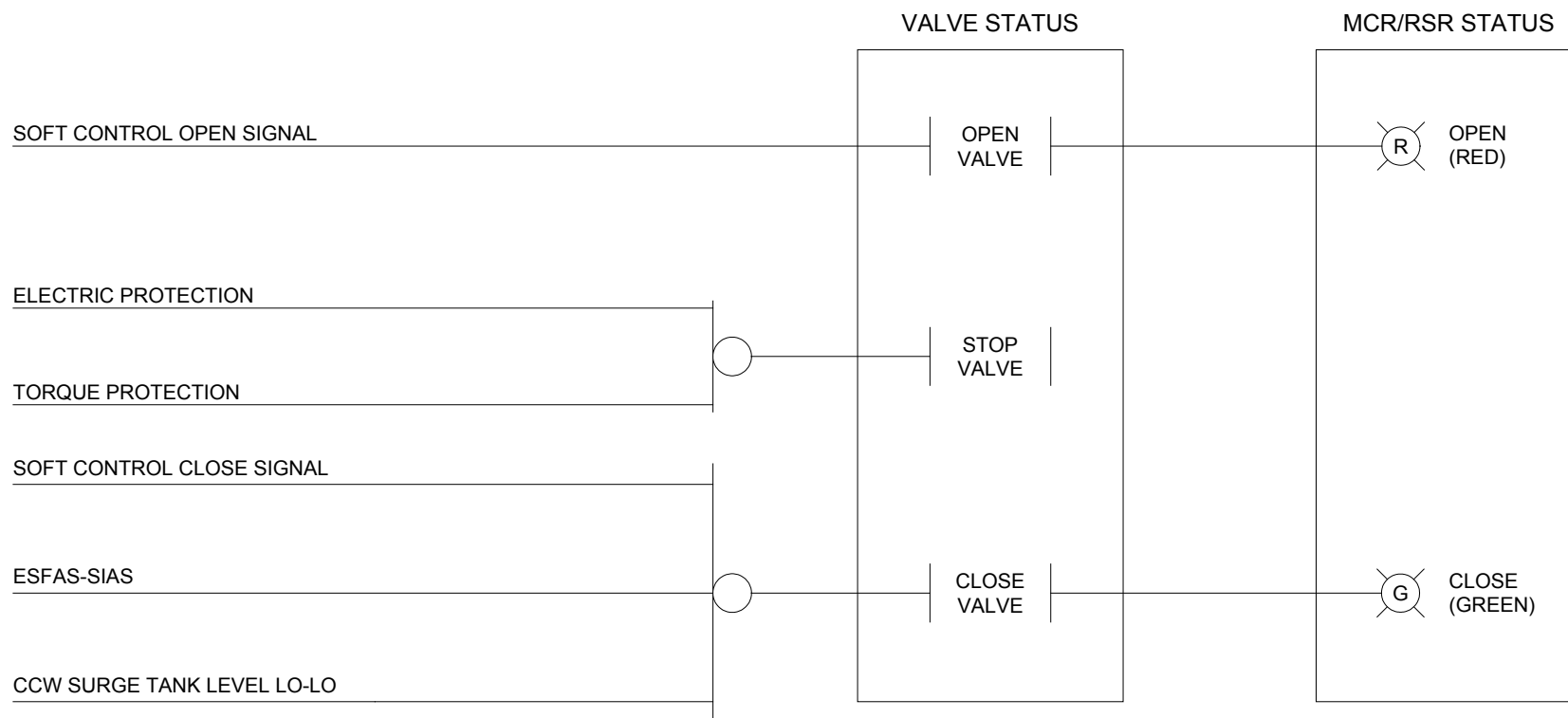


Figure 7.6-3 Interlocks for Component Cooling Water Non-essential Supply and Return Header Isolation Valves in the Division I and Cross Connection Line Isolation Valves

APR1400 DCD TIER 2

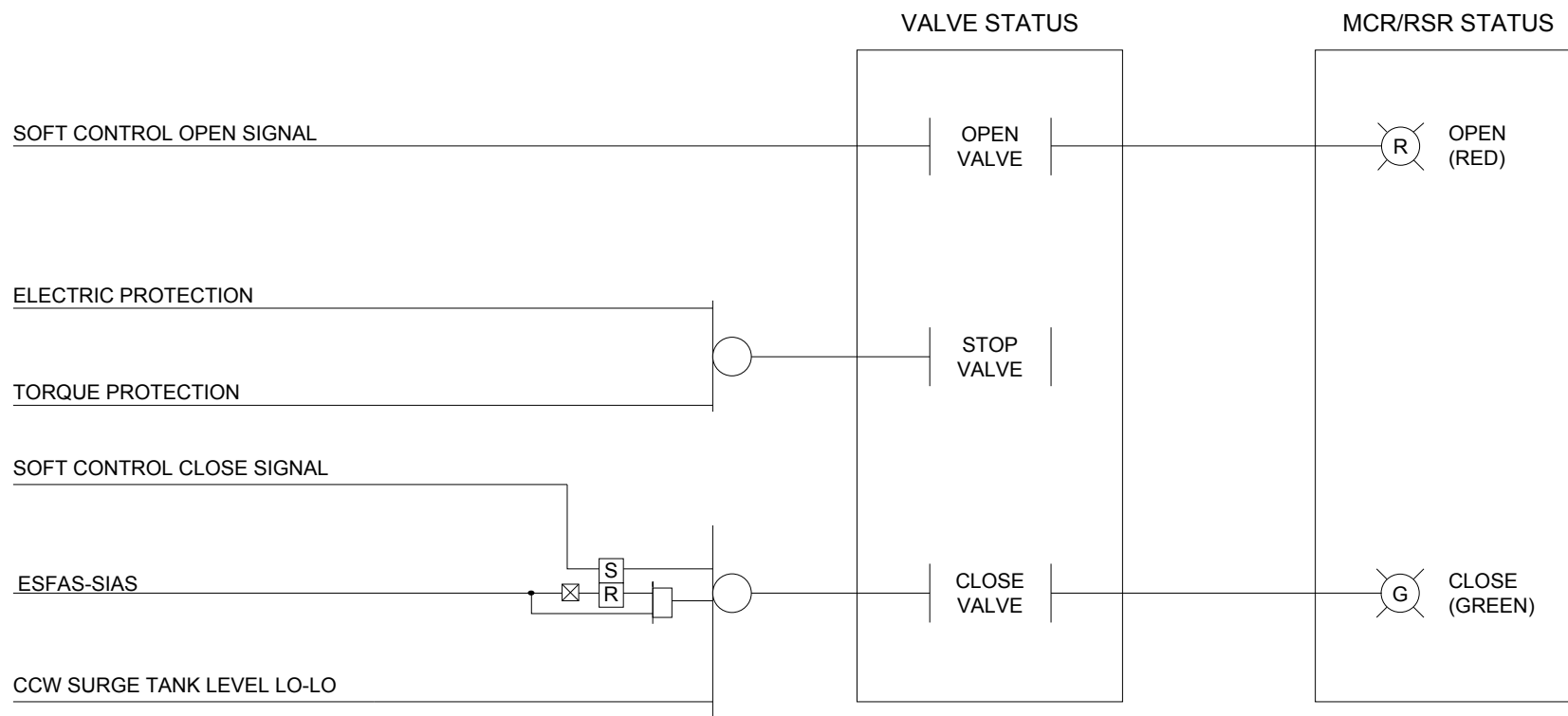


Figure 7.6-4 Interlocks for Component Cooling Water Non-essential Supply and Return Header Isolation Valves in the Division II

APR1400 DCD TIER 2

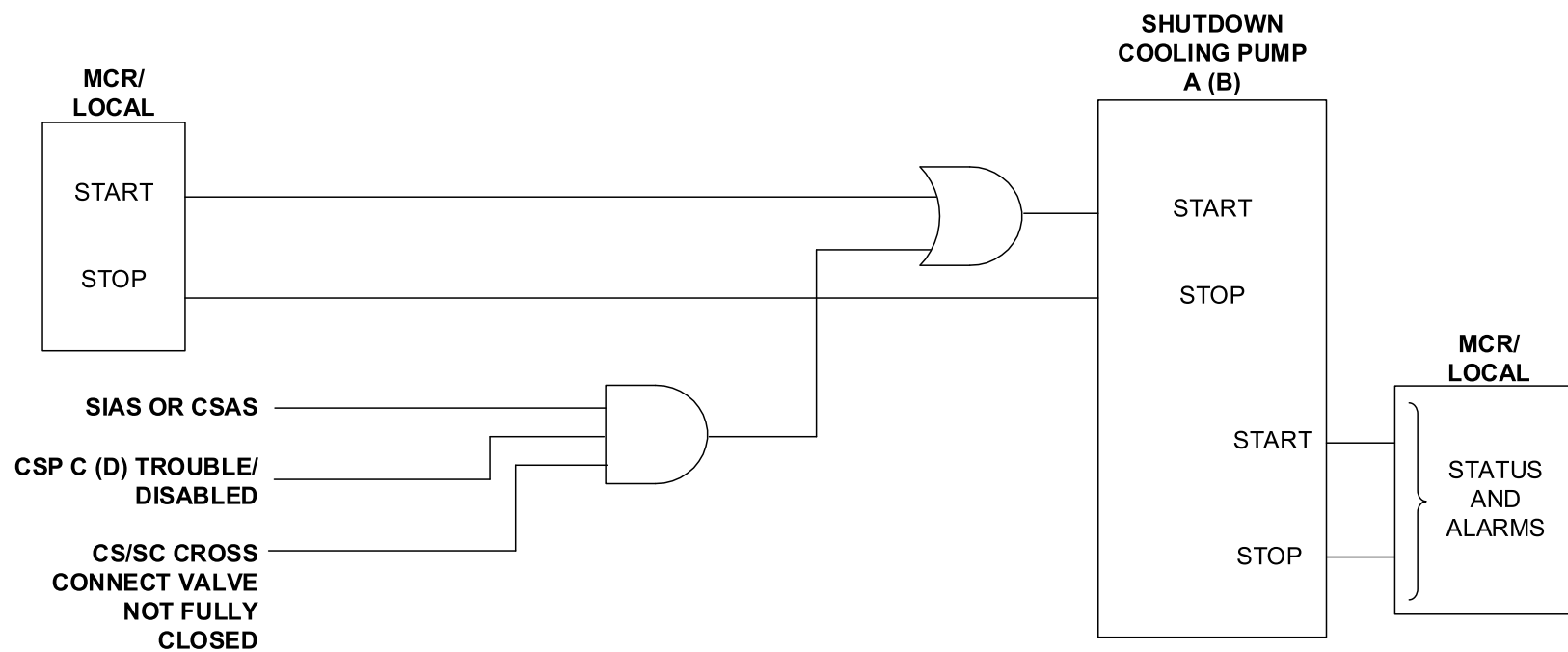


Figure 7.6-5 Interlocks for Both Shutdown Cooling Pump and Containment Spray Pump

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 failure of non-safety control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrence (AOO) in Chapter 15, each control function of Nuclear Steam Supply System (NSSS) is distributed to the separate control group that consists of at least one separate controller. The control groups for NSSS control functions are listed in Table 7.7-1.

APR1400 DCD TIER 2

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), 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 functions.

The control functions performed by non-safety control systems are assigned to separate control groups to enhance the plant availability. The main control groups are selected according to their important to availability control functions, such as turbine bypass control, feedwater control, pressurizer pressure/level control, reactor makeup control/reactor coolant pump (RCP) seal injection, control rod control, RCP control, non-1E alternating current (AC) power control, condenser vacuum and low pressure feedwater heater control, turbine control, high pressure feedwater heater control. The other control functions that are not included in the main control groups are assigned to the miscellaneous BOP control group. The miscellaneous BOP control group includes: circulating water control, condensate pump control, condensate polishing control, spent fuel pool cleaning control, radwaste control, extraction steam control, auxiliary steam control, non-safety HVAC control, non-essential chilled water control, instrument air control, service air control, alternate AC generator control, and deaerator control.

The control systems are implemented on a digital platform that is diverse in both hardware and software 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 that is 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,

APR1400 DCD TIER 2

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 for power maneuvers. 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.

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 changes 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

APR1400 DCD TIER 2

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 (IFPD) to convert these signals to direct current pulses that are transmitted to the control element drive mechanism (CEDM) coils to cause CEA motion.

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

APR1400 DCD TIER 2

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 full-strength 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.

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 UEL, LEL and rod drop contact signals from RSPTs are interfaced to the DRCS via optical isolation to provide separation and independence.

APR1400 DCD TIER 2

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 IFPD in the MCR.

The CWP interlock is interfaced to the protection systems via optical isolation to provide separation and independence.

b. Pressurizer pressure and level control systems

1) 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.

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.

APR1400 DCD TIER 2

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.

2) 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.

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 IFPD 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:

APR1400 DCD TIER 2

- 1) Steady-state operations
- 2) 1 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) 1 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 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.

APR1400 DCD TIER 2

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 the opening of pressurizer or main steam safety valves. See 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

APR1400 DCD TIER 2

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 SBSCS permissive controller to limit the effect of SBSCS main controller failure. See 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 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

APR1400 DCD TIER 2

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 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

APR1400 DCD TIER 2

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 power maneuvers. 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.

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.

APR1400 DCD TIER 2

There are 61 fixed in-core neutron flux detector assemblies with 5 self-powered Rhodium detectors and 1 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.
- 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

APR1400 DCD TIER 2

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 isolation devices 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 to follow the turbine load changes. Startup and control signal processing drawers are independent of the safety channels.

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 Modes 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.

APR1400 DCD TIER 2

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. The P-CCS sends process variables and P-CCS status information to the IPS and QIAS-N. In case the P-CCS is unavailable, non-safety signals for monitoring safe shutdown are hardwired to the QIAS-N. The components are assigned to the group controller for system-level control and loop controller (LC) for component-level control to minimize the plant impact due to system or component failures, as shown in Figure 7.7-8.

Standardized logics 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 turbine/generator control system and provides system-level status information to the IPS and QIAS-N. The MCR/RSR master transfer switches have the function to disable the P-CCS controls in the MCR and to enable the P-CCS controls in the RSR.

The P-CCS LCs are located in the vicinity of the controlled component. The LC and internal data communications are redundant.

The non-safety soft control on the IFPD provides human-system interfaces (HSIs) for P-CCS controls.

l. 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, heated junction

APR1400 DCD TIER 2

thermocouple (HJTC) probes monitor the level in the RV. These systems are also used to monitor the 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 pressurizer (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.

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

APR1400 DCD TIER 2

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.

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 at least three 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 the average of the input channels. If the deviation between the input channels exceeds an acceptable level, the input channel that has less deviation from the PRV is used as the controlling signal.

The signal validation logic functions as follows:

APR1400 DCD TIER 2

- 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)
- 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 IFPD in the MCR. Two valves are powered from Vital A power, and the other two are powered from Vital B power.

APR1400 DCD TIER 2

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

The HMS allows adiabatic, controlled burning of hydrogen at low concentrations during degraded core accident conditions. Divisionalized 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 is designed against aircraft impact to meet the requirements of 10 CFR 50.150 (Reference 11). 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 five minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to the 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 consists of divisionalized safety control and non-safety controls to achieve plant hot shutdown. The signals from the RCC are

APR1400 DCD TIER 2

routed from the RCC to the I&C equipment room as well as to the motor control center (MCC) through multiplexers.

The RCC is designed with the following design features:

- The RCC provides manual control and monitoring means to bring the plant to hot standby under accident conditions.
- The RCC is manipulated by one reactor operator who monitors and controls the plant.
- For control and monitoring, the RCC provides four divisionalized ESCMs for safety component control and process monitoring. Conventional hardwired switches, related indicators, and non-safety component control are also provided.
- The ESCMs and conventional switches in the RCC are physically separated from the MCR and RSR. These ESCMs are connected to the ESF-CCS LC in the remote multiplexer room through a dedicated route which is separated from the routes of the MCR and the RSR. The conventional switches are connected to the P-CCS cabinets in the remote multiplexer room through a dedicated route. This route also is separated from the routes of the MCR and the RSR.
- In normal conditions, the MCR/RCC transfer switch is in MCR mode and the signals from the control channel gateway (CCG) of the RCC are disconnected. When the MCR/RCC transfer switch is switched to the RCC mode, the signals from the CCG of the RCC are connected to the ESF-CCS LC and the signals from CCG of the MCR are disconnected.
- No single credible event that would require the concurrent evacuation of the MCR and the RSR (or fire damage in the MCR and RSR) would make the RCC inoperable.
- The ESF-CCS LCs and P-CCS LCs that are related with plant hot shutdown are interfaced with the RCC panel.

APR1400 DCD TIER 2

- MCR/RCC transfer switches are located in the MCR. MCR/RCC transfer switches are provided for safety division A, B, C, D, and the non-safety division. One transfer switch is provided for each division of ESF-CCS LC and each division of P-CCS LC, respectively. These transfer switches disconnect signal paths between the ESCMs in the MCR and the RSR and ESF-CCS LC in the remote multiplexer room.
- The RCC panel room is located on the opposite side of the plant from the MCR and the RSR so that an aircraft impact cannot affect the MCR, RSR, and the RCC panel.
- The ESCMs on the RCC are seismically and environmentally qualified as class 1E.
- The ESCMs on the RCC have same design features as those on the MCR and the RSR. The ESCMs are verified to meet independence, physical separation, and EMI/RFI requirements as described in DCD Tier 1, Section 2.5.4.1, Items 2 and 16 and as detailed in the corresponding ITAAC.

The I&C system architecture for the RCC panel is shown in Figure 7.7-14

7.7.1.2 Main Control Room 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 an adjacent meeting room.
- 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 SRP 9.5.1.1 (Reference 1), which requires consideration of the exposure to fires that cause damage or require personnel evacuation. Redundant divisions of safety equipment are designed to accommodate separation by locating them in different unmanned I&C equipment rooms. MCR/RSR master 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. The layout of the MCR is shown in Figure 7.7-13.

- a. MCR and consoles

Conformance with GDC 19 is achieved by implementation of the MCR and RSR.

The main operating area of the MCR is designed to continuously accommodate the normal and shift operating staff.

The MCR, which includes a meeting room adjacent to the main operating area, is able to accommodate the operating staff.

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 IFPDs, pointing devices, and ESCMs.

The IFPDs and ESCMs on the operator console are used as the primary means of operation as follows:

APR1400 DCD TIER 2

- 1) The IFPDs are used for non-safety components controlled by the P-CCS during normal, abnormal, and accident conditions.
- 2) The ESCMs are used for safety components controlled by the ESF-CCS during normal, abnormal, and accident conditions, except during a common-cause failure (CCF) of digital safety I&C systems.

The I&C systems to protect against potential CCF of digital safety I&C systems is described in Section 7.8.

The safety console provides the operator with credited backup control, alarm, and indication.

The safety console contains ESCMs, a mini-LDP, QIAS-N FPDs, QIAS-P FPDs, operator modules, diverse manual ESF actuation switches, DIS FPDs, and minimum inventory switches.

The MCR operator consoles and safety console are seismically qualified to perform their safety functions during and following a seismic event.

To minimize the potential for multiple division damage within the MCR console or RSC, the following design features are employed:

- 1) Low energy circuits (switch contact and lamps) are used to the maximum extent practical.
- 2) 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 (Reference 12).
- 3) Electrical independence of divisionalized circuits is maintained throughout the MCR operator consoles and safety console enclosures.

Although the design features above minimize the potential for multiple redundant division damage, the following design features accommodate such a catastrophic event:

APR1400 DCD TIER 2

- 1) All MCR circuits (e.g., flat panel displays, switches) are isolated from the electronics (e.g., controller cabinets, monitoring systems, instrumentations) to which they interface. Similarly, all RSC circuits are isolated from the electronics. Therefore, the MCR operator consoles, LDP, safety console, and RSC circuits are inherently isolated from each other.
- 2) All MCR operator consoles, safety console, and RSC circuits are designed passively. Momentary contacts are used for all switches, and the memory of MCR operator consoles and safety console commands is retained only in electronics 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.
- 3) 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.

The workstation disable switch (WDS) is to disconnect the signal interface of the IFPD and peripheral devices (e.g., mouse, keyboard) from the node of the DCN-I network should these non-safety devices generate spurious signals.

The WDS is located on each operator console and is a hardwired two-position (enable/disable) type of cam switch. Therefore, there are five WDSs for the RO, TO, EO, SS, and STA console. The keyboard, monitor, and mouse of the operator console are connected to the keyboard/video/mouse (KVM) extender. The KVM extender sends signals over an internal communication cable between the KVM extender and the network switch. When the WDS is switched to the disable mode, the switch disconnects 120 Vac power that comes from the power branch of the non-safety vital bus power supply system (VBPSS) to the KVM extender on the corresponding operator console. The configuration of the WDS will be shown in Figure 7.7-15.

APR1400 DCD TIER 2

The WDS does not have any software and, therefore, is not subject to a software CCF. The failure of a WDS does not impact any safety devices, including ESCMs at the operator console, because the WDS does not have any interfaces with safety devices. If a single failure of a WDS occurs, the operator can use the IFPD and peripheral devices at another operator console. A multiple failure of all five WDSs occurring concurrently is highly unlikely because the WDSs are hardwired devices and each WDS is separated, which enables an operator to perform the required operator actions on the safety console.

MCR/RSR master 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 the 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.

b. TSC and ERF Interfaces

The guidance for the TSC and the ERF is defined in NUREG-0696 (Reference 13). 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.

APR1400 DCD TIER 2

7.7.1.3 Large Display Panel

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 Information Processing System

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 and RSR 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 the information flat panel display (IFPD) 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.

APR1400 DCD TIER 2

- 2) Performs application processing on the acquired data via NSSS, BOP and general plant monitoring program tasks.
- 3) Provides detailed plant process data to the operating staff via the IFPD 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 control.
- 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.
- 13) Indicates the quality of the input values. The quality is specified as follows:
 - a) Good Scan is on and point is in range
 - b) Fair Operator entered value
 - c) Poor Generated from certain algorithms if some input were bad and some input were good

APR1400 DCD TIER 2

- d) Bad Scan is off (with no operator entered value) or sensor has failed, out of engineering range

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

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 IFPD 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:

1) 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 workstations via data communication network.

The IPS application functions minimize processor loading, simplify task scheduling, and minimize the potential for unintended interactions among application tasks.

2) Engineering workstation

APR1400 DCD TIER 2

An engineering workstation 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.

3) Information flat panel display

IFPD consists of a flat panel display, pointing device, display processor, and communication interface. Each IFPD is driven by a dedicated display processor.

The display system communicates with the IPS servers and engineering workstation over a data communication network. The ESCMs connected to the IFPD are physically and electrically isolated from the IPS.

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. Information processing system 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. Nuclear application programs

APR1400 DCD TIER 2

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.

1) 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 IPS 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 No.1 (Reference 14).

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 critical safety function identified by the functional requirements analysis (FRA) described in Section 18.3, including at a minimum the following critical safety functions:

- a) Core reactivity control
- b) Maintenance of vital auxiliaries
- c) Reactor coolant system inventory control
- d) Reactor coolant system pressure control
- e) Core heat removal
- f) Reactor coolant system heat removal
- g) Containment isolation
- h) Containment temperature and pressure control
- i) Containment combustible gas control (radioactive emissions control)

APR1400 DCD TIER 2

SPADES+ provides the capability to display the success path status for each critical safety function and initiates an alarm when the function becomes inoperable.

2) 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 the Functional Design Requirements for a Core Operating Limit Supervisory System for APR1400 Technical Report (Reference 5) and Overview Description of the Core Operating Limit Supervisory System (Reference 15). 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.

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:

- a) The safety limit is not exceeded as a result of any anticipated operational occurrence (AOO).
- b) 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 because 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

APR1400 DCD TIER 2

maintenance of core conditions within the LCOs of the 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 IFPD:

- a) Linear heat rate core power operating limit
- b) DNBR core power operating limit
- c) Total core power
- d) Margin between core power and nearest core power operating limit
- e) Axial shape index

The COLSS alarms are initiated if:

- a) Core power exceeds a core power operating limit.
- b) Axial shape index exceeds its limits.

APR1400 DCD TIER 2

- c) Azimuthal tilt exceeds the azimuthal tilt limit.

The Technical Specifications for the reactor core provide an alternate means of monitoring the LCOs in the event the IPS is out of service. When the IPS is out of service, the 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.

- 3) Control element assembly application program

The CEA application program is provided to help the operator monitor CEA-related Technical Specifications as follows:

- a) Power-dependent insertion limits are operating limits on the allowable insertion of the full-strength (regulating) CEAs as a function of reactor power.
- b) 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. Some of the group positions are calculated in CEA application programs and the results of calculation are used for the COLSS.
- c) The CEA application program monitors the insertion and withdrawal sequence of CEA groups.
- d) The CEA application program monitors the insertion and withdrawal sequence of CEA groups. An out-of-sequence alarming signal is generated if improper sequence or separation between CEA groups is detected.
- e) CEA exposures are calculated every hour and reported once a day.

- 4) Deviation and setpoint monitoring program

The IPS performs deviation and setpoint monitoring for two multi division, separate systems: the core protection calculator system (CPCS) and the plant

APR1400 DCD TIER 2

protection system (PPS). Data received from these systems consist of sensor inputs, setpoints, and calculated values.

5) 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.

e. 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.

f. Interface applications

The IPS interface applications are as follows:

1) Interface with soft control for non-safety components

The IFPD 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.

The IFPD 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 IFPD. The soft control is described in Section 18.7.

2) Interface with LDP

The IPS provides plant information periodically to the LDP as follows:

APR1400 DCD TIER 2

- a) Plant process status including status of major plant systems, status of major system components, and values of parameters calculated by the IPS
- b) 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.

3) Interface with the ESF-CCS soft control module

The IFPD 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 IFPD 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.

g. 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.

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 IFPDs and the LDP.

APR1400 DCD TIER 2

7.7.1.5 Nuclear Steam Supply System 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 unidirectional ex-core neutron flux signals from the ENFMS detectors through the Class 1E qualified isolation devices 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 to meet 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.

APR1400 DCD TIER 2

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 a single failure do not cause plant conditions that are more severe than those described in Chapter 15. The single failure list for the safety analysis is provided in Table 15.0-4. The safety analysis of Chapter 15 does not require these systems to remain functional.

Control groups of major control functions and postulated events due to a single failure of a control group are described in Table 7.7-1. The evaluation results of multiple function failures due to a single failure of a shared signal are described in the Control System CCF Analysis Technical Report (Reference 10).

The following expected failures caused by control system CCF are evaluated to confirm that the event consequences of Chapter 15 are still effective and the analysis acceptance criteria are met.

- a. The results of multiple failures of a single control group due to control system CCF meet the AOO acceptance criteria of Chapter 15.
- b. The results of multiple failures of more than one control group due to control system CCF meet the PA acceptance criteria of Chapter 15.

APR1400 DCD TIER 2

- c. The results of multiple failures of IFPD control commands due to control system CCF meet the PA acceptance criteria of Chapter 15.

The Control System CCF Analysis Technical Report describes the detailed assumptions and evaluation results for the above postulated control system CCFs.

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 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 Diversity and Defense-in-Depth

The non-safety control systems are implemented on diverse platforms from the safety systems to preclude concurrent CCF of both control and safety systems, as described in the Diversity and the Defense-in-Depth Technical Report (Reference 8). The software CCF of non-safety control systems is described in the Control System CCF Analysis Technical Report.

The diverse I&C functions that are designed to protect against the potential CCF of the digital safety I&C systems are described in Section 7.8.

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 separation and electrical isolation and maintain communication independence from the safety systems.
- c. Safety functions are not controlled by non-safety soft controls on the IFPD.
- d. For important control functions, multiple sensors are used, and a control signal validation algorithm is applied.
- e. The non-safety control systems include 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.

APR1400 DCD TIER 2

7.7.2.10 Control of Access

Equipment related to control systems that is 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. Access to engineering workstations 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-safety systems that interface with safety systems are designed so that credible failures in the control and monitoring systems do not impact the operation of safety systems. The control systems have physical separation and electrical isolation, and maintain communication independence from the safety systems.

The HSI for MCR and RSR is designed in accordance with the Style Guide.

7.7.4 Combined License Information

No combined license (COL) information is required with regard to Section 7.7.

APR1400 DCD TIER 2

7.7.5 References

1. NUREG-0800, Standard Review Plan, Section 9.5.1.1, "Fire Protection Program," U.S. Nuclear Regulatory Commission, February 2009.
2. Regulatory Guide 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Rev. 4, U.S. Nuclear Regulatory Commission, June 2006.
3. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Rev. 1, U.S. Nuclear Regulatory Commission, February 2010.
4. APR1400-E-I-NR-14012-P, "Style Guide," Rev. 2, KEPCO & KHNP, January 2018.
5. APR1400-F-C-NR-14002-P, "Functional Design Requirements for a Core Operating Limit Supervisory System for APR1400," Rev. 1, KEPCO & KHNP, February 2017.
6. Regulatory Guide 1.133, "Loose-Part Detection Program for the Primary System of Light-Water-Cooled Reactors," Rev. 1, U.S. Nuclear Regulatory Commission, May 1981.
7. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.
8. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
9. APR1400-Z-A-NR-14019-P, "CCF Coping Analysis," Rev. 3, KEPCO & KHNP, July 2018.
10. APR1400-Z-J-NR-14012-P, "Control System CCF Analysis," Rev. 3, KEPCO & KHNP, May 2018.
11. 10 CFR 50.150, "Aircraft Impact Assessment," U.S. Nuclear Regulatory Commission.
12. IEEE Std. 383-2003, "IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

APR1400 DCD TIER 2

13. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, 1981.
14. NUREG-0737, Supplement No. 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability," U.S. Nuclear Regulatory Commission, 1983.
15. CEN-312-P, "Overview Description of the Core Operating Limit Supervisory System," Rev. 01-P, Combustion Engineering, Inc., November 1986.

APR1400 DCD TIER 2

Table 7.7-1

Control Groups for the NSSS Control Functions

Control Group ⁽³⁾	Postulated Events due to a Single Failure in the Corresponding Control Group ⁽¹⁾				
	Excessive or Deficient Feedwater Flow	Full Open of Any One TBV	Excessive Charging Flow or Excessive PZR Spray	Uncontrolled CEA Withdrawal	Inadvertent Deboration
SG 1 FW Control (FWCS 1)	×				
SG 2 FW Control (FWCS 2)	×				
PZR Pressure Control (PPCS)			× (Excessive PZR Spray)		
PZR Level Control (PLCS)			× (Excessive Charging Flow)		
Turbine Bypass Control (SBCS Main)		× ⁽²⁾			
Turbine Bypass Control (SBCS Permissive)		×			
Reactor Makeup Control (CVCS)					×
Control Rod Control (RRS/RPCS)				×	
Control Rod Control (DRCS)				× ⁽²⁾	

(1) This table describes that one control group failure does not cause credible failures in other control groups.

(2) An interlock signal is provided for this control group from a separate control group or safety systems, to limit the failure effect of the control group.

(3) Each control group consists of at least one separate controller. A detailed description of all control groups including BOP control functions is provided in the Control System CCF Analysis Technical Report.

(4) Postulated events due to a single failure of non-safety control system do not cause plant conditions more severe than those described in the analysis of AOO in Chapter 15. Refer to the Control System CCF Analysis Technical Report.

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. See Subsection 7.2.1.7.	Interlock: Blocks control rod withdrawal on automatic, manual group and manual individual DRCS control modes.

APR1400 DCD TIER 2

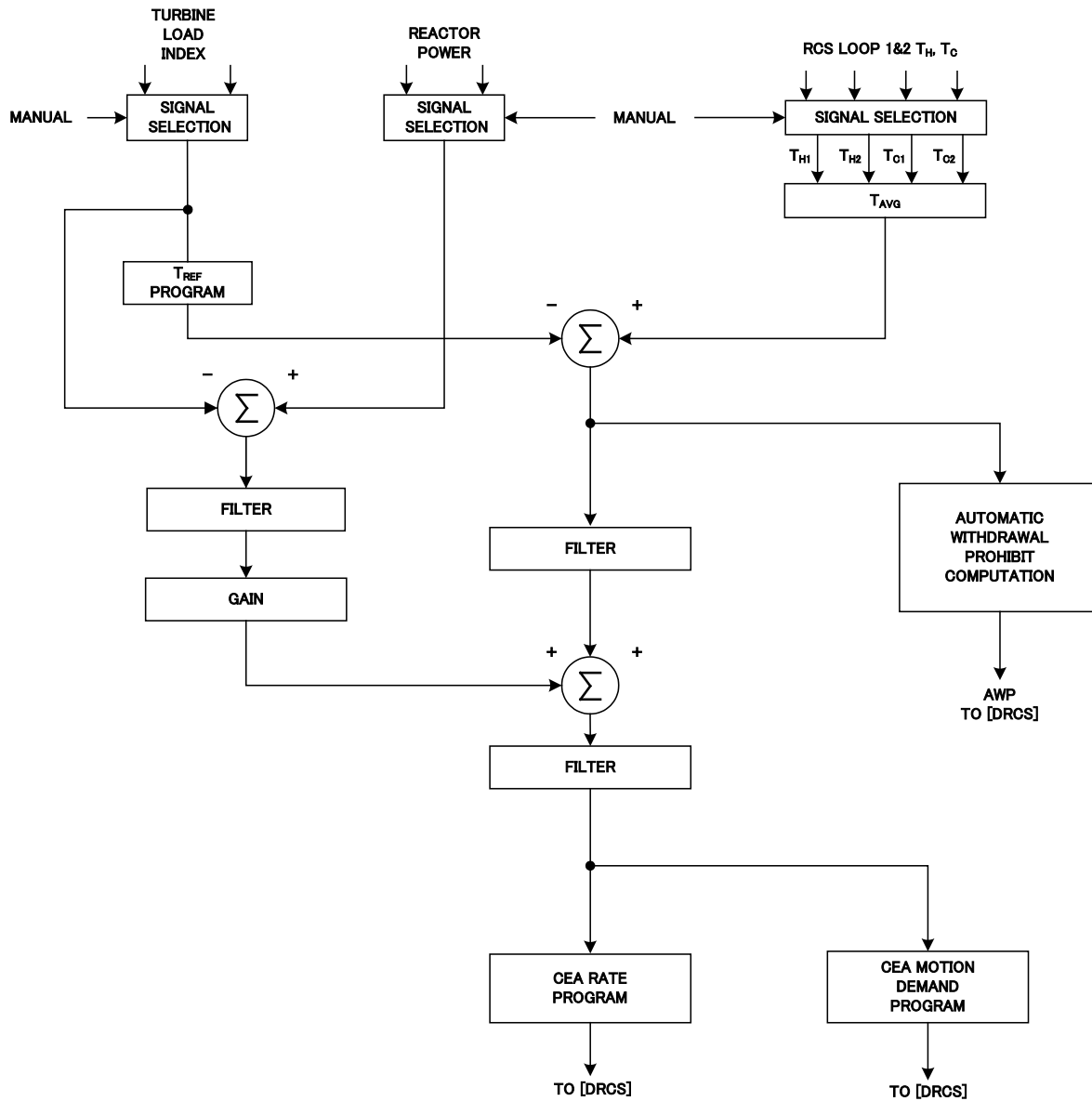


Figure 7.7-1 Reactor Regulating System Block Diagram

APR1400 DCD TIER 2

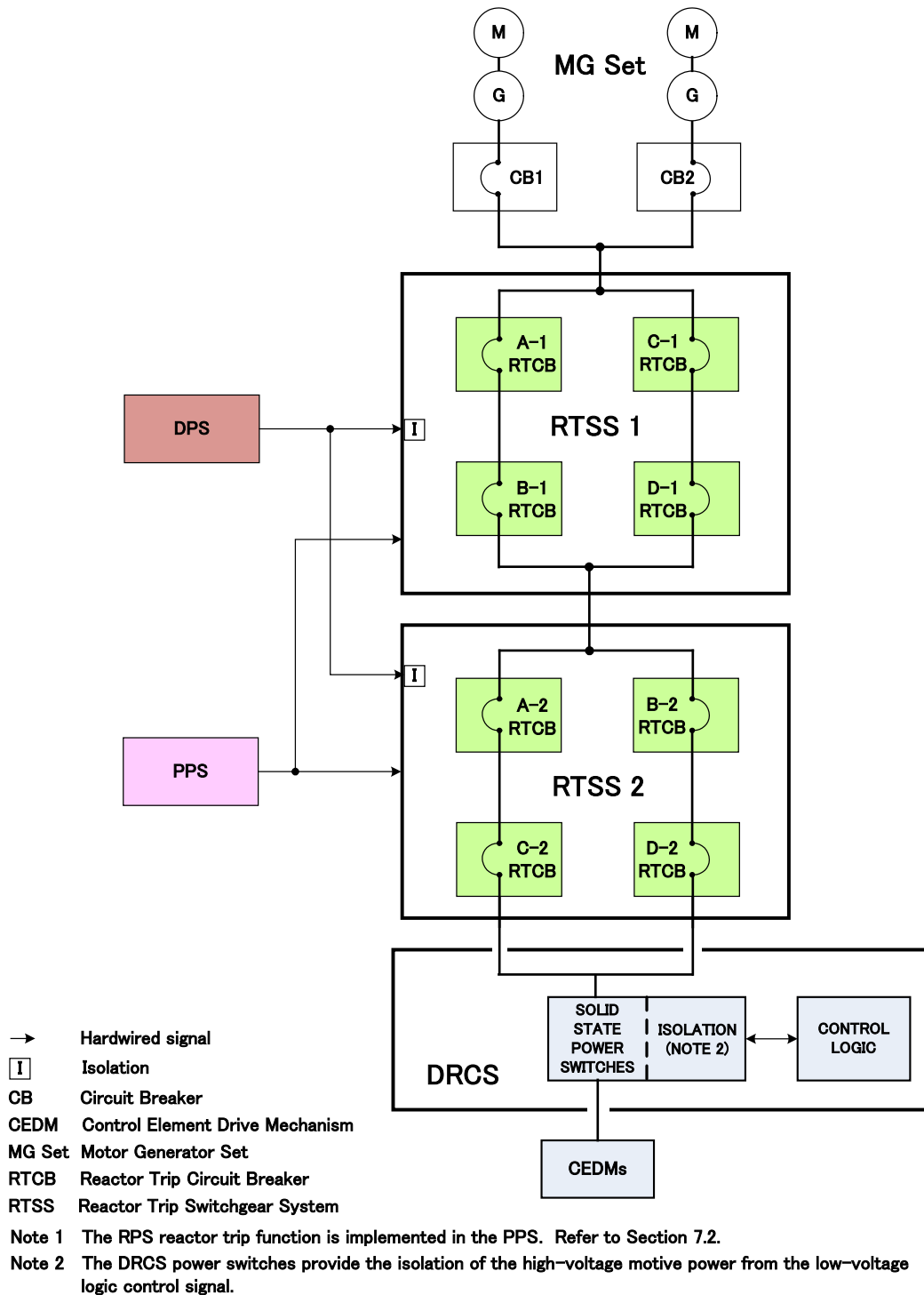


Figure 7.7-2 Digital Rod Control System - Reactor Protection System Interface Block Diagram

APR1400 DCD TIER 2

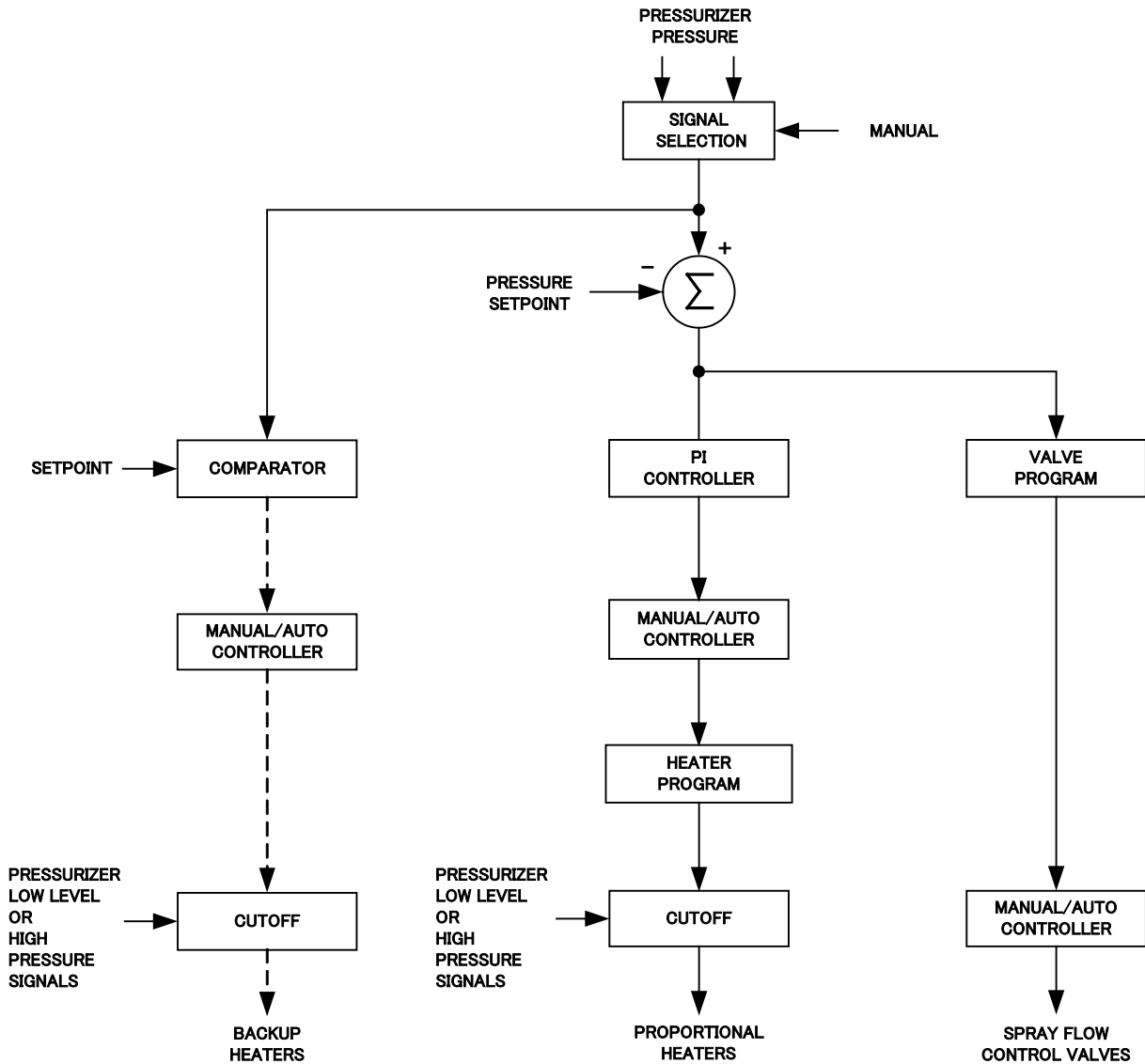


Figure 7.7-3 Pressurizer Pressure Control System Block Diagram

APR1400 DCD TIER 2

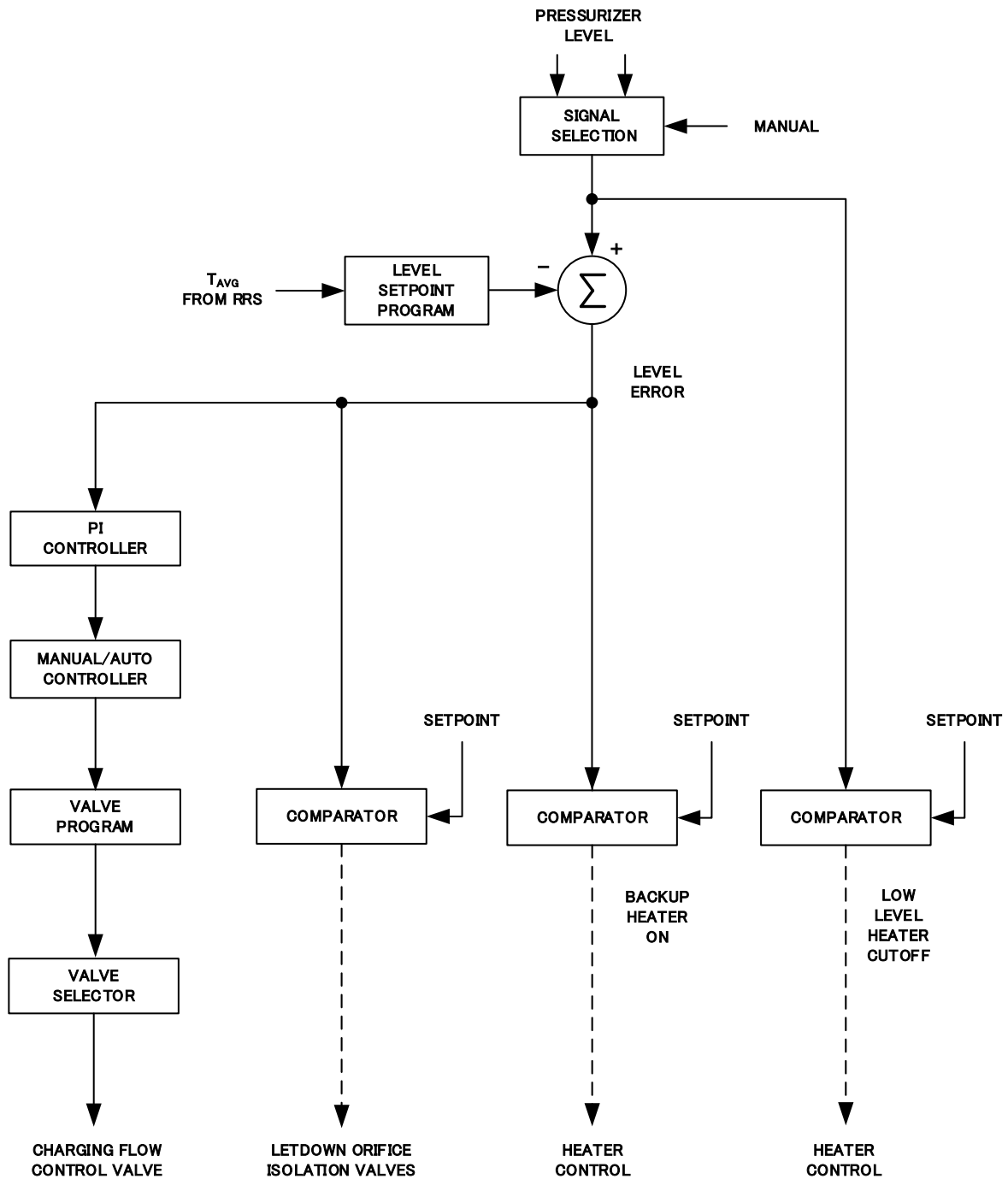


Figure 7.7-4 Pressurizer Level Control System Block Diagram

APR1400 DCD TIER 2

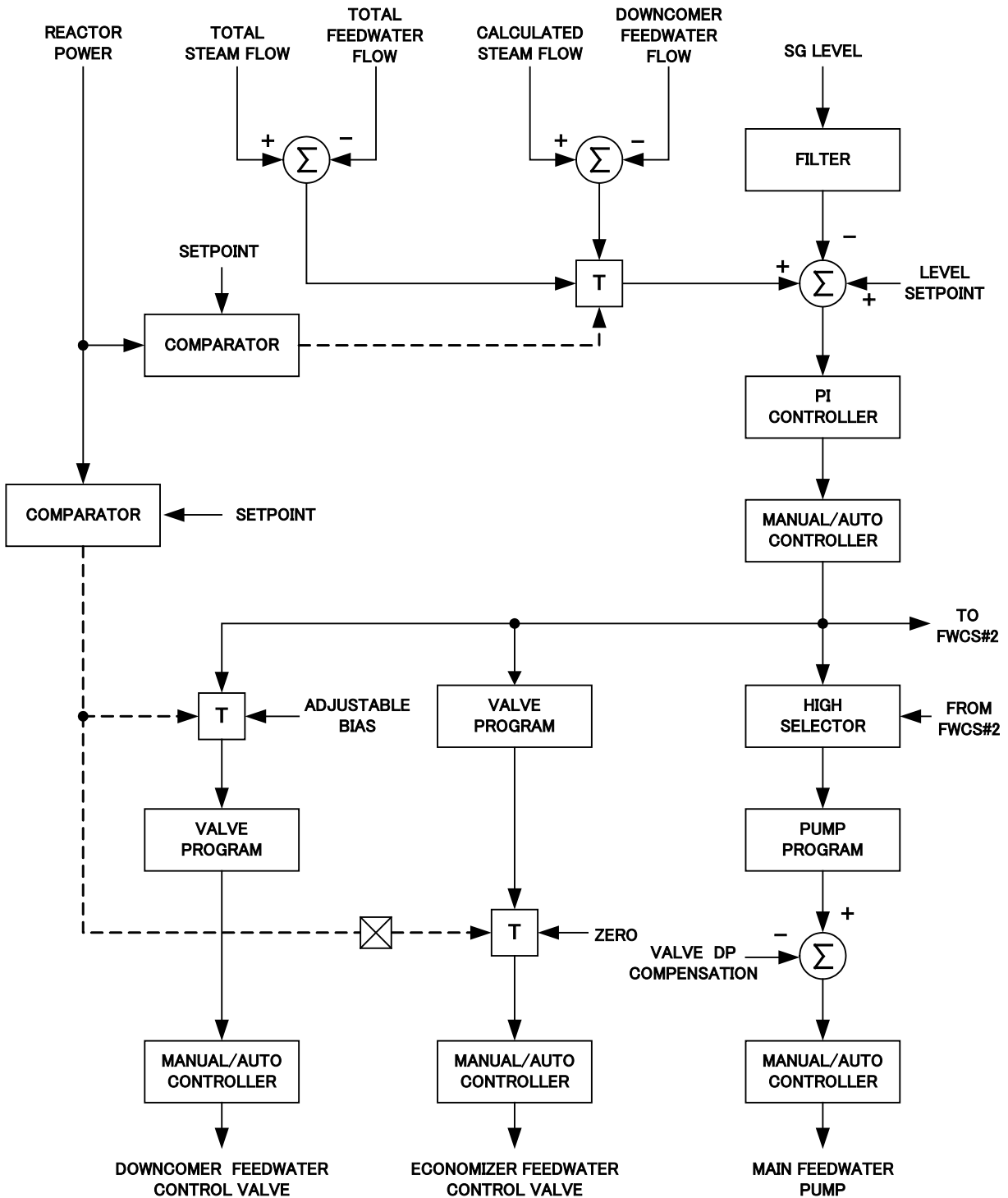
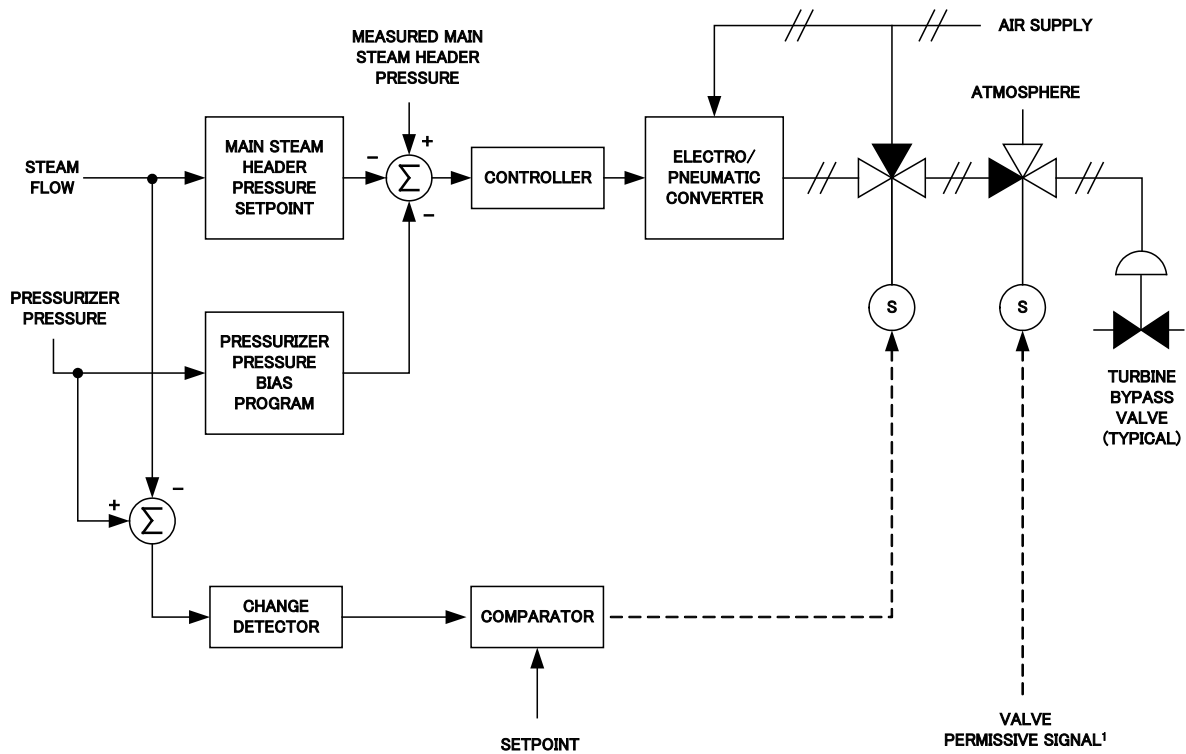


Figure 7.7-5 Feedwater Control System Block Diagram

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

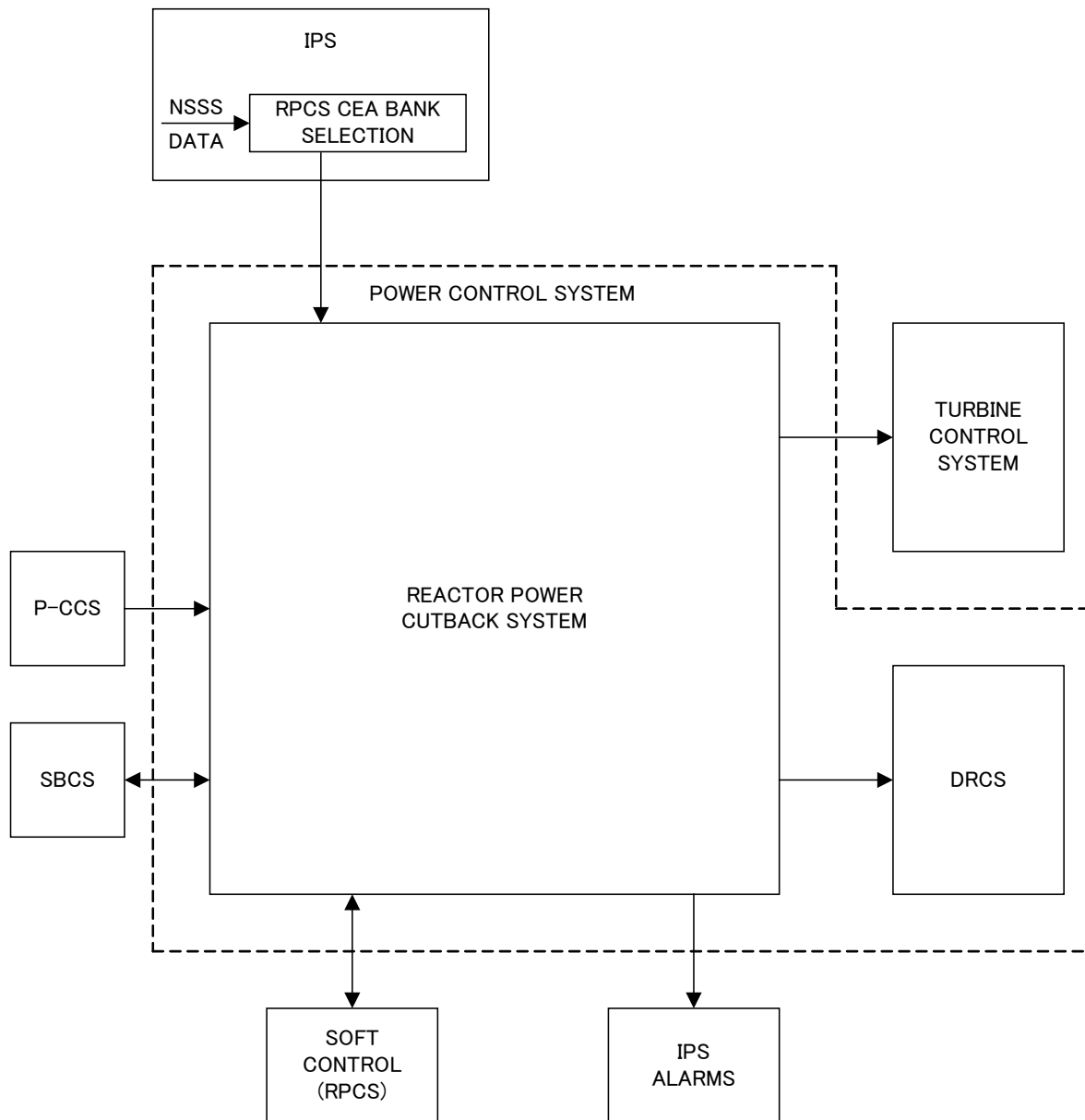
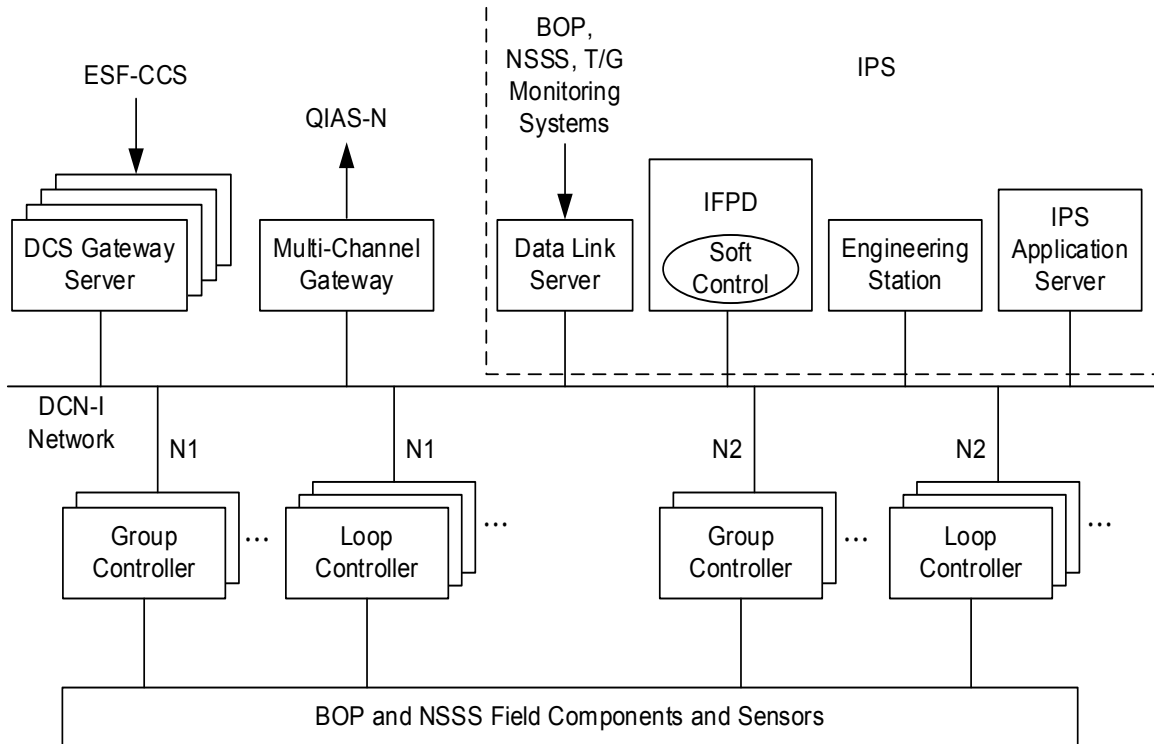


Figure 7.7-7 Reactor Power Cutback System Simplified Block Diagram

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

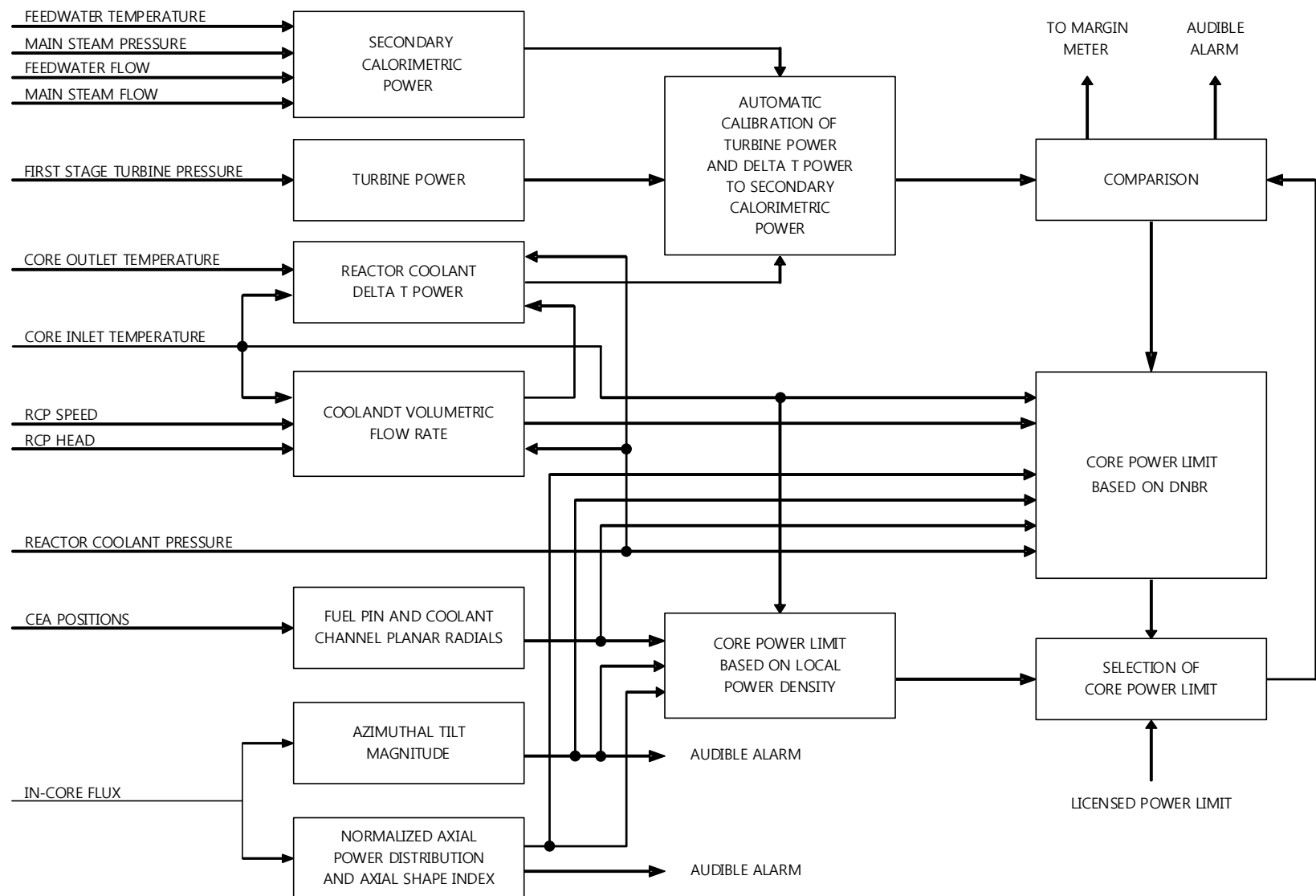
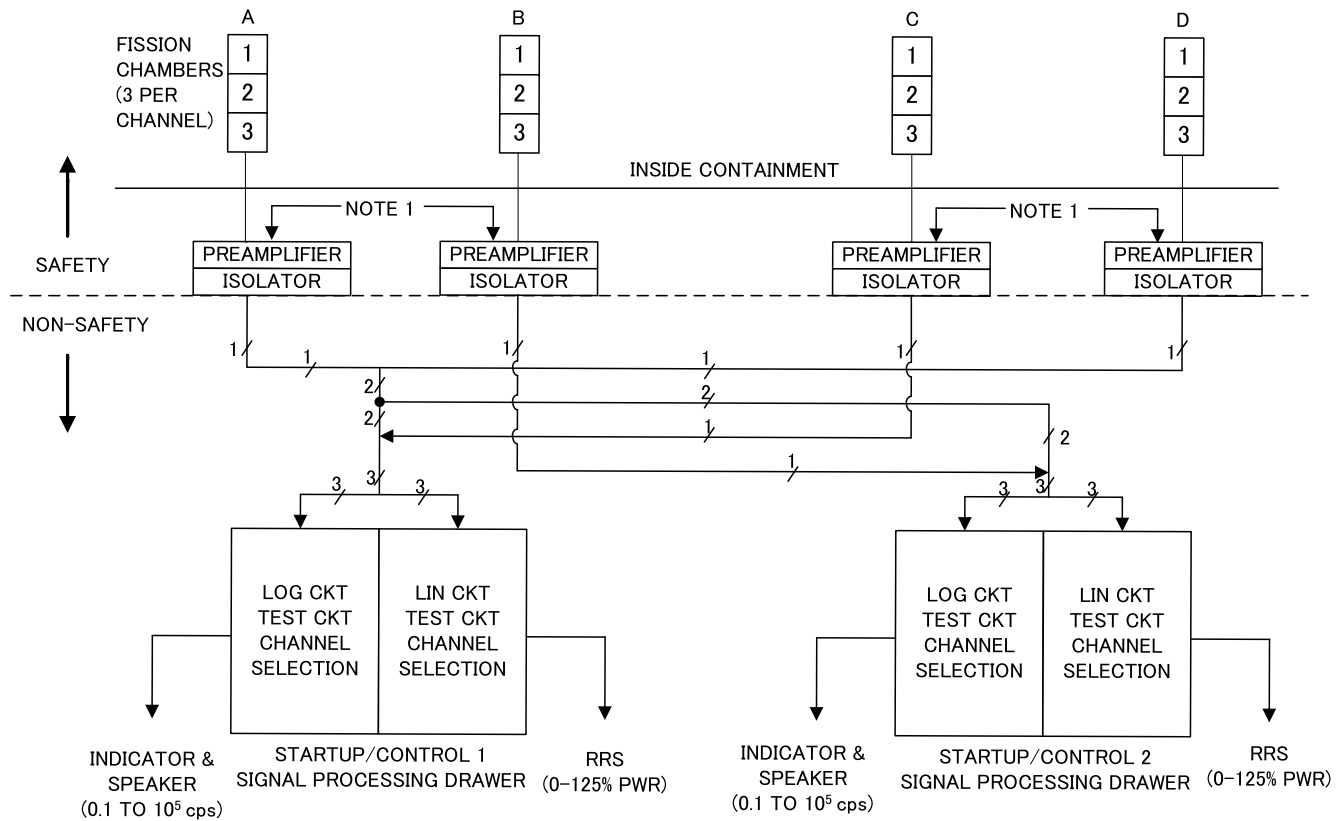


Figure 7.7-9 Core Operating Limit Supervisory System Functional Diagram

APR1400 DCD TIER 2



NOTE

1. THE PREAMPLIFIER PROVIDES SIGNALS FOR STARTUP AND CONTROL FUNCTION THROUGH QUALIFIED ISOLATOR.
2. 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

