2.5 INSTRUMENTATION AND CONTROLS

2.5.1 Reactor Trip System and Engineered Safety Feature Systems

2.5.1.1 Design Description

The reactor trip (RT) system and the engineered safety feature (ESF) system and the associated field equipment are part of the protection and safety monitoring system (PSMS). The PSMS includes the reactor protection system (RPS), the engineered safety features actuation system (ESFAS), the safety logic system (SLS) and the safety grade human system interface system (HSIS). The PSMS consists of four safety divisions.

The purpose of the PSMS is to provide protection against unsafe reactor operation during steady-state and transient power operation by automatically tripping the reactor and actuating necessary engineered safety features. These trip and actuation functions are implemented by the RT system and the ESF system, respectively. The safety grade HSIS includes conventional switches for manual actuation of reactor trip and ESF actuation. Table 2.5.1-1 shows equipment names and classifications of the PSMS and the field equipment for the RT system and the ESF system.

The safety visual display units (VDUs) and the safety VDU processors, which are part of the PSMS, provide monitoring and control for the safety-related plant components and instrumentation, including monitoring and control for the credited manual operator actions. The operational VDUs, which are part of the plant control and monitoring system (PCMS), also provide monitoring and control for the safety-related plant components and instrumentation, including the monitoring and control for the credited manual operator actions and monitoring of automatic ESF actuations.

1. The functional arrangement of the RPS is as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-2, and as shown in Figures 2.5.1-1 and 2.5.1-2.

2. The functional arrangements of the ESFAS, SLS and HSIS are as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-3, and as shown in Figures 2.5.1-2 and 2.5.1-3.

3. The functional arrangement of the RTBs is as described in the Design Description of Subsection 2.5.1 and as shown in Figure 2.5.1-4.

4. Conventional PSMS switches in the MCR can be used to provide manual initiation for reactor trip and ESF Manual Actuations identified in Tables 2.5.1-2 and 2.5.1-3.

5. The seismic Category I equipment identified in Table 2.5.1-1 can withstand seismic design basis loads without loss of safety function.

6. The Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.

7. The RPS, ESFAS, SLS, safety VDU processor, and safety VDU are qualified to meet the electromagnetic conditions that would exist based on the equipment location in the facility, without loss of safety function.

8. The Class 1E equipment listed in Table 2.5.1-1 is located in a facility area that provides protection from accident related hazards such as missiles, pipe breaks and flooding.

9. The Class 1E PSMS equipment listed in Table 2.5.1-1 is powered from two safety-related power sources: the first source is its respective Class 1E division and the second source is from another division to ensure reliable power to each division of the PSMS.

10.a The redundant divisions of PSMS and field equipment listed in Table 2.5.1-1 are physically separated and electrically independent of each other and physically separated and electrically independent of any non-safety systems.

10.b Deleted.

11. The PSMS, via PCMS, provides the operator with: (1) non-safety HSIS indications of the bypassed or inoperable status indication (BISI) for RT actuation, ESF actuations identified in Table 2.5.1-3, and interlocks important to safety identified in Table 2.5.1-4; and (2) the ability to manually actuate the BISI for protective actions.

12. The PSMS cabinets have key locks and door position alarms, and are located in a vital area of the facility.

13. Redundant safety equipment of the PSMS and field equipment listed in Table 2.5.1-1 are provided with a clear means of identification.

14.a The PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit.

14.b Once initiated (automatically or manually), the intended sequences of safety-related functions as identified in Tables 2.5.1-2 and 2.5.1-3 of the PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.

15. Deleted.

16. The PSMS signals are derived from direct measurements described in Table 2.5.1-2 and Table 2.5.1-3.

17.a The PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules.

17.b A single channel or division of the PSMS can be bypassed to allow on-line testing, maintenance or repair and this capability does not prevent the PSMS from performing its safety function.

18. The PSMS automatically removes the operating bypasses listed in Table 2.5.1-7 when permissive conditions are not met.

19. Deleted.

20. Deleted.

21. The RT logic of the PSMS is designed to fail to a safe state such that loss of electrical power to a division of PSMS results in a trip condition for that division. Loss of electrical power to a division of the PSMS ESF logic does not result in ESF actuation.

22. The RT and ESF actuation instrumentation that is required to function during normal operation, anticipated operational occurrence (AOO) and postulated accident (PA) conditions is provided with adequate range to monitor normal operating, AOO and PA events. The monitored variables are listed in Tables 2.5.1-2 and 2.5.1-3.

23. The PSMS provides the interlocks important to safety identified in Table 2.5.1-4.

~~24. The PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.~~

24. Software Program Manuals (SPM) is implemented to manage the PSMS software lifecycle process in each software lifecycle phase.

25.a Manual control signals from the safety VDU override and can disable manual control signals from the operational VDU by the priority logic in the PSMS.~~Manual controls from the operational VDU are blocked from the safety VDU and can be disabled manually from the safety VDU. The logic in the SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESF actuation signal.~~

25.b Automatic ESFAS actuation signals identified in Table 2.5.1-3 and ~~the~~ automatic interlock~~s~~ signals important to safety identified in Table 2.5.1-4 in the PSMS override the manual and automatic control signals from the PCMS ~~control signals~~ to the safety-related components by the priority logic in the PSMS.

26. A signal selection algorithm (SSA) is provided in the PCMS for the monitoring variables as listed in Table 2.5.1-5 to ensure the PCMS does not take control action that results in a condition which requires RT or ESF action based on a single instrument channel failure or a single RPS division failure.

27. Input sensors from each division of the PSMS as identified in Table 2.5.1-2 and Table 2.5.1-3 are compared continuously in the PCMS to allow detection of out-of-tolerance sensors.

28. Deleted.

29.a ESF systems are automatically initiated from signals that originate in the RPS as described in Table 2.5.1-3.

29.b Manual actuation of ESF systems is carried out through a diverse signal path that bypasses the RPS.

30.a Deleted.

30.b Deleted.

2.5.1.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.1-6 describes the ITAAC for the RT system and the ESF system.

Table 2.5.1-1 Equipment Names and Classifications of PSMS and Field Equipment for RT System and ESF System

Equipment Name	Seismic Category I	Class 1E	Qualification for Harsh Environment
PSMS			
RPS Division A/B/C/D	Yes	Yes	No
ESFAS Division A/B/C/D	Yes	Yes	No
SLS Division A/B/C/D	Yes	Yes	No
MCR*[1] Safety VDU Division A/B/C/D	Yes	Yes	No
RSR*[2] Safety VDU Division A/B/C/D	Yes	Yes	No
Safety VDU Processor Division A/B/C/D	Yes	Yes	No
MCR Division Level Switches A/B/C/D	Yes	Yes	No
MCR/RSR Transfer Panels*[3]	Yes	Yes	No
Field Equipment			
RTB Division A/B/C/D	Yes	Yes	No
RT and ESF Measurement Instrumentation	Yes	Yes	Yes*[4]/No

Note1: Main Control Room
Note2: Remote Shutdown Room
Note3: Transfer function is described in Subsection 2.5.2.
Note4: Field equipment which is located in the harsh environment

Table 2.5.1-2 Reactor Trip and Monitored Variables

Actuation Signal	Monitored Variables
High Source Range Neutron Flux	Neutron Flux
High Intermediate Range Neutron Flux	Neutron Flux
High Power Range Neutron Flux (Low Setpoint)	Neutron Flux*1
High Power Range Neutron Flux (High Setpoint)	Neutron Flux*1
High Power Range Neutron Flux Positive Rate	Neutron Flux*1
High Power Range Neutron Flux Negative Rate	Neutron Flux*1
Over Temperature ΔT	Reactor Coolant Temperature*2
	Pressurizer Pressure
	Neutron Flux*1
Over Power ΔT	Reactor Coolant Temperature*2
	Neutron Flux*1
Low Reactor Coolant Flow	Reactor Coolant Flow
Low Reactor Coolant Pump Speed	Reactor Coolant Pump Speed
Low Pressurizer Pressure	Pressurizer Pressure
High Pressurizer Pressure	Pressurizer Pressure
High Pressurizer Water Level	Pressurizer Water Level
Low Steam Generator Water Level	Steam Generator Water Level
High-High Steam Generator Water Level	Steam Generator Water Level
ECCS Actuation	Refer to ECCS Actuations in Table 2.5.1-3.
Manual Actuation	Manual Switch Position (Reactor Trip Switch)

Notes:
1: Power Range Neutron flux is a spatially dependent variable due to axial variations.
2. Reactor Coolant System hot leg (3 sensors) is spatially dependent.

Table 2.5.1-3 ESF Actuations and Monitored Variables (Sheet 1 of 3)

ESF Function	Actuation Signal	Monitored Variables
ECCS Actuation	Low Pressurizer Pressure	Pressurizer Pressure
	Low Main Steam Line Pressure	Main Steam Line Pressure
	High Containment Pressure	Containment Pressure
	Manual Actuation	Manual Switch Position (ECCS Actuation Switch)
Main Steam Line Isolation	High-High Containment Pressure	Containment Pressure
	Low Main Steam Line Pressure	Main Steam Line Pressure
	High Main Steam Line Pressure Negative Rate	Main Steam Line Pressure
	Manual Actuation	Manual Switch Position (Main Steam Line Isolation Switch)
Containment Isolation Phase A	ECCS Actuation	ECCS Actuation Signal
	Manual Actuation	Manual Switch Position (Containment Isolation Switch)
Containment Isolation Phase B	High-3 Containment Pressure	Containment Pressure
	Manual Actuation	Manual Switch Position (Containment Spray Switch)
Containment Purge Isolation	ECCS Actuation	ECCS Actuation Signal
	High Containment Area Radiation	Containment Area Radiation
	Manual Actuation	Manual Switch Position (Containment Isolation Switch) (Containment Spray Switch)
Containment Spray	High-3 Containment Pressure	Containment Pressure
	Manual Actuation	Manual Switch Position (Containment Spray Switch)

Table 2.5.1-3 ESF Actuations and Monitored ~~Parameters~~ Variables (Sheet 2 of 3)

ESF Function	Actuation Signal	Monitored Variables
Emergency Feedwater Actuation	ECCS Actuation	ECCS Actuation Signal
	Low Steam Generator Water Level	Steam Generator Water Level
	Loss of Offsite Power	Class 1E 6.9kV Bus Voltage
	Manual Actuation	Manual Switch Position (Emergency Feedwater Actuation Switch)
Emergency Feedwater Isolation Loop A (Loop B, C, D) *1	Low Main Steam Line Pressure	Main Steam Line Pressure
	High Steam Generator Water level	Steam Generator Water Level
	Manual Actuation	Manual Switch Position (Emergency Feedwater Isolation Switch)
Main Control Room Isolation	ECCS Actuation	ECCS Actuation Signal
	High Main Control Room Outside Air Intake Radiation	Main Control Room Outside Air Intake Gas Radiation
		Main Control Room Outside Air Intake Iodine Radiation
		Main Control Room Outside Air Intake Particulate Radiation
	Manual Actuation	Manual Switch Position (Main Control Room Isolation Switch)
Main Feedwater Regulation Valve Closure	Low T_{avg} coincident with RT (P-4)	Reactor Coolant Temperature*2
		Reactor Trip (RTB Open)
Main Feedwater Isolation	High-High Steam Generator Water Level	Steam Generator Water Level
	ECCS Actuation	ECCS Actuation Signal
	Manual Actuation	Manual Switch Position (Main Feedwater Isolation Switch)

Note1: Loop A isolation is initiated by steam generator water level signal and main steam line pressure signal from loop A. All loops are identical (e.g., loop B isolation is initiated by the signal from loop B).
Note 2: Reactor Coolant System hot leg (3 sensors) is spatially dependent.

