

2.4.4 Safety Automation System

1.0 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 a design basis event.
- Provides control and monitoring of safety related functions of auxiliary support systems.
- Provides acquisition and processing of Type A, B and C post-accident monitoring variables for display to the operators in the main control room (MCR) and on the remote shutdown station (RSS).
- Provides a safety interlock function.

2.0 Arrangement

2.1 SAS equipment is located as listed in Table 2.4.4-1—Safety Automation System Equipment.

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

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 loss of safety function.

4.0 I&C Design Features, Displays and Controls

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

4.2 The SAS receives input signals from the sources listed in Table 2.4.4-2—Safety Automation System Input Signals.

4.3 The SAS provides the output signals listed in Table 2.4.4-3—Safety Automation System Output Signals.

4.4 The SAS provides the interlocks listed in Table 2.4.4-4—Safety Automation System Interlocks.

- 4.5 The SAS 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.
 6. Final Documentation Phase.
- 4.6 Electrical isolation is provided on connections between the four SAS divisions.
- 4.7 Electrical isolation is provided on connections between SAS equipment and non-Class 1E equipment.
- 4.8 Communications independence is provided between the four 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 design basis events (DBE) are performed in the presence of the following:
- Single detectable failures within the SAS 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.
- 4.11 The equipment for each SAS 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.
- 4.12 Locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.
- 4.13 Key lock 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 one of the SAS divisions is out of service. Out of service divisions of SAS are indicated in the MCR.
- 4.15 The operational availability of each input variable listed can be confirmed during reactor operation including post-accident periods.

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

5.0 Electrical Power Design Features

5.1 Class 1E SAS 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 2.4.4-5 lists the SAS ITAAC.

Table 2.4.4-1—Safety Automation System Equipment

Description	Tag Number ⁽¹⁾	Location	Seismic Category	IEEE Class 1E⁽²⁾
SAS Cabinets, Division 1	30DRA1	Safeguard Building 1	I	1 ^N 2 ^A
SAS Cabinets, Division 2	30DRA2	Safeguard Building 2	I	2 ^N 1 ^A
SAS Cabinets, Division 3	30DRA3	Safeguard Building 3	I	3 ^N 4 ^A
SAS Cabinets, Division 4	30DRA4	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 2.4.4-2—Safety Automation System Input Signals

Item #	Signal	Source	# Divisions	IEEE Class 1E
1	Steam Generator Pressure	Protection System	4	Yes
2	Main Steam Relief Control Valve Position	Main Steam System	4	Yes
3	Core Thermal Power	Protection System	4	Yes
4	Main Steam Relief Isolation Valve Position	Main Steam System	4	Yes
5	Steam Generator Level Wide Range	Protection System	4	Yes
6	Emergency Feedwater System Flow	Emergency Feedwater System	4	Yes

Table 2.4.4-3—Safety Automation System Output Signals

Item #	Output Signal	Signal Generation	Recipient	# Divisions	IEEE Class 1E
1	EFW Flow Control Valve Position Signal	Auto	PACS	4	Yes
2	EFW SG Level Control Valve Position Signal	Auto	PACS	4	Yes
3	Main Steam Relief Control Valve Signal	Auto	PACS	4	Yes

Table 2.4.4-4—Safety Automation System Interlocks

Isolation of Component Cooling Water System (CCWS) Trains

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	SAS equipment is located as listed in Table 2.4.4-1.	Inspections will be performed of the location of the SAS equipment.	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 four divisions of the SAS.	Inspections will be performed to verify that the divisions of the SAS are located in separate Safeguard Buildings.	The four 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.	<p>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 SAS equipment and non-Class 1E equipment.</p> <p>b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment.</p>	<p>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 SAS equipment and non-Class 1E equipment.</p> <p>b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment. Reconciliation is performed of any deviations to the design.</p>
3.1	Equipment identified as Seismic Category I in Table 2.4.4-1 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 2.4.4-1 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 2.4.4-1 can withstand seismic design basis loads without loss of safety function.

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. Inspections will be performed of the Seismic Category I equipment listed in Table 2.4.4-1 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 2.4.4-1 including anchorage is installed as specified on the construction drawings.
4.1	Class 1E SAS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Type tests or type tests and analysis of these will be performed for the Class 1E equipment listed in Table 2.4.4-1.	A report exists and concludes that the equipment identified as Class 1E in Table 2.4.4-1 can perform its safety function when subjected to electromagnetic interference EMI, RFI, ESD, and power surges.
4.2	The SAS receives input signals from the sources listed in Table 2.4.4-2.	Tests will be performed to verify the existence of input signals.	The SAS receives input signals from the sources listed in Table 2.4.4-2.
4.3	The SAS provides the output signals listed in Table 2.4.4-3.	Tests will be performed to verify the existence of output signals.	The SAS provides output signals to the recipients listed in Table 2.4.4-3.
4.4	The SAS provides the interlocks listed in Table 2.4.4-4.	Tests will be performed using test signals to verify the operation of the interlocks listed in Table 2.4.4-4.	The interlocks listed in Table 2.4.4-4 respond as specified when activated by a test signal.
4.5	The SAS 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.	a. Analyses will be performed to verify that the outputs for the SAS basic design phase conform to the requirements of that phase. {{DAC}} b. Analyses will be performed to verify that the outputs for the SAS detailed design phase conform to the requirements of that phase. {{DAC}}	a. A report exists and concludes that the outputs conform requirements of the basic design phase of the SAS. {{DAC}} b. A report exists and concludes that the outputs conform to requirements of the detailed design phase of the SAS. {{DAC}}