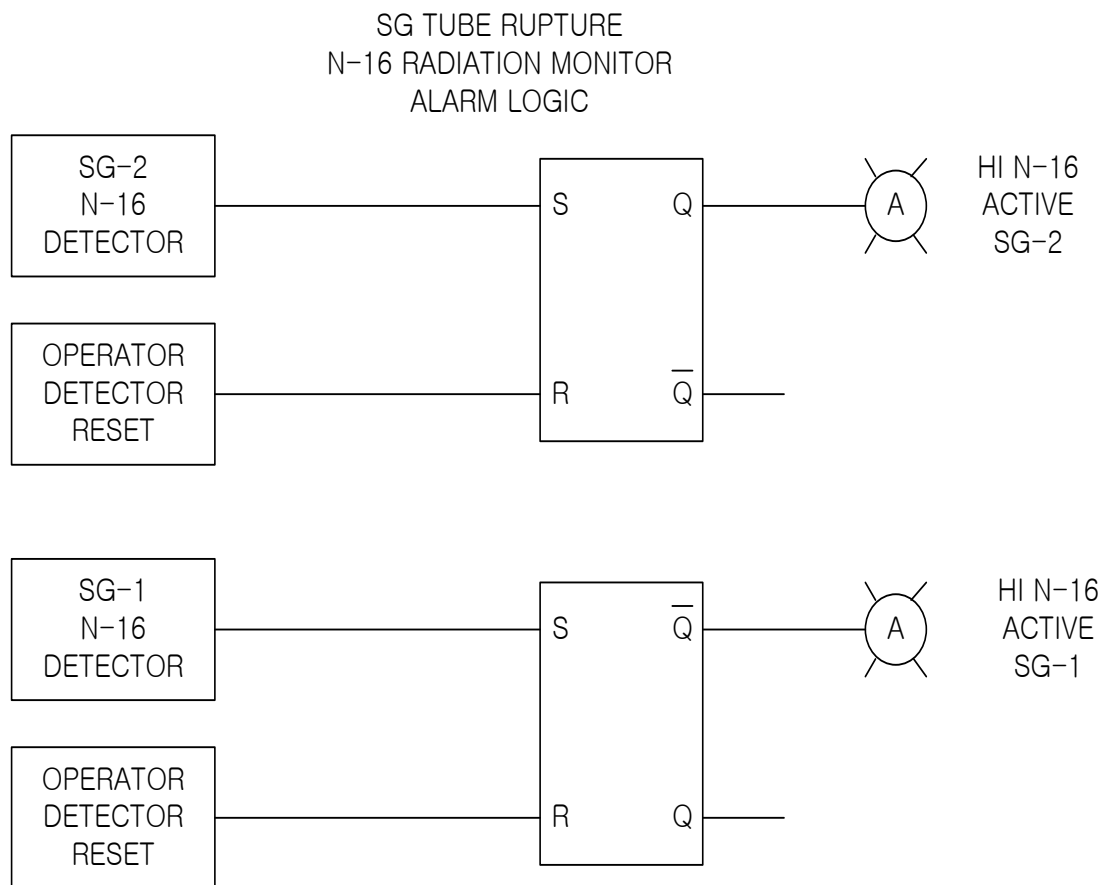


Figure 7.7-11 N-16 Detection and Alarm Logic

APR1400 DCD TIER 2

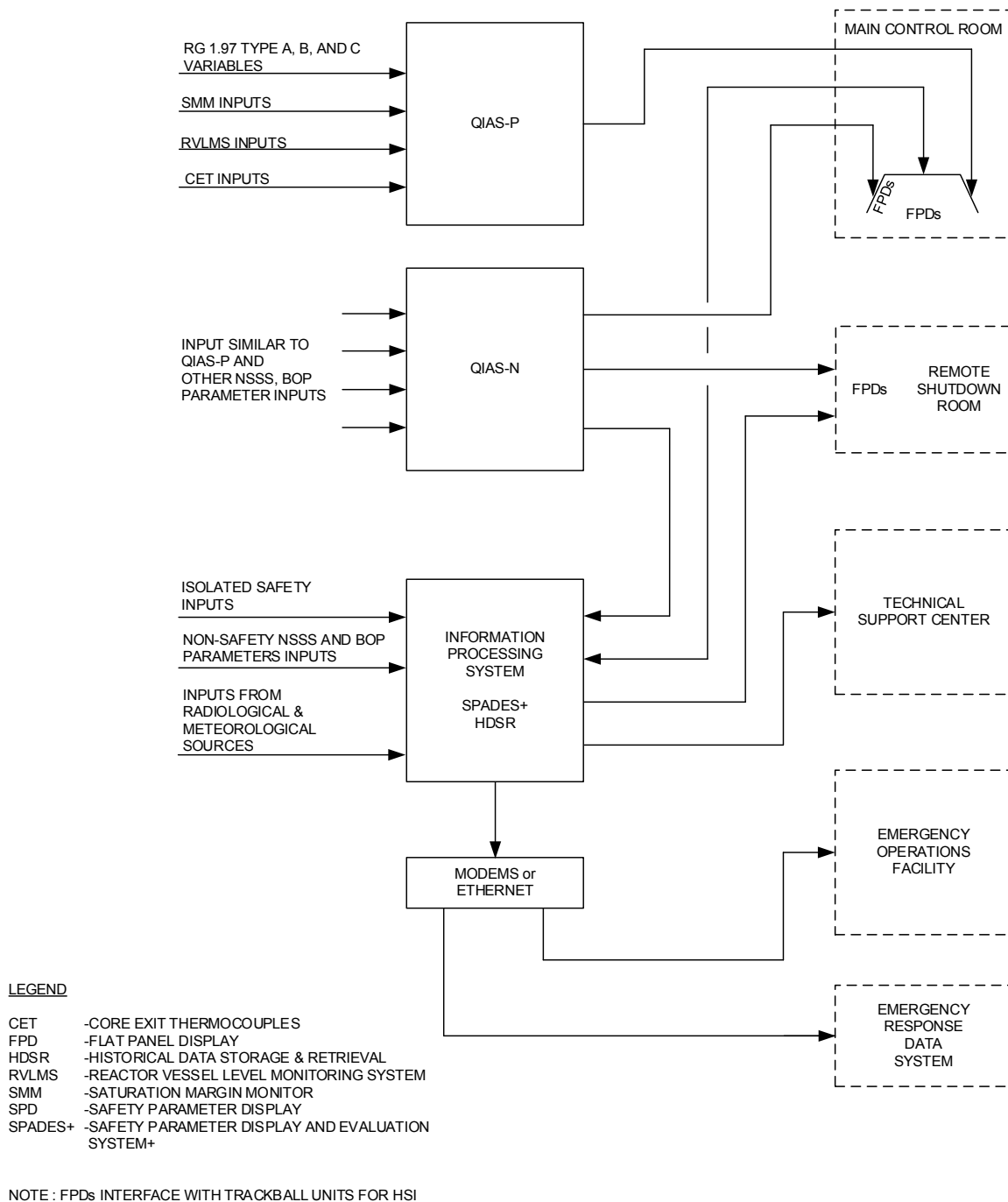


Figure 7.7-12 HSI Information Processing Block Diagram

APR1400 DCD TIER 2

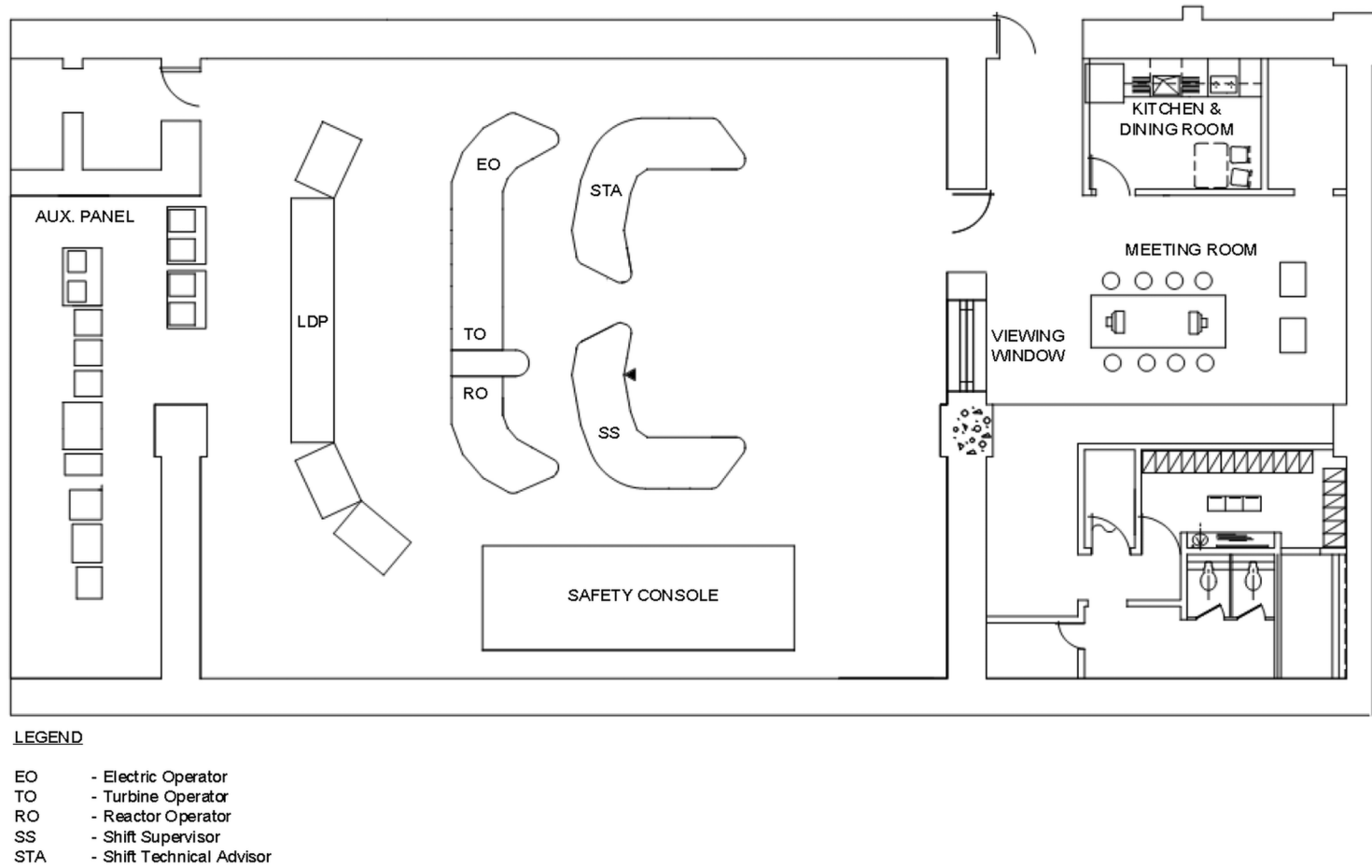


Figure 7.7-13 Layout of Main Control Room

APR1400 DCD TIER 2

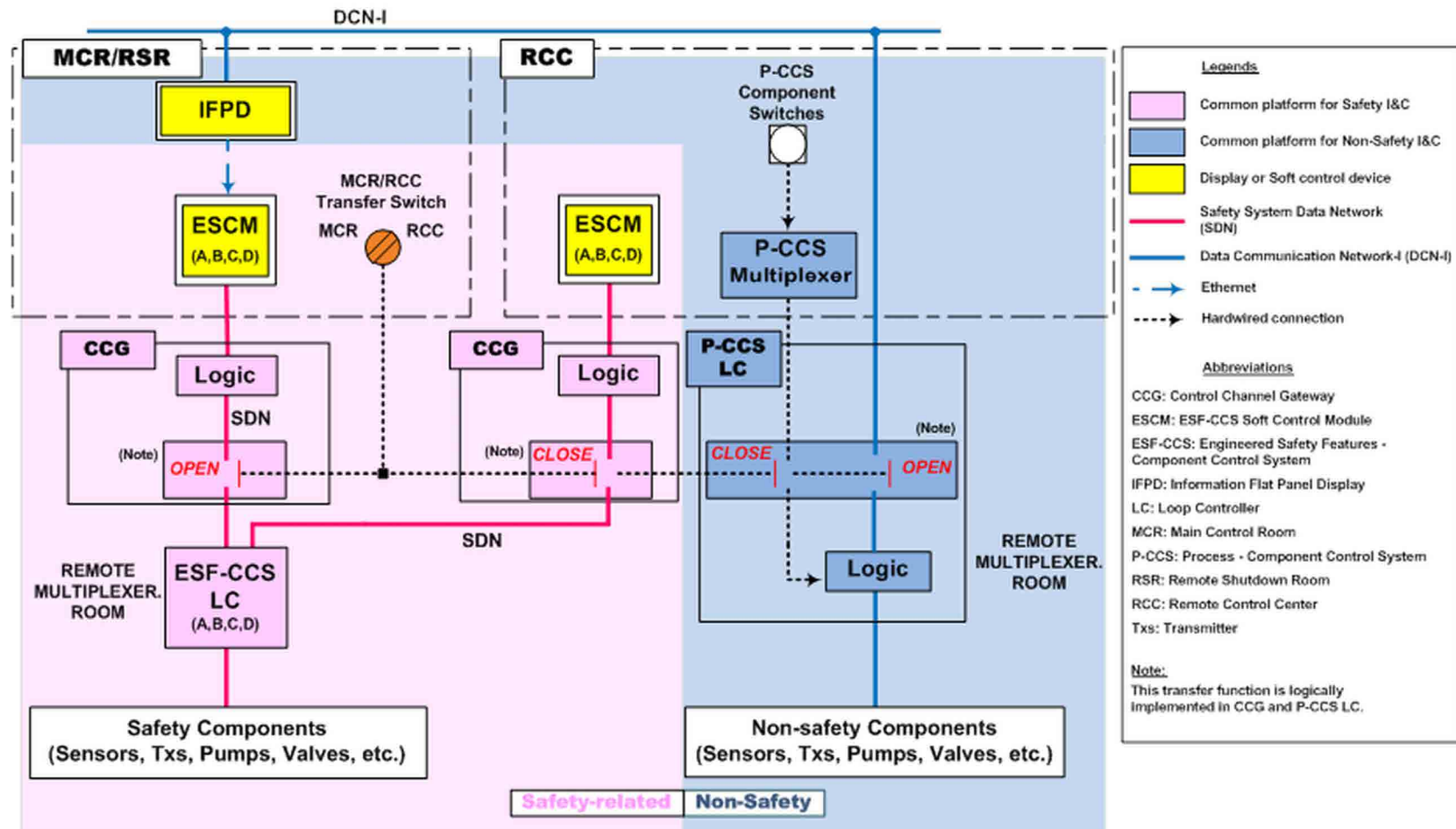


Figure 7.7-14 I&C System Architecture for the RCC Panel

APR1400 DCD TIER 2

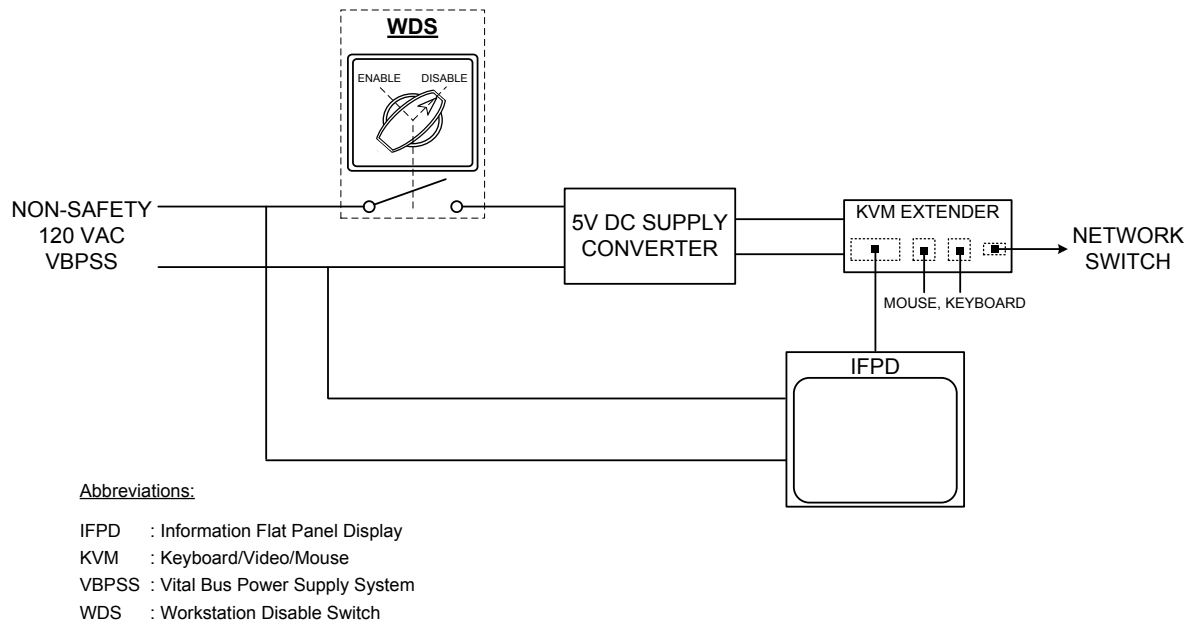


Figure 7.7-15 Configuration of Workstation Disable Switch

APR1400 DCD TIER 2

7.8 Diverse Instrumentation and Control Systems

The diverse actuation system (DAS) consists of the diverse instrumentation and control (I&C) systems that are provided to protect against potential common-cause failure (CCF) of digital safety I&C systems including 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 engineered safety features (ESF) actuation (DMA) switches, and the diverse indication system (DIS).

For the ATWS mitigation, the DPS is provided to meet the requirements of 10 CFR 50.62 (Reference 1). In addition, the DPS, DIS, and DMA switches are provided to comply with Staff Requirements Memorandum (SRM) on SECY-93-087 (Reference 2) and BTP 7-19 (Reference 5). The DPS and DMA switches are independent and diverse from the PPS and ESF-CCS. The DMA switches are located in the main control room (MCR) for manual ESF actuation of critical safety functions.

The 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 ATWS and to mitigate 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.

The DPS and DMA switches are connected to the component interface module (CIM) to cope with a CCF of the PPS and ESF-CCS. The interface description of the DPS and DMA switches are described in the Component Interface Module Technical Report (Reference 12).

APR1400 DCD TIER 2

7.8.1 System Description

7.8.1.1 Diverse Protection System

The DPS augments the PPS to meet the requirements of 10 CFR 50.62 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 the 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 a 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 receives analog signal inputs from isolation devices in the auxiliary process cabinet - safety (APC-S). The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

The DPS is composed of four channels with one cabinet per channel, and each DPS cabinet is located in a separate room. Each DPS channel is powered from two redundant non-Class

APR1400 DCD TIER 2

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.

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 (TCBs) 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 TCBs while the PPS de-energizes the undervoltage trip coil to cause the RTSS TCBs 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 3-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. See Figure 7.8-3 for the DPS turbine trip signal.

Auxiliary Feedwater System Actuation Signal

The DPS initiates an 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 prioritized in the component interface module (CIM) using state-based priority logic, so that either system can actuate the auxiliary feedwater. The safe state for state-based priority logic is shown in Table 7.8-4. Isolation is provided at the ESF-CCS loop controller cabinet to maintain electrical isolation between the DPS and CIM. See Figure 7.8-4 for the DPS-AFAS.

Safety Injection System Actuation Signal

The DPS also initiates an 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 prioritized in the CIM using state-based priority logic, so that either system can actuate the SIS. The safe state for state-based priority logic is shown in Table 7.8-5. Isolation is provided at the ESF-CCS loop controller cabinet to maintain electrical isolation between the DPS and CIM. See Figure 7.8-5 for the DPS-SIAS.

7.8.1.2 Diverse Manual Engineered Safety Features Actuation Switches

The DMA switches permit the operator to manually actuate ESF systems from the MCR after a postulated CCF of the PPS and ESF-CCS.

The DMA switches provide the SIAS, main steam isolation signal (MSIS), containment isolation actuation signal (CIAS), containment spray actuation signal (CSAS), AFAS-1, AFAS-2 and signal for auxiliary feedwater flow/steam generator (SG) level. Table 7.8-3 identifies diverse automatic and manual actuation signals. The DMA switches are hardwired to the CIM through the isolation devices and are independent and diverse from the safety system. The auxiliary feedwater flow/SG1 level and auxiliary feedwater flow/SG2 level are manual stations required to control auxiliary feedwater flow/SG level after the activation of diverse AFAS-1 and AFAS-2.

Each signal of the DMA switches actuates necessary ESF systems to perform the ESF functions. The functions of the DMA switches are enabled by the DMA enable switch on the safety console. The DMA switches block diagram is shown in Figure 7.8-6.

7.8.1.3 Diverse Indication System

The DIS provides functions to monitor critical variables following a postulated software CCF of the safety computer systems. The DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet - safety (APC-S) and the analog part of the qualified indication and alarm system - P (QIAS-P). The APC-S employs no functional programmable unit. Thus, the APC-S is not susceptible to a postulated software CCF. The QIAS-P is composed of two parts which have no functional interaction with each other. One part is a computer part which employs the functional programmable units. The computer part is susceptible to a postulated software CCF. The other one is an analog part

APR1400 DCD TIER 2

which employs no functional programmable unit, and is not susceptible to a postulated software CCF. In addition, the safety computer systems including the computer part of the QIAS-P are designed under the safety common platform (i.e., PLC-based), while the DIS is designed under the different FLC based platform. Therefore, the DIS is independent and diverse from the computer part of QIAS-P. Moreover, to meet the independence requirements between the safety-related systems and the non-safety systems, the DIS is electrically isolated and physically separated from the APC-S and the analog part of 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 computer part of the QIAS-P. The control function is manually transferred from the computer part of 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 seismic Category II. In addition, the DIS human system interface equipment on the MCR safety console is qualified as seismic Category II and powered by non-class 1E vital bus.

7.8.2 Design Basis Information

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).

APR1400 DCD TIER 2

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.

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 resulting logic becomes 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 to remote shutdown room (RSR) control transfer, which enables the plant operation in the RSR. When the DPS-SIAS operating bypass is enabled, the bypass status is indicated in the MCR.

APR1400 DCD TIER 2

Use of Digital Systems

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.

Environmental Qualification

The 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 Systems

The DPS is electrically isolated and physically separated from the protection systems. The engineered safety feature actuation signals initiated by the DPS are isolated in the protection systems. The DPS receives the hardwired process signal inputs from isolation devices in the APC-S. The qualified isolation devices are part of the safety system.

Diversity

The DPS is diverse from the sensor signal processing 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 TCBs 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 TCBs. The PPS reactor trip de-energizes the undervoltage trip coils of the RTSS TCBs.

The DPS is diverse from the sensor signal processing output to the CIM for the ESF actuation of auxiliary feedwater and safety injection.

APR1400 DCD TIER 2

Diversity and Defense-in-Depth

The defense-in-depth and diversity (D3) approach is based on the following principles:

- a. Mitigate the potential impact of software CCF.
- b. Cope with software CCF concurrent with AOOs and PAs.

Sensors and analog signal processing equipment are shared by the DPS and PPS. These are analog equipment, and are not affected by the software CCF.

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.

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 of 10 CFR Part 50
(References 13 through 16)
- b. IEEE Std. 603, Clause 5.6.3 (Reference 7)
- c. 10 CFR 50.62
- d. Staff Requirements Memorandum on SECY-93-087, Item II.Q
- e. NUREG-0800, Chapter 7, Branch Technical Position 7-19

7.8.2.2 Diverse Manual Engineered Safety Features Actuation Switches

The DMA switches are provided to permit the operator to manually actuate the ESF functions from the MCR.

The DMA switches are diverse from the manual and automatic logic functions performed by the PPS and ESF-CCS.

Basic design bases are described below.

APR1400 DCD TIER 2

Quality

The DMA switches are classified as a non-safety system, but they are implemented by Class 1E qualified devices with seismic qualification according to IEEE Std. 344 (Reference 18).

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.

Environmental Qualification

The DMA switches are qualified according to IEEE Std. 323 (Reference 17) to perform their intended protective function during design basis events.

Independence from the Protection Systems

The DMA switches are connected directly to fan-out devices in the MCR safety console to distribute the manual ESF actuation signals to individual component controls. The DMA switches are hardwired to the CIM in the ESF-CCS loop controller through an interposing relay for isolation. The interposing relay is classified as part of the safety system and implemented by a Class 1E qualified device. The relay receives power from the power supply of the corresponding safety division.

Single Failure

Because the DMA switches are a non-safety system, the DMA switches 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 to priority logic of the CIM, and priority logic is implemented by hardware devices.

APR1400 DCD TIER 2

Diversity and Defense-in-Depth

The DMA switches are designed to comply with the regulatory position in SRM on SECY-93-087, Item II.Q, and with BTP 7-19. 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 the PPS and 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 containment integrity. The switches in the MCR provide for manual ESF actuation, as shown in Table 7.8-3.

The DMA switches are hardwired to the CIM through the isolation devices and are independent and diverse from the PPS and 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 parameters
- c. A subset of 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 safety I&C systems by receiving input signals from safety I&C systems through qualified isolation devices. 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. Conformance with GDCs 1, 13, and 19 is described in the Diversity and Defense-in-Depth Technical Report (Reference 6).

APR1400 DCD TIER 2

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.

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 Systems

The DIS is isolated from the QIAS-P and APC-S, in accordance with the independence requirements of IEEE Std. 603 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.

Diversity and Defense-in-Depth

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 safety I&C systems including the 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 digital safety I&C systems including 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.

Conformance 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 in safety systems, to place the plant in a safe shutdown condition, and to 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 human factors engineering 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 software CCF in the safety I&C systems including the PPS and ESF-CCS could prevent any actuation or control (automatic and manual) or cause spurious actuation of their associated safety equipment. Table 7.8-2 shows the plant functions and systems that are not affected by the software 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. In addition, the postulated software CCF may cause the PPS and ESF-CCS data that are passed to the IPS to be invalid. During the software CCF event, the data passed to 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

The evaluation of design basis events consists of a qualitative evaluation and quantitative analysis.

a. Qualitative evaluation

The qualitative evaluation assesses the diversity and defense-in-depth 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

APR1400 DCD TIER 2

assumes continued operability of the RCPs (except the events in which the event initiator is loss of power to the reactor coolant pumps (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.

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 combined license (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," U.S. Nuclear Regulatory Commission.
2. Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs" Item II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, July 21, 1993.
3. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," U.S. Nuclear Regulatory Commission, January 16, 1985.
4. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.

APR1400 DCD TIER 2

5. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Rev. 6, U.S. Nuclear Regulatory Commission, July 2012.
6. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
7. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.
8. IEEE Std. 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," Institute of Electrical and Electronics Engineers, 1992.
9. APR1400-Z-A-NR-14019-P, "CCF Coping Analysis," Rev. 3, KEPCO & KHNP, July 2018.
10. APR1400-Z-J-NR-14004-P, "Uncertainty Methodology and Application for Instrumentation," Rev. 2, KEPCO & KHNP, January 2018.
11. APR1400-Z-J-NR-14005-P, "Setpoint Methodology for Safety-Related Instrumentation," Rev. 2, KEPCO & KHNP, January 2018.
12. APR1400-E-J-NR-14001-P, "Component Interface Module," Rev. 1, KEPCO & KHNP, March 2017.
13. 10 CFR Part 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," U.S. Nuclear Regulatory Commission.
14. 10 CFR Part 50, Appendix A, General Design Criterion 13, "Instrumentation and Control," U.S. Nuclear Regulatory Commission.
15. 10 CFR Part 50, Appendix A, General Design Criterion 19, "Control Room," U.S. Nuclear Regulatory Commission.
16. 10 CFR Part 50, Appendix A, General Design Criterion 24, "Separation of Protection and Control Systems," U.S. Nuclear Regulatory Commission.
17. IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

APR1400 DCD TIER 2

18. IEEE Std. 344-2004, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, 2005.

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 (2,400 psia)	≤ 0.85
Pressurizer pressure for SIAS	Pressure transmitter	4	0 to 210.93 kg/cm ² A (0 to 3,000 psig)	114.6 kg/cm ² A (1,630 psia)	≤ 1.15 ⁽²⁾
Containment pressure for reactor trip	Pressure transmitter	4	-300 to 1,200 cmH ₂ O (-4 to 17 psig)	210.9 cmH ₂ O (3.0 psig)	≤ 1.15
Steam generator level (wide range) for AFAS	Differential pressure transmitter	4/steam generator	0 to 100 % WR	22.4 % WR	≤ 1.25 ⁽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 in Subsection 7.8.5. DPS has different setpoints from PPS so that PPS actuates prior to DPS. See Tables 7.2-4 and 7.3-5A for PPS and ESF-CCS setpoints.

(2) The response time includes the sensor and DPS, but it does not include the final actuation device.

APR1400 DCD TIER 2

Table 7.8-2

Diverse Functions Remain Available after the Software CCF of Safety Instrumentation and Control Systems

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, CIM	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	CIM (located in ESF-CCS loop controller 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) See 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 (division A)	1/1
	Diverse manual AFAS-2	1 switch (division B)	1/1
	Diverse manual SIAS	2 switches (divisions A and C)	1/1
	Diverse manual MSIS-1A	1 switch (division A)	1/1
	Diverse manual MSIS-1B	1 switch (division A)	1/1
	Diverse manual MSIS-2A	1 switch (division A)	1/1
	Diverse manual MSIS-2B	1 switch (division A)	1/1
	Diverse manual CSAS	2 switches (divisions A and C)	1/1
	Diverse manual CIAS	1 switch (division 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

Table 7.8-5 (1 of 2)

Safe State of ESF Components for State-Based Priority

Train (Division)	Component	Related Signal	State
A (A1)	SIP 1 Isolation Valve	SIAS	Open
	SIT 1 Isolation Valve	SIAS	Open
	SIT Fill and Drain Line Isolation Valve	SIAS	Close
	Check Valve Leakage Line Isolation Valve	SIAS	Close
	Letdown Isolation Valve	SIAS	Close
	SI Pump #1	SIAS	Start Run
C (A2)	SIP 3 Isolation Valve	SIAS	Open
	SIT 3 Isolation Valve	SIAS	Open
	SIT Fill and Drain Line Isolation Valve	SIAS	Close
	Check Valve Leakage Line Isolation Valve	SIAS	Close
	SI Pump #3	SIAS	Start Run
B (B1)	SIP 2 Isolation Valve	SIAS	Open
	SIT 2 Isolation Valve	SIAS	Open
	SIT Fill and Drain Line Isolation Valve	SIAS	Close
	Check Valve Leakage Line Isolation Valve	SIAS	Close
	SIT Fill Line Isolation Valve	SIAS	Close
	Letdown Isolation Valve	SIAS	Close
	SI Pump #2	SIAS	Start Run
D (B2)	SIP 4 Isolation Valve	SIAS	Open
	SIT 4 Isolation Valve	SIAS	Open
	SIT Fill and Drain Line Isolation Valve	SIAS	Close
	Check Valve Leakage Line Isolation Valve	SIAS	Close
	SI Pump #4	SIAS	Start Run

APR1400 DCD TIER 2

Table 7.8-5 (2 of 2)

Train (Division)	Component	Related Signal	State
A (A1)	SG Blowdown Containment Isolation Valve	AFAS	Close
	AFW Pump Turbine Steam Supply Valve	AFAS	Open
	AFW Pump (Motor Driven) #1	AFAS	Start Run
	AFW Modulating Valve	AFAS	Permit Modulation
	AFW Isolation Valve	AFAS	Open
C (A2)	Steam Supply Isolation Valve	AFAS	Open
	AFW Isolation Valve	AFAS	Open
B (B1)	SG Blowdown Containment Isolation Valve	AFAS	Close
	AFW Pump Turbine Steam Supply Valve	AFAS	Open
	AFW Pump (Motor Driven) #2	AFAS	Start Run
	AFW Modulating Valve	AFAS	Permit Modulation
	AFW Isolation Valve	AFAS	Open
D (B2)	Steam Supply Isolation Valve	AFAS	Open
	AFW Isolation Valve	AFAS	Open

APR1400 DCD TIER 2

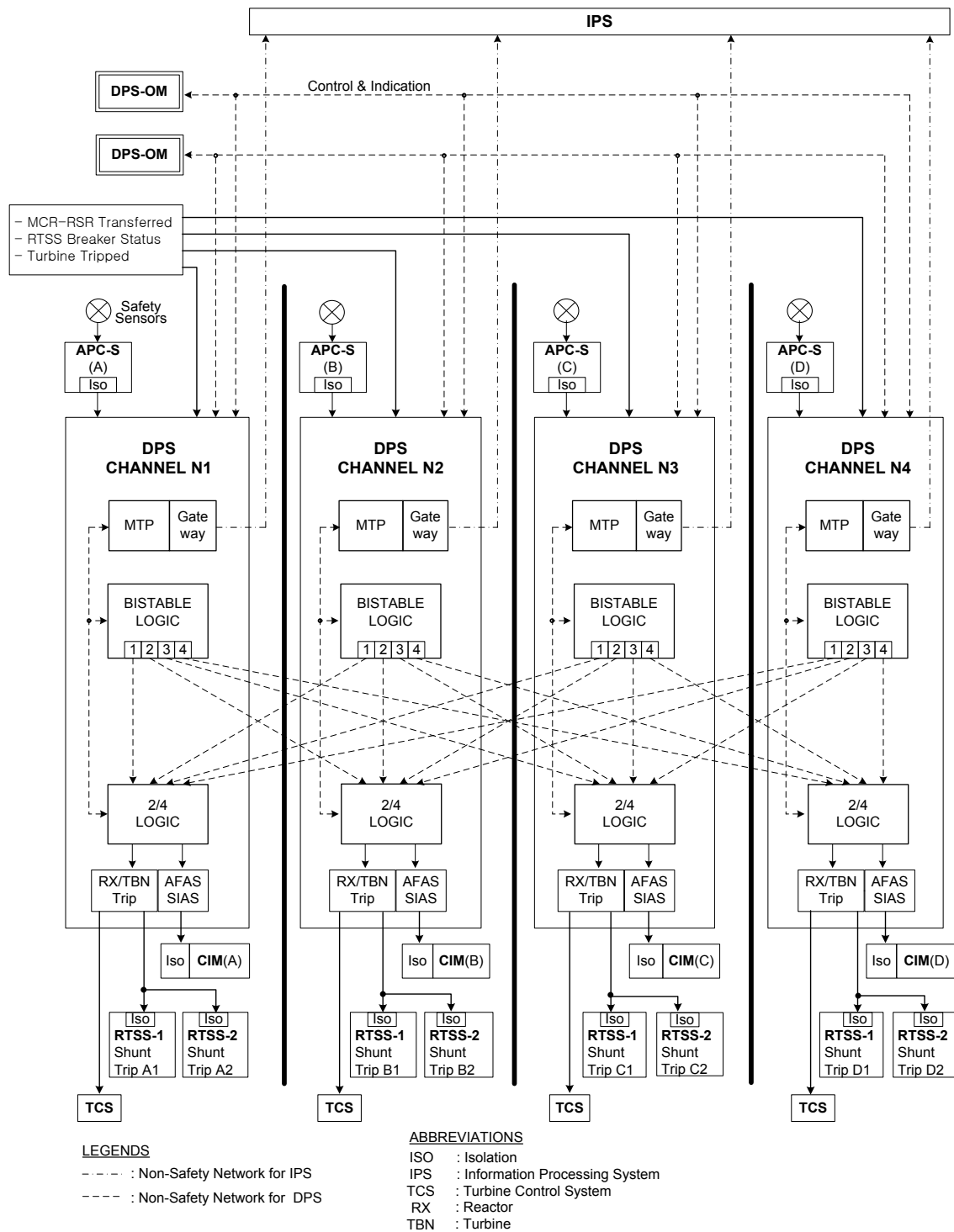


Figure 7.8-1 Diverse Protection System Block Diagram

APR1400 DCD TIER 2

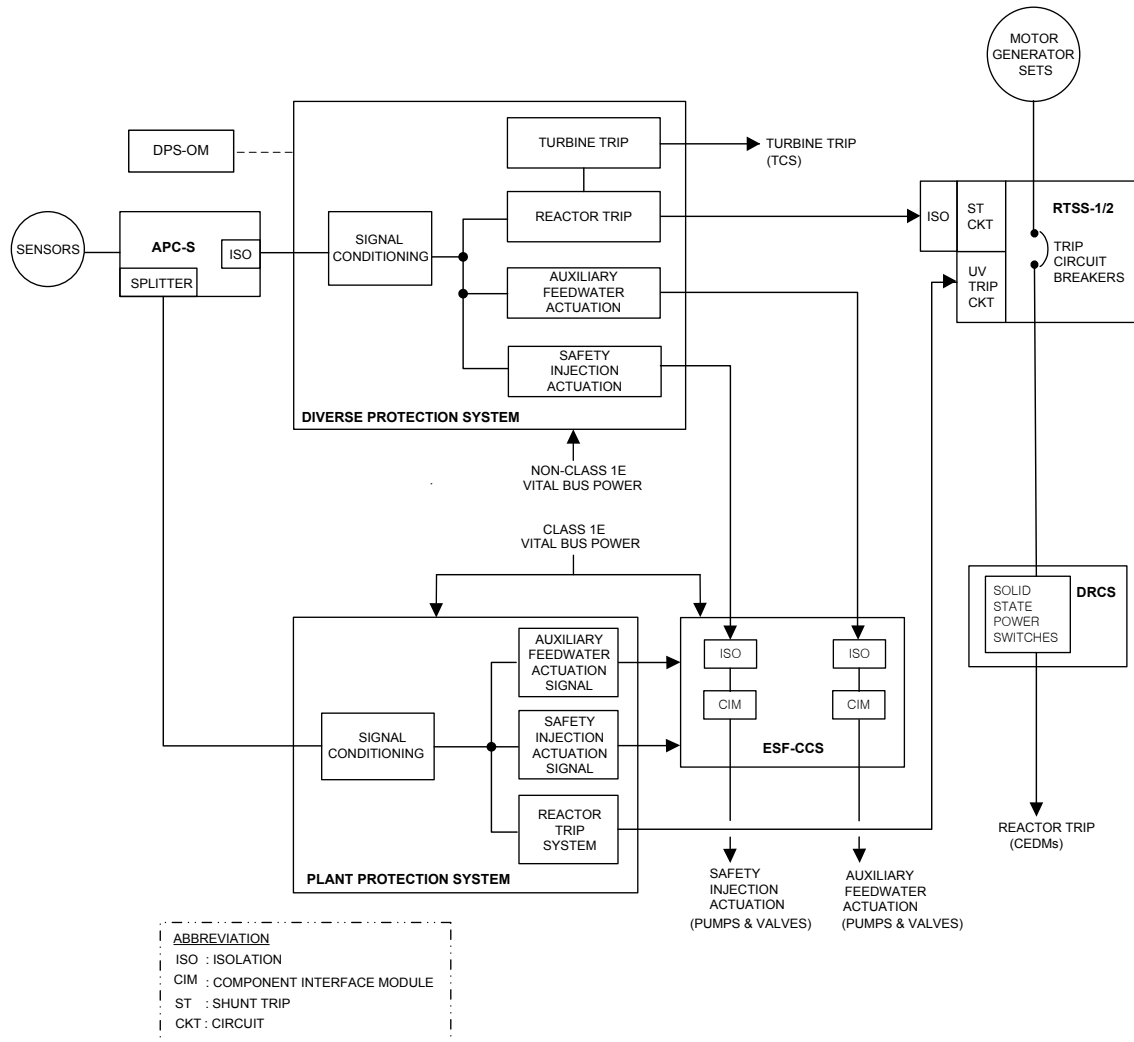
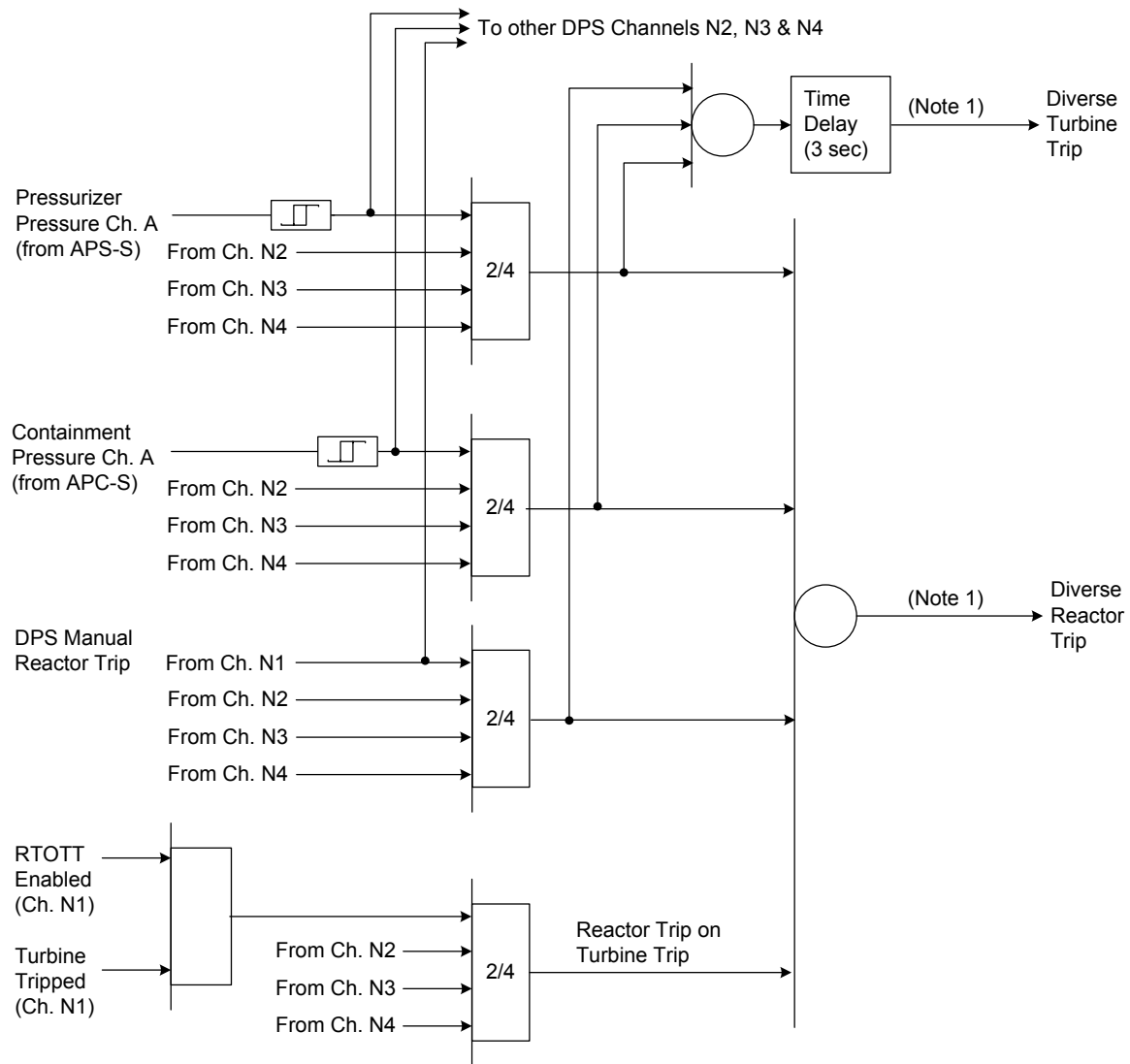


Figure 7.8-2 Diverse Reactor Trip, Turbine Trip, AFWS and SIS Actuation

APR1400 DCD TIER 2



ABBREVIATION & LEGEND

RTOTT : Reactor Trip on Turbine Trip

 : Setpoint Comparison (High Threshold)

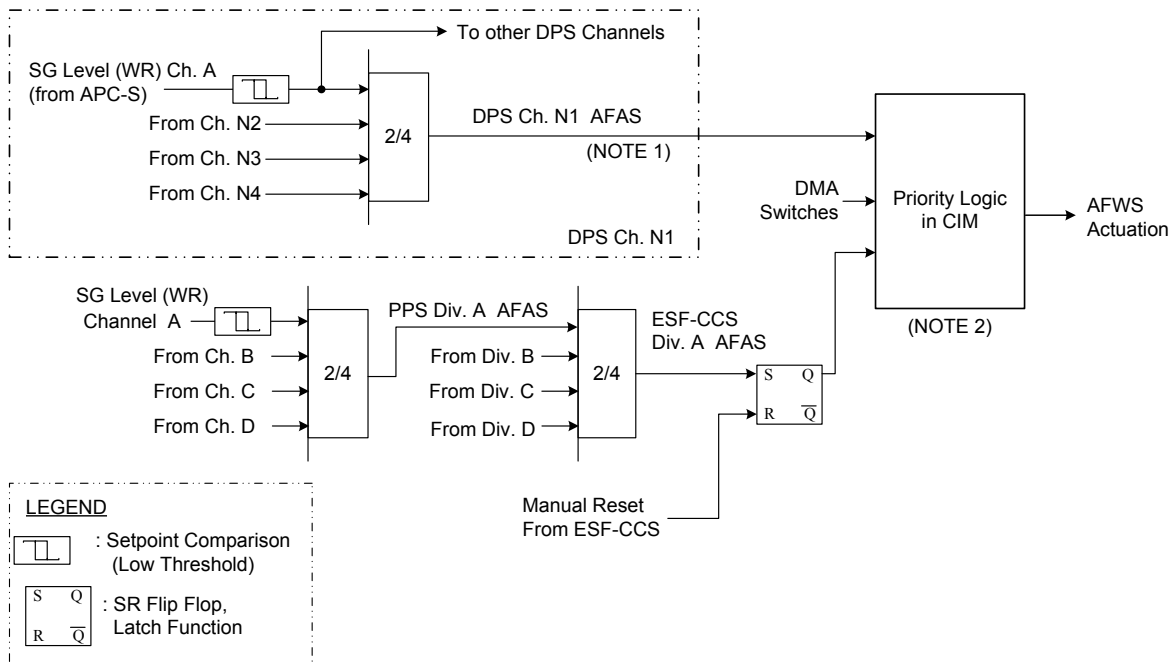
DPS Ch. N1

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.

Figure 7.8-3 Diverse Reactor Trip and Turbine Trip

APR1400 DCD TIER 2

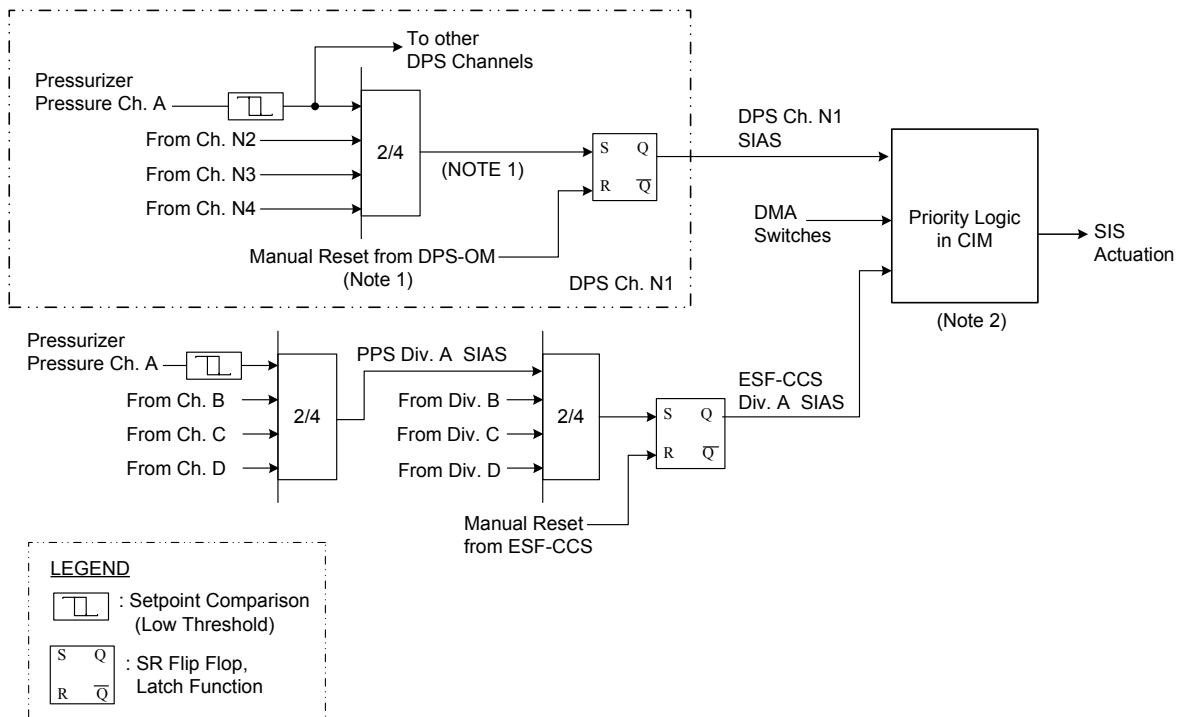


Notes:

1. The DPS-AFAS related components cycle its operation, which is ON if SG level goes below the DPS-AFAS setpoint, and OFF if SG level is above the DPS-AFAS setpoint plus hysteresis.
2. The priority logic in the CIM is implemented by hardware device. The CIM prioritizes input signals from the ESF-CCS, DPS, DMA switches, and front panel control switch according to the priority logic. The detailed priority logic design is described in the Component Interface Module Technical Report (Reference 12).
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

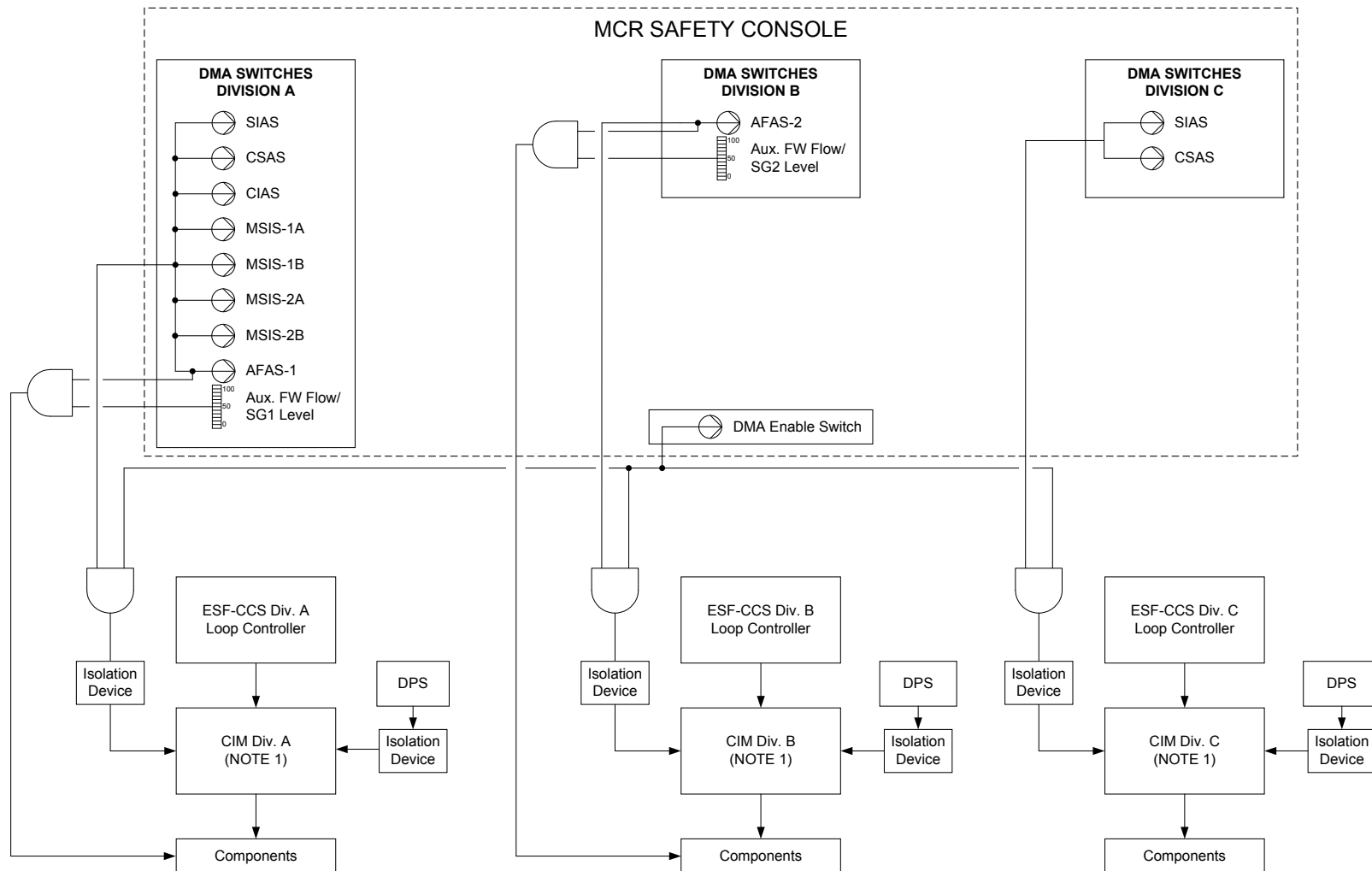
APR1400 DCD TIER 2



- 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. The priority logic in the CIM is implemented by hardware device. The CIM prioritizes input signals from the ESF-CCS, DPS, DMA switches, and front panel control switch according to the priority logic. The detailed priority logic design is described in the Component Interface Module Technical Report (Reference 12).
 3. This diagram is for the DPS Channel N1. Channels N2, N3, and N4 are the same as Channel N1.

Figure 7.8-5 Diverse SIS Actuation

APR1400 DCD TIER 2



NOTE

1. The input signals of the DMA switches are directly connected to the CIM through the isolation devices. The priority logic section of the CIM is implemented by non-software based device.

Figure 7.8-6 DMA Switches Block Diagram

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 send 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 seismically and environmentally qualified and classified as an important-to-safety (ITS) software class
- b. Serial data link (SDL), which is seismically and environmentally qualified and classified as a safety-critical (SC) software class but the interdivisional interface and test processor (ITP) data link and ITP to QIAS-N SDLs are exceptionally classified as ITS software class
- c. Data communication network-information (DCN-I) network, which is classified as an important-to-availability (ITA) software class

Data communication systems provide data communication within a safety division, between safety divisions, 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 divisions and between safety systems and non-safety systems. See Figure 7.9-1 for an illustration of the interconnections of the three communication networks.

APR1400 DCD TIER 2

7.9.1.1 Safety System Data Network for Safety Systems

The SDN is used for communication between safety systems within one division. Intra-division communications is a separated and isolated SDN from other divisions. The SDN is a broadcasting network with deterministic characteristics (repeatable and predictable).

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 ITP through the SDN.

Bistable processors and LCL processors receive testing data from the MTP through the SDN.

b. Core protection calculator system (CPCS)

The CPCS sends data for monitoring all processors, including inputs and calculated output to the MTP, OM, and ITP through the SDN.

c. Engineered safety features – component control system (ESF-CCS)

The ESF-CCS group controller (GC) sends system status data to the MTP and ITP through the SDN.

The ESF-CCS loop controller (LC) sends system status data to the MTP through the SDN.

d. Qualified indication and alarm system – P (QIAS-P)

The QIAS-P processor sends the value and system status data to the IPS and QIAS-N through the MTP and ITP, respectively, which provide data communication isolation function and electrical isolation function. The QIAS-P processor communicates with 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 equipment feedback signal 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) in the PPS, ITP, ESF-CCS GC, and LC for receiving status information through the SDN.

j. CCG

The CCG sends component control signals to the ESF-CCS LC through the SDN. The CCG receives the feedback data from the LC through the SDN.

7.9.1.2 Serial Data Link for Safety Systems

The SDL is used for predefined data transmissions between each processor within a division. The SDL is also used to send broadcast data to other divisions and non-safety systems. The SDL meets the communication isolation guidance of IEEE Std. 7-4.3.2 (Reference 1) as endorsed by NRC RG 1.152 (Reference 8). 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 division does not adversely affect the operation of other divisions.

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

1) SDL for LCL voting logic

There are two sets of interdivisional communication SDLs per redundant PPS division. Each BP sends data to the LCL processors through the SDL.

2) SDL for ESF-CCS GC voting logic (actuation logic)

Each LCL processor sends engineered safety features actuation system (ESFAS) initiation signals to the GCs for selective 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 sends CEA position signals to the CPP and CEAC processor through CPPs in the same channel and other channels using the SDLs.

The CPP sends target CEA position signals to the CPC in the same channel through the SDLs.

The CEAC sends penalty factors and target CEA position signals to the CPC in the same channel via the SDLs.

c. ESF-CCS

The ESF-CCS consists of data links for delivering control signals and data network for delivering status and monitoring signals. The data link is implemented by the SDLs.

The ESF-CCS control signals are sent to the LCs from the GCs through the SDLs.

APR1400 DCD TIER 2

Minimum inventory (MI) control signals from the MI switches on the safety console are connected to the CPM of main control room (MCR). MI system-level control signals initiated by MI system-level switches are sent to the GCs through the SDL. MI component-level control signals initiated by MI component-level switches are sent to the LCs via the CCG through the SDL.

The operating bypass and setpoint reset switch signals are also sent to the PPS BP via the divisionalized CPM through the SDLs.

The CPM of remote shutdown room (RSR) sends MCR/RSR master transfer switch signals to the CCG and the GCs through the SDL.

7.9.1.3 Data Communication Network-Information Network for Non-Safety Systems

The DCN-I network provides non-safety data communication network to integrate the data from safety and non-safety systems. The signal connections for the DCN-I network is as follows:

- a. IPS server
- b. Information flat panel display (IFPD)
- c. Engineering workstation
- d. Computer-based procedure (CBP) system server
- e. Distributed control system (DCS) gateway server to be interfaced with the MTP in each safety division
- f. Multi-channel gateway to be interfaced with the QIAS-N MTP
- g. P-CCS GCs and LCs (including the nuclear steam supply system process control system controller)
- h. Balance of plant (BOP) monitoring systems
- i. Turbine/generator control system (T/GCS)
- j. Power control system (PCS)

APR1400 DCD TIER 2

- k. Fixed in-core detector amplifier system (FIDAS)
- l. NSSS integrity monitoring system (NIMS)

The DCN-I network is independent of the QIAS-N network. The DCN-I network uses different data communication hardware and protocols from the QIAS-N network.

All data paths between the DCN-I network and safety systems via information gateways are fiber-optic cables to provide electrical isolation.

The DCN-I network is a redundant network but not physically separated and electrically isolated. A single failure in the DCN-I network does not cause a total loss of data transmission capability between systems that interface with the DCN-I network. The IPS server processors interface with the DCN-I network 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 network. The IPS server processors communicate with the IPS display systems through the DCN-I network.

An evaluation is performed to demonstrate that the throughput, capacity, response time, and data accuracy of DCN-I network meet the requirements of the supported instrumentation and control (I&C) systems. Expected error rates and their effects on 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 sends data to the IPS through the DCS gateway server using the fiber-optic cable unidirectionally. Therefore, the failure of the DCS gateway server does not prevent the MTP from performing the intended functions.

- b. ITP

The ITP sends the status and alarm information to the QIAS-N through the SDL unidirectionally. Therefore the failure of the QIAS-N does not prevent the ITP from performing the intended functions.

APR1400 DCD TIER 2

c. DCS gateway server

The DCS gateway server receives data from the MTP using unidirectional Ethernet communication with fiber optic isolation. Besides the MTP, there are no other safety systems that directly send data to the DCS gateway server.

d. Non-safety standalone I&C systems

Non-safety standalone I&C systems of APR1400 consist of T/GCS, seismic monitoring system (SMS), vibration monitoring system (VMS), NIMS, and FIDAS. SMS, VMS, and FIDAS have no interface with safety I&C systems. However, T/GCS has interface with PPS and NIMS has interface with the ex-core neutron flux monitoring system (ENFMS). The interface between T/GCS and PPS and between NIMS and ENFMS is all unidirectional signal interfaces from the safety system to the non-safety system through Class 1E qualified isolation devices.

Data Communication from Non-Safety System to Safety System

Ethernet communication is used to communicate from the IFPD to the ESCM. The connection does not transfer any safety or control information to perform any safety or control functions. The signal from the IFPD provides component identification information to the ESCM. This signal is used for bringing up the control template on the ESCM display and is not used for performing any control functions. Therefore, the ESF-CCS division does not rely on information from the IFPD to accomplish its function.

Compliance with DI&C-ISG-04 regarding communication from the IFPD to the ESCM is described in Appendix C of the Safety I&C System Technical Report (Reference 3).

Data Communication between the QIAS-N and Other Systems

a. QIAS-N network

The QIAS-N network is used for signal connections as follows:

- 1) QIAS-N processor
- 2) QIAS-N display

3) QIAS-N MTP

The QIAS-N network is dedicated network implemented by the SDN. The intra-division network for the safety systems such as PPS, ESFCCS, and CPCS is also implemented by the SDN. However, these networks are different and designed in such a way that safety systems do not receive any signals from non-safety systems. These networks are also physically separated and electrically isolated.

The QIAS-N network use different data communication hardware and protocols from the DCN-I network. The QIAS-N network is physically separated and electrically isolated from the DCN-I network.

All data paths between the QIAS-N network and safety systems are fiber-optic cables to provide electrical isolation. The QIAS-N network is seismically qualified as seismic Category I.

The QIAS-N network is a redundant network. The QIAS-N processor 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.

The QIAS-N communicates with display devices such as a mini-large display panel (mini-LDP), QIAS-N flat panel displays (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 demonstrate 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 on system safety, reliability, and performance are also evaluated. The error rates include errors in device addressing and signal data attributes.

b. Communications between the IPS and QIAS-N

APR1400 DCD TIER 2

The data communication path through a multi-channel gateway is connected between the QIAS-N network and the DCN-I network for the IPS. Electrical isolation is maintained between the QIAS-N network and DCN-I network by way of the gateway and the fiber-optic cable that provides isolation. Since the electrical isolation is maintained between the IPS and QIAS-N, a failure of the IPS does not adversely affect the QIAS-N and vice versa.

An evaluation is performed to demonstrate that the throughput, capacity, response time, and data accuracy of the communications between the IPS and QIAS-N meet the requirements of the supported I&C systems. Potential errors and their impact on 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 a safety system.
- b. The components and modules in the P-CCS and PCS data communication system are designed as a non-safety system.
- c. The components and modules in the IPS and QIAS-N data communication network are designed as a non-safety system.

7.9.2.2 Data Communication Systems Software Quality

Details of the software quality for the data communication systems are as follows:

APR1400 DCD TIER 2

- a. The SDL software quality embedded in the PPS BP, LCL processor, CPC, CEAC, CPP, ESF-CCS GC/LC, and CPM for performing reactor protection system (RPS) and ESFAS functions is the SC.
- b. The SDN software quality embedded in the MTP, ITP, OM, and QIAS-P is the ITS.

Data communication system software quality for the interfaces between the IPS and QIAS-N is as follows:

- a. The DCN-I network software quality embedded in the P-CCS, PCS, and IPS is the 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.

- 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 (repeatable and predictable). 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.

APR1400 DCD TIER 2

The execution sequence of an application program is repeated at predetermined intervals.

c. Time delays within the data communication system

The delays of data transport due to data communication in the data communication system are included in the response time calculation. The response time calculations are validated by vendor test and site test to verify the performance.

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 data communication with the emergency operations facility, technical support center, and emergency response data system (see Figure 7.7-12).

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, and potential hazards to the data communication system and from the data communication system therefore do not prevent operation of the safety functions.

APR1400 DCD TIER 2

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 is 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.

Access to the cabinets is normally required only during system testing, calibration, and 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 division are physically separated and functionally isolated from other divisions. 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 that the requirements of the single failure criteria are satisfied. The FMEA shows that a single failure does not adversely affect other systems and divisions such as redundant PPS divisions or ESF-CCS divisions.

7.9.2.7 Independence

The data communication systems are designed to maintain the independence between the safety divisions, and between the safety system and non-safety system. Fiber-optic cables are used to meet the isolation and independence requirements outlined in NRC RG 1.75 (Reference 5). Exceptions for the SDL are discussed in Appendix C in the Safety I&C System Technical Report.

APR1400 DCD TIER 2

7.9.2.8 Fail-Safe Failure Modes

Fail-safe failure modes for data communication systems are 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 failures of the system. System testing and inoperable surveillance in accordance with the Technical Specifications in the Chapter 16 detect all additional credible failures that could cause miss-operation or failure.

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 a data communication system is indicated on display and alarm systems.

7.9.2.11 Electromagnetic Interference and Radio-Frequency Interference Susceptibility

The SDN and SDL equipment is qualified in accordance with MIL Std. 461E (Reference 9) and IEC 61000 Part 4 Series (Reference 10) as endorsed by NRC RG 1.180 (Reference 6). The equipment is tested for both conducted and radiated signals as follows:

- a. Electromagnetic interference and radio-frequency interference (EMI/RFI) emissions
- b. EMI/RFI susceptibility / immunity
- c. Surge withstand capability

The DCN-I network equipment is tested for EMI/RFI emission so that any safety equipment is not affected.

7.9.2.12 Diversity and Defense-in-Depth

Data communication systems were postulated to fail as a result of a software common-cause failure of the safety systems in accordance with the guidance presented in BTP 7-19

APR1400 DCD TIER 2

(Reference 11). 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 network is seismically qualified as seismic Category II.

7.9.3 Analysis

The data communication systems (1) comply with the recommendations in the regulatory guides and industry codes and standards that are applicable to these systems, (2) are in conformance to the requirements of GDC 1 (Reference 12).

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. These results show compliance with the staff positions in DI&C-ISG-04.

7.9.4 Combined License Information

No combined license (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," Institute of Electrical and Electronics Engineers, 2003.
2. DI&C-ISG-04, "Highly-Integrated Control Rooms – Communications Issues (HICRc)," Rev. 1, U.S. Nuclear Regulatory Commission, March 2009.

APR1400 DCD TIER 2

3. APR1400-Z-J-NR-14001-P, "Safety I&C System," Rev. 3, KEPCO & KHNP, May 2018.
4. APR1400-Z-J-NR-14003-P, "Software Program Manual," Rev. 3, KEPCO & KHNP, May 2018.
5. Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems," Rev. 3, U.S. Nuclear Regulatory Commission, February 2005.
6. Regulatory Guide 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems," Rev. 1, U.S. Nuclear Regulatory Commission, October 2003.
7. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," Rev. 3, KEPCO & KHNP, May 2018.
8. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, U.S. Nuclear Regulatory Commission, July 2011.
9. MIL-STD-461E, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment," U.S. Department of Defense, August 1999.
10. IEC 61000-4 Series, "Electromagnetic Compatibility-Testing and Measurement Techniques," International Electrotechnical Commission.
11. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," Rev. 6, U.S. Nuclear Regulatory Commission, July 2012.
12. 10 CFR Part 50, Appendix A, General Design Criterion 1, "Quality Standards and Records," U.S. Nuclear Regulatory Commission.

APR1400 DCD TIER 2

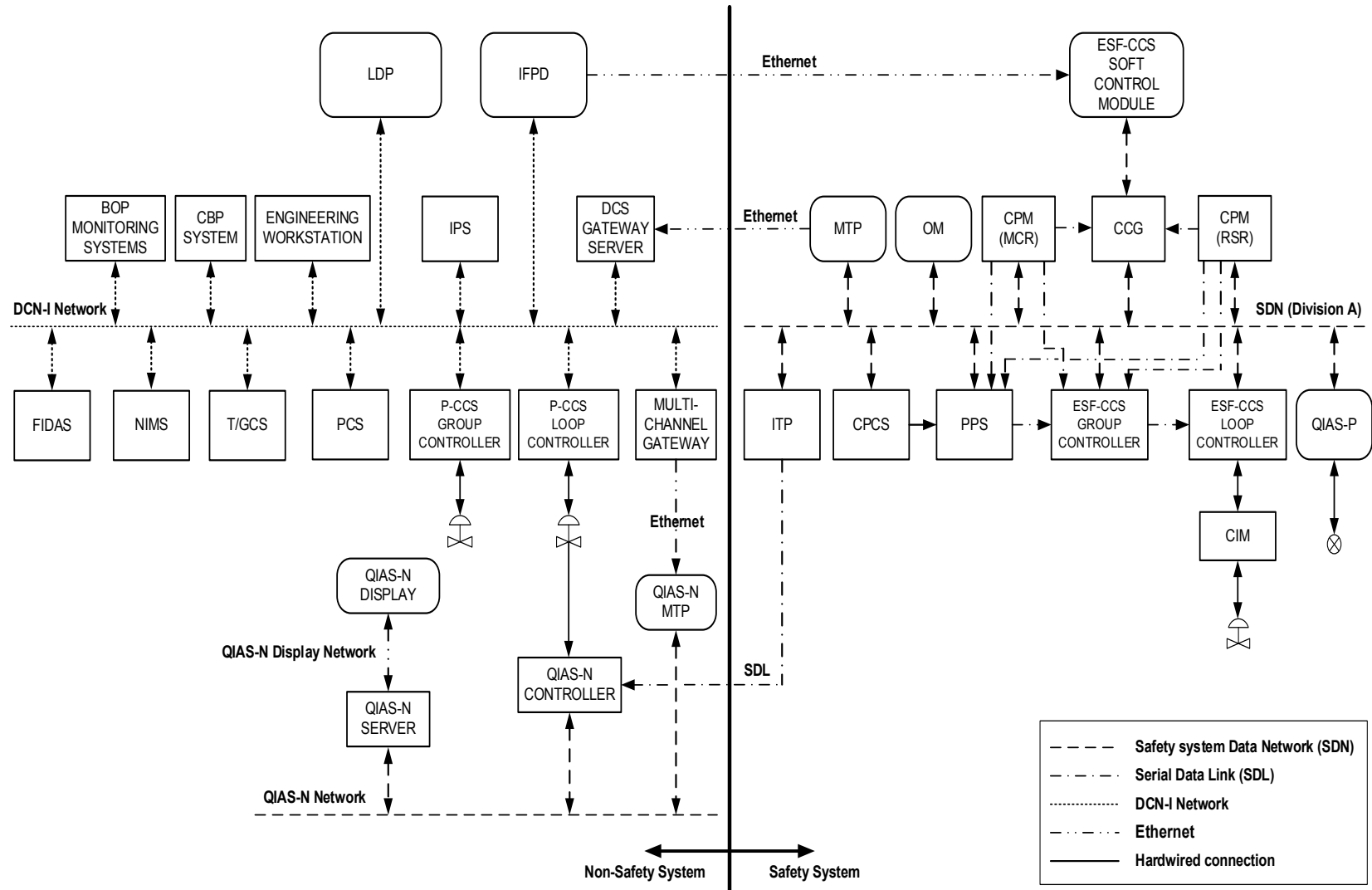


Figure 7.9-1 Data Communication Block Diagram