2.4 Instrumentation and Control Systems

2.4.1 Protection System

Design Description

1.0 System Description

The protection system (PS) is provided to sense conditions requiring protective action and automatically initiate the safety systems required to mitigate the event.

The PS provides the following safety-related functions:

- Performs automatic initiation of reactor trip (RT) functions.
- Performs automatic initiation of engineered safety feature (ESF) functions.
- Provides for initiation of RT manual functions.
- Provides for actuation of ESF manual functions.
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions.
- Generates permissive signals that maintain safety-related interlocks.

2.0 Arrangement

2.1 The location of the PS equipment is as listed in Table 2.4.1-1—Protection System Equipment.

2.2 Physical separation exists between the divisions of the PS as listed in Table 2.4.1-1.

2.3 Physical separation exists between Class 1E PS equipment and non-Class 1E equipment.

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without a loss of safety function(s).

4.0 I&C Design Features, Displays, and Controls

4.1 The PS generates automatic RT functions for the input variables listed in Table 2.4.1-2—Protection System Automatic Reactor Trip Functions and Input Variables.

4.2 The PS generates automatic ESF functions for the input variables listed in Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Functions and Input Variables when the trip limit is reached. The ESF functions remain following removal of the signal. The ESF functions are removed when the ESF functions are manually reset. Deliberate manual action is required to return the safety systems to normal.

4.3 The permissives listed in Table 2.4.1-5—Protection System Permissives and Operating Bypasses provide operating bypass capability for the corresponding PS functions.

4.4 Communications independence is provided between the PS divisions.

4.5 The PS is capable of performing its safety function when PS equipment is in maintenance bypass. Bypassed PS equipment is indicated on the PICS operator workstations in the MCR.

4.6 PS setpoints associated with the automatic RT functions listed in Table 2.4.1-2 and the automatic ESF functions listed in Table 2.4.1-3 are determined using a methodology that addresses:

- The determination of applicable contributors to instrumentation loop errors.
- The method in which the errors are combined.
- How the errors are applied to the design analytical limits.

4.7 Deleted.

4.8 Electrical isolation is provided on connections between Class 1E PS equipment and non-Class 1E equipment to prevent the propagation of credible electrical faults.

4.9 The PS uses TXS system communication messages that are sent with a specific protocol.

4.10 Class 1E PS equipment listed in Table 2.4.1-1 can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.11 Controls on the PICS operator workstations in the MCR perform the manual system actuation functions listed in Table 2.4.1-4—Protection System Manually Actuated Functions.

4.12 Controls on the PICS operator workstations in the MCR and RSS perform validation or inhibition of manual permissives listed in Table 2.4.1-5.

4.13 The PS performs interlock functions listed in Table 2.4.1-6—Protection System Interlocks.

4.14 The PS design and application software are developed using a process composed of six lifecycle phases with each phase having outputs which must conform to the requirements of that phase. The six lifecycle phases are the following:

1. Basic Design Phase.
2. Detailed Design Phase.
3. Manufacturing Phase.

4. System Integration and Testing Phase.

5. Installation and Commissioning Phase.

6. Final Documentation Phase.

4.15 Deleted.

4.16 Electrical isolation is provided on connections between the PS divisions to prevent the propagation of credible electrical faults.

4.17 Communications independence is provided between PS equipment and non-Class 1E equipment.

4.18 The PS is designed so that safety-related functions required for an anticipated operational occurrence (AOO) or postulated accident (PA) are performed in the presence of the following:

- Single detectable failures within the PS.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

4.19 Equipment markings for each PS division are distinctly identified and distinguishable from other identifying markings placed on the equipment.

4.20 Locking mechanisms are provided on the PS cabinet doors. PS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.

4.21 CPU state switches are provided at the PS cabinets to restrict modifications to the PS software.

4.22 The operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods:

- By perturbing the monitored variable.
- By introducing and varying, a substitute input of the same nature as the measured variable.
- By cross-checking between channels that bear a known relationship to each other.
- By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.

4.23 Deleted.

4.24 The PS response time from sensor output through equipment actuation for the RT functions listed in Table 2.4.1-2 and ESF functions listed in Table 2.4.1-3 is less than the value required to satisfy the design basis safety analysis response time assumptions.

4.25 Hardwired disconnects exist between the service unit (SU) and each divisional monitoring and service interface (MSI) of the PS. The hardwired disconnects prevent the connection of the SU to more than a single division of the PS.

4.26 PS self-test features are capable of detecting and responding to faults consistent with the design requirements of PS.

4.27 During data communication, the PS function processors receive all messages, but only the pre-defined messages for that specific PS function processor are considered valid and used. Other messages are ignored.

4.28 For each AOO or PA, a primary and secondary RT function using different sensors as input are identified and assigned to different PS subsystems.

5.0 Electrical Power Design Features

5.1 Equipment designated as Class 1E in Table 2.4.1-1 are powered from the Class 1E division as listed in Table 2.4.1-1 in a normal or alternate feed condition.

6.0 Environmental Qualifications

6.1 Equipment designated as mild environment in Table 2.4.1-1 can perform their function under normal environmental conditions, anticipated operational occurrences, and accident and post-accident environmental conditions.

Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.1-7 lists the PS ITAAC.

Table 2.4.1-1—Protection System Equipment

Description	Tag Number(1)	Location	Seismic Category	IEEE Class 1E(2)	Environment
PS Cabinets, Division 1	30CLE	Safeguard Building 1	I	1^{N} 2^{A}	Mild
PS Cabinets, Division 2	30CLF	Safeguard Building 2	I	2^{N} 1^{A}	Mild
PS Cabinets, Division 3	30CLG	Safeguard Building 3	I	3^{N} 4^{A}	Mild
PS Cabinets, Division 4	30CLH	Safeguard Building 4	I	4^{N} 3^{A}	Mild

1. Equipment Tag numbers are provided for information and are not part of the design certification.

2. ^{N} denotes the division the equipment is normally powered from. ^{A} denotes the division the equipment is powered from when alternate feed is implemented.

Table 2.4.1-2—Protection System Automatic Reactor Trip Functions and Input Variables
Sheet 1 of 2

Reactor Trip Function	Input Variable
High Linear Power Density (HLPD)	Neutron Flux - Self Powered Neutron Detectors
Low Departure from Nucleate Boiling Ratio (DNBR)	Neutron Flux - Self Powered Neutron Detectors
	Cold Leg Temperature (NR)
	Reactor Coolant Pump (RCP) Speed
	RCS Loop Flow
	Temperature Compensated Rod Cluster Control Assembly Analog Position
	Pressurizer Pressure (NR)
High Neutron Flux Rate of Change	Neutron Flux - Power Range Detectors
High Core Power Level	Cold Leg Temperature (WR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (NR)
	RCS Loop Flow
Low RCP Speed	RCP Speed
Low RCS Flow Rate in Two Loops	RCS Loop Flow
Low–Low RCS Flow Rate in One Loop	RCS Loop Flow
Low Doubling Time	Neutron Flux - Intermediate Range Detectors
High Neutron Flux	Neutron Flux - Intermediate Range Detectors
Low Pressurizer Pressure	Pressurizer Pressure (NR)
High Pressurizer Pressure	Pressurizer Pressure (NR)
High Pressurizer Level	Pressurizer Level (NR)
Low Hot Leg Pressure	Hot Leg Pressure (WR)
Steam Generator (SG) Pressure Drop	SG Pressure
Low Steam Generator Pressure	SG Pressure
High Steam Generator Pressure	SG Pressure
Low Steam Generator Level	SG Level (NR)
High Steam Generator Level	SG Level (NR)
High Containment Pressure	Containment Equipment Compartment Pressure
	Containment Service Compartment Pressure (NR)

Table 2.4.1-2—Protection System Automatic Reactor Trip Functions and Input Variables
Sheet 2 of 2

Reactor Trip Function	Input Variable
Low Saturation Margin	Cold Leg Temperature (WR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (NR)
	RCS Loop Flow
On Automatic Safety Injection System (SIS) Actuation	SIS Actuation Signal
On Emergency Feedwater System (EFWS) Actuation on Low Steam Generator Level	EFWS Actuation Signal

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Functions and Input Variables
Sheet 1 of 2

Engineered Safety Feature Function	Input Variable
Safety Injection System Actuation	Pressurizer Pressure (NR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (WR)
	Hot Leg Loop Level
Emergency Feedwater System Actuation	SG Level (WR)
	SG Pressure
	LOOP Signal
	SIS Actuation Signal
Emergency Feedwater System Isolation	SG Level (WR)
	SG Pressure
	SG Isolation Signal
Partial Cooldown Actuation	SIS Actuation Signal
	Reactor Trip Initiated Signal
Main Steam Relief Isolation Valve (MSRIV) Opening	SG Pressure
	Hot Leg Pressure (WR)
	Hot Leg Temperature (WR)
Main Steam Relief Train (MSRT) Isolation	SG Pressure
Main Steam Isolation	SG Pressure
	SG Isolation Signal
	Containment Equipment Compartment Pressure
	Containment Service Compartment Pressure (NR)
Main Feedwater Isolation and Startup and Shutdown System (SSS) Isolation	SG Level (NR)
	SG Pressure
	Reactor Trip Initiated Signal
	SG Isolation Signal
	Containment Equipment Compartment Pressure
	Containment Service Compartment Pressure (NR)
Containment Isolation Stage 1	Containment Equipment Compartment Pressure
	Containment Service Compartment Pressure (NR)
	Containment Service Compartment Pressure (WR)
	Containment High Range Activity
	SIS Actuation Signal

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Functions and Input Variables
Sheet 2 of 2

Engineered Safety Feature Function	Input Variable
Containment Isolation Stage 2	Containment Service Compartment Pressure (WR)
CVCS Charging Isolation	Pressurizer Level (NR)
CVCS Isolation for Anti-Dilution	Boron Concentration
	Boron Temperature
	CVCS Charging Line Flow
	Cold Leg Temperature (WR)
Emergency Diesel Generator Actuation	6.9kV Bus Voltage
	SIS Actuation Signal
PSRV Opening	Hot Leg Pressure (NR)
SG Isolation	Main Steam Line Activity
	SG Level (NR)
	Partial Cooldown Actuated Signal
Reactor Coolant Pump Trip	RCP Differential Pressure
	SIS Actuation Signal
	Containment Isolation Stage 2 Signal
Main Control Room Air Conditioning System (CRACS) Isolation and Filtering	MCR Air Intake Duct Activity
	Containment Isolation Stage 1 Signal
Turbine Trip	Reactor Trip Initiated Signal
Loss of Offsite Power (LOOP)	6.9kV Bus Voltage
	SIS Actuation Signal
Hydrogen Mixing Dampers Opening	Containment Service Compartment Pressure (NR)
	Containment Equipment Compartment/ Containment Service Compartment Differential Pressure

Table 2.4.1-4—Protection System Manually Actuated Functions

Reactor Trip
Containment Isolation (Stage 1)
Containment Isolation (Stage 2)
CVCS Charging Isolation
CVCS Isolation on Anti-Dilution Mitigation
EDG Actuation
EFWS Actuation
EFWS Isolation
Extra Borating System Isolation
Hydrogen Mixing Dampers Opening
CRACS Isolation and Filtering
Main Feedwater (MFW) Full Load Isolation
Main Steam Isolation
MSRIV Opening
MSRT Isolation
Partial Cooldown Actuation
PSRV Opening
RCP Trip
SG Isolation
SIS Actuation
Turbine Trip

Table 2.4.1-5—Protection System Permissives and Operating Bypasses
Sheet 1 of 3

Permissive	Inhibit	Validate	MCR Control	RSS Control	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P2	Automatic	Automatic			Low DNBR RT	
					HLPD RT	
					Low RCS Flow Rate RT	
					Low RCP Speed RT	
					Low Pressurizer Pressure RT	
P3	Automatic	Automatic			Low-Low RCS Flow Rate RT	
P5	Automatic	Automatic			High Core Power Level RT	
					Low Saturation Margin RT	
P6	Automatic	Manual	X	X		High Neutron Flux RT
						Low Doubling Time RT
P7	Automatic	Automatic			CVCS Isolation on ADM at Standard Shutdown Conditions	CVCS Isolation on ADM at Shutdown Conditions
					CVCS Isolation on ADM at Standard Shutdown Conditions with Manual Calculation	
P8	Automatic	Automatic			CVCS Isolation on ADM at Power	CVCS Isolation on ADM at Standard Shutdown Conditions
						CVCS Isolation on ADM at Standard Shutdown Conditions with Manual Calculation

Table 2.4.1-5—Protection System Permissives and Operating Bypasses
Sheet 2 of 3

Permissive	Inhibit	Validate	MCR Control	RSS Control	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P12	Automatic	Manual	X	X		High Pressurizer Level RT
						Low Hot Leg Pressure RT
						Low SG Pressure RT
						MSRT Isolation (manual)
						MSRT Isolation (low SG pressure)
						Main Steam Isolation (low SG pressure)
						Startup and Shutdown System (SSS) Isolation (low SG pressure)
						SIS Actuation (low pressurizer pressure)
						SIS Actuation (low delta P_{sat})
P13	Automatic	Manual	X	X		Low SG Level RT
						High SG Level RT
						EFWS Actuation (low SG level)
						EFWS Actuation (SIS + LOOP)
						EFWS Actuation (manual)
						EFWS Isolation (manual)
						MFW Full Load Isolation (high SG level)
						SSS Isolation (high SG level for period of time)
						SG Isolation

Table 2.4.1-5—Protection System Permissives and Operating Bypasses
Sheet 3 of 3

Permissive	Inhibit	Validate	MCR Control	RSS Control	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P14	Manual	Manual	X	X		Partial Cooldown Actuation
P15	Automatic	Manual	X	X		SIS Actuation (low delta Psat)
						SIS Actuation (low RCS loop level)
P16	Manual	Manual	X	X		Align SIS from cold leg injection to hot leg injection
P17	Automatic	Manual	X	X	PSRV Opening (high Hot Leg pressure)	CVCS Charging Isolation (high Pressurizer level)
P18	Automatic	Automatic				Repositioning of the SG transfer valves

Table 2.4.1-6—Protection System Interlocks

RHR Suction Valves Interlock
MHSI Large Miniflow Line Valves Interlock
Safety Injection Accumulator Valves Interlock
SG Transfer Valves Interlock

Table 2.4.1-7—Protection System ITAAC
Sheet 1 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the PS equipment is as listed in Table 2.4.1-1.	An inspection of the location of the as-built PS equipment will be performed.	The PS equipment listed in Table 2.4.1-1 is located as listed in Table 2.4.1-1.
2.2	Physical separation exists between the divisions of the PS as listed in Table 2.4.1-1.	An inspection will be performed to verify that the as-built divisions of the PS are located in separate Safeguard Buildings.	The divisions of the PS are located in separate Safeguard Buildings as listed in Table 2.4.1-1.
2.3	Physical separation exists between Class 1E PS equipment and non-Class 1E equipment.	a. An analysis will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve physical separation between as-built Class 1E PS equipment and as-built non-Class 1E equipment.	a. A report defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve physical separation between Class 1E PS equipment and non-Class 1E equipment.
		b. An inspection will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between as-built Class 1E PS equipment and as-built non-Class 1E equipment.	b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E PS equipment and non-Class 1E equipment.

Table 2.4.1-7—Protection System ITAAC
Sheet 2 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
3.1	Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without a loss of safety function(s).	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the equipment identified as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Test/analysis reports conclude that the equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without a loss of safety function(s).
		b. An inspection will be performed of the as-built equipment identified as Seismic Category I in Table 2.4.1-1 to verify that the equipment, including anchorage, are installed in a condition bounded by the tested or analyzed condition.	b. Inspection reports conclude that the equipment identified as Seismic Category I in Table 2.4.1-1, including anchorage, are installed in a condition bounded by the tested or analyzed condition.
4.1	The PS generates automatic RT functions for the input variables listed in Table 2.4.1-2.	a. A test will be performed on the PS using test input signals to verify that an RT signal is generated for the input variables listed in Table 2.4.1-2 when a test input signal reaches the trip limit.	a. The PS generates an RT signal after the test input signal reaches the trip limit for the input variables listed in Table 2.4.1-2.
		b. A test will be performed to verify that the RT breakers open when a trip limit in the PS is reached.	b. The RT breakers open after the PS reaches the trip limit for one RT function.

Table 2.4.1-7—Protection System ITAAC
Sheet 3 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.2	The PS generates automatic ESF functions for the input variables listed in Table 2.4.1-3 when the trip limit is reached. The ESF functions remain following removal of the signal. The ESF functions are removed when the ESF functions are manually reset. Deliberate manual action is required to return the safety systems to normal.	A test will be performed on the PS to verify that automatic ESF functions are generated for the input variables listed in Table 2.4.1-3 when the trip limit is reached.	The PS generates an ESF function when the trip limit is reached for the input variables listed in Table 2.4.1-3. The ESF functions remain following removal of the signal. The ESF functions are removed when the ESF functions are manually reset. Deliberate manual action is required to return the safety systems to normal.
4.3	The permissives listed in Table 2.4.1-5 provide operating bypass capability for the corresponding PS functions.	a. A test will be performed using test input signals for each function listed as being bypassed by an inhibited permissive in Table 2.4.1-5 to verify that each function is bypassed when test input signals representing the corresponding inhibited permissive signal are present.	a. The functions listed as being bypassed by inhibited permissives in Table 2.4.1-5 are bypassed when test input signals representing the corresponding inhibited permissive are present.
		b. A test will be performed using test input signals for each function listed as being bypassed by a validated permissive in Table 2.4.1-5 to verify that each function is bypassed when test input signals representing the corresponding validated permissive signal are present.	b. The functions listed as being bypassed by validated permissives in Table 2.4.1-5 are bypassed when test input signals representing the corresponding validated permissive are present.

Table 2.4.1-7—Protection System ITAAC
Sheet 4 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.4	Communications independence is provided between the PS divisions.	Tests using test input signals, analyses, or a combination of tests using test input signals and analyses will be performed to verify that communications independence is provided between the PS divisions.	Communications independence between the PS divisions is provided by: • The PS function processors do not interface directly with a network. Separate PS communication modules interface directly with the network. • Separate send and receive data channels are used in both the communications module and the PS function processor. • The PS function processors operate in a strictly cyclic manner. • The PS function processors operate asynchronously from the PS communications module.
4.5	The PS is capable of performing its safety function when PS equipment is in maintenance bypass. Bypassed PS equipment is indicated on the PICS operator workstations in the MCR.	a. A test of the PS will be performed to verify the maintenance bypass functionality. b. A test will be performed to verify bypassed PS equipment is indicated on the PICS operator workstations in the MCR.	a. The PS can perform its safety functions when PS equipment is in maintenance bypass. b. Bypassed PS equipment is indicated on the PICS operator workstations in the MCR.

Table 2.4.1-7—Protection System ITAAC
Sheet 5 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.6	PS setpoints associated with the automatic RT functions listed in Table 2.4.1-2 and the automatic ESF functions listed in Table 2.4.1-3 are determined using a methodology that addresses: ● The determination of applicable contributors to instrumentation loop errors. ● The method in which the errors are combined. ● How the errors are applied to the design analytical limits.	An analysis will be performed to verify that PS setpoints are determined using a documented methodology that addresses: ● The determination of applicable contributors to instrumentation loop errors. ● The method in which the errors are combined. ● How the errors are applied to the design analytical limits.	A report concludes that the PS setpoints associated with the automatic RT functions listed in Table 2.4.1-2 and the automatic ESF functions listed in Table 2.4.1-3 are determined using a documented methodology: ● For the determination of applicable contributors to instrument loop error. ● For combining instrument loop errors. ● For how the errors are applied to the design analytical limits.
4.7	Deleted.	Deleted.	Deleted.
4.8	Electrical isolation is provided on connections between Class 1E PS equipment and non-Class 1E equipment to prevent the propagation of credible electrical faults.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between Class 1E PS equipment and non-Class 1E equipment. b. An inspection will be performed on connections between as-built Class 1E PS equipment and non-Class 1E equipment.	a. A report concludes that the Class 1E isolation devices used between Class 1E PS equipment and non-Class 1E equipment prevent the propagation of credible electrical faults. b. Class 1E electrical isolation devices exist on connections between Class 1E PS equipment and non-Class 1E equipment.

Table 2.4.1-7—Protection System ITAAC
Sheet 6 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	The PS uses TXS system communication messages that are sent with a specific protocol.	A test will be performed on PS equipment to verify that PS communication messages are sent with a specific protocol.	The TXS system communication messages use a specific protocol structure and message error determination. Messages are validated by the following series of checks: ● Message header check contains the following: – Protocol version – Sender ID – Receiver ID – Message ID – Message type – Message length ● Message age is monitored. ● Message cyclic redundancy check is performed so that if one of the checks fails, the affected data are marked with an error status.
4.10	Class 1E PS equipment listed in Table 2.4.1-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Type tests or type tests and analyses will be performed to demonstrate that the Class 1E PS equipment listed in Table 2.4.1-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Equipment identified as Class 1E in Table 2.4.1-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.
4.11	Controls on the PICS operator workstations in the MCR perform the manual system actuation functions listed in Table 2.4.1-4.	Tests will be performed using controls on the PICS operator workstations in the MCR.	Controls on the PICS operator workstations in the MCR perform the manual system actuation functions listed in Table 2.4.1-4.

Table 2.4.1-7—Protection System ITAAC
Sheet 7 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.12	Controls on the PICS operator workstations in the MCR and RSS perform validation or inhibition of the manual permissives listed in Table 2.4.1-5.	a. Tests will be performed to verify the functionality of the manual permissive controls on the PICS operator workstations in the MCR.	a. For the manual permissives listed in Table 2.4.1-5, the permissive status is present in the PS actuation logic units (ALU) after the corresponding controls on the PICS operator workstations in the MCR are manually actuated.
		b. Tests will be performed to verify the functionality of the manual permissive controls on the PICS operator workstations in the RSS.	b. For the manual permissives listed in Table 2.4.1-5, the permissive status is present in the PS actuation logic units (ALU) after the corresponding controls on the PICS operator workstations in the RSS are manually actuated.
4.13	The PS performs interlock functions listed in Table 2.4.1-6.	Tests will be performed on the PS using test input signals to verify operation of the interlocks.	The interlocks listed in Table 2.4.1-6 respond as specified when activated by a test input signal.

Table 2.4.1-7—Protection System ITAAC
Sheet 8 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.14	The PS design and application software are developed using a process composed of six lifecycle phases, with each phase having outputs which must conform to the requirements of that phase. The six lifecycle phases are the following: 1. Basic Design Phase. 2. Detailed Design Phase. 3. Manufacturing Phase. 4. System Integration and Testing Phase. 5. Installation and Commissioning Phase. 6. Final Documentation Phase.	a. Analyses will be performed to verify that the outputs for the PS Basic Design Phase conform to the requirements of that phase.	a. A report concludes that the outputs conform to requirements of the Basic Design Phase of the PS.
		b. Analyses will be performed to verify that the outputs for the PS Detailed Design Phase conform to the requirements of that phase.	b. A report concludes that the outputs conform to requirements of the Detailed Design Phase of the PS.
		c. Analyses will be performed to verify that the outputs for the PS Manufacturing Phase conform to the requirements of that phase.	c. A report concludes that the outputs conform to the requirements of the Manufacturing Phase of the PS.
		d. Analyses will be performed to verify that the outputs for the PS System Integration and Testing Phase conform to the requirements of that phase.	d. A report concludes that the outputs conform to the requirements of the System Integration and Testing Phase of the PS.
		e. Analyses will be performed to verify that the outputs for the PS Installation and Commissioning Phase conform to the requirements of that phase.	e. A report concludes that the outputs conform to the requirements of the Installation and Commissioning Phase of the PS.
		f. Analyses will be performed to verify that the outputs for the PS Final Documentation Phase conform to the requirements of that phase.	f. A report concludes that the outputs conform to the requirements of the Final Documentation Phase of the PS.

Table 2.4.1-7—Protection System ITAAC
Sheet 9 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.15	Deleted.	Deleted.	Deleted.
4.16	Electrical isolation is provided on connections between the PS divisions to prevent the propagation of credible electrical faults.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices on connections between the PS divisions. b. An inspection will be performed on connections between as-built PS divisions.	a. A report concludes that the Class 1E isolation devices used between PS divisions prevent the propagation of credible electrical faults. b. Class 1E electrical isolation devices exist on connections between PS divisions.
4.17	Communications independence is provided between PS equipment and non-Class 1E equipment.	Tests, analyses, or a combination of tests and analyses will be performed on the PS equipment to verify that communications independence is provided between PS equipment and non-Class 1E equipment.	Communications independence is provided between PS equipment and non-Class 1E equipment by: ● Data communications between PS function processors and non-Class 1E equipment are through a Monitoring and Service Interface (MSI). ● The MSI does not interface directly with a network. Separate communication modules interface directly with the network. ● Separate send and receive data channels are used in both the communications module and the MSI. ● The MSI operates in a strictly cyclic manner. ● The MSI operates asynchronously from the communications module. ● The PS uses a Class 1E hardware device to send unidirectional signals to non-safety-related I&C systems.

Table 2.4.1-7—Protection System ITAAC
Sheet 10 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.18	The PS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following: ● Single detectable failures within the PS. ● Failures caused by the single failure. ● Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.	A failure modes and effects analysis will be performed on the PS at the level of replaceable modules and components.	A report concludes that the PS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following: ● Single detectable failures within the PS. ● Failures caused by the single failure. ● Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.
4.19	Equipment markings for each PS division are distinctly identified and distinguishable from other identifying markings placed on the equipment.	An inspection will be performed on the as-built PS equipment to verify that the equipment markings for each PS division are distinctly identified and distinguishable from other markings placed on the equipment.	Equipment markings for each PS division are distinctly identified and distinguishable from other identifying markings placed on the equipment.
4.20	Locking mechanisms are provided on the PS cabinet doors. PS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.	a. A test will be performed to verify that the locking mechanisms on the PS cabinet doors operate properly. b. A test will be performed to verify that PS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.	a. The locking mechanisms on the PS cabinet doors operate properly. b. PS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.

Table 2.4.1-7—Protection System ITAAC
Sheet 11 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.21	CPU state switches are provided at the PS cabinets to restrict modifications to the PS software.	a. An inspection will be performed to verify the existence of CPU state switches at the as-built PS cabinets that restrict modifications to the PS software. b. Tests will be performed to verify that the CPU state switches restrict modifications to the PS software.	a. CPU state switches are provided at the PS cabinets. b. CPU state switches at the PS cabinets restrict modifications to the PS software.
4.22	The operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods: ● By perturbing the monitored variable. ● By introducing and varying, a substitute input of the same nature as the measured variable. ● By cross-checking between channels that bear a known relationship to each other. ● By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.	An analysis will be performed to demonstrate that the operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods: ● By perturbing the monitored variable. ● By introducing and varying, a substitute input of the same nature as the measured variable. ● By cross-checking between channels that bear a known relationship to each other. ● By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.	A report concludes that the operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods: ● By perturbing the monitored variable. ● By introducing and varying, a substitute input of the same nature as the measured variable. ● By cross-checking between channels that bear a known relationship to each other. ● By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.
4.23	Deleted.	Deleted.	Deleted.

Table 2.4.1-7—Protection System ITAAC
Sheet 12 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.24	The PS response time from sensor output through equipment actuation for the RT functions listed in Table 2.4.1-2 and ESF functions listed in Table 2.4.1-3 is less than the value required to satisfy the design basis safety analysis response time assumptions.	Tests will be performed to verify PS response times are less than the value required to satisfy the design basis safety analysis response time assumptions.	A report concludes that PS response times are less than the value required to support the safety analysis response time assumptions for the RT functions listed in Table 2.4.1-2 and ESF functions listed in Table 2.4.1-3.
4.25	Hardwired disconnects exist between the SU and each divisional MSI of the PS. The hardwired disconnects prevent the connection of the SU to more than a single division of the PS.	a. An inspection of the as-built hardwired disconnects between the SU and each divisional MSI of the PS will be performed. b. A test of the hardwired disconnects between the SU and each divisional MSI of the PS will be performed.	a. Hardwired disconnects exist between the SU and each divisional MSI of the PS. b. The hardwired disconnects prevent the connection of the SU to more than a single division of the PS.
4.26	PS self-test features are capable of detecting and responding to faults consistent with the design requirements of PS.	a. Type tests, analyses or a combination of type tests and analyses will be performed to demonstrate that faults requiring detection through self-test features are detected by the PS equipment. b. Type tests, analyses or a combination of type tests and analyses will be performed to demonstrate that upon detection of faults through self-test features, the PS equipment responds according to the type of fault.	a. A report concludes that the PS equipment is capable of detecting faults required to be detected by self-test features. b. A report concludes that upon detection of faults through self-test features, the PS equipment responds according to the type of fault.

Table 2.4.1-7—Protection System ITAAC
Sheet 13 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.27	During data communication, the PS function processors receive all messages, but only the pre-defined messages for that specific PS function processor are considered valid and used. Other messages are ignored.	a. An analysis will be performed to define the pre-defined messages for that specific PS function processor. b. A test will be performed to verify that the PS function processors receive all messages, but only the pre-defined messages for that specific function processor are considered valid and used. Other messages are ignored.	a. A report defines the pre-defined messages for that specific PS function processor. b. The PS function processors receive all messages, but only the pre-defined messages for that specific function processor are considered valid and used. Other messages are ignored.
4.28	For each AOO or PA, a primary and secondary RT function using different sensors as input are identified and assigned to different PS subsystems.	a. An analysis will be performed to identify the primary and secondary RT function for each AOO or PA. b. An inspection will be performed to verify that for each AOO or PA, the primary and secondary RT function using different sensors as input are assigned to different as-built PS subsystems.	a. A report identifies the primary and secondary RT function for each AOO or PA. b. For each AOO or PA, the primary and secondary RT function using different sensors as input are assigned to different PS subsystems.
5.1	Equipment designated as Class 1E in Table 2.4.1-1 are powered from the Class 1E division as listed in Table 2.4.1-1 in a normal or alternate feed condition.	a. Testing will be performed by providing a test input signal in each normally aligned division. b. Testing will be performed by providing a test input signal in each division with the alternate feed aligned to the divisional pair.	a. The test input signal provided in the normally aligned division is present at the respective Class 1E equipment identified in Table 2.4.1-1. b. The test input signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E equipment identified in Table 2.4.1-1.

Table 2.4.1-7—Protection System ITAAC
Sheet 14 of 14

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
6.1	Equipment designated as mild environment in Table 2.4.1-1 can perform their function under normal environmental conditions, anticipated operational occurrences, and accident and post-accident environmental conditions.	a. Type tests or type tests and analysis will be performed to demonstrate the ability of the equipment designated as mild environment in Table 2.4.1-1 to perform their function under normal environmental conditions, containment test conditions, anticipated operational occurrences, and accident and post-accident environmental conditions.	a. EQDPs conclude that the equipment designated as mild environment in Table 2.4.1-1 can perform their function under normal environmental conditions, containment test conditions, anticipated operational occurrences, and accident and post-accident environmental conditions, including the time required to perform the listed function.
		b. An inspection will be performed of the as-built equipment designated as mild environment in Table 2.4.1-1 to verify that the equipment, including the associated cables, wiring, and terminations located in a mild environment, are bounded by the type test or combination of type tests and analyses.	b. A report exists and concludes that the equipment designated as mild environment in Table 2.4.1-including the associated cables, wiring, and terminations located in a mild environment, are bounded by the type test or combination of type tests and analyses.

Next File