Table 2.5.1-3 ESF Actuations and Monitored ~~Parameters~~ Variables (Sheet 3 of 3)

ESF Function	Actuation Signal	Monitored Variables
CVCS Isolation	High Pressurizer Water Level	Pressurizer Water Level
	Manual Actuation	Manual Switch Position (CVCS Isolation Switch)

Table 2.5.1-4 Interlocks Important to Safety

Containment Spray/Residual Heat Removal Pump Hot Leg Isolation Valve Open Permissive Interlock
~~Simultaneous-Open Block Interlock with Residual Heat Removal Discharge Line Containment Isolation Valve and Containment Spray Header Containment Isolation Valve~~
Simultaneous-Open Block Interlock with Containment Spray/Residual Heat Removal Pump Hot Leg Isolation Valve and Containment Spray Header Containment Isolation Valve
Reactor Makeup Water Line Isolation Interlock
Accumulator Discharge Valve Open Interlock
Component Cooling Water Supply and Return Header Tie Line Isolation Interlock
RCP Thermal Barrier Heat Exchanger Component Cooling Water Return Line Isolation Interlock
Low-Pressure Letdown Line Isolation Interlock

Table 2.5.1-5 Monitored Variables Using Signal Selection Algorithms (SSA)

Power Range Neutron Flux
Reactor Coolant Temperature
Pressurizer Pressure
Pressurizer Water Level
Steam Generator Water Level
Main Steam Line Pressure
Turbine Inlet Pressure

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 1 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The functional arrangement of the RPS is as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-2, and as shown in Figures 2.5.1-1 and 2.5.1-2.	1. Inspection of the as-built RPS will be performed.	1. The as-built RPS conforms to the functional arrangement as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-2, and as shown in Figures 2.5.1-1 and 2.5.1-2.
2. The functional arrangements of the ESFAS, SLS and HSIS are as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-3, and as shown in Figures 2.5.1-2 and 2.5.1-3.	2. Inspection of the as-built ESFAS, SLS and HSIS will be performed.	2. The as-built ESFAS, SLS and HSIS conform to the functional arrangement as described in the Design Description of Subsection 2.5.1 and in Table 2.5.1-3, and as shown in Figures 2.5.1-2 and 2.5.1-3.
3. The functional arrangement of the RTBs is as described in the Design Description of Subsection 2.5.1 and as shown in Figure 2.5.1-4.	3. Inspection of the as-built RTBs will be performed.	3. The as-built RTBs conform to the functional arrangement as described in the Design Description of Subsection 2.5.1 and as shown in Figure 2.5.1-4.
4. Conventional PSMS switches in the MCR can be used to provide manual initiation for reactor trip and ESF Manual Actuations identified in Tables 2.5.1-2 and 2.5.1-3.	4. A test of the as-built conventional PSMS manual actuation switches for RT and ESF functions will be performed.	4. As-built conventional PSMS switches in the MCR can be used to provide manual initiation for the reactor trip Manual Actuation identified in Table 2.5.1-2 and the ESF Manual Actuations identified in Table 2.5.1-3.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. The seismic Category I equipment identified in Table 2.5.1-1 can withstand seismic design basis loads without loss of safety function.	5.i Inspections will be performed to verify that the as-built seismic Category I equipment identified in Table 2.5.1-1 is located in a seismic Category I structure.	5.i The as-built seismic Category I equipment identified in Table 2.5.1-1 is located in a seismic Category I structure.
	5.ii Type tests, analyses, or a combination of type tests and analyses, of seismic Category I equipment identified in Table 2.5.1-1 will be performed using analytical assumptions, or will be performed under conditions which bound the seismic design basis requirements.	5.ii A report exists and concludes that the seismic Category I equipment identified in Table 2.5.1-1 can withstand seismic design basis loads without loss of safety function.
	5.iii Inspections and analyses will be performed to verify the as-built seismic Category I equipment identified in Table 2.5.1-1, including anchorages, is seismically bounded by the tested or analyzed conditions.	5.iii A report exists and concludes that the as-built seismic Category I equipment identified in Table 2.5.1-1, including anchorages, is seismically bounded by the tested or analyzed conditions.
6. The Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.	6.i Type tests or a combination of type tests and analyses using the design environmental conditions, or under the conditions which bound the design environmental conditions, will be performed on Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment.	6.i A report exists and concludes that the Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform its safety function.
	6.ii Inspection will be performed of the as-built Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment and the associated wiring, cables, and terminations located in a harsh environment.	6.ii The as-built Class 1E equipment and the associated wiring, cables, and terminations identified in Table 2.5.1-1 as being qualified for a harsh environment are bounded by type tests or a combination of type tests and analyses.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
7. The RPS, ESFAS, SLS, safety VDU processor, and safety VDU are qualified to meet the electromagnetic conditions that would exist based on the equipment location in the facility, without loss of safety function.	7. Type tests or a combination of type tests and analyses will be performed on the equipment.	7. A report exists and concludes that the RPS, ESFAS, SLS, safety VDU processor, and safety VDU are qualified to meet the electromagnetic conditions that would exist based on the equipment location in the facility, without loss of safety function.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 4 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
8. The Class 1E equipment listed in Table 2.5.1-1 is located in a facility area that provides protection from accident related hazards such as missiles, pipe breaks and flooding.	8. An inspection of the as-built equipment location will be performed.	8. The as-built equipment listed in Table 2.5.1-1 is located in a plant area that provides protection from accident related hazards such as missiles, pipe breaks and flooding.
9. The Class 1E PSMS equipment listed in Table 2.5.1-1 is powered from two safety-related power sources: the first source is its respective Class 1E division and the second source is from another division to ensure reliable power to each division of the PSMS.	9. Inspection of the as-built PSMS equipment will be performed.	9. The Class 1E as-built PSMS equipment listed in Table 2.5.1-1 is powered from two safety-related power sources: the first source is its respective Class 1E division and the second source is from another division of the PSMS.
10.a The redundant divisions of PSMS and field equipment listed in Table 2.5.1-1 are physically separated and electrically independent of each other and physically separated and electrically independent of any non-safety systems.	10.a.i 1) An inspection of the as-built PSMS and field equipment will be performed to verify physical separation. 2) Analyses, tests or a combination of analyses and tests of the as-built PSMS and field equipment will be performed to verify its electrical independence.	10.a.i 1) The as-built PSMS and field equipment redundant divisions' physical separation is provided by distance or barriers in accordance with RG 1.75. 2) A report exists and concludes that as-built PSMS and field equipment redundant divisions' electrical independence is achieved by independent power sources and electrical circuits for each division, and by fiber optic cable interfaces, conventional isolators, or other proven isolation methods or devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 5 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	10.a.ii Type tests or analyses, or a combination of type tests and analyses of the isolation devices will be performed.	10.a.ii A report exists and concludes that the isolation devices prevent credible faults.
10.b Deleted.	10.b.i Deleted.	10.b.i Deleted.
	10.b.ii Deleted.	10.b.ii Deleted.
11. The PSMS, via PCMS, provides the operator with: (1) non-safety HSIS indications of the bypassed or inoperable status indication (BISI) for RT actuation, ESF actuations identified in Table 2.5.1-3, and interlocks important to safety identified in Table 2.5.1-4; and (2) the ability to manually actuate the BISI for protective actions.	11. A test of the as-built equipment will be performed.	11. The as-built PSMS, via the as-built PCMS, provides the operator with: (1) automatic non-safety HSIS BISI for RT actuation, ESF actuations identified in Table 2.5.1-3, and interlocks important to safety identified in Table 2.5.1-4 and (2) the ability to manually actuate the BISI for these protective actions.
12. The PSMS cabinets have key locks and door position alarms, and are located in a vital area of the facility.	12.i A test of the as-built PSMS cabinets for key lock capability, and a test of door position alarms, will be performed.	12.i Each cabinet of the as-built PSMS has key locking capability, and alarms are received in the as-built MCR when cabinet doors are opened.
	12.ii An inspection of the as-built PSMS cabinets will be performed for the installed location.	12.ii Each cabinet of the as-built PSMS is located in a vital area of the facility.
13. Redundant safety equipment of the PSMS and field equipment listed in Table 2.5.1-1 are provided with a clear means of identification.	13. An inspection of the as-built equipment for conformance with equipment color coding requirements will be performed.	13. The as-built equipment listed in Table 2.5.1-1 complies with the color coding requirements.
14.a The PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit.	14.a A test of the as-built PSMS will be performed.	14.a The as-built PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 6 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
14.b Once initiated (automatically or manually), the intended sequences of safety-related functions as identified in Tables 2.5.1-2 and 2.5.1-3 of the PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.	14.b A test of the as-built PSMS will be performed.	14.b Once initiated (automatically or manually), the intended sequences of safety-related functions as identified in Tables 2.5.1-2 and 2.5.1-3 of the as-built PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.
15. Deleted.	15. Deleted.	15. Deleted.
16. The PSMS signals are derived from direct measurements described in Table 2.5.1-2 and Table 2.5.1-3.	16. An inspection of the as-built PSMS will be performed to verify that input signals are from direct measurement of sensor output described in Table 2.5.1-2 and Table 2.5.1-3.	16. The input signals to the as-built PSMS are derived from direct measurements described in Table 2.5.1-2 and Table 2.5.1-3.
17.a The PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules.	17.a Tests and analyses of the as-built PSMS will be performed.	17.a A report exists and concludes that the as-built PSMS is designed to facilitate recognition and location of malfunctioning components or modules.
17.b A single channel or division of the PSMS can be bypassed to allow on-line testing, maintenance or repair and this capability does not prevent the PSMS from performing its safety function.	17.b Tests will be performed to confirm the as-built channel or division bypass capabilities and to confirm the function of the bypass interlock logic.	17.b A single channel or division of the as-built PSMS can be bypassed to allow on-line testing, maintenance or repair and this capability does not prevent the PSMS from performing its safety function.
18. The PSMS automatically removes the operating bypasses listed in Table 2.5.1-7 when permissive conditions are not met.	18. A test of the as-built PSMS will be performed.	18. The as-built PSMS automatically removes the operating bypasses listed in Table 2.5.1-7 when permissive conditions are not met.
19. Deleted.	19. Deleted.	19. Deleted.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 7 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
20. Deleted.	20. Deleted.	20. Deleted.
21. The RT logic of the PSMS is designed to fail to a safe state such that loss of electrical power to a division of PSMS results in a trip condition for that division. Loss of electrical power to a division of the PSMS ESF logic does not result in ESF actuation.	21. A test will be performed by disconnecting the electrical power to each division of the as-built PSMS.	21. Each division of the as-built RT logic of the as-built PSMS fails to a safe state upon loss of electrical power to the division (i.e., results in a trip condition for that division), and loss of electric power to a division of the as-built PSMS ESF logic does not result in ESF actuation.
22. The RT and ESF actuation instrumentation that is required to function during normal operation, anticipated operational occurrence (AOO) and postulated accident (PA) conditions is provided with adequate range to monitor normal operating, AOO and PA events. The monitored variables are listed in Tables 2.5.1-2 and 2.5.1-3.	22. An inspection of the as-built RT and ESF actuation instrumentation ranges will be performed.	22. The ranges of the as-built PSMS RT and ESF actuation instrumentation that is required to function during normal operation, anticipated operational occurrences (AOO) and postulated accident (PA) conditions, and that is listed in Tables 2.5.1-2 and 2.5.1-3, meet design requirements.
23. The PSMS provides the interlocks important to safety identified in Table 2.5.1-4.	23. A test of the as-built PSMS will be performed.	23. The as-built PSMS provides the interlocks important to safety identified in Table 2.5.1-4 when the simulated plant process signals reach a predetermined limit.
~~24. The PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.~~	~~24. Inspections of the as-built hardware and software life cycle documentation of the PSMS will be performed.~~	~~24. The as-built PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.~~

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 8 of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
24. Software Program Manual (SPM) is implemented to manage the PSMS software lifecycle process in each software lifecycle phase.	24.i An inspection will be performed for the plant requirements phase result summary report of PSMS software in accordance with the SPM.	24.i The plant requirements phase result summary report exists and concludes that the plant requirements phase activities of PSMS software are performed in accordance with the SPM.
	24.ii An inspection will be performed for the system requirements phase result summary report of PSMS software in accordance with the SPM.	24.ii The system requirements phase result summary report exists and concludes that the system requirements phase activities of PSMS software are performed in accordance with the SPM.
	24.iii An inspection will be performed for the design phase result summary report of PSMS software in accordance with the SPM.	24.iii The design requirements phase result summary report exists and concludes that the design phase activities of PSMS software are performed in accordance with the SPM.
	24.iv An inspection will be performed for the implementation phase result summary report of PSMS software in accordance with the SPM.	24.iv The implementation phase result summary report exists and concludes that the implementation phase activities of PSMS software are performed in accordance with the SPM.
	24.v An inspection will be performed for the test phase result summary report of PSMS software in accordance with the SPM.	24.v The test phase result summary report exists and concludes that the test phase activities of PSMS software are performed in accordance with the SPM.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 9 of 109)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	24.vi An inspection will be performed for the installation phase result summary report of PSMS software in accordance with the SPM.	24.vi The installation phase result summary report exists and concludes that the installation phase activities of PSMS software are performed in accordance with the SPM.
25.a Manual control signals from the safety VDU override and can disable manual control signals from the operational VDU to the PSMS by the priority logic in the PSMS. ~~Manual controls from the operational VDU are blocked from the safety VDU and can be disabled manually from the safety VDU. The logic in the SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESF actuation signal.~~	25.a A Test~~s~~ of the as-built PSMS, including safety VDU, will be performed using simulated signals.	25.a Simulated manual control signals from the as-built safety VDU override and can disable simulated manual control signals from the operational VDU to the PSMS by the priority logic in the as-built PSMS. ~~Manual controls from the operational VDU are blocked from the as-built safety VDU and can be disabled manually from the as-built safety VDU. The logic in the as-built SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESF actuation signal.~~
25.b Automatic ESFAS actuation signals identified in Table 2.5.1-3 and the interlocks important to safety identified in Table 2.5.1-4 override the manual and automatic control signals from the PCMS ~~control signals~~ to the safety-related components by the priority logic in the PSMS.	25.b A test of the as-built PSMS will be performed by using simulated signals. ~~to confirm that simulated ESFAS actuation signals identified in Table 2.5.1-3 and the interlocks important to safety identified in Table 2.5.1-4 override as-built PCMS control signals.~~	25.b ~~As-built PCMS control signals are overridden by s~~Simulated automatic ESFAS actuation signals identified in Table 2.5.1-3 and ~~the~~ automatic interlock~~s~~ signals important to safety identified in Table 2.5.1-4 in the as-built PSMS override the simulated manual and automatic control signals from the PCMS to the safety-related components by the priority logic in the as-built PSMS.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 10~~9~~ of 10~~9~~)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
26. A signal selection algorithm (SSA) is provided in the PCMS for the monitoring variables as listed in Table 2.5.1-5 to ensure the PCMS does not take control action that results in a condition which requires RT or ESF action based on a single instrument channel failure or a single RPS division failure.	26. A test of the as-built PCMS SSA functions will be performed using simulated signals.	26. The as-built PCMS SSA functions to ensure the PCMS does not take control action that results in a condition which requires RT or ESF action based on a single instrument channel failure or a single RPS division failure, for the monitored variables listed in Table 2.5.1-5.
27. Input sensors from each division of the PSMS as identified in Table 2.5.1-2 and Table 2.5.1-3 are compared continuously in the PCMS to allow detection of out-of-tolerance sensors.	27. A test of the as-built PCMS function will be performed utilizing simulated signals.	27. Input sensors as identified in Table 2.5.1-2 and Table 2.5.1-3 from each division of the as-built PSMS that are out-of-tolerance can be detected by the PCMS.
28. Deleted.	28. Deleted.	28. Deleted.
29.a ESF systems are automatically initiated from signals that originate in the RPS as described in Table 2.5.1-3.	29.a A test of the as-built PSMS will be performed.	29.a As-built ESF systems are automatically initiated from signals that originate in the as-built RPS as described in Table 2.5.1-3.
29.b Manual actuation of ESF systems is carried out through a diverse signal path that bypasses the RPS.	29.b A test of the as-built PSMS will be performed.	29.b Manual actuation of the as-built ESF systems is carried out through a diverse signal path that bypasses the as-built RPS.
30.a Deleted.	30.a Deleted.	30.a Deleted.
30.b Deleted.	30.b Deleted.	30.b Deleted.

Table 2.5.1-7 Operating Bypasses

Designation		RT and/or ESF	Function
P-6	Intermediate Range Neutron Flux Above or Below Setpoint	RT	Below setpoint • Remove manual operating bypass for high source range neutron flux reactor trip.
P-7	Turbine Inlet Pressure (P-13) or Power Range Neutron Flux (P-10) Above Setpoint or Turbine Inlet Pressure (P-13) and Power Range Neutron Flux (P-10) Below Setpoint	RT	Above setpoint • Remove operating bypass for low pressurizer pressure reactor trip. • Remove operating bypass for low reactor coolant flow reactor trip. • Remove operating bypass for low RCP speed reactor trip. • Remove operating bypass for high pressurizer water level reactor trip. • Remove operating bypass for high-high SG water level reactor trip. • Remove operating bypass for reactor trip by turbine trip.
P-10	Power Range Neutron Flux Above or Below Setpoint	RT	Below setpoint • Remove manual operating bypass for high intermediate range neutron flux reactor trip. • Remove manual operating bypass for high power range neutron flux (low setpoint) reactor trip.
P-11	Pressurizer Pressure Above or Below Setpoint	ESF	Above setpoint • Remove manual operating bypass for low pressurizer pressure ECCS actuation. • Remove manual operating bypass for high-high SG water level MFW isolation function for all MFW pumps, all MFW isolation valves, and all SG water filling control valves. • Remove manual operating bypass for high pressurizer water level CVCS. • Remove manual operating bypass for EFW isolation. • Remove manual operating bypass for low main steam line pressure ECCS actuation. • Remove manual operating bypass for low main steam line pressure main steam line isolation.

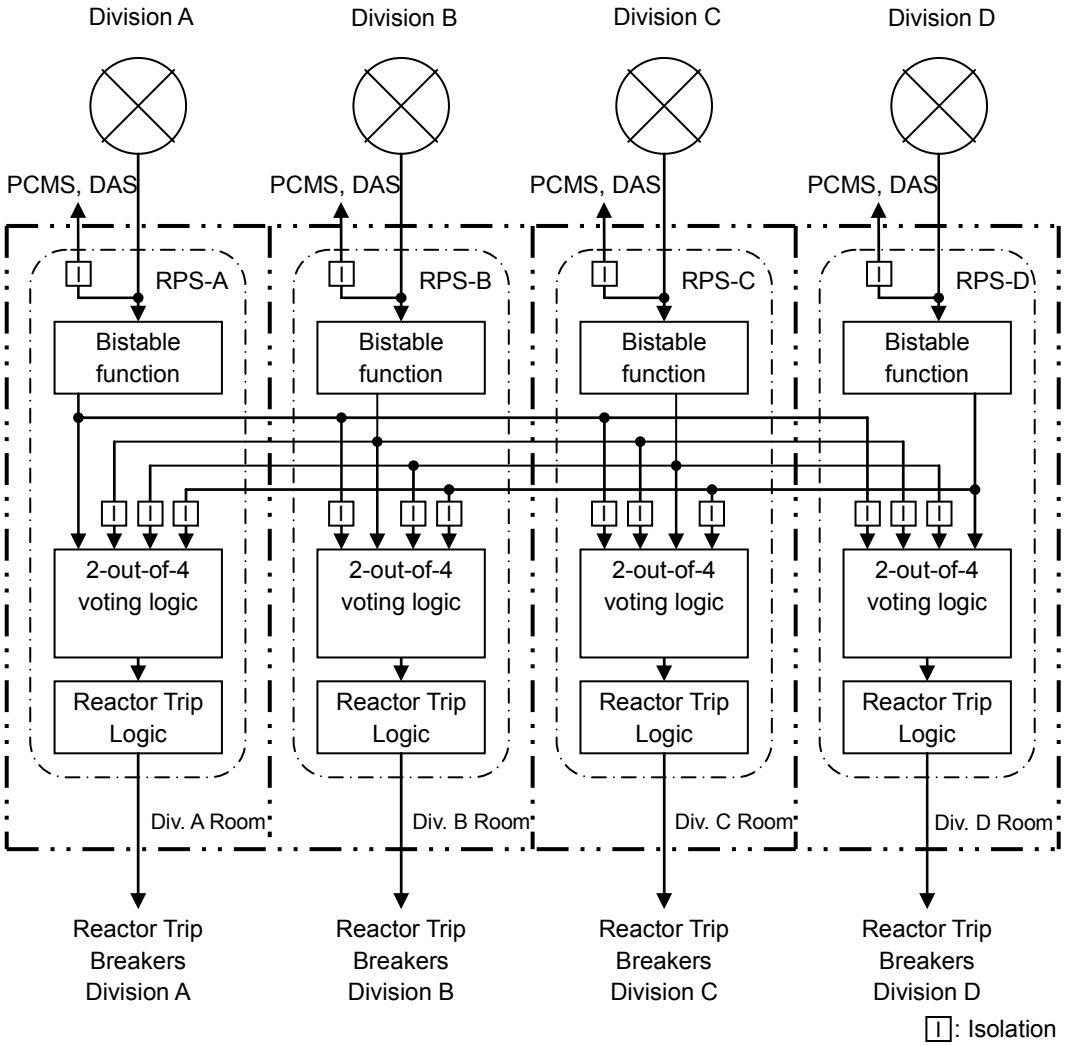


Figure 2.5.1-1 Configuration of the Reactor Trip System

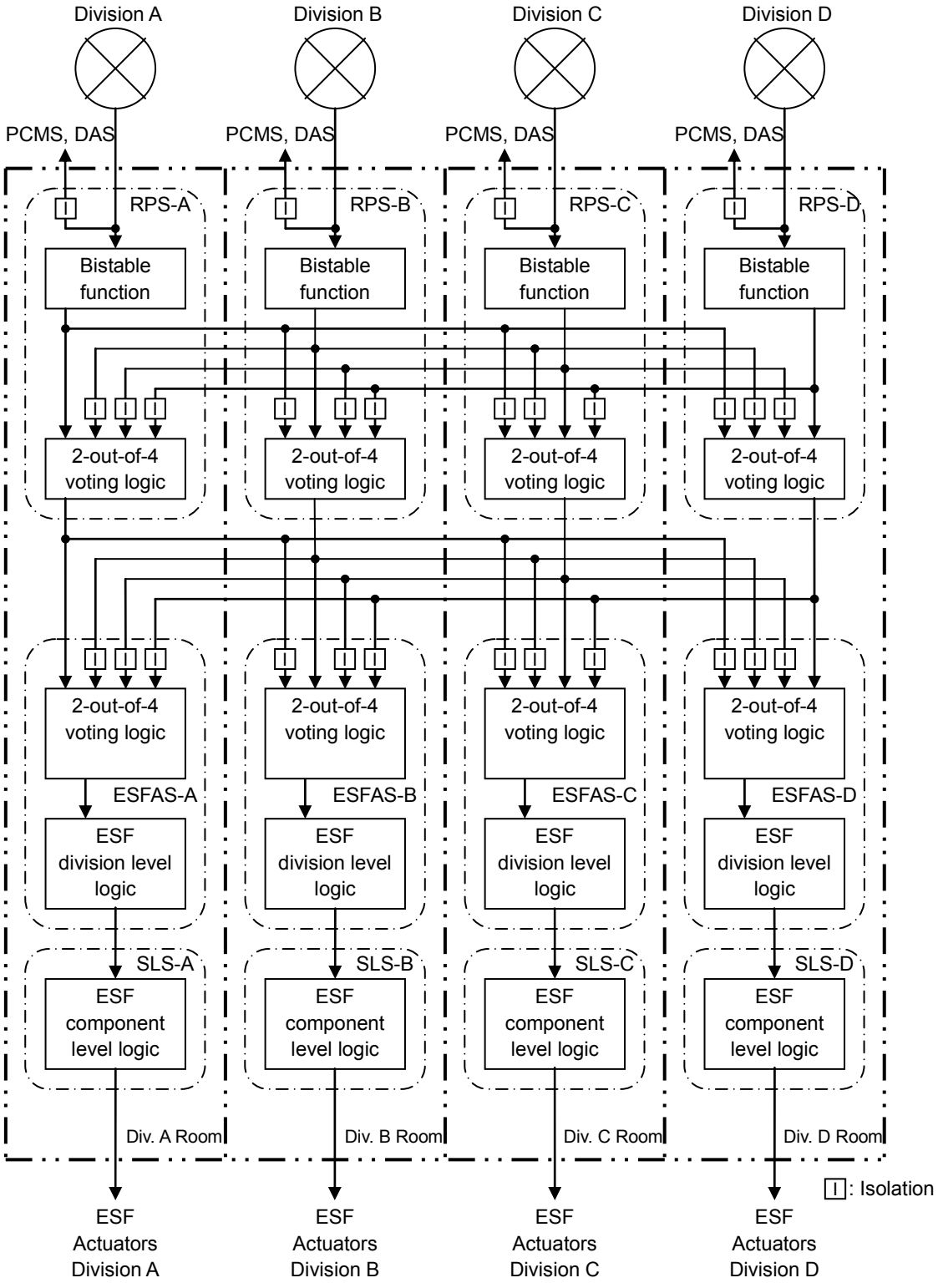
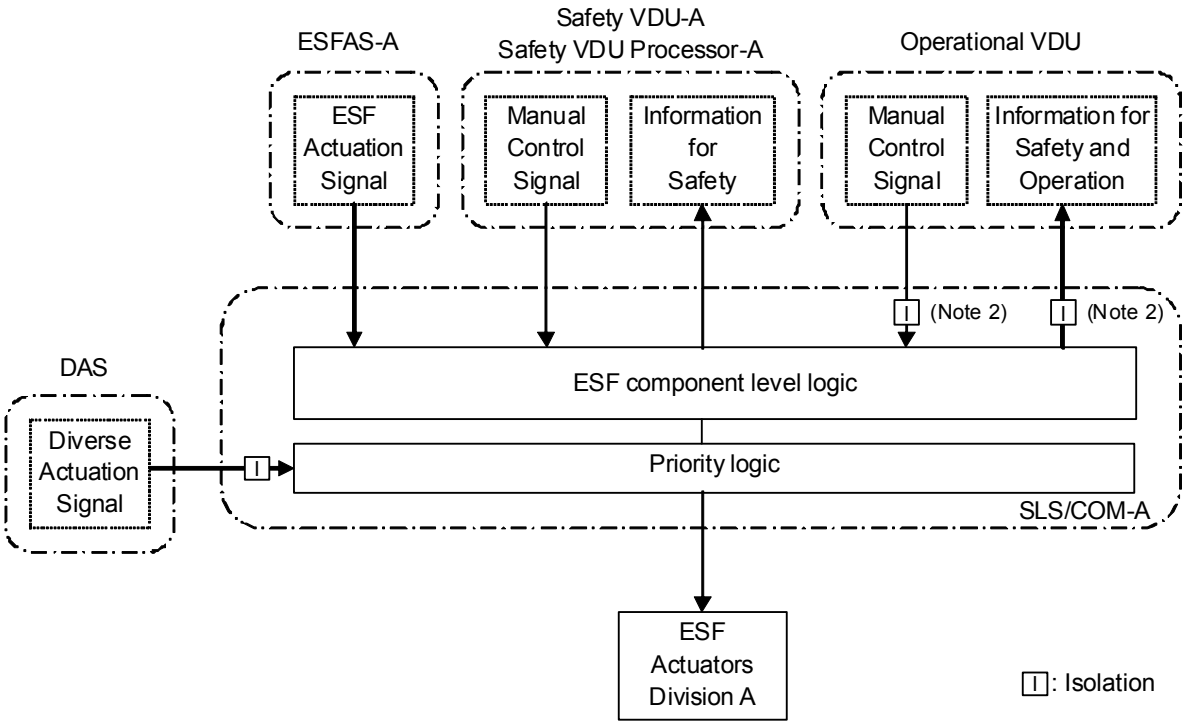
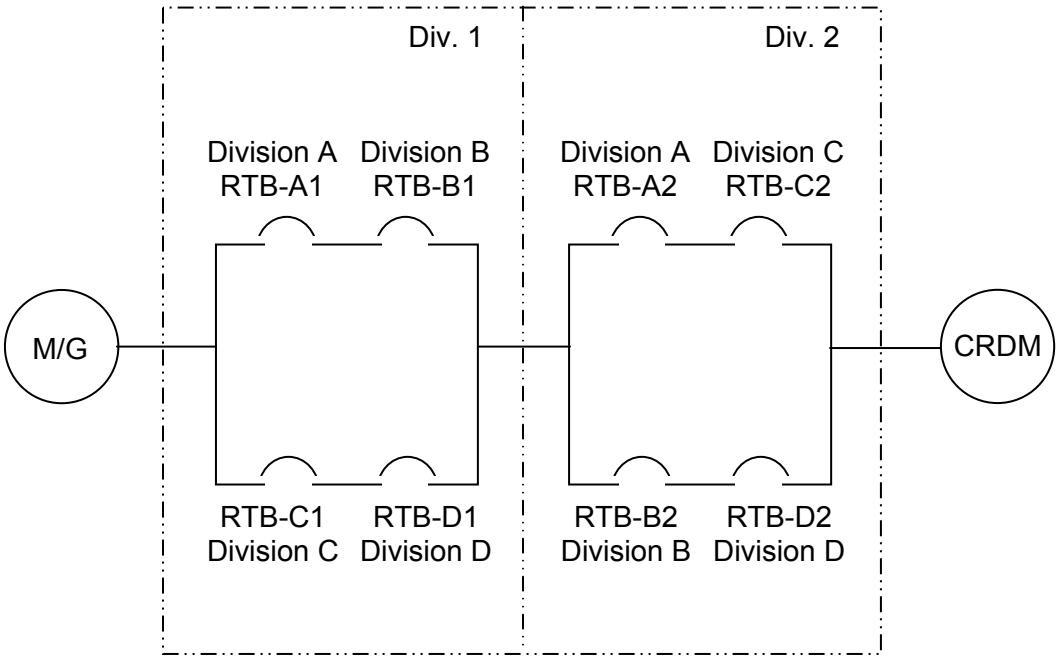


Figure 2.5.1-2 Configuration of the Engineered Safety Feature System



Note 1: Division A system is shown for the representative configuration.
Note 2: Isolation is performed in communication system.

Figure 2.5.1-3 Configuration of the Safety Grade Component Control System



M/G: Motor-Generator Set

CRDM: Control Rod Drive Mechanism

Note: Div. 1 and Div. 2 show the separate fire area.

Figure 2.5.1-4 Configuration of the Reactor Trip Breakers

2.5.2 Systems Required for Safe Shutdown

2.5.2.1 Design Description

Safe shutdown can be achieved from the MCR or the remote shutdown room (RSR) using redundant safety-related instrumentation and control (I&C) systems of the PSMS, including the RPS, ESFAS, SLS and safety VDUs. The operational VDUs may also be used for monitoring safety-related instrumentation and manually controlling safety-related components. Normal shutdown can also be achieved from the MCR or RSR using non-safety instrumentation and non-safety component controls via the PCMS, including the operational VDUs, in addition to the above safety-related I&C systems.

There are no plant systems specifically and solely dedicated as safe shutdown or normal shutdown systems.

The systems required for safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Second, the systems provide the RHR capability to maintain adequate core cooling. A boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin.

Manual controls through the safety VDUs or the operational VDUs in the MCR or the RSR, allow operators to transition to and maintain hot standby, and transition to and maintain cold shutdown through hot shutdown. If the MCR is uninhabitable, the same control and monitoring of the safe shutdown and the normal shutdown functions can be performed from the RSR.

1. The PSMS controls and monitors the systems required for the safe shutdown functions identified in Tables 2.5.2-1 and 2.5.2-2.

2.a The MCR/RSR transfer switches provide the capability to transfer PSMS controls between the MCR and the RSR. Separate transfer switches are provided for each of the four PSMS divisions.

2.b The MCR/RSR transfer switches provide the capability to transfer PCMS controls between the MCR and the RSR.

2.c Deleted.

3. Electrical isolation is provided between the MCR and the RSR.

4. The RSR and the MCR/RSR transfer switch cabinet outside the MCR can be locked to prevent unauthorized access. Alarms indicating access to the MCR/RSR transfer switch locations are provided in the MCR.

5. Redundant safety-related equipment of the safe shutdown systems identified in Tables 2.5.2-1 and 2.5.2-2, and the MCR/RSR transfer switches, are provided with a clear means of identification.

6. The functional arrangement of the SLS and HSIS for the safe shutdown systems is as described in the Design Description of Subsection 2.5.2.1 and as shown in Figure 2.5.2-1.

7. Upon manual reactor trip from the remote shutdown console (RSC), once initiated, the reactor trip and turbine trip functions continue until completion.

2.5.2.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.2-3 describes the ITAAC for the systems required for safe shutdown.

Table 2.5.2-1 Safe Shutdown Functions and Related Process Systems for Hot Standby

Trip the reactor which accomplishes the reactor shutdown condition (RT)
RCS heat removal by the following measures: - Main steam release to atmosphere (MSS) - Provide EFW to SGs (EFWS and MSS) - Supply boric acid water to RCS (SIS) - Component cooling by operating CCW and ESW (CCWS and ESWS)
RCS pressure control (RCS)
Provide HVAC functions to the required areas (MCR HVAC, ESFVS, ECWS)
Utilize the emergency power source (EPS) for the above functions in the event of LOOP*[1]

Note1: Loss of Offsite Power

Table 2.5.2-2 Safe Shutdown Functions and Related Process Systems for Cold Shutdown through Hot Shutdown

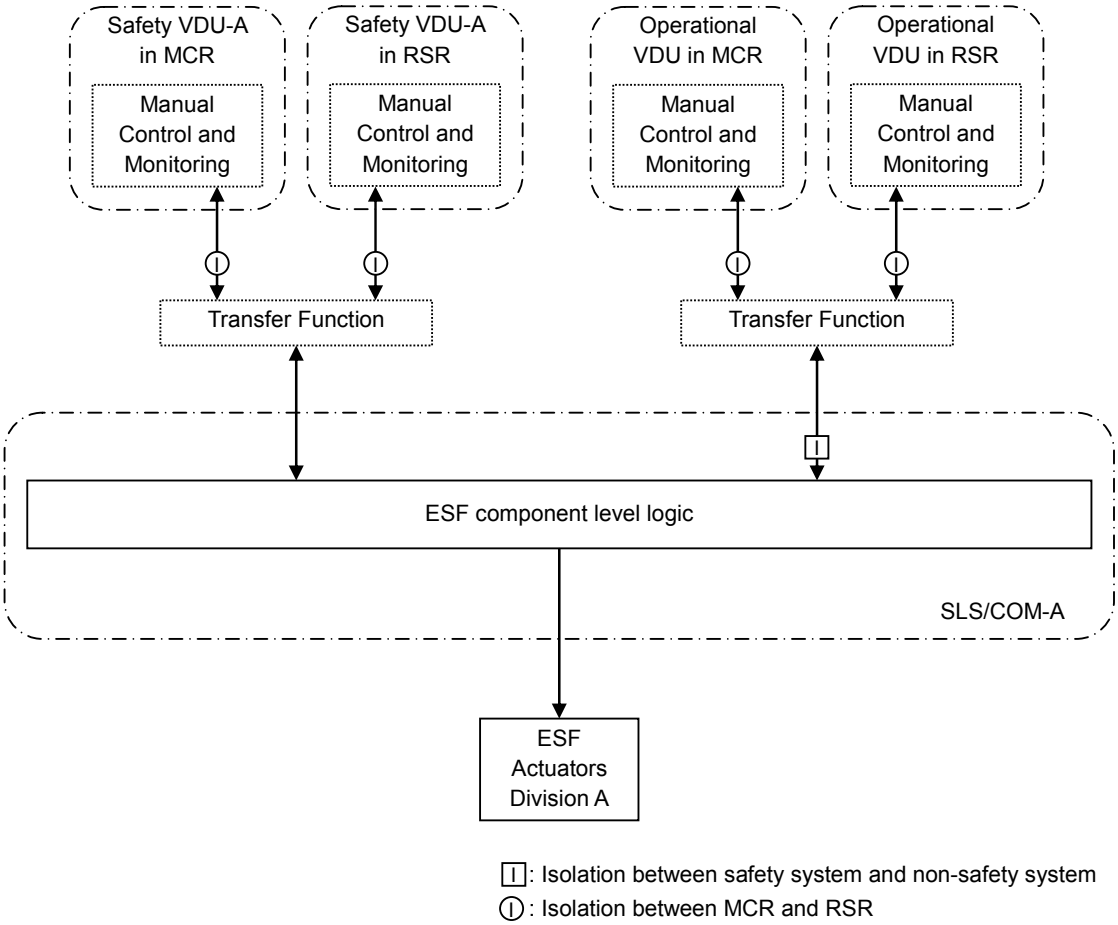
Remove heat from the RCS by the following measures: - Main steam release to atmosphere - Provide EFW to SGs (EFWS and MSS) - Operate RHRS
RCS pressure control (RCS)
Supply boric acid water to RCS (SIS)
Component cooling by operating CCW and ESW (CCWS and ESWS)
Provide HVAC functions to the required areas (MCR HVAC, ESFVS, ECWS)
Monitor neutron flux
Manually initiate appropriate ESF system(s) for shutdown operating bypasses (ECCS Actuation Signal Block, Main Steam Line Pressure signal Block)
Utilize the emergency power source (EPS) for the above functions in the event of LOOP

Table 2.5.2-3 Systems Required for Safe Shutdown Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The PSMS controls and monitors the systems required for the safe shutdown functions identified in Tables 2.5.2-1 and 2.5.2-2.	1. Inspections and tests of the as-built systems required for the safe shutdown functions identified in Tables 2.5.2-1 and 2.5.2-2, will be performed.	1. The as-built systems required for the safe shutdown functions identified in Tables 2.5.2-1 and 2.5.2-2, can be controlled and monitored by the as-built PSMS.
2.a The MCR/RSR transfer switches provide the capability to transfer PSMS controls between the MCR and the RSR. Separate transfer switches are provided for each of the four PSMS divisions.	2.a A test of the as-built PSMS transfer capability will be performed to demonstrate the disabling of the MCR controls and enabling of the RSR controls. This test can be conducted on a sample basis for at least one set of controls within each of the four PSMS divisions.	2.a The as-built MCR/RSR transfer switches transfer controls between the MCR and the RSR separately for each as-built PSMS safety division, as follows: 1. Controls at the RSR are disabled when controls are active in the MCR for each respective as-built PSMS division. 2. Controls at the MCR are disabled when controls are active in the RSR for each respective as-built PSMS division.
2.b The MCR/RSR transfer switches provide the capability to transfer PCMS controls between the MCR and the RSR.	2.b A test of the as-built PCMS transfer capability will be performed to demonstrate the disabling of the MCR controls and enabling of the RSR controls. This test can be conducted on a sample basis for at least one set of controls within each controller of the PCMS.	2.b The as-built MCR/RSR transfer switches transfer PCMS control between the MCR and the RSR as follows: 1. Controls at the RSR are disabled when controls are active in the MCR for each of the as-built controllers of the PCMS. 2. Controls at the MCR are disabled when controls are active in the RSR for each of the as-built controllers of the PCMS.
2.c Deleted.	2.c Deleted.	2.c Deleted.

Table 2.5.2-3 Systems Required for Safe Shutdown Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. Electrical isolation is provided between the MCR and the RSR.	3. An inspection of the as-built PSMS will be performed.	3. The as-built PSMS provides interfaces from the I&C equipment rooms to the MCR and the RSR using fiber optic cable or qualified electrical isolation devices.
4. The RSR and the MCR/RSR transfer switch cabinet outside the MCR can be locked to prevent unauthorized access. Alarms indicating access to the MCR/RSR transfer switch locations are provided in the MCR.	4.i An inspection of the as-built MCR/RSR transfer switch locations to verify access control by keylock will be performed.	4.i The as-built RSR and the as-built MCR/RSR transfer switch cabinet outside the MCR can be locked to prevent unauthorized access.
	4.ii A test of the access alarms for the as-built RSR and MCR/RSR transfer switch cabinet outside the MCR will be performed.	4.ii Access to the as-built RSR and access to the as-built MCR/RSR transfer switch cabinet outside the MCR is alarmed in the as-built MCR.
5. Redundant safety-related equipment of the safe shutdown systems identified in Tables 2.5.2-1 and 2.5.2-2, and the MCR/RSR transfer switches, are provided with a clear means of identification.	5. Inspection of the as-built systems identified in Tables 2.5.2-1 and 2.5.2-2, and the MCR/RSR transfer switches, for conformance with color coding requirements will be performed.	5. The as-built equipment of the safe shutdown systems identified in Tables 2.5.2-1 and 2.5.2-2, and the MCR/RSR transfer switches, comply with the color coding requirements.
6. The functional arrangement of the SLS and HSIS for the safe shutdown systems is as described in the Design Description of Subsection 2.5.2.1 and as shown in Figure 2.5.2-1.	6. Inspection of the as-built SLS and HSIS for the safe shutdown systems will be performed.	6. The as-built SLS and HSIS for the safe shutdown systems conforms to the functional arrangement as described in the Design Description of Subsection 2.5.2.1 and as shown in Figure 2.5.2-1.
7. Upon manual reactor trip from the remote shutdown console (RSC), once initiated, the reactor trip and turbine trip functions continue until completion.	7. A test of the as-built RSC will be performed.	7. Upon manual reactor trip from the as-built RSC, once initiated, the reactor trip and turbine trip functions continue until completion.



Note: Division A system is shown as a representative configuration.

Figure 2.5.2-1 Configuration of the SLS and HSIS for Safe Shutdown

2.5.3 Diverse Actuation System

2.5.3.1 Design Description

The DAS is a non-safety system that is diverse from the PSMS software and the digital platform of the PSMS. Therefore, a software or digital platform common cause failure (CCF) in the digital safety and non-safety systems (PSMS and PCMS), would not affect the DAS. The DAS provides monitoring, control and actuation capability of safety and the non-safety systems required to mitigate the AOOs and the PAs, concurrent with a CCF that could disable the functions of the PSMS and the PCMS.

The DAS consists of two subsystems. Each subsystem includes a diverse automatic actuation cabinet (DAAC) located in separate rooms. A diverse HSI panel (DHP) located in the MCR includes HSI components for both DAS subsystems. A manual actuation permissive switch located in the MCR, but physically separated from the DHP, is required for the manual actuations identified in Tables 2.5.3-2 and 2.5.3-3.

1.a The functional arrangement of the DAS is as described in the Design Description of Subsection 2.5.3.1 and as shown in Figure 2.5.3-1. Variables monitored by the DAS are as indicated in Table 2.5.3-1.

1.b The DAS is physically separated and electrically independent from the PSMS.

1.c DAS controls are provided in the MCR to manually actuate equipment identified in Table 2.5.3-2, and to manually actuate functions identified in Table 2.5.3-3.

1.d The DAS provides automatic actuation of the equipment and for the functions identified in Tables 2.5.3-2 and 2.5.3-3, respectively, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits.

1.e The DAS prevents spurious actuation due to single failures or due to a fire or seismic event. Spurious actuations are prevented by the DAS as follows:

- Automatic DAS functions are actuated by two subsystems and DAS actuation needs coincidence of both subsystems.
- The DAS prevents spurious actuation due to a seismic event. Thus the SSE will not result in a DAS failure that adversely affects the PSMS.
- The redundant DAS cabinets are located in separate fire areas to prevent spurious actuation from a fire in one area.
- Manual DAS functions identified in Tables 2.5.3-2 and 2.5.3-3 require actuation of two switches in the MCR. Separation between the permissive switch and the DHP prevents a fire in one switch location from affecting the other switch location.

2. The DAS has the following capabilities:

- Operates with both DAAC subsystems operable (i.e., in a two-out-of-two configuration), or with one subsystem manually tripped and one subsystem operable.
- The system can be tested manually without causing component actuation.
- Loss of power or removal of a module does not cause spurious DAS actuation.
- Capability to bypass failed sensors functions.

3. The DAS equipment, including input and output interfaces, signal processing and HSI, consists of conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits, switches, indicators).

4. The DAS equipment used for the anticipated transient without scram (ATWS) mitigation (i.e., reactor trip, turbine trip and emergency feedwater actuation) is diverse from the hardware used for the reactor trip function of the PSMS. This design commitment does not apply to measurement instrumentation and signal splitters, which distribute measurement signals to the DAS and the PSMS.

5. Deleted.

2.5.3.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.3-4 describes the ITAAC for the DAS.

Table 2.5.3-1 Variables Monitored by DAS

Critical Safety Function	Variables
Reactivity Control	Wide Range Neutron Flux
RCS Integrity	Pressurizer Pressure
	Reactor Coolant Pressure
Core Heat Removal	Reactor Coolant Cold Leg Temperature
RCS Inventory Control	Pressurizer Water Level
Secondary Heat Sink	Steam Generator Water Level
	Main Steam Line Pressure
Containment Integrity	Containment Pressure

Table 2.5.3-2 Equipment Actuated by DAS

Safety Function/Associated Components	Actuation Type
Diverse Reactor Trip (M/G set trip)	Automatic/Manual (MCR)
Turbine Trip	Automatic/Manual (MCR)
Emergency Feedwater Pump	Automatic/Manual (MCR)
Safety Injection Pump	Automatic/Manual (MCR)
Safety Depressurization Valve	Manual (MCR)
Main Steam Depressurization Valve	Manual (MCR)
Steam Generator Blowdown Isolation Valve	Automatic/Manual (MCR)
Main Feedwater Regulation Valve	Automatic/Manual (MCR)
Emergency Feedwater Control Valve	Manual (MCR)
Containment Isolation Valves	Manual (MCR)
Main Steam Line Isolation Valve	Manual (MCR)

Table 2.5.3-3 DAS Functions and Actuation Signals

DAS Function	Actuation Signal
Reactor Trip, Turbine Trip and Main Feedwater Isolation	Low Pressurizer Pressure
	High Pressurizer Pressure
	Low Steam Generator Water Level
	Manual Switch Signal
Emergency Feedwater Actuation	Low Steam Generator Water Level
	Manual Switch Signal
ECCS Actuation	Low-Low Pressurizer Pressure
	Manual Switch Signal
Containment Isolation	Manual Switch Signal
Main Steam Isolation	Manual Switch Signal

Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 4)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1.a The functional arrangement of the DAS is as described in the Design Description of Subsection 2.5.3.1 and as shown in Figure 2.5.3-1. Variables monitored by the DAS are as indicated in Table 2.5.3-1.	1.a Inspection of the as-built DAS will be performed.	1.a The as-built DAS conforms to the functional arrangement as described in the Design Description of Subsection 2.5.3.1 and as shown in Figure 2.5.3-1. Variables monitored by the DAS are as indicated in Table 2.5.3-1.
1.b The DAS is physically separated and electrically independent from the PSMS.	1.b.i An inspection of the as-built DAS will be performed for physical separation of the DAS from the as-built PSMS.	1.b.i Physical separation of the as-built DAS from the as-built PSMS is provided by locating the as-built DAAC in separate rooms, and locating the as-built DHP in the MCR.
	1.b.ii Analyses, tests or a combination of analyses and tests of the as-built DAS will be performed to verify its electrical independence from the as-built PSMS.	1.b.ii A report exists and concludes that electrical independence of the as-built DAS from the as-built PSMS is achieved by using independent power sources for the as-built DAAC and the as-built DHP, and by using qualified electrical fault isolation devices.
1.c DAS controls are provided in the MCR to manually actuate equipment identified in Table 2.5.3-2, and to manually actuate functions identified in Table 2.5.3-3.	1.c Tests will be performed to verify the as-built equipment listed in Table 2.5.3-2 can be operated, and to verify the manual actuation functions in Table 2.5.3-3, using as-built DAS manual controls in the as-built MCR.	1.c As-built DAS controls in the as-built MCR operate the as-built equipment listed in Table 2.5.3-2, and provide manual actuation capability for the actuation functions identified in Table 2.5.3-3.

Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 4)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1.d The DAS provides automatic actuation of the equipment and for the functions identified in Tables 2.5.3-2 and 2.5.3-3, respectively, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits.	1.d Tests will be performed to verify DAS automatic actuation capability for the as-built equipment listed in Table 2.5.3-2, and to verify the automatic actuation functions in Table 2.5.3-3, using simulated signals.	1.d The DAS provides automatic actuation of the equipment identified in Table 2.5.3-2, and automatic actuation for the functions identified in Table 2.5.3-3, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits.
1.e The DAS prevents spurious actuation due to single failures or due to a fire or seismic event. Spurious actuations are prevented by the DAS as follows: • Automatic DAS functions are actuated by two subsystems and DAS actuation needs coincidence of both subsystems. • The DAS prevents spurious actuation due to a seismic event. Thus the SSE will not result in a DAS failure that adversely affects the PSMS. • The redundant DAS cabinets are located in separate fire areas to prevent spurious actuation from a fire in one area. • Manual DAS functions identified in Tables 2.5.3-2 and 2.5.3-3 require actuation of two switches in the MCR. Separation between the permissive switch and the DHP prevents a fire from one switch location from affecting the other switch location.	1.e.i Test and analysis will be performed to verify the as-built DAS prevents spurious actuation due to single failures or due to a seismic event.	1.e.i A report exists and concludes that the as-built DAS prevents spurious actuation due to single failures or due to a seismic event as follows. • Automatic DAS functions are actuated by two as-built subsystems and DAS actuation needs coincidence of both subsystems. • The as-built DAS prevents spurious actuation due to a seismic event.

Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 4 of 4)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	1.e.ii Test and inspection of the as-built DAS will be performed to verify the existence of a manual permissive switch, to verify the DAS permissive switch is physically located separate from the DHP, and to verify physical separation of redundant DACC cabinets.	1.e.ii The as-built DAS: • Redundant DAAC cabinets are located in separate equipment rooms. • Includes a manual permissive switch that prevents spurious manual actuation for those signals with only one manual actuation switch, as identified in Table 2.5.3-3. • The manual permissive switch is physically separated from the DHP to prevent a fire that starts in one switch location from affecting the other switch location.
2. The DAS has the following capabilities: • Operates with both DAAC subsystems operable (i.e., in a two-out-of-two configuration), or with one subsystem manually tripped and one subsystem operable. • The system can be tested manually without causing component actuation. • Loss of power or removal of a module does not cause spurious DAS actuation. • Capability to bypass failed sensors functions.	2. Tests of the as-built DAS will be performed. The tests will include tests of the manual controls, loss of power, and module removal, as well as simulated signal inputs to test the system.	2. A report exists and concludes that the as-built DAS has the following capabilities: • Operates with both as-built DAAC subsystems operable (i.e., in a two-out-of-two configuration), or with one subsystems manually tripped and one subsystems operable. • The system can be tested manually without causing component actuation. • Loss of power or removal of a module does not cause spurious DAS actuation. • Capability to bypass failed sensors functions.

Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 5 of 4)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
3. The DAS equipment, including input and output interfaces, signal processing and HSI, consists of conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits, switches, indicators).	3. Inspection of the as-built DAS will be performed.	3. The as-built DAS equipment consists of conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits, switches, indicators).
4. The DAS equipment used for the anticipated transient without scram (ATWS) mitigation (i.e., reactor trip, turbine trip and emergency feedwater actuation) is diverse from the hardware used for the reactor trip function of the PSMS. This design commitment does not apply to measurement instrumentation and signal splitters, which distribute measurement signals to the DAS and the PSMS.	4. Inspection of the as-built DAS and RT system hardware within the as-built PSMS will be performed.	4. The as-built DAS equipment used for the ATWS mitigation (i.e., reactor trip, turbine trip and emergency feedwater actuation) is diverse from the hardware used for the reactor trip function of the as-built PSMS.
5. Deleted.	5. Deleted.	5. Deleted.

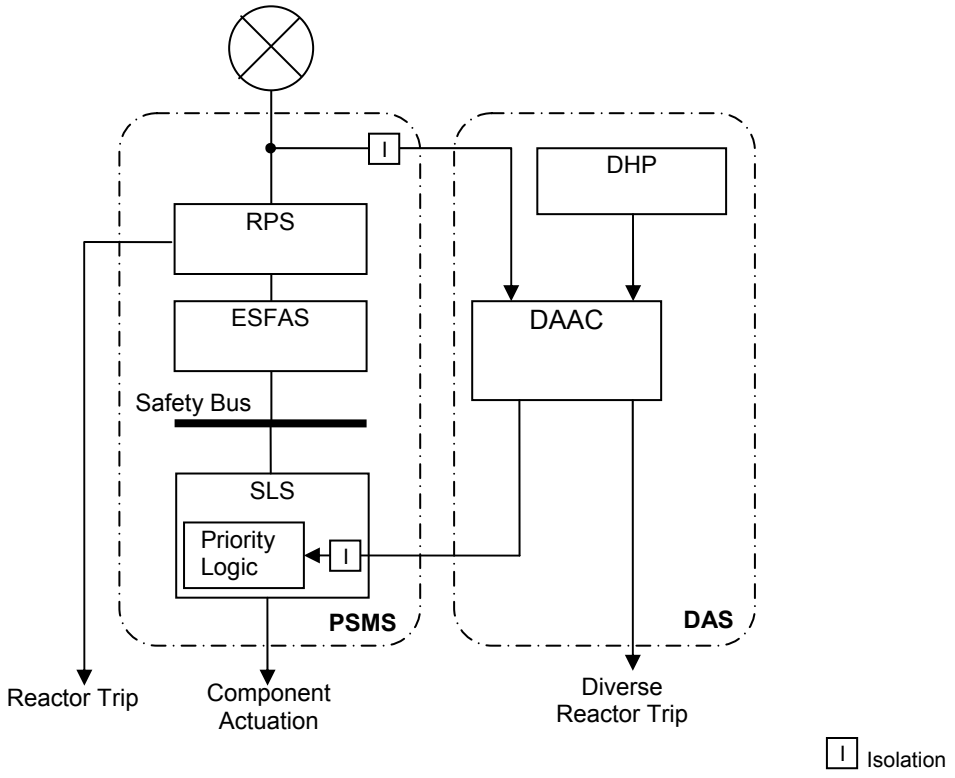


Figure 2.5.3-1 DAS Configuration

2.5.4 Information Systems Important to Safety

2.5.4.1 Design Description

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

The information important to safety includes the following:

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

The PAM variables are identified in Table 2.5.4-1, and the alarms for the credited manual operator actions are identified in Table 2.5.4-3.

1. PAM variables as identified in Table 2.5.4-1, BISI, SPDS information, and plant alarms for credited manual operator actions as identified in Table 2.5.4-3, for information systems important to safety, are provided on safety and non-safety HSI equipment at the MCR, RSR, and TSC, as shown in Figure 2.5.4-1.

2. Deleted.

3. The field instrumentation for the PAM variables identified in Table 2.5.4-1 that is subjected to a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.

4. Deleted.

2.5.4.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.4-2 describes the ITAAC for the information systems important to safety.

Table 2.5.4-1 Post Accident Monitoring Variables

Reactor Coolant Hot Leg Temperature (Wide Range)
Reactor Coolant Cold Leg Temperature (Wide Range)
Reactor Coolant Pressure
Degrees of Subcooling
Pressurizer Water Level
Steam Generator Water Level (Wide Range)
Steam Generator Water Level (Narrow Range)
Main Steam Line Pressure
Emergency Feedwater Flow
Wide Range Neutron Flux
Core Exit Temperature
Containment Pressure
Reactor Vessel Water Level
Containment Isolation Valve Position (Excluding Check Valves)
Refueling Water Storage Pit Water Level (Wide Range)
Refueling Water Storage Pit Water Level (Narrow Range)
Emergency Feedwater Pit Water Level
Containment High Range Area Radiation

Table 2.5.4-2 Information Systems Important to Safety Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 2)

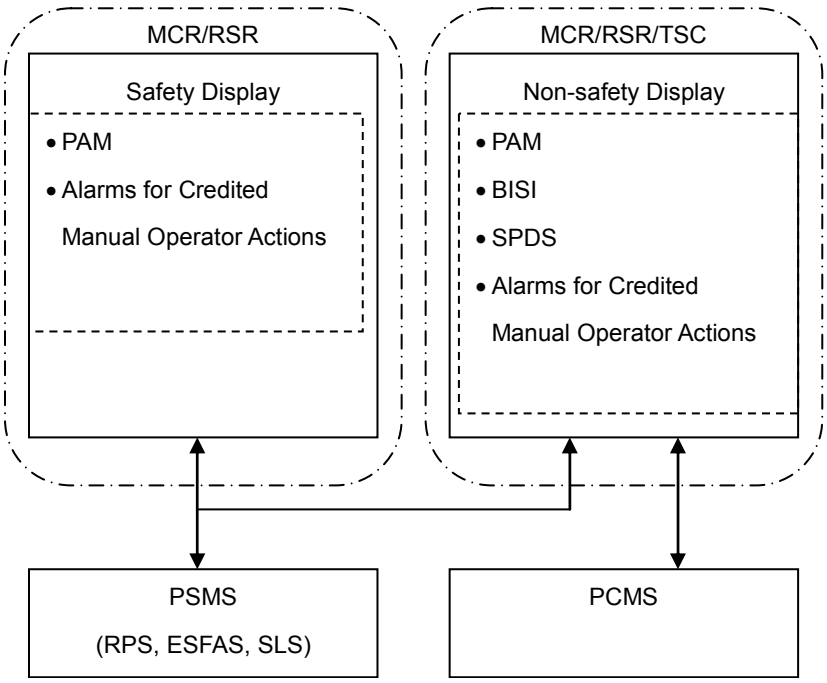
Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. PAM variables as identified in Table 2.5.4-1, BISI, SPDS information, and plant alarms for credited manual operator actions as identified in Table 2.5.4-3, for information systems important to safety, are provided on safety and non-safety HSI equipment at the MCR, RSR, and TSC, as shown in Figure 2.5.4-1.	1. An inspection will be performed of the MCR, RSR, and TSC for retrievability of alarms and displays for information systems important to safety.	1. Displays for PAM variables identified in Table 2.5.4-1, BISI, SPDS, and plant alarms for credited manual operator actions as identified in Table 2.5.4-3, for information systems important to safety, can be retrieved on non-safety HSI equipment in the as-built MCR, RSR, and TSC, as shown in Figure 2.5.4-1. Displays for PAM variables as identified in Table 2.5.4-1 and alarms for credited manual actions as identified in Table 2.5.4-3, for information systems important to safety, can be retrieved on safety HSI equipment in the as-built MCR and RSR, as shown in Figure 2.5.4-1.
2. Deleted.	2. Deleted.	2. Deleted.
3. The field instrumentation for the PAM variables identified in Table 2.5.4-1 that is subjected to a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.	3.i Type tests or a combination of type tests and analyses using the design environmental conditions, or under the conditions which bound the design environmental conditions, will be performed on the field instrumentation for the PAM variables identified in Table 2.5.4-1 that is subjected to a harsh environment.	3.i A report exists and concludes that the field instrumentation for the PAM variables identified in Table 2.5.4-1 that is subjected to a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.
	3.ii Inspection will be performed of the as-built field instrumentation for the PAM variables identified in Table 2.5.4-1 that is subjected to a harsh environment, and the associated wiring, cables, and terminations located in a harsh environment.	3.ii The as-built field instrumentation and the associated wiring, cables, and terminations for the PAM variables identified in Table 2.5.4-1 that are subjected to a harsh environment are bounded by type tests or a combination of type tests and analyses.

Table 2.5.4-2 Information Systems Important to Safety Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
4. Deleted.	4. Deleted.	4. Deleted.

Table 2.5.4-3 Alarms for Credited Manual Operator Actions

Control Rod Insertion Limit Alarm
~~High Source Range Neutron Flux Alarm~~Reactor Makeup Water Flow Rate Deviation Alarm
Boric Acid Flow Rate Deviation Alarm
High Primary Makeup Water Flow Rate Alarm
High Pressurizer Water Level Alarm
Main Steam Line Radiation (N-16) Alarm
Low Pressurizer Water Level against Program Water Level Alarm
Containment High Range Area Radiation Alarm
Low Volume Control Tank Water Level Alarm



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

Figure 2.5.4-1 Configuration of the PSMS and PCMS for Information Systems Important to Safety

2.5.5 Control Systems Not Required for Safety

2.5.5.1 Design Description

The non-safety PCMS provides for automatic and manual control of non safety-related plant components, and monitoring of non safety-related plant instrumentation. The operational VDUs which are part of the PCMS, provide monitoring and control for safety-related plant components and instrumentation, including monitoring and control for the credited manual operator actions. The PCMS regulates conditions in the plant automatically in response to changing plant processes and load demand to establish and maintain plant operating conditions within prescribed limits. The PCMS controls and monitors neutron flux, temperature, pressure, liquid level, flow and other process parameters throughout the plant.

The PCMS is fully redundant to ensure single malfunctions do not result in loss of any control, monitoring or alarm functions. The PCMS is powered from two nonsafety-related UPSs to ensure reliability.

1. The functional arrangement of the PCMS is as described in the Design Description of Subsection 2.5.5.1 and in Table 2.5.5-2.

2. Deleted.

3. Deleted.

4. For a control command to be generated from the PCMS Operational VDUs for safety related components, two distinct operator actions, at a minimum, are required.

2.5.5.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.5-1 describes the ITAAC for the control systems not required for safety.

Table 2.5.5-1 Control Systems Not Required for Safety Inspections, Tests, Analyses, and Acceptance Criteria

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The functional arrangement of the PCMS is as described in the Design Description of Subsection 2.5.5.1 and in Table 2.5.5-2.	1. Inspection of the as-built PCMS will be performed.	1. The as-built PCMS conforms to the functional arrangement as described in the Design Description of Subsection 2.5.5.1 and in Table 2.5.5-2.
2. Deleted.	2. Deleted.	2. Deleted.
3. Deleted.	3. Deleted.	3. Deleted.
4. For a control command to be generated from the PCMS Operational VDUs for safety-related components, two distinct operator actions, at a minimum, are required.	4. Type test of the PCMS will be performed for each type of soft control command.	4. A minimum of two distinct operator actions are required to generate safety-related component control commands from a PCMS Operational VDU.

Table 2.5.5-2 Arrangement of Control Systems Not Required for Safety

PCMS (CONTROL) FUNCTION GROUP	DESCRIPTION
REACTOR CONTROL SYSTEM GROUP 1	A-SG FEEDWATER CONTROL
	A-MAIN STEAM RELIEF VALVE CONTROL
REACTOR CONTROL SYSTEM GROUP 2	B-SG FEEDWATER CONTROL
	B-MAIN STEAM RELIEF VALVE CONTROL
	PRESSURIZER PRESSURE CONTROL
REACTOR CONTROL SYSTEM GROUP 3	C-SG FEEDWATER CONTROL
	C-MAIN STEAM RELIEF VALVE CONTROL
	PRESSURIZER WATER LEVEL CONTROL
	CONTROL ROD INSERTION MONITORING
REACTOR CONTROL SYSTEM GROUP 4	D-SG FEEDWATER CONTROL
	D-MAIN STEAM RELIEF VALVE CONTROL
REACTOR CONTROL SYSTEM GROUP 5	TURBINE BYPASS CONTROL
	REACTOR MAKEUP CONTROL
REACTOR CONTROL SYSTEM GROUP 6	CONTROL ROD CONTROL
TURBINE PROTECTION SYSTEM	TURBINE PROTECTION CONTROL
BOP CONTROL SYSTEM	BALANCE OF PLANT CONTROL
	AUXILIARY EQUIPMENT CONTROL
TURBINE EHG CONTROL SYSTEM	TURBINE ELECTRICAL-HYDRAULIC GOVERNOR CONTROL
ELECTRICAL CONTROL SYSTEM	ELECTRICAL SYSTEM CONTROL

2.5.6 Data Communication Systems

2.5.6.1 Design Description

The data communication systems (DCS) consist of:

- Plant-wide unit bus
- Safety bus (for each PSMS division)
- Data links for point-to-point communication
- Input/Output (I/O) bus
- Maintenance network for each PSMS division and the PCMS

The DCS is a distributed and highly interconnected system, which has communication independence to prevent electrical and communication processing faults in one safety division (or the non-safety PCMS) from adversely affecting the performance of safety functions in other divisions. Qualified fiber-optic isolators are used to prevent electrical faults from transferring between divisions, and between safety and non-safety systems. Communication faults are prevented through data integrity verification.

A non-redundant non-safety multi-drop maintenance network is provided separately within each PSMS division and within the PCMS. The maintenance network is used to transmit signals between the engineering tools and the PSMS or PCMS system management module of each controller.

1. The functional arrangement of the DCS is as described in the Design Description of Subsection 2.5.6.1 and as shown in Figure 2.5.6-1.

2. The DCS provides throughput to meet the response time requirements for all safety functions under the full range of applicable conditions enumerated in the design basis. On-line diagnostics do not interrupt plant control.

3. The DCS provides external networks with a communications link via the unit management computer (UMC) which is connected to the unit bus. The UMC provides a firewalled interface, which allows only outbound communication from the unit bus to external networks. There are no other connections from external sources to the DCS.

4. The safety-related portions of the DCS are located in a facility area that provides protection from natural phenomena hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding.

5. The PSMS application setpoints, constants and application software are changeable only by removing the CPU module that contains the memory devices from the controller and placing it in a dedicated re-programming chassis.

6. Digital communication independence is achieved by communication processors that are independent of RT and ESF actuation processing functions of the redundant divisions of the PSMS, and also between non-safety systems and the PSMS.

2.5.6.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.6-1 describes the ITAAC for the DCS.

Table 2.5.6-1 Data Communication Systems Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1. The functional arrangement of the DCS is as described in the Design Description of Subsection 2.5.6.1 and as shown in Figure 2.5.6-1.	1. Inspection of the as-built DCS will be performed.	1. The as-built DCS conforms to the functional arrangement as described in the Design Description of Subsection 2.5.6.1 and as shown in Figure 2.5.6-1.
2. The DCS provides throughput to meet the response time requirements for all safety functions under the full range of applicable conditions enumerated in the design basis. On-line diagnostics do not interrupt plant control.	2. Type tests, analyses or a combination of type tests and analyses of the DCS will be performed.	2. A report exists and concludes that the DCS provides throughput to meet the response time requirements for all safety functions under the full range of applicable conditions enumerated in the design basis, and that on-line diagnostics do not interrupt plant control.
3. The DCS provides external networks with a communications link via the unit management computer (UMC) which is connected to the unit bus. The UMC provides a firewalled interface, which allows only outbound communication from the unit bus to external networks. There are no other connections from external sources to the DCS.	3. Inspection and analyses of the as-built DCS will be performed.	3 A report exists and concludes that: (1) the as-built DCS provides external networks with a communications link via the as-built unit management computer (UMC), which is connected to the as-built unit bus; (2) the as-built UMC provides a firewalled interface, which allows only outbound communication from the as-built unit bus to external networks; and (3) there are no other connections from external sources to the as-built DCS.
4. The safety-related portions of the DCS are located in a facility area that provides protection from natural phenomena hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding.	4. An inspection of the as-built equipment location will be performed.	4. The safety- related portions of the as-built DCS are located in an as-built facility area that provides protection from natural phenomena hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding.

Table 2.5.6-1 Data Communication Systems Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 2)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
5. The PSMS application setpoints, constants and application software are changeable only by removing the CPU module that contains the memory devices from the controller and placing it in a dedicated re-programming chassis.	5. Type tests of the PSMS changeability will be performed.	5. The PSMS application setpoints, constants and application software are changeable only by removing the CPU module that contains the memory devices from the controller and placing it in a dedicated re-programming chassis.
6. Digital communication independence is achieved by communication processors that are independent of RT and ESF actuation processing functions of the redundant divisions of the PSMS, and also between non-safety systems and the PSMS.	6.i An inspection of the as-built PSMS will be performed to verify communication processors are installed.	6.i Communication processors exist in the as-built PSMS for digital communication between redundant divisions of the PSMS and between non-safety systems and the PSMS.
	6.ii Type tests or analyses, or a combination of type tests and analyses of the digital communication independence will be performed.	6.ii A report exists and concludes that digital communication independence is achieved by communication processors that are independent of trip and actuation processing functions.

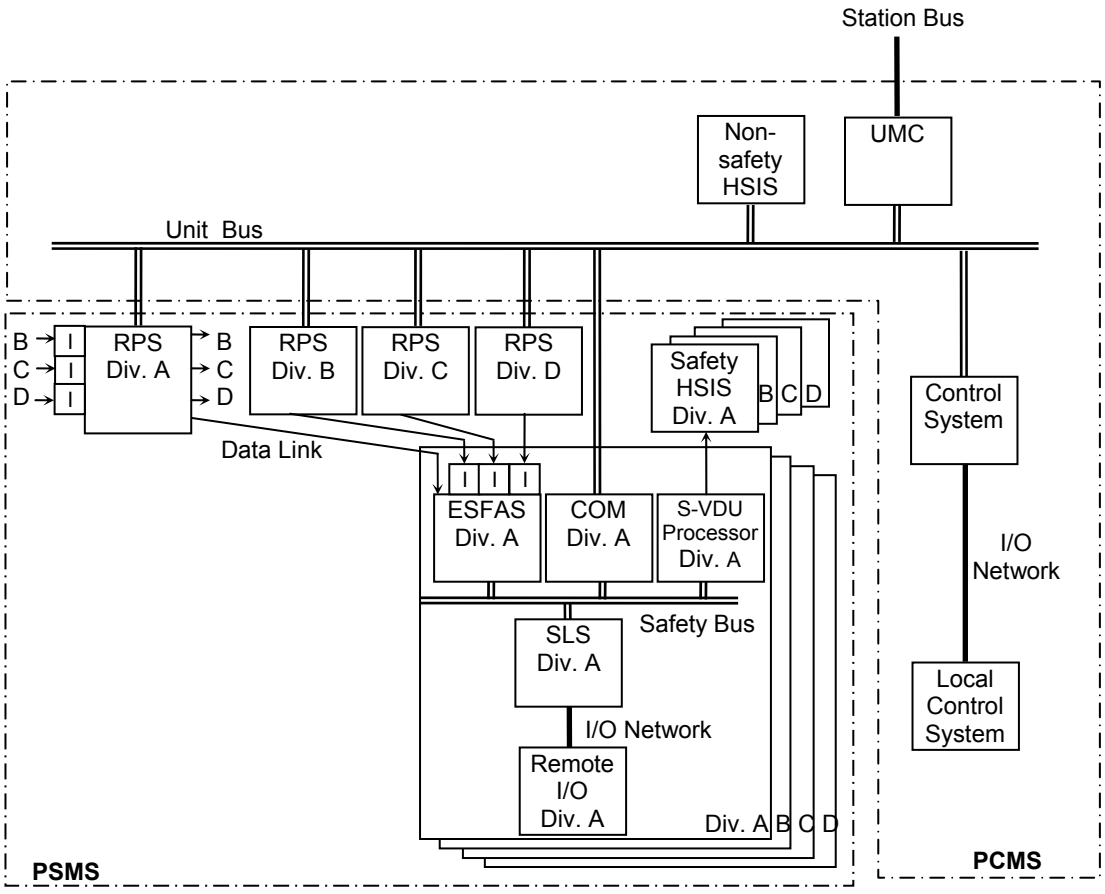


Figure 2.5.6-1 DCS Configuration