2.4.4 Safety Automation System

Design Description

1.0 System Description

The safety automation system (SAS) provides control and monitoring of safety systems.

The SAS provides the following safety-related functions:

- Provides control and monitoring of systems required to transfer the plant to cold shutdown and maintain it in this state following an anticipated operational occurrence (AOO) or postulated accident (PA).
- Provides control and monitoring of safety-related functions of auxiliary support systems.
- Provides safety interlock functions.

2.0 Arrangement

2.1 The location of the SAS equipment is as listed in Table 2.4.4-1—Safety Automation System Equipment.

2.2 Physical separation exists between the divisions of the SAS as listed in Table 2.4.4-1.

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

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without a loss of safety function(s).

4.0 I&C Design Features, Displays, and Controls

4.1 Class 1E SAS equipment listed in Table 2.4.4-1 can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.2 Deleted.

4.3 The SAS provides output signals to the recipients listed in Table 2.4.4-3—Safety Automation System Interlocks.

4.4 The SAS performs interlock functions listed in Table 2.4.4-3.

4.5 The SAS 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.

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

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

4.8 Communications independence is provided between the SAS divisions.

4.9 Communications independence is provided between SAS equipment and non-Class 1E equipment.

4.10 The SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the following:

- Single failures within the SAS.
- 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.

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

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

4.13 CPU state switches are present at the SAS cabinets to restrict modifications to the SAS software.

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

4.15 The operational availability of each input variable listed in Table 2.4.4-2 listed 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.

4.16 Deleted.

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

4.18 The SAS generates automatic ESF and EAS functions for the input variables listed in Table 2.4.4-2 when the trip limit is reached. The ESF and EAS functions remain following removal of the signal. The ESF and EAS functions are removed when input signals that represent the completion of the ESF and EAS functions are present.

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

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

4.21 SAS connections to the SICS are hardwired for manual grouped controls.

4.22 SAS manual grouped controls and indications are available on the SICS in the MCR.

4.23 Deleted.

5.0 Electrical Power Design Features

5.1 Equipment designated as Class 1E in Table 2.4.4-1 are powered from the Class 1E division as listed in Table 2.4.4-1 in a normal or alternate feed condition.

6.0 Environmental Qualification

6.1 Equipment designated as mild environment in Table 2.4.4-1 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 2.4.4-4 lists the SAS ITAAC.

Table 2.4.4-1—Safety Automation System Equipment

Description	Tag Number(1)	Location	Seismic Category	IEEE Class 1E(2)	Environment
SAS Cabinets, Division 1	30DRA1	Safeguard Building 1	I	1^{N} 2^{A}	Mild
SAS Cabinets, Division 2	30DRA2	Safeguard Building 2	I	2^{N} 1^{A}	Mild
SAS Cabinets, Division 3	30DRA3	Safeguard Building 3	I	3^{N} 4^{A}	Mild
SAS Cabinets, Division 4	30DRA4	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 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 1 of 9

System	Function Name	Input Variable
Annulus Ventilation System (AVS)	Accident Filtration Train Heater Control	Isolation Damper Position
		Heater Fan Signal
		Post Heater Temperature
	Accident Train Switchover	Pressure
		Differential Pressure
		Post Heater Temperature
		Filter Bank Isolation Inlet Damper Position
		Filter Bank Isolation Outlet Damper Position
		Exhaust Fan Signal
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2 and Train 2 to Train 1	Train 1 ESWS Pump Discharge Pressure
		Train 1 Pump Discharge Pressure
		Train 1 Flow Rate
		Train 2 ESWS Pump Discharge Pressure
		Train 2 Pump Discharge Pressure
		Train 2 Flow Rate
	CCWS Common 2.b Automatic Backup Switchover of Train 3 to Train 4 and Train 4 to Train 3	Train 3 ESWS Pump Discharge Pressure
		Train 3 Pump Discharge Pressure
		Train 3 Flow Rate
		Train 4 ESWS Pump Discharge Pressure
		Train 4 Pump Discharge Pressure
		Train 4 Flow Rate
	CCWS Emergency Temperature Control	Heat Exchanger Temp
		Heat Exchanger Bypass Valve Position

