Engineering Standard

SAES-J-601 29 June 2005

Emergency Shutdown and Isolation Systems

Saudi Aramco DeskTop Standards

Table of Contents

1 Scope

1.1 This standard defines the requirements for the design, specification, installation, commissioning and testing of Emergency Shutdown Systems (ESD), emergency isolation and depressuring systems and equipment protection systems.

1.2 This standard adheres to the implementation of ESD systems according to IEC 61511 and ISA S84.01 including the determination and verification of safety integrity levels (SIL) for each ESD Loop.

1.3 SAES-B-058 and its referenced standards provide the basis for applying ESD functions to process equipment and facilities.

1.4 The requirements of this standard also applies to the design of pneumatic, hydraulic, pneumatic-hydraulic, electro-hydraulic, electric-electric, or programmable controller based ESD systems for off-shore and on-shore wellhead shutdown systems, tie-in platforms and packaged ESD systems.

2 Conflicts and Deviations

2.1 Conflicts between this standard and other applicable Saudi Aramco Engineering Standards (SAESs), Materials System Specifications (SAMSSs), Standard Drawings (SASDs), or industry standards, codes, and forms shall be resolved in writing by the Company or Buyer Representative through the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

2.2 Direct all requests to deviate from this standard in writing to the Company or Buyer Representative, who shall follow internal company procedure SAEP-302 and forward such requests to the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

3 References

The selection of material and equipment, and the design, construction, maintenance, and repair of equipment and facilities covered by this standard shall comply with the latest edition of the references listed below, unless otherwise noted.

3.1 Saudi Aramco References

Saudi Aramco Engineering Procedures

SAEP-302	*Instructions for Obtaining a Waiver of a Mandatory Saudi Aramco Engineering Requirement*
SAEP-354	*High Integrity Protective Systems*

Saudi Aramco Engineering Standards

SAES-B-006	*Fireproofing for Plants*
SAES-B-009	*Fire Protection and Safety Requirements for Offshore Protection Facilities*
SAES-B-057	*Safety Requirements: Refrigerated and Pressure Storage Vessels*
SAES-B-058	*Emergency Shutdown, Isolation, and Depressuring*
SAES-B-064	*Onshore and Nearshore Pipeline Safety*
SAES-B-070	*Bulk Plants*
SAES-J-002	*Technically Acceptable Instruments*
SAES-J-005	*Instrumentation Drawings and Forms*
SAES-J-100	*Process Flow Metering*
SAES-J-200	*Pressure*
SAES-J-300	*Level*
SAES-J-400	*Temperature*
SAES-J-600	*Pressure Relief Devices*
SAES-J-602	*Burner Management, Combustion and Waterside Control Systems for Water Tube Boilers*
SAES-J-603	*Process Heater Safety Systems*
SAES-J-604	*Protective and Condition Monitoring Equipment for Rotating Machinery*
SAES-J-901	*Instrument Air Supply Systems*
SAES-J-902	*Electrical Systems for Instrumentation*
SAES-L-108	*Selection of Valves*
SAES-Z-001	*Process Control Systems*

Saudi Aramco Materials System Specifications

04-SAMSS-051	*Ball Valves, API SPEC 6D*
04-SAMSS-052	*Ball Valves, API SPEC 6A*
34-SAMSS-621	*ESD Systems – Hardwired – Solid-State, Non Programmable*
34-SAMSS-622	*ESD Systems – Electromagnetic Relay*

34-SAMSS-623	*Programmable Controller Based ESD Systems*
34-SAMSS-624	*Wellhead Control, Monitoring and Shutdown Systems*
34-SAMSS-634	*Local ZV Control Systems*
34-SAMSS-716	*Pneumatic Actuators On-Off Service*
34-SAMSS-717	*Hydraulic Valve Actuators Systems*
34-SAMSS-718	*Electric Motor Operated Valve Actuators*

Saudi Aramco Standard and Library Drawings

DE-950065 Sht 1	*Local Shut-Down Cabinet with Partial Stroke Test for Double Acting Actuators*
DE-950065 Sht 2	*Local Shut-Down Cabinet with Partial Stroke Test for Single Acting, Spring Return Actuators*
DB-950106 Sht 1	*Smart ZV – Single Acting Actuators*
DB-950106 Sht 2	*Smart ZV – Double Acting Actuators*

Saudi Aramco Engineering Report

SAER-5437	*Guidelines for Conducting HAZOP Studies*

3.2 Industry Codes and Standards

American Petroleum Institute

API SPEC 6FA	*Specification for Fire Test for Valves*
API SPEC 6D	*Specification for Pipeline Valves*
API RP 521	*Guide for Pressure-Relieving and Depressuring Systems*
API STD 598	*Valve Inspection and Testing*
API STD 607	*Fire Test for Soft-Seated Quarter-Turn Valves*
API STD 670	*Vibration, Axial Position, and Bearing Temperature Monitoring Systems*

British Standards

BS 6755 Part 2	*Testing of Valves*

National Fire Protection Association

NFPA 70	*National Electrical Code (NEC)*

The Instrumentation, Systems, and Automation Society (ISA)

ANSI/ISA S5.2	*Binary Logic Diagrams for Process Operations*
ANSI/ISA S18.1	*Specifications and Guides for the Use of General Purpose Annunciators*
ANSI/ISA S84.01	*Application of Safety Instrumented Systems for the Process Industries*

The International Electrotechnical Commission (IEC)

IEC 61511	*Functional Safety – Safety Instrumented Systems for the Process Industry Sector*

4 Definitions

4.1 Abbreviations

CPU	Central Processor Unit
DCS	Distributed Control System
DMR	Dual Modular Redundant
EFS	Electrical Fail-safe
EIV	Emergency Isolation Valve
ESD	Emergency Shutdown System
HAZOP	Hazards and Operability Study
HIPS	High Integrity Protective System
I/O	Input/Output
HMI	Human Machine Interface
MOV	Motor Operated Valve
OPC	Object Linking and Embedding for Process Control
PFD	Probability of Failure on Demand
RTD	Resistance Temperature Detector
SIL	Safety Integrity Level
SIF	Safety Instrumented Function
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
TMR	Triple-Modular Redundant ESD System
UPS	Uninterruptible Power Supply
ZV	Power Operated Emergency Isolation Valve

4.2 Terms

Dual Modular Redundant (1oo2D) ESD System: An ESD system which uses two separate processors each with its own separate I/O modules, bus structure, chassis, software and power supplies, to vote input signals in a 1oo2 arrangement. Sensor signals are separated into two isolated paths to two separate input modules where signals are conditioned and communicated by separate busses to separate processors. A valid input signal on either leg of the system will initiate the desired logic response via two separate, fail-safe, output modules.

Emergency Depressuring System: A system of valves, piping, actuating devices, and ESD logic used during an emergency to rapidly and safely reduce pressure in process equipment by controlled venting to a disposal system such as a flare, burn pit or storage. Logic for automated emergency depressuring systems resides within an ESD system. Refer to API RP 521, Guide for Pressure-Relieving and Depressuring Systems, for design guidelines.

Emergency Isolation Valve (EIV): A valve that, in event of fire, rupture, or loss of containment, reverts to a fail-safe position to stop the release of flammable or combustible liquids, combustible gas, or potentially toxic material. An EIV can be either hand-operated or power-operated (air, hydraulic, or electrical actuation). A power-operated EIV is commonly designated as a ZV in piping and instrumentation drawings and the two terms can be used interchangeable for the purposes of this standard. ZVs can be actuated either by an ESD system or by a local and/or remote actuating button, depending on the design of the facility. Application guidelines for applying hand-operated or power operated EIVs are listed in SAES-B-058.

Emergency Shutdown System (ESD): A system composed of sensors, logic solvers, and final control elements for the purpose of taking the process, or specific equipment in the process to a safe state when predetermined conditions are violated. The system is designed to isolate, de-energize, shutdown or depressure equipment in a process unit. Another term commonly used throughout the hydrocarbon and petrochemical industry is a Safety Instrumented System (SIS).

ESD Loop: A safety instrumented function consisting of input devices, logic solver and final output devices. Another term commonly used throughout the industry is a Safety Instrumented Function (SIF).

Fail-Safe: The capability to go to a predetermined safe state in the event of a specific malfunction.

Fault-Tolerant System: A system incorporating design features which enable the system to detect and log transient or steady-state fault conditions and take appropriate corrective action while remaining on-line and performing its specified function.

First Out Alarm: ESD logic that discriminates from a group of inputs the input that tripped first to cause a shutdown.

HAZOP: A systematic, detailed analysis technique applied to processes to identify hazards which have the potential to place the process plant, environment or personnel at risk. The HAZOP study identifies abnormal process deviations that may require additional protective functions. The HAZOP analysis shall follow the guidelines of SAER-5437, Saudi Aramco HAZOP Engineering Report.

High Integrity Protective Systems (HIPS): High availability, fail-safe SIL-3 ESD systems, designed to augment safety relief devices or mitigate worst-case relieving loads, or that function in lieu of over-pressure protective devices in wellhead, flare, or off-sites pipelines.

Probability of Failure on Demand (PFD): A value that indicates the probability that a device or system will fail to respond to a demand in a specified interval of time. PFD equals 1 minus availability.

Process Critical Equipment: Rotating equipment including turbines, electric driven pumps, compressors or generators handling combustible, flammable or toxic materials and use drivers equal to or greater than 1,000HP. Process critical equipment also includes rotating equipment that is categorized as critical by a process hazards analysis.

Process Safety Time: The period of time between a trip point being reached and a hazardous event occurring if no safety measures such as a shutdown are taken.

Proven-in-use: When a documented assessment has shown that the device, based on previous use, is suitable for use in ESD systems.

Safety Availability: The fraction of time that a safety system is able to perform its designated function when the process is operating. The safety system is unavailable when it has failed dangerously or is in bypass. Safety availability is equal to 1 minus the PFD (dangerous) of the safety function.

Safe State: The predetermined safe position of the process equipment device under control, as determined by operational experience, a preliminary hazards analysis or formal HAZOP study. Unless otherwise specified, the safe-state is

"de-energized" i.e., without power, pneumatic, or hydraulic supply.

Safety Integrity Level (SIL): The level of overall availability for an ESD loop or ESD system component calculated as 1 minus the sum of the average probability of dangerous failure on demand.

SIL-1: availability of 90-99%

SIL-2: availability of 99-99.9%

SIL-3: availability of 99.9-99.99%

Safety Life Cycle: The sequence of activities involved in the implementation of ESD systems from initial conception through to decommissioning (refer to ANSI/ISA S84.01 and IEC 61511).

Safety Requirements Specification: The specification that contains the requirements of the safety instrumented functions that have to be performed by the ESD system and include a list of ESD loops, their respective SIL assignment, a description of the logic function and the trip setting.

Shall: Indicates a mandatory requirement.

Smart ZV: A "Smart" ZV is a pneumatically operated emergency isolation valve that utilizes smart valve positioner technology to improve the diagnostic coverage and testing capabilities of ZVs. Reference library drawings are DB-950106 Sht. 1 & 2, Smart ZV – Single and Double Acting, respectively.

Triple Modular Redundant (2003) ESD: Fault tolerant systems using 3 separate processors with triplicated I/O and bus structure. Each processor executes its individual application program, simultaneously verifying data, executing logic instructions, control calculations, clock and voter/synchronization signals and performing comprehensive system diagnostics. Process outputs are sent via triplicated paths to output modules where they are voted (2oo3) to ensure logic and output integrity.

5 General Design Guidelines

Saudi Aramco ESD systems consist of four Layers of Shutdown and/or isolation as described below. Non-ESD logic may exist in the regulatory control system to apply process interlocks and alarms.

5.1 Description of ESD Layers of Shutdown

TOTAL PLANT SHUTDOWN: A total plant ESD effectively shuts down the total plant or facility under emergency conditions. Isolation valves are closed to

stop the flow of combustible, flammable or potentially toxic fluids, stop the heat input to process heaters or reboilers, and rotating equipment. Activation of total plant ESD will not stop or impede the operation of fire protection or suppression systems, deluge systems, sump pumps, or critical utilities such as instrument or process air.

UNIT ISOLATION AND DEPRESSURING: This shutdown layer isolates an entire process unit, process train or process area involved in a fire or other emergency, thus limiting the supply of fuel. This includes pumps, vessels, compressors, etc., which comprise an entire process unit up to and including plot limit boundaries. Associated emergency depressuring systems for process vessels and equipment shall be applied when it is necessary to reduce the potential of a boiling liquid expanding vapor explosion (BLEVE), or to reduce inventories of hazardous materials.

EQUIPMENT ISOLATION SYSTEM: A system of emergency isolation valves used to isolate individual equipment within a process unit and prevent the release or potentially toxic material in the event of fire, rupture or loss of containment.

EQUIPMENT PROTECTION SYSTEMS: Systems provided for the protection of centrifugal pumps, rotating and reciprocating gas compressors, gas expansion and combustion gas turbines (CGTs), electric motors, generators; and forced or induced draft air fans. Equipment protection systems may be supplied as part of the ESD, DCS, PLC or auxiliary control system (refer to SAES-J-604).

5.2 Safety Integrity Levels (SIL)

SIL-1, 2, and 3 assignments shall be made for each ESD loop based on the criteria and requirements listed in paragraph 5.3 or by completing a risk analysis in conjunction with a HAZOP using the methodology described in ANSI/ISA S84.01 and IEC 61511. If a risk analysis indicates a different SIL than the SIL specified in paragraph 5.3, the SIL assigned by the risk analysis shall be used.

Exception:

Application of ANSI/ISA S84.01 and IEC 61511, including SIL determination and verification, is not required for watertube boiler safety systems based on SAES-J-602 nor on process heater safety systems based on SAES-J-603.

5.3 Safety Integrity Level (SIL) Determination

5.3.1 SIL-1 Applications:

a. All process ESD applications including battery limits isolation for hydrocarbon lines and fire-hazardous pumps and compressors.

b. Emergency depressuring or liquid pull-down systems (either automatic or manually initiated) used to rapidly and safely reduce pressure in process equipment.

c. Process critical rotating machinery equipment protection systems including displacement, vibration, lubrication and seal fluid minimum flow, pressure and leakage systems.

5.3.2 SIL-2 Applications:

a. Critical high pressure, high temperatures and/or catalytic reaction processes that involve a high probability of capital, personnel or environmental risk during startup, shutdown or nuisance trip situations.

5.3.3 SIL-3, Applications:

a. High integrity protective systems (HIPS) that are used in lieu of a separate mechanical over-pressure protective device such as a pressure relief valve.

b. Flare gas load mitigation systems.

c. Wellhead shutdown systems for high pressure, sour gas wells (e.g., Khuff gas).

5.4 Segregation

5.4.1 ESD systems, associated logic and alarms shall be designed such that they are segregated from, and totally independent of other regulatory control and monitoring systems.

5.4.2 Interfaces between ESD systems and regulatory controls shall be performed in a discrete, hardwired manner or via an acceptable data communications interface, per paragraph 7.9.

5.4.3 Startup permissive signals and valve/pump status signals that are not shutdown initiators are considered non-ESD and may use simplex I/O circuitry.

5.5 Failure Modes

ESD systems and their associated loops shall fail to the safe state or position upon loss of the ESD signal, electric power, pneumatic or hydraulic supplies. The safe state shall be the de-energized mode unless otherwise documented by a process hazards or risk analysis, operational experience or licensor agreements. ESD modules, subsystem components, sensors and final control elements shall be specified and configured so that when de-energized they will fail to a defined

safe state or position, for example with valves the defined failure position may be fail-open, fail-closed or fail-steady. The failure mode of the sensors and final control elements shall be clearly indicated on the respective instrument specification sheet.

5.6 High Integrity Protection Systems (HIPS)

HIPS shall use a dedicated ESD system unless otherwise determined by the HIPS committee. Multiple HIPS applications may reside in the same HIPS logic solver. Refer to SAEP-354 procedures for the application, design and documentation of HIPS.

6 Input Devices

This section provides the criteria for the design and selection of input devices to be used for ESD service which includes transmitters, transducers, process activated switches, push/pull buttons and relays.

6.1 Design Criteria for Input Devices

6.1.1 ESD input devices shall be "smart" digital or analog transmitters unless they are not suitable for the intended process service or measurement application.

6.1.2 ESD input sensors shall meet or exceed all specified process and environmental conditions. ESD sensors shall be capable of being monitored and tested while in-service.

6.1.3 ESD sensors shall be reliable and purchased from approved vendors listed in SAES-J-002.

6.1.4 "Smart" ESD transmitters shall be write-protected at the transmitter to prevent inadvertent modification.

6.1.5 A diagnostic alarm for an ESD input device failure (i.e., short circuit, high range, frozen signal, open circuit and low range) shall be configured using signal over and under range limits and indicated to the operator as a high priority alarm on his workstation/HMI so that immediate corrective action is taken to have the transmitter repaired or replaced.

6.1.6 ESD transmitters shall be configured to have a defined failure mode, i.e., in the direction opposite to the trip setting or in the direction of the trip setting.

6.1.7 The transmitter failure mode and ESD transmitter validation logic shall be applied to minimize spurious trips and spurious alarms. In addition

the use of filters for transmitter validation and time delays to shutdown shall not compromise the intended function of the ESD loop under all transmitter failure scenarios.

Commentary:

Time delay shutdowns may be used to ensure that operators take action to repair or replace faulty ESD transmitters. When time delays are applied they should provide the operator with sufficient time to respond to the alarm. The typical values used for time delay shutdown are less than 60 minutes.

6.1.8 ESD transmitters which are voted in ESD logic (i.e., 1oo2, 2oo2 or 2oo3) shall be configured to fail in the direction of the trip.

6.1.9 Discrete hard-wired, ESD push/pull buttons shall be configured as direct, normally closed inputs into shutdown logic. ESD buttons installed in outdoor environments shall only use hermetically sealed or totally encapsulated switch assemblies and contact blocks to avoid degradation of switch contact surfaces in dusty, humid or corrosive environments.

6.1.10 ESD loops using thermocouple or RTD inputs shall incorporate burnout or open-circuit protection logic. Unless otherwise stated in the SRS, a thermocouple or RTD burnout causing open circuit shall initiate an ESD trip signal.

6.1.11 Thermocouple inputs shall use temperature transmitters wired to ESD I/O modules.

6.1.12 Process actuated switches shall only be used when "smart" ESD digital or analog transmitters are not suitable for the intended process service or measurement application. Process actuated switches shall be selected to be closed during normal process operation and shall open when the shutdown condition is reached.

6.1.13 Proximity or micro-switches used as ESD input devices shall be hermetically sealed or totally encapsulated to avoid the degradation of contact surfaces in dusty, humid or corrosive environments.

6.1.14 When a pressure switch is used, a pressure gauge shall be installed on the same side of the process block valve as the pressure switch and have its own isolation valve.

6.1.15 ESD input devices shall be clearly identified in the field from conventional regulatory control instrumentation. Acceptable methods of identification are a fixed label containing the tag description in printed/embossed white writing on a red background or marking the

instrument terminal cover red. It shall be obvious from a distance, to both maintenance and operations that these devices are part of the ESD system.

6.2 Process Taps and Connections

An ESD sensor shall have its own dedicated process tap or connection separate from a process control or monitoring instrument. Each transmitter shall be capable of being calibrated in-service independently.

ESD level inputs shall have separate process taps located at the same elevation as the process control and monitoring transmitter taps. ESD level transmitters shall be calibrated for the same range as the process control level transmitter and designed with its own local level sight gauge and drain/vent valves.

Exceptions:

Differential pressure transmitters used for ESD and process control service may be installed in parallel using the same primary element (e.g., orifice plate, venturi, and flow nozzle) provided they have independent process isolation valves. Individual transmitters shall be capable of being isolated while the other remains in service.

ESD Level transmitters may use the same process taps as the process control or monitoring transmitters when the tap nozzle size is at least 2 inches, the process is non-plugging and the common isolation valves on the tap nozzle are car sealed open. In addition, ESD and process control level transmitters shall have independent level bridle isolation valves and shall be calibrated for the same range. The ESD and process control/monitoring level transmitters shall be designed with local level sight gauge and their own drain/vent valves to allow independent isolation and calibration while the other remains in service. See SAES-J-300 for additional level requirements.

6.3 Multiple ESD Functions

A single transmitter may be used to provide both Low-Low (LL) and High-High (HH) ESD input signals if that the transmitter's calibrated range spans both LL and HH trip settings, and that it is acceptable to bypass both LL and HH inputs at the same time when performing maintenance on the transmitter.

6.4 Redundant ESD Devices

6.4.1 Multiple process measuring devices (dual or triplicated) shall be used when the findings of a process hazards analysis recommend the use of multiple devices or when calculations show that the reliability (MTBF) or the safety availability (1-PFD) of a single instrument is unacceptable.

6.4.2 Process applications involving the use of multiple, voted input devices include:

a. LL instrument air header pressure which initiates a plant or module ESD. Refer to SAES-J-901.

b. Equipment Protection systems involving dual radial, x-y, displacement/vibration sensors, axial thrust sensors, bearing temperature sensors, lubrication and seal fluid sensors, and speed pickups used for stopping or to govern rotating equipment which is process critical. Refer to SAES-J-604.

c. Boiler-steam drum LL/HH level measurement: Three separate transmitters shall be used to measure steam drum level. Two of these devices may be used in conjunction with the drum LL or HH level switch in a 2oo3 voting scheme to trip the boiler on loss of level, or liquid carry-over. Refer to SAES-J-602.

d. HH level measurement in refrigerated and/or pressure storage vessels such as LPG vessels. Multiple level transmitters are used both for measurement and alarm purposes as well as for shutdown. Refer to SAES-B-057.

6.4.3 Voted input signals shall be assigned to separate input modules when they are available.

Commentary Note:

When using 2oo3 input voting, one of the three ESD inputs may utilize an isolated output signal from a regulatory control or process monitoring instrument providing it meets the requirements detailed in Section 6.1.

6.5 Time Delays and Filters

6.5.1 The justification for applying a time delay or filter to an ESD input shall be based on an analysis of:

a. Process variable dynamics (i.e., the transient behavior of the process that may require filtering or the use of a time delay).

b. Mechanical noise or vibration which contributes to unreliable or spurious ESD device trips.

c. The proximity of an ESD device operating point to its trip setting that might result in a spurious or premature device trip when a process disturbance or transient is encountered.

d. Sensor response time characteristics such as inherent sensor lag, dead-time or signal dampening.

6.5.2 If an analysis of an ESD device's operating history or trip report data reveals that a filter or time delay element is needed to prevent spurious ESD trips resulting from process transients or disturbances, an adjustable time delay element shall be inserted within the ESD application program to condition the respective ESD input.

6.6 Shutdown and Reset Buttons

6.6.1 ESD Shutdown Buttons

6.6.1.1 Push or pull buttons shall be used to manually initiate a shutdown, and shall be readily accessible to operations personnel, either within an operator's console HMI, in a strategic location inside the control room, and within the process facility itself as per SAES-B-058.

6.6.1.2 ESD push buttons shall be provided with an extended guard, shroud or similar feature to reduce the risk of accidental actuation. Pull buttons do not require a physical protective guard or shroud.

6.6.1.3 Software configured ESD push buttons initiated from an operator's workstation are acceptable provided that a physical, hard-wired button is provided elsewhere on the console or within his work area, which accomplishes the same function. In addition, the communication guidelines of paragraph 7.9 shall be followed and the ESD shutdown command shall include an associated confirmation step before the ESD command is executed.

6.6.1.4 ESD logic shall be configured such that the momentary actuation of the ESD push or pull button will initiate a shutdown.

6.6.1.5 The re-energization of ESD system logic and output devices shall only be permissible by separate, manual reset action. Automatic reset action for ESD logic manipulating final shutdown elements is not permissible.

6.6.1.6 Actuation of a manual ESD push/pull shutdown button or software-configured ESD shutdown button in an electronic system shall initiate an event log to time-tag the actuation of the ESD button by its specific tag number and descriptor.

6.6.2 ESD Reset Buttons

6.6.2.1 ESD logic shall be designed such that if it is de-energized for any reason, it can only be reset or reenergized by deliberate, momentary actuation of a reset button. If an ESD system has been reset or is in its normal operating state, the reactivation of its reset button shall not result in any abnormal transient or change of state within the ESD logic.

6.6.2.2 For programmable electronic ESD systems reset buttons shall be initiated from an operator's workstation HMI and adhere to the communication guidelines of paragraph 7.9.

6.6.2.3 Actuation of a manual reset push button in an electronic system shall also initiate an event log, to time-tag the actuation of the reset by its specific tag number and descriptor.

6.6.2.4 For non programmable ESD systems a reset push button shall be located in close proximity to the ESD shutdown push/pull button within the operator's console/HMI.

6.6.2.5 Resetting ESD system logic shall not cause a ZV or other equipment to automatically return to its normal operating position or state.

6.7 ESD Input, Output and Startup Bypasses

6.7.1 ESD Input Bypasses

6.7.1.1 All shutdown sensing devices shall have an input bypass switch to facilitate maintenance or testing. Bypass switches shall be software-configured using a restrictive access mechanism such as a key lock or password with a separate confirmation step. Hardwired bypass switches shall only be used for non-programmable type ESD systems or where operator workstations are not available.

6.7.1.2 Activation of an input bypass switch shall confirm the bypass logic and cause an associated status light or graphic window to be illuminated. Activation or deactivation of a bypass switch shall initiate an alarm and in an electronic system shall initiate an event log which archives the change of state of the bypass switch with its tag number and descriptor.

6.7.1.3 Input bypass switches are not required for ESD transmitters that are voted in the ESD logic as 2oo2 or 2oo3.

6.7.1.4 Input bypasses shall not result in the loss of measurement and/or annunciation of the condition being monitored by the ESD.

6.7.2 ESD Output Bypasses

Output bypass switches shall not be used.

6.7.3 ESD Startup Bypasses

6.7.3.1 Automatic startup bypass shall be configured for devices which would prevent the normal startup of plant equipment such as minimum flow, level, pressure, temperature, motor load startup-current and vibration. Startup bypasses shall be automatically reset when the plant or equipment reaches normal operating parameters or when a prescribed time period has elapsed.

6.7.3.1 Activation or deactivation of an automatic startup bypass switch shall initiate an event log which archives the change of state of the bypass switch with its tag number and descriptor.

6.8 ESD Alarm and Pre-Alarm Requirements

6.8.1 Process Pre-Alarms

6.8.1.1 Process alarms which precede an ESD trip-point are required where there is sufficient time for the operator to take corrective action to stabilize the process or to prevent a plant shutdown. Process alarms shall be handled in accordance with SAES-Z-001.

6.8.1.2 Analog ESD signals shall not be used as regulatory control variables.

6.8.1.3 A pre-alarm may be generated from an ESD sensor when there is a backup or inferred measurement that allows the process to be monitored while the ESD sensor is in bypass or if maintenance can be done off-line.

6.8.2 ESD Alarm Annunciation

6.8.2.1 A shutdown initiating device shall be interconnected to a discrete, multi-point alarm annunciator or to an alarm annunciator display configured within the regulatory control system.

6.8.2.2 Annunciator logic and functionality shall perform first out alarm discrimination of ESD inputs.

6.8.2.3 ESD inputs shall be annunciated via a unique, audible alarm each time an ESD signal is initiated. The audible alarm shall continue to sound until acknowledged or reset by an operator.

6.8.2.4 Alarms shall be annunciated for failures to ESD auxiliary systems, including low instrument air pressure, loss of one or more power sources/supplies and loss of hydraulic pressure.

6.8.3 Output Validation, Verification and Annunciation

The change of state of the final ESD device shall be monitored by a separate field sensor such as limit switch, position transmitter or motor contactor auxiliary contact. ESD application programs shall compare ESD output commands with final device feedback signals and provide an event log and alarm when the final device does not reach the intended ESD state within an acceptable time.

6.8.4 ESD Annunciator Panels

6.8.4.1 Dedicated stand-alone annunciators shall only be used where regulatory control based alarm and annunciation systems are impractical or unavailable.

6.8.4.2 If dedicated, stand-alone annunciators are required, multi-point solid-state, or microprocessor-based annunciators shall be used. Annunciators shall be powered from a UPS and shall utilize solid state plug-in modules or cards with a minimum of 20% spare points and windows provided for new installations.

6.8.4.3 ESD input alarms shall be combined into first-out groups, within each ESD system, to distinguish between initial and subsequent alarms.

6.8.4.4 The visual display of annunciator windows used for ESD service shall have back-lit, red plastic windows on which the alarm identification is permanently marked or engraved in black letters. A minimum of two lamps shall be used for back-lighting.

6.8.4.5 A lamp-test push button shall be provided for each multi-point annunciator unit to permit a simultaneous test of all annunciator window lamps.

6.8.4.6 ESD annunciators shall incorporate a unique audible signaling device which is differentiated from a regulatory alarm, and which sounds each time an alarm signal is received. The audible ESD alarm shall continue to sound until acknowledged or reset by an operator.

6.8.4.7 The standard alarm annunciation sequence and functionality shall be as per ISA S18.1, Sequence No. F3A.

6.9 Recommended ESD Inputs and Process Measuring Devices

Shutdown devices are recommended in the following cases:

6.9.1 Low-Low Flow (Ref. SAES-J-100)

a. Centrifugal and positive displacement pumps to prevent overheating and subsequent pump failure from operating at flow rates less than the required minimum flow.

b. Inputs to reactors or converters where damage to the catalyst will result from the failure of feed gas flow.

c. Where damage to piping or heater tubes will occur due to reduced flow velocities.

6.9.2 Pressure (Ref. SAES-J-200)

6.9.2.1 Low-low pressure shutdown inputs are recommended for process equipment such as shipping or booster pumps which are susceptible to damage in the event of low-low inlet or outlet pressure.

6.9.2.2 High-high pressure shutdown inputs and alarms are recommended for:

a. All process systems containing flammable or toxic fluids and which are protected against process upsets by relief valves. The ESD trip setting shall be set below that of the relief valve, unless a process hazards analysis demonstrates otherwise.

b. Seal leakage detection systems on pumps.

6.9.3 Level (Ref. SAES-J-300)

6.9.3.1 Direct process actuated, float/displacer and cage type level switches may be used only by exception when process conditions preclude the use of transmitters. Level switches or

transmitters shall be capable of being isolated from process taps and incorporate a separate drain and vent valve for testing and calibration of the level device.

6.9.3.2 Low-low level shutdown inputs are recommended for any vessel where a loss of level would result in damage to process equipment or release of hydrocarbons, toxic or dangerous materials to atmosphere, e.g., sour water systems.

6.9.3.3 High-high level shutdown inputs are recommended for fuel gas scrubbers, compressor suction separators, or knock-out drums, or for vessels containing both liquid and vapor, where vapor is released to a fuel gas system or to the atmosphere.

6.9.4 Temperature (Ref. SAES-J-400)

6.9.4.1 Analog 4-20 ma DC output smart temperature transmitters with ambient temperature compensation are recommended for measuring ESD temperature signals.

Exception:

Capillary or bimetallic type, direct process actuated temperature switches (with associated indicating gauge) can be used where transmitters are not suitable.

6.9.4.2 Low-low temperature shutdown inputs are recommended for cases in which process upsets may cause operating temperatures to drop below the design limitations of process equipment or cause undesirable phase changes in process fluids.

6.9.4.3 High-high temperature shutdown inputs and alarms are recommended for:

a. Compressor and turbine lube-oil and outlet discharge temperatures.

b. Rotating equipment bearing temperatures.

c. Process vessels, reactors or converters where HH temperature excursions or process upsets may cause equipment malfunction, internal damage or unsafe operating conditions.

6.9.5 Vibration (Ref. SAES-J-604)

Radial shaft vibration monitoring, bearing housing vibration monitoring,

and axial position monitoring for rotating equipment protection systems (i.e., pumps, compressors, turbines and gearboxes) shall be in accordance with SAES-J-604 and API STD 670.

7 ESD Systems and Auxiliary Equipment

This section establishes the criteria for the design of ESD and the related auxiliary equipment such as power supplies and grounding.

7.1 Programmable Controller Based ESD Systems

Technically acceptable Dual Modular Redundant (1oo2D), or Triple Modular Redundant (2oo3), programmable controller based ESD systems shall be applied to SIL 1-3 safety shutdown functions. For specific material requirements for programmable controller based ESD systems, refer to 34-SAMSS-623.

7.2 Solid-state or Relay Based ESD Systems

Solid-state or relay-based, non programmable ESD systems, shall not be used unless prior written approval is obtained from the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran. For specific material requirements for solid-state or relay based ESD systems, refer to 34-SAMSS-621 or 34-SAMSS-622 respectively.

Approval for the use of relay-based ESD system is conditional on an evaluation meeting the following criteria:

a. An ESD system that involves a limited number of relays (typically, less than 50).

b. An ESD system that does not need to detect transient or steady-state errors or fault conditions, or incorporate self-diagnostic logic, or take appropriate corrective action, while remaining on-line to ensure fulfillment of its specified safety-shutdown function.

c. An ESD system that does not need to be interfaced to a DCS or other regulatory control system via a communications port(s).

d. An existing ESD system that requires minor modifications, but will not need to be substantially reconfigured, modified, or expanded at a future date.

e. An ESD system that utilizes mainly discrete input and output devices, with minimal timers, counters or analog devices.

7.3 Pneumatic, Hydraulic or Hybrid ESD Systems for Wellhead Shutdown

For specific material requirements for Wellhead Control, Monitoring and

Shutdown Systems refer to 34-SAMSS-624.

7.4 General Requirements for ESD Systems

7.4.1 Programmable controller based ESD systems shall be designed such that the input to output scan time (i.e., composite scan time) of the logic solver does not exceed 100mS. Using an alternative composite scan time for the logic solver requires the concurrence of the Manager, P&CSD based on a documented process safety time calculation and analysis of all ESD loops in the system. The selected scan time shall be less than the fastest process safety time required for the system.

7.4.2 Rotating machinery equipment which is not process critical may have the equipment protection logic implemented within the DCS, auxiliary system or an approved programmable ESD. When using an ESD system for equipment protection on non process critical rotating equipment simplex input and output circuitry may be used. Refer to SAES-J-604.

7.4.3 Gas detection shall not be implemented in an ESD system unless there is an intended shutdown function involved.

7.5 Power Supplies

7.5.1 ESD systems and field devices shall be powered from negative-leg, grounded power supplies that are in-turn, powered from separate branch circuits of UPS systems. Standard ESD logic voltage for system modules and field instrumentation shall be 24 VDC.

7.5.2 For minor additions or modifications to existing ESD systems, 120 VAC, 60 Hz, 48VDC or 125VDC power may be used to power ESD systems and field devices.

7.6 Sequence of Events (SOE)

A SOE utility within the ESD system shall time stamp and log the change of state of discrete ESD input devices, shutdown buttons, manual reset buttons, and the transition of analog/digital devices past shutdown limits. The event logs shall be time-stamped within 100mS, logged by device tag number and descriptor and provide a first out log.

7.7 Input and Output Signal Isolation

7.7.1 Individual input/output signal point isolation, if required, shall be accomplished by using I/O modules that incorporate individual point isolation. If discrete ESD input signals must be replicated prior to being input to an ESD input module, individual rail-mounted, optical isolators

shall be installed within ESD cabinets. Opto-isolator wiring and circuitry shall be passive and shall under no circumstances compromise ESD signal integrity.

7.7.2 If isolated solid-state outputs are used to achieve signal isolation, they shall be rated for the maximum load and in-rush current of the intended final device (e.g., motor control circuit contactor).

7.7.3 Relays shall be used for replication of ESD system inputs or outputs when solid-state isolation devices are incapable of meeting signal isolation specifications. Electric relays shall be dust-tight when installed in indoor and hermetically-sealed if installed outdoors.

7.8 Wiring Methods, Grounding and Ground Fault Detection Systems (GFD)

7.8.1 ESD wiring methods for connecting field devices to field junction boxes, through to marshaling cabinets shall be consistent with the requirements of SAES-J-902.

7.8.2 ESD equipment shall comply with NFPA 70 requirements and be referenced to plant instrument ground. ESD system grounds shall consist of separate, isolated ground buses to handle specific requirements for AC safety grounds and signal wiring shields/DC reference grounds.

7.8.3 Ungrounded or floating ESD systems shall not be used except where modifications are required to existing ungrounded systems or equipment and require the concurrence of the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

7.8.4 Process facilities using ungrounded DC supply voltages for ESD systems shall incorporate GFD systems to monitor leakage current to ground. GFD circuitry shall be designed to continuously monitor floating electrical circuits within field wiring and alert maintenance personnel, via an integral alarm indicator (LED or lamp) and a set of contacts routed to an annunciator, when resistance to earth falls below a nominal 1 K ohms.

7.8.4.1 Commercially available modular type GFD components shall be used for GFD systems. GFD should be performed on an individual loop basis to be able to discriminate line faults for a maximum grouping of 40 I/O points per GFD module.

7.8.4.2 The ground fault detector shall be capable of detecting independent ground faults for different groups of points, without adversely affecting other point groupings, when using

the same power supply. Potential faults or failures within GFD modules, circuitry or external wiring shall in no way compromise the integrity of ESD inputs and outputs.

7.9 Communication between Systems

7.9.1 No restrictions are placed upon the transmission of READ-ONLY data from an ESD system to an external DCS or auxiliary control system.

7.9.2 ESD bi-directional communication paths and devices used to transmit READ-WRITE data such as time synchronization signals, ESD input bypass requests, ESD shutdown or reset commands shall comply with the following:

7.9.2.1 Communication paths and devices shall be dedicated, functionally redundant, utilizing electrically and physically isolated communications interfaces, with automatic fail-over to a healthy communications channel.

7.9.2.2 Communication interfaces shall be off-the-shelf, using existing, industry standard media and communications protocols such as OPC, Modbus or Ethernet.

7.9.2.3 The protocol data message transmission shall incorporate error checking schemes such as Cyclical Redundancy Checking (CRC), Longitudinal Redundancy Checking (LRC) or Check Sums, in conjunction with bit parity checks, fail-safe transmission time-out, message fault words, and loss of communication path alarms.

7.9.2.4 The ESD operating system and application program is write-protected, such that CPU is protected from alteration by a combination of either data locking devices, key lock, or password security techniques.

7.9.2.5 Source password or key lock protection, in conjunction with a separate confirmation acknowledge step is required to accept bypass commands.

7.9.2.6 The normal operation of the ESD system shall not be impaired by any communication path or device failure.

7.9.3 No changes shall be allowed to ESD application programs via an external communications interface.

8 Final Shutdown Devices

Final shutdown instruments generally consist of two distinct classes of devices:

a. Power-operated emergency isolation valves (ZVs) that prevent the flow of process fluids, (i.e., hydrocarbons, hydrogen, cryogenics, etc.) or toxic materials into or out of a vessel, pipe, or a process plant/unit, or

b. Interposing relays or energy interruption devices. These are devices which safely and reliably interrupt the flow of energy or power to a particular piece of equipment or process area, e.g., motor starter cutouts for electric driