2.4 Instrumentation and Control Systems

2.4.1 Protection System

1.0 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 manual initiation of RT functions.
- Provides for manual actuation of ESF 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 PS equipment is located as listed in Table 2.4.1-1—Protection System Equipment.

2.2 Physical separation exists between the four divisions of the PS.

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 loss of safety function.

4.0 I&C Design Features, Displays and Controls

4.1 The PS generates automatic RT signals.

4.2 The PS generates automatic ESF signals.

4.3 The permissives provide operating bypass capability for the corresponding PS functions.

4.4 Communication independence is provided between the four PS divisions.

4.5 The PS is capable of performing its safety function when PS equipment is in maintenance bypass (inoperable). Bypassed PS equipment is indicated in the MCR.

4.6 Setpoints associated with the automatic RT signals and the automatic ESF signals are determined using a methodology that addresses the determination of applicable contributors to instrumentation loop errors, the method in which the errors are combined, and how the errors are applied to the design analytical limits.

4.7 Input variables provide the inputs for generating RT signals and ESF signals.

4.8 Electrical isolation is provided on connections between PS equipment and non-Class 1E equipment.

4.9 Deleted.

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

4.11 Controls exist in the MCR to allow manual actuation at the system level.

4.12 Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives.

4.13 The PS performs interlock functions..

4.14 The PS system 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 Controls exist in the RSS that allow manual actuation of RT.

4.16 Electrical isolation is provided on connections between the four PS divisions.

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 design basis events (DBE) are performed in the presence of the following:

- Single detectable failures within the PS concurrent with identifiable but non-detectable failures.

- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.

4.19 The equipment for each PS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.

4.20 Locking mechanisms are provided on the PS cabinet doors. Opened PS cabinet doors are indicated in the MCR.

4.21 Key lock switches are provided at the PS cabinets to restrict modifications to the PS software.

4.22 The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.

4.23 The PS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods.

4.24 The PS response time for RT and ESF signals is less than the value required to satisfy the design basis safety analysis response time assumptions.

5.0 Electrical Power Design Features

5.1 Class 1E PS components are powered from a Class 1E division in a normal or alternate feed condition.

6.0 System 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)
PS Cabinets, Division 1	30CLE	Safeguard Building 1	I	1^N 2^A
PS Cabinets, Division 2	30CLF	Safeguard Building 2	I	2^N 1^A
PS Cabinets, Division 3	30CLG	Safeguard Building 3	I	3^N 4^A
PS Cabinets, Division 4	30CLH	Safeguard Building 4	I	4^N 3^A

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

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

Table 2.4.1-2—Protection System Automatic Reactor Trip Signals and Input Variables (2 Sheets)

Reactor Trip Signal	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
	Rod Control Cluster Assembly Position
	Pressurizer Pressure
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 Loop Flow Rate (two loops)	RCS Loop Flow
Low–Low Loop Flow Rate (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 Service Compartment Pressure (NR)
	Containment Equipment Compartment Pressure
Low Saturation Margin	Cold Leg Temperature (WR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (NR)
	RCS Loop Flow
On Safety Injection System (SIS) Actuation	SIS Actuation Signal

Table 2.4.1-2—Protection System Automatic Reactor Trip Signals and Input Variables (2 Sheets)

Reactor Trip Signal	Input Variable
On Emergency Feedwater System (EFWS) Actuation	EFWS Actuation Signal

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Signals and Input Variables (2 Sheets)

Engineered Safety Feature Signal	Input Variable
Safety Injection System Actuation	Pressurizer Pressure (NR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (WR)
	RCS Loop Level
Emergency Feedwater System Actuation	SG Level (WR)
	LOOP Signal
	SIS Actuation signal
Emergency Feedwater System Isolation	SG Level (WR)
	SG Isolation Signal
Partial Cooldown Actuation	SIS Actuation signal
Main Steam Relief Train (MSRT) Opening	SG Pressure
MSRT Isolation	SG Pressure
Main Steam Isolation	SG Pressure
	SG Isolation Signal
Main Feedwater Isolation	SG Level (NR)
	SG Pressure
	RT Breaker Position
	SG Isolation Signal
Containment Isolation Stage 1	Containment Service Compartment Pressure (NR)
	Containment Service Compartment Pressure (WR)
	Containment Equipment Compartment Pressure
	Containment High Range Activity
	SIS Actuation Signal
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 Flow
	Cold Leg Temperature (WR)

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Signals and Input Variables (2 Sheets)

Engineered Safety Feature Signal	Input Variable
Emergency Diesel Generator Actuation	LOOP Signal
	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
	Containment Isolation Stage 2 Signal
Main Control Room Air Conditioning System (CRACS) Isolation and Filtering	MCR Air Intake Duct Activity
Turbine Trip	RT Breaker Position
Loss of Offsite Power (LOOP)	Bus loss of voltage
	Bus degraded voltage

Table 2.4.1-4—Protection System Manually Actuated Functions

Reactor Trip
SIS Actuation
Partial Cooldown Actuation
MSRT Actuation
MSRT Isolation
Main Steam Isolation
Main Feedwater (MFW) Isolation
Containment Isolation
SG Isolation
CRACS Isolation and Filtering
EDG Actuation
EFWS Isolation
EFWS Actuation
CVCS Isolation
Anti-Dilution Isolation
PSRV Opening
RCP Trip

Table 2.4.1-5—Protection System Permissives and Operating Bypasses (2 Sheets)

Permissive	Inhibit	Validate	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P2	Automatic	Automatic	Low DNBR RT	
			HLPD RT	
			Low RCS Loop Flow RT	
			Low RCP Speed RT	
			Low Pressurizer Pressure RT	
P3	Automatic	Automatic	Low-Low RCS Loop RT	
P5	Automatic	Automatic	High Core Power Level RT	
			Low Saturation Margin RT	
P6	Automatic	Manual		High Neutron Flux RT
				Low Doubling Time RT
P12	Automatic	Manual		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)
				MFW Startup and Shutdown System (SSS) Isolation (low SG pressure)
P13	Automatic	Manual		Low SG Level RT
				High SG Level RT
				EFWS Actuation (low SG level)
				EFWS Actuation (SIS + LOOP)
				EFWS Actuation (manual)
				EFWS Isolation (high SG level)

Table 2.4.1-5—Protection System Permissives and Operating Bypasses (2 Sheets)

Permissive	Inhibit	Validate	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P13	Automatic	Manual		EFWS Isolation (manual)
				MFW Full Load Isolation (high SG level)
				MFW SSS Isolation (high SG level for period of time + RT)
				SG Isolation
P14	Manual	Manual		Partial Cooldown Actuation
P17	Automatic	Manual	PSRV Opening	CVCS Charging Isolation (high Pressurizer level)

Table 2.4.1-6—Protection System Interlocks

RHR Suction Valves
MHSI Large Miniflow Line Valves
Safety Injection Accumulator Valves

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	PS equipment is located as listed in Table 2.4.1-1.	Inspections will be performed of the location of the PS equipment.	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 four divisions of the PS.	Inspections will be performed to verify that the divisions of the PS are located in separate safeguard buildings	The four 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. Design analyses will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E PS equipment and non-Class 1E equipment. b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E PS equipment and non-Class 1E equipment.	a. A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E PS equipment and 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. Reconciliation is performed of any deviations to the design.
3.1	Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment listed 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. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. Inspections will be performed of the Seismic Category I equipment listed in Table 2.4.1-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	b. Inspection reports exist and conclude that the Seismic Category I equipment listed in Table 2.4.1-1 including anchorage is installed as specified on the construction drawings.
4.1	The PS generates automatic RT signals.	a. Tests will be performed on the PS using test signals to verify that the RT breakers open when a trip limit in the PS is reached	a. The RT breakers open after a test signal reaches the trip limit in the PS for one RT function.
		b. Tests will be performed on the PS using test signals to verify that a RT signal is generated for the input variables listed in Table 2.4.1-2 when a test signal reaches the trip limit..	b. The PS generates a RT signal after the test signal reaches the trip limit for the input variables listed in Table 2.4.1-2.
4.2	The PS generates automatic ESF signals.	Tests will be performed on the PS using test signals to verify that a ESF signal is generated for the input variables listed in Table 2.4.1-3 when a test signal reaches the trip limit.	The PS generates a ESF signal after the test signal reaches the trip limit for the input variables listed in Table 2.4.1-3. The ESF signals remain following removal of the test signal. The ESF signals are removed when test signals that represent the completion of the ESF function are present. Deliberate operator action is required to return the PS to normal.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.3	The permissives provide operating bypass capability for the corresponding PS functions.	a. For each function listed as being bypassed by an inhibited permissive in Table 2.4.1-5, tests will be performed to verify that each function is bypassed when test signals representing the corresponding inhibited permissive signal are present. For each function listed as being bypassed by an inhibited permissive in Table 2.4.1-5, tests will be performed to verify the automatic removal of the bypass when test signals representing the corresponding inhibited permissive are removed.	a. The functions listed as being bypassed by inhibited permissives in Table 2.4.1-5 are bypassed when test signals representing the corresponding inhibited permissive are present and the bypasses are automatically removed when test signals representing the corresponding inhibited permissive are removed.
		b. For each function listed as being bypassed by a validated permissive in Table 2.4.1-5, tests will be performed to verify that each function is bypassed when test signals representing the corresponding validated permissive signal are present. For each function listed as being bypassed by a validated permissive in Table 2.4.1-5, tests will be performed to verify the automatic removal of the bypass when test signals representing the corresponding validated permissive are removed.	b. The functions listed as being bypassed by validated permissives in Table 2.4.1-5 are bypassed when test signals representing the corresponding validated permissive are present and the bypasses are automatically removed when test signals representing the corresponding validated permissive are removed.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.4	Communication independence is provided between the four PS divisions.	Tests, analyses, or a combination of tests and analyses will be performed on the PS equipment.	A report exists and concludes that: • The PS function processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor 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 processors.
4.5	The PS is capable of performing its safety function when PS equipment is in maintenance bypass (inoperable). Bypassed PS equipment is indicated in the MCR.	a. A test of the PS will be performed to verify the maintenance bypass functionality. b. Tests will be performed to verify the existence of indications in the MCR when PS equipment is in maintenance bypass (inoperable).	a. The PS can perform its safety functions when PS equipment is in maintenance bypass (inoperable). b. Bypassed PS equipment is indicated in the MCR.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.6	Setpoints associated with the automatic RT signals and the automatic ESF signals are determined using a methodology that addresses the determination of applicable contributors to instrumentation loop errors, the method in which the errors are combined, and how the errors are applied to the design analytical limits.	a. An inspection will be performed to verify the existence of an established methodology for determining the PS setpoints. b. An analysis will be performed to verify that the PS setpoints for the functions listed in Table 2.4.1-2 and Table 2.4.1-3 are determined using the documented methodology.	a. An established methodology for determining PS setpoints exists. b. A report exists and concludes that the PS setpoints associated with the automatic RT signals listed in Table 2.4.1-2 and the automatic ESF signals listed in Table 2.4.1-3 are determined using a documented methodology: (1) For the determination of applicable contributors to instrument loop error. (2) For combining instrument loop errors. (3) For how the errors are applied to the design analytical limits.
4.7	Input variables provide the inputs for generating RT signals and ESF signals.	a. An analysis will be performed on the PS software design to verify that the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 provide the inputs for generating the RT signals in Table 2.4.1-2 and the ESF signals in Table 2.4.1-3.	a. A report exists and concludes that each RT signal listed in Table 2.4.1-2 and each ESF signal listed in Table 2.4.1-3, the input variables associated with the signals are used in the PS software design for generating each signal

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. Inspections, tests, or combinations of inspections and tests will be performed on the PS equipment to verify that the sensors that provide the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 are connected to the correct input terminals of the PS as specified in the construction drawings.	b. The sensors that provide the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 are connected to the correct input terminals of the PS as specified in the construction drawings.
4.8	Electrical isolation is provided on connections between PS equipment and non-Class 1E equipment.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between PS equipment and non-Class 1E equipment.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between PS equipment and non-Class 1E equipment.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between PS equipment and non-Class 1E equipment.	b. A report exists and concludes that the Class 1E isolation devices used between PS equipment and non-Class 1E equipment prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between PS equipment and non-Class 1E equipment.	c. Class 1E electrical isolation devices exist on connections between PS equipment and non-Class 1E equipment.
4.9	Deleted.	Deleted.	Deleted.
4.10	Class 1E PS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Type tests or type tests and analyses of these will be performed on the Class 1E equipment listed in Table 2.4.1-1.	A report exists and concludes that the 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.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.11	Controls exist in the MCR that allow manual actuation at the system level.	Tests will be performed to verify the correct functionality of the controls in the MCR.	For each function in Table 2.4.1-4, the PS generates actuation signals after the corresponding controls in the MCR are manually activated. Deliberate manual action is required to return the PS to normal.
4.12	Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives.	Tests will be performed to verify the correct functionality of the controls in the MCR and RSS.	For each of the manual permissives in Table 2.4.1-5, the correct permissive status is present in the PS actuation logic units (ALU) after the corresponding controls in the MCR and RSS are manually activated.
4.13	The PS performs interlock functions..	Tests will be performed on the as-built PS using test signals to simulate plant conditions that require the interlock functions listed in Table 2.4.1-6.	The PS generates the correct output signals for each interlock function listed in Table 2.4.1-6 when the test signals are such that the interlock function is required.
4.14	The PS system design and application software are developed using a process composed of six life cycle phases, with each phase having outputs which must conform to the requirements of that phase. The six life cycle 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.	a. Analyses will be performed to verify that the outputs for the PS basic design phase conform to the requirements of that phase. **{{DAC}}** b. Analyses will be performed to verify that the outputs for the PS detailed design phase conform to the requirements of that phase. **{{DAC}}** c. Analyses will be performed to verify that the outputs for the PS manufacturing phase conform to the requirements of that phase.	a. A report exists and concludes that the outputs conform requirements of the basic design phase of the PS. **{{DAC}}** b. A report exists and concludes that the outputs conform to requirements of the detailed design phase of the PS. **{{DAC}}** c. A report exists and concludes that the outputs conform to the requirements of the manufacturing phase of the PS.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
	6) Final Documentation Phase.	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 exists and 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 exists and 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 exists and concludes that the outputs conform to the requirements of the final documentation phase of the PS.
4.15	Controls exist in the RSS that allow manual actuation of RT.	Tests will be performed to verify the correct functionality of the controls in the RSS.	The correct actuation signals are present at the RT devices after the corresponding controls in the RSS are manually activated.
4.16	Electrical isolation is provided on connections between the four PS divisions.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the four PS divisions.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the four PS divisions.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the four PS divisions.	b. A report exists and concludes that the Class 1E isolation devices used between the four PS divisions prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between the four PS divisions.	c. Class 1E electrical isolation devices exist on connections between the four PS divisions.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
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.	A report exists and concludes that: • Data communications between PS function processors and non-Class 1E equipment is through a Monitoring and Service Interface (MSI). • The MSI processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the MSI processor. • The MSI processors operate in a strictly cyclic manner. • The MSI processors operate asynchronously from the communications processors.
4.18	The PS is designed so that safety-related functions required for DBE are performed in the presence of the following: • Single detectable failures within the PS concurrent with identifiable but non-detectable failures. • Failures caused by the single failure. • Failures and spurious system actions that cause or are caused by the DBE 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 exists and concludes that the PS is designed so that safety-related functions required for DBE are performed in the presence of the following: • Single detectable failures within the PS concurrent with identifiable but non-detectable failures. • Failures caused by the single failure. • Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.19	The equipment for each PS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.	Inspections will be performed on the PS equipment to verify that the equipment for each PS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	The equipment for each PS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.
4.20	Locking mechanisms are provided on the PS cabinet doors. Opened PS cabinet doors are indicated in the MCR.	a. Inspections will be performed to verify the existence of locking mechanisms on the PS cabinet doors.	a. Locking mechanisms exist on the PS cabinet doors.
		b. Tests will be performed to verify the proper operation of the locking mechanisms on the PS cabinet doors.	b. The locking mechanisms on the PS cabinet doors operate properly.
		c. Tests will be performed to verify an indication exists in the MCR when a PS cabinet door is in the open position.	c. Opened PS cabinet doors are indicated in the MCR.
4.21	Key lock switches are provided at the PS cabinets to restrict modifications to the PS software.	a. Inspections will be performed to verify the existence of key lock switches that restrict modifications to the PS software.	a. Key lock switches are provided at the PS cabinets.
		b. Tests will be performed to verify that the key lock switches restrict modifications to the PS software	b. Key lock switches at the PS cabinets restrict modifications to the PS software.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.22	The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.	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 exists and 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	The PS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods.	A TELEPERM XS platform changes analysis will be performed on the PS hardware and system software to verify its conformance to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A report exists and concludes that the PS hardware modules and system software modules: a. Conform to the key TELEPERM XS design principles. **{{DAC}}** b. Conform to the key TELEPERM XS processing features. **{{DAC}}** c. Conform to the key TELEPERM XS communication independence features. **{{DAC}}**

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
			d. Do not introduce more than a minimal increase in the likelihood of occurrence of a software malfunction relative to predecessor modules. **{{DAC}}** e. Do not introduce more than a minimal increase in the consequences of a malfunction relative to predecessor modules. **{{DAC}}** f. Do not create the possibility for a malfunction with a different result relative to predecessor modules. **{{DAC}}** g. Were developed according to procedures that do not result in a reduction in the TELEPERM XS quality methods. **{{DAC}}**
4.24	The PS response time for RT and ESF signals is less than the value required to satisfy the design basis safety analysis response time assumptions.	a. Analyses will be performed to determine the required response time from sensor to ALU output, including sensor delay, which supports the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.	a. A report exists and identifies the required response time from sensor to ALU output which supports the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.

Table 2.4.1-7—Protection System ITAAC (13 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. Tests, analyses, or a combination of tests and analyses will be performed on the PS equipment that contributes to RT and ESF signal response times.	b. A report exists and concludes that PS response times from sensor to ALU output support the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.
5.1	Class1E PS components are powered from a Class 1E division in a normal or alternate feed condition.	a. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 by providing a test signal in each division with the alternate feed aligned to the divisional pair.	a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.1-1. b. The test signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E components identified in Table 2.4.1-1.

Next File