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 2 of 9

System	Function Name	Input Variable
	CCWS Emergency Leak Detection	Surge Tank Level
		OCWS Chiller Inlet Flow
		OCWS Chiller Outlet Flow
		Common Supply Outlet Flow
		Common Supply Inlet Flow
	CCWS Emergency Leak Detection – Switchover Valves Leakage or Failure	Surge Tank 1 Level
	CCWS Switchover Valves Interlock	Common 1a Supply Valve Position
		Common 1a Return Valve Position
		Common 1b Supply Valve Position
		Common 1b Return Valve Position
	CCWS RCP Thermal Barrier Containment Isolation Valve Interlock	Common 1b Return Outer CIV Position
		Common 1b Supply Outer CIV Position
		Common 2b Return Outer CIV Position
		Common 2b Supply Outer CIV Position
		Common 1b Return Inner CIV Position
		Common 1b Supply Inner CIV Position
		Common 2b Return Inner CIV Position
		Common 2b Supply Inner CIV Position

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 3 of 9

System	Function Name	Input Variable
	CCWS RCP Thermal Barrier Containment Isolation Valve Opening Interlock	Common 1b Return Outer CIV Position
		Common 1b Supply Outer CIV Position
		Common 2b Return Outer CIV Position
		Common 2b Supply Outer CIV Position
		Common 1b Return Inner CIV Position
		Common 1b Supply Inner CIV Position
		Common 2b Return Inner CIV Position
		Common 2b Supply Inner CIV Position
	SCWS Condenser Supply Water Flow Control	Condenser Refrigerant Pressure
Emergency Feedwater System (EFWS)	SG Level Control	SG Level
	Pump Flow Protection	Pump Discharge Flow
Essential Service Water Pump Building Ventilation System (ESWPBVS)	ESWPBVS ESWS Pump Rooms Temperature Control	Outside Air Temperature
Essential Service Water System (ESWS)	ESW Flood Prevention in the Safeguard Building	Non-Controlled Area of Safeguard Building Sump Level
Fuel Building Ventilation System (FBVS)	Safety-Related Room Heater Control	Room Temperature
	FBVS EBS / FPCS Pump Rooms Heat Removal	Pump Room Temperature
	Isolation of FBVS on Containment Isolation	Containment Isolation Signal
	Isolation of the Fuel Pool Room	Fuel Pool Room Activity
		Fuel Pool Temperature
	Isolation of the Emergency Airlock and Equipment Hatch Fuel Building Areas	Reactor Building Activity

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 4 of 9

System	Function Name	Input Variable
Fuel Pool Cooling and Purification System (FPCPS)	FPCPS Pump Trip on Low Spent Fuel Pool (SFP) Level	SFP Level (WR)
In-Containment Refueling Water Storage Tank System (IRWST)	IRWST Boundary Isolation for Preserving IRWST Water Inventory Interlock	IRWST Level
Main Control Room Air Conditioning System (CRACS)	Iodine Filtration Train Heater Control	Carbon Filter Isolation Damper Position
		Protective Switch Temperature
		ESF Filtration Booster Fan Status
	Heater Control for Outside Inlet Air	Downstream Temperature
		Inlet Damper Position
		Outlet Damper Position
	Pressure Control	MCR Differential Pressure
	Cooler Temperature Control	Supply Air Temperature
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Pressure Control	MSRIV Position
		MSRIV Actuation Signal (from PS)
		MSRT Setpoint (from PS)
		SG Pressure
	Steam Generator MSRCV Regulation during Standby Position Control	MSRCV Position
		Nuclear Power Calculation (from PS)

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 5 of 9

System	Function Name	Input Variable
Safeguard Building Controlled-Area Ventilation System (SBVS)	SIS/RHRS Pump Rooms Heat Removal	LHSI Pump Room Temperature
		MHSI Pump Room Temperature
		SIS Actuation (from PS)
		LHSI/RHR Pump Running Signal
		LHSI/RHR Pump Stopped Signal
		MHSI Pump Running Signal
		MHSI Pump Stopped Signal
	CCWS/EFWS Valve Rooms Heat Removal	Room Temperature
	Isolation of Mechanical Areas of Safeguard Building on Containment Isolation	Containment Isolation Signal
	Iodine Filtration Train Electric Heater Control	Post Heater Temperature
		Isolation Dampers Position
		Heater Fan Signal
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply and Recirculation Exhaust Air Flow Control	Supply Air Temperature Downstream of Heaters
		Protective Switch Temperature
		Outside Air Temperature
		Outside Air Damper Open Position Signal
		Outside Air Damper Closed Position Signal
		Exhaust Damper Open Position Signal
		Exhaust Damper Closed Position Signal
		Recirculation Damper Open Position Signal
		Recirculation Damper Closed Position Signal

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 6 of 9

System	Function Name	Input Variable
	Supply Fan Safe Shut-off	Recirc / Exhaust Fan Stopped Signal
		Outside Air Damper Closed Position Signal
		Recirculation Damper Closed Position Signal
	Recirculation Fan Safe Shut-off	CCW Pump Room Temperature
		EFW Pump Room Temperature
	Exhaust Fan Safe Shut-off	Exhaust Damper Closed Position
	Supply Air Temperature Heater Control	Supply Air Downstream of Heaters Temperature
		Filter Bank Differential Pressure
	Freeze Protection	Outside Air Temperature
	Supply Air Temperature Control for Supply Air Cooling	Supply Air Downstream of Humidifier Temperature
	Battery Room Heater Control	Battery Room Temperature
		Supply Air Downstream of Heaters Flow
	Battery Room Supply Air Temperature Control	Battery Room Supply Air Temperature
	Emergency Feed Water System (EFWS) Pump Room Heat Removal	EFWS Pump Room Temperature
	Component Cooling Water System (CCWS) Pump Room Heat Removal	CCWS Pump Room Temperature

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 7 of 9

System	Function Name	Input Variable
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure Interlock	Train 1 Chiller Evaporator Outlet Temperature
		Train 1 Chiller Evaporator Flow Signal
		Train 1 Cross-Tie Valves Position Signal
		Train 2 Cross-Tie Valves Position Signal
		Train 2 Circulating Pump 1 Running Signal
		Train 2 Circulating Pump 2 Running Signal
		Train 2 Evaporator ΔP Signal
		Train 2 Chiller Evaporator Flow Signal
	SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure Interlock	Train 1 Circulating Pump 1 Running Signal
		Train 1 Circulating Pump 2 Running Signal
		Train 1 Evaporator ΔP Signal
		Train 1 Chiller Evaporator Flow Signal
		Train 1 Cross-Tie Valves Position Signal
		Train 2 Cross-Tie Valves Position Signal
		Train 2 Chiller Evaporator Flow Signal
		Train 2 Chiller Evaporator Outlet Temperature

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 8 of 9

System	Function Name	Input Variable
	SCWS Train 3 to Train 4 Switchover on Train 3 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure Interlock	Train 3 Chiller Evaporator Outlet Temperature
		Train 3 Chiller Evaporator Flow Signal
		Train 3 Cross-Tie Valves Position Signal
		Train 4 Cross-Tie Valves Position Signal
		Train 4 Circulating Pump 1 Running Signal
		Train 4 Circulating Pump 2 Running Signal
		Train 4 Evaporator ΔP Signal
		Train 4 Chiller Evaporator Flow Signal
	SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure Interlock	Train 3 Circulating Pump 1 Running Signal
		Train 3 Circulating Pump 2 Running Signal
		Train 3 Evaporator ΔP Signal
		Train 3 Chiller Evaporator Flow Signal
		Train 3 Cross-Tie Valves Position Signal
		Train 4 Cross-Tie Valves Position Signal
		Train 4 Chiller Evaporator Flow Signal
		Train 4 Chiller Evaporator Outlet Temperature

Table 2.4.4-2—Safety Automation System Automatic Functions and Input Variables
Sheet 9 of 9

System	Function Name	Input Variable
Safety Injection and Residual Heat Removal System (SIS/RHRS)	Automatic RHRS Flow Rate Control	RHRS Flow Rate Signal
		RHRS Temperature
		RHRS Pump Discharge Pressure
	RHR Isolation Valves Interlock	LHSI Suction Isolation Valve Position
		RHR 1st RCPB Isolation Valve Position
		RHR 2nd RCPB Isolation Valve Position

Table 2.4.4-3—Safety Automation System Interlocks

CCWS Switchover Valves Interlock
CCWS RCP Thermal Barrier Containment Isolation Valve Interlock
CCWS RCP Thermal Barrier Containment Isolation Valves Opening Interlock
IRWST Boundary Isolation for Preserving IRWST Water Inventory Interlock
SCWS Train 1 to Train 2 Switchover on Train 1 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock
SCWS Train 2 to Train 1 Switchover on Train 2 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock
SCWS Train 3 to Train 4 Switchover on Train 3 / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock
SCWS Train 4 to Train 3 Switchover on Train 4 Loss of Pump / Loss of Chiller / SCWS Chiller Evaporator Water Flow Control / LOOP Re-Start Failure Interlock
RHR Isolation Valves Interlock

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 1 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the SAS equipment is as listed in Table 2.4.4-1.	An inspection of the location of the as-built SAS equipment will be performed.	The SAS equipment listed in Table 2.4.4-1 is located as listed in Table 2.4.4-1.
2.2	Physical separation exists between the divisions of the SAS as listed in Table 2.4.4-1.	An inspection will be performed to verify that the as-built divisions of the SAS are located in separate Safeguard Buildings.	The divisions of the SAS are located in separate Safeguard Buildings as listed in Table 2.4.4-1.
2.3	Physical separation exists between Class 1E SAS 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 SAS 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 SAS 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 SAS 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 SAS equipment and non-Class 1E equipment.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 2 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
3.1	Equipment identified as Seismic Category I in Table 2.4.4-1 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 2.4.4-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements. b. An inspection will be performed of the as-built equipment identified as Seismic Category I in Table 2.4.4-1 to verify that the equipment, including anchorage, are installed in a condition bounded by the tested or analyzed condition.	a. Test/analysis reports conclude that the equipment identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without a loss of safety function(s). b. Inspection reports conclude that the equipment identified as Seismic Category I in Table 2.4.4-1, including anchorage, are installed in a condition bounded by the tested or analyzed condition.
4.1	Class 1E SAS equipment listed in Table 2.4.4-1 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 SAS equipment listed in Table 2.4.4-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Equipment identified as Class 1E in Table 2.4.4-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.
4.2	Deleted.	Deleted.	Deleted.
4.3	The SAS provides output signals to the recipients listed in Table 2.4.4-3.	A test will be performed to verify that the SAS provides output signals to the recipients listed in Table 2.4.4-3.	The SAS provides output signals to the recipients listed in Table 2.4.4-3.
4.4	The SAS performs interlock functions listed in Table 2.4.4-3.	Tests will be performed on the SAS using test input signals to verify operation of the interlocks.	The interlocks listed in Table 2.4.4-3 respond as specified when activated by a test input signal.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 3 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.5	The SAS 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 SAS 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 SAS.
		b. Analyses will be performed to verify that the outputs for the SAS 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 SAS.
		c. Analyses will be performed to verify that the outputs for the SAS 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 SAS.
		d. Analyses will be performed to verify that the outputs for the SAS 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 SAS.
		e. Analyses will be performed to verify that the outputs for the SAS 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 SAS.
		f. Analyses will be performed to verify that the outputs for the SAS 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 SAS.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 4 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.6	Electrical isolation is provided on connections between the SAS 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 SAS divisions. b. An inspection will be performed on connections between as-built SAS divisions.	a. A report concludes that the Class 1E isolation devices used between SAS divisions prevent the propagation of credible electrical faults. b. Class 1E electrical isolation devices exist on connections between SAS divisions.
4.7	Electrical isolation is provided on connections between Class 1E SAS 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 SAS equipment and non-Class 1E equipment. b. An inspection will be performed on connections between as-built Class 1E SAS equipment and non-Class 1E equipment.	a. A report concludes that the Class 1E isolation devices used between Class 1E SAS 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 SAS equipment and non-Class 1E equipment.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 5 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.8	Communications independence is provided between the SAS 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 SAS divisions.	Communications independence between the SAS division is provided by: • The SAS function processors do 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 SAS function processor. • The SAS function processors operate in a strictly cyclic manner. • The SAS function processors operate asynchronously from the SAS communications module.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 6 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	Communications independence is provided between SAS equipment and non-Class 1E equipment.	Tests, analyses, or a combination of tests and analyses will be performed on the SAS equipment to verify that communications independence is provided between SAS equipment and non-Class 1E equipment.	Communications independence between SAS equipment and non-Class 1E equipment is provided by: ● Data communications between SAS 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 SAS uses a hardware device to ensure that unidirectional signals are sent to non-safety-related I&C systems.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 7 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.10	The SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the following: ● Single failures within the SAS. ● 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 SAS at the level of replaceable modules and components.	A report concludes that the SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the following: ● Single failures within the SAS. ● 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.
4.11	Equipment markings for each SAS division are distinctly identified and distinguishable from other identifying markings placed on the equipment.	An inspection will be performed on the as-built SAS equipment to verify that the equipment markings for each SAS division are distinctly identified and distinguishable from other markings placed on the equipment.	Equipment markings for each SAS division are distinctly identified and distinguishable from other identifying markings placed on the equipment.
4.12	Locking mechanisms are provided on the SAS cabinet doors. SAS 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 SAS cabinet doors operate properly. b. A test will be performed to verify that SAS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.	a. The locking mechanisms on the SAS cabinet doors operate properly. b. SAS cabinet doors that are not closed are indicated on the PICS operator workstations in the MCR.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 8 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.13	CPU state switches are present at the SAS cabinets to restrict modifications to the SAS software.	a. An inspection will be performed to verify the existence of CPU state switches at the as-built SAS cabinets that restrict modifications to the PS software.	a. CPU state switches are provided at the SAS cabinets.
		b. Tests will be performed to verify that the CPU state switches restrict modifications to the SAS software.	b. CPU state switches at the SAS cabinets restrict modifications to the SAS software.
4.14	The SAS is capable of performing its safety function when SAS equipment is in maintenance bypass. Bypassed SAS equipment is indicated on the PICS operator workstations in the MCR.	a. A test of the SAS will be performed to verify the maintenance bypass functionality.	a. The SAS can perform its safety functions when SAS equipment is in maintenance bypass.
		b. A test will be performed to verify bypassed SAS equipment is indicated on the PICS operator workstations in the MCR.	b. Bypassed SAS equipment is indicated on the PICS operator workstations in the MCR.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 9 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.15	The operational availability of each input variable listed in Table 2.4.4-2 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.	Analysis will be performed to demonstrate that the operational availability of each input variable listed in Table 2.4.4-2 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 2.4.4-2 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.
4.16	Deleted.	Deleted.	Deleted.
4.17	Hardwired disconnects exist between the SU and each divisional MSI of the SAS. The hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.	a. An inspection of the as-built hardwired disconnects between the SU and each divisional MSI of the SAS will be performed. b. A test of the hardwired disconnects between the SU and each divisional MSI of the SAS will be performed.	a. Hardwired disconnects exist between the SU and each divisional MSI of the SAS. b. The hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 10 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.18	The SAS generates automatic ESF and EAS functions for the input variables listed in Table 2.4.4-2 when the trip limit is reached. The ESF and EAS functions remain following removal of the signal. The ESF and EAS functions are removed when input signals that represent the completion of the ESF and EAS functions are present.	A test will be performed on the SAS to verify that automatic ESF and EAS functions are generated for the input variables listed in Table 2.4.4-2 when the trip limit is reached.	The SAS generates an ESF and EAS function when the trip limit is reached for the input variables listed in Table 2.4.4-2. The ESF and EAS functions remain following removal of the signal. The ESF and EAS functions are removed when the ESF and EAS functions are manually reset.
4.19	During data communication, the SAS function processors receive all messages, but only the pre-defined messages for that specific SAS 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 SAS function processor. b. A test will be performed to verify that the SAS 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 SAS function processor. b. The SAS 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.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 11 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.20	SAS self-test features are capable of detecting and responding to faults consistent with the design requirements of SAS.	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 SAS equipment.	a. A report concludes that the SAS equipment is capable of detecting faults required to be detected by self-test features.
		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 SAS equipment responds according to the type of fault.	b. A report concludes that upon detection of faults through self-test features, the SAS equipment responds according to the type of fault.
4.21	SAS connections to the SICS are hardwired for manual grouped controls.	An inspection will be performed to verify that as-built SAS connections to the SICS are hardwired for manual grouped controls.	SAS connections to the SICS are hardwired for manual grouped controls.
4.22	SAS manual grouped controls and displays are available on the SICS in the MCR.	a. Tests will be performed to verify that SAS displays are indicated on the SICS in the MCR.	a. SAS displays are indicated on the SICS in the MCR.
		b. Tests will be performed using SAS manual grouped controls in the MCR.	b. Controls on the SICS in the MCR perform manual grouped controls from the SICS in the MCR.
4.23	Deleted.	Deleted.	Deleted.

Table 2.4.4-4—Safety Automation System ITAAC
Sheet 12 of 12

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
5.1	Equipment designated as Class 1E in Table 2.4.4-1 are powered from the Class 1E division as listed in Table 2.4.4-1 in a normal or alternate feed condition.	a. Testing will be performed by providing a test input signal in each normally aligned division.	a. The test input signal provided in the normally aligned division is present at the respective Class 1E equipment identified in Table 2.4.4-1.
		b. Testing will be performed by providing a test input signal in each division with the alternate feed aligned to the divisional pair.	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 2.4.4-1.
6.1	Equipment designated as mild environment in Table 2.4.4-1 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 2.4.4-1 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 2.4.4-1 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 2.4.4-1 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 2.4.4-1, 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