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
	3) Manufacturing Phase. 4) System Integration and Testing Phase 5) Installation and Commissioning Phase. 6) Final Documentation Phase.	c. Analyses will be performed to verify that the outputs for the SAS manufacturing phase conform to the requirements of that phase. 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. e. Analyses will be performed to verify that the outputs for the SAS installation and commissioning phase conform to the requirements of that phase.. f. Analyses will be performed to verify that the outputs for the SAS final documentation phase conform to the requirements of that phase.	c. A report exists and concludes that the outputs conform to the requirements of the manufacturing phase of the SAS. d. A report exists and concludes that the outputs conform to the requirements of the system integration and testing phase of the SAS. e. A report exists and concludes that the outputs conform to the requirements of the installation and commissioning phase of the SAS. f. A report exists and concludes that the outputs conform to the requirements of the final documentation phase of the SAS.
4.6	Electrical isolation is provided on connections between the four SAS divisions.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the four SAS divisions. b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the four SAS 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 SAS divisions. b. A report exists and concludes that the Class 1E isolation devices used between the four SAS divisions prevent the propagation of credible electrical faults.

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		<p>c. Inspections will be performed on connections between the four SAS divisions.</p>	<p>c. Class 1E electrical isolation devices exist on connections between the four SAS divisions.</p>
4.7	<p>Electrical isolation is provided on connections between SAS equipment and non-Class 1E equipment.</p>	<p>a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between SAS equipment and non-Class 1E equipment.</p> <p>b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between SAS equipment and non-Class 1E equipment.</p> <p>c. Inspections will be performed on connections between SAS equipment and non-Class 1E equipment.</p>	<p>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 SAS equipment and non-Class 1E equipment.</p> <p>b. A report exists and concludes that the Class 1E isolation devices used between SAS equipment and non-Class 1E equipment prevent the propagation of credible electrical faults.</p> <p>c. Class 1E electrical isolation devices exist on connections between SAS equipment and non-Class 1E equipment.</p>

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.8	Communications independence is provided between the four SAS divisions.	Tests, analyses, or a combination of tests and analyses will be performed on the SAS equipment.	<p>A report exists and concludes that:</p> <ul style="list-style-type: none"> • The SAS 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 SAS function processor. • The SAS function processors operate in a strictly cyclic manner. • The SAS function processors operate asynchronously from the SAS communications processors.

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	<p>Communications independence is provided between SAS equipment and non-Class 1E equipment.</p>	<p>Tests, analyses, or a combination of tests and analyses will be performed on the SAS equipment.</p>	<p>A report exists and concludes that:</p> <ul style="list-style-type: none"> • Data communications between SAS 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 function processor. • The MSI processors operate in a strictly cyclic manner. • The MSI processors operate asynchronously from the communications processors.
4.10	<p>The SAS is designed so that safety-related functions required for DBE are performed in the presence of the following:</p> <ul style="list-style-type: none"> • Single detectable failures within the SAS 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. 	<p>A failure modes and effects analysis will be performed on the SAS at the level of replaceable modules and components.</p>	<p>A report exists and concludes that the SAS is designed so that safety-related functions required for DBE are performed in the presence of the following:</p> <ul style="list-style-type: none"> • Single detectable failures within the SAS 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 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.11	The equipment for each SAS 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 SAS equipment to verify that the equipment for each SAS 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 SAS 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.
4.12	Locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.	<ul style="list-style-type: none"> a. Inspections will be performed to verify the existence of locking mechanisms on the SAS cabinet doors. b. Tests will be performed to verify the proper operation of the locking mechanisms on the SAS cabinet doors. c. Tests and inspections will be performed to verify an indication exists in the MCR when a SAS cabinet door is in the open position. 	<ul style="list-style-type: none"> a. Locking mechanisms exist on the SAS cabinet doors. b. The locking mechanisms on the SAS cabinet doors operate properly. c. Opened SAS cabinet doors are indicated in the MCR.
4.13	Key lock switches are present at the SAS cabinets to restrict modifications to the SAS software.	<ul style="list-style-type: none"> a. Inspections will be performed to verify the existence of key lock switches that restrict modifications to the SAS software. b. Tests will be performed to verify that the key lock switches restrict modifications to the SAS software. 	<ul style="list-style-type: none"> a. Key lock switches are provided at the SAS cabinets. b. Key lock switches at the SAS cabinets restrict modifications to the SAS software.

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.14	The SAS is capable of performing its safety function when one of the SAS divisions is out of service. Out of service divisions of SAS are indicated in the MCR.	<p>a. A test of the SAS will be performed to verify the SAS can perform its safety function when one of the SAS divisions is out of service.</p> <p>b. Inspections will be performed to verify the existence of indication in the MCR when a SAS division is placed out of service.</p>	<p>a. The SAS can perform its safety functions when one of the SAS divisions is out of service.</p> <p>b. Out of service divisions of SAS are indicated in the MCR.</p>
4.15	The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.	<p>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:</p> <ul style="list-style-type: none"> • 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. 	<p>A report exists and 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:</p> <ul style="list-style-type: none"> • 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.

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.16	<p>The SAS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods. {{DAC}}</p>	<p>A TELEPERM XS platform changes analysis will be performed on the SAS hardware and system software to verify its conformance to the key TELEPERM XS principles, features, and quality methods. {{DAC}}</p>	<p>A report exists and concludes that the SAS hardware modules and system software modules:</p> <ul style="list-style-type: none"> 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}} 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}}

Table 2.4.4-5—Safety Automation System ITAAC (10 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
5.1	Class 1E SAS components are powered from a Class 1E division in a normal or alternate feed condition.	<ul style="list-style-type: none"> a. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 by providing a test signal in each division with the alternate feed aligned to the divisional pair. 	<ul style="list-style-type: none"> a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.4-1. 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 2.4.4-1.

[Next File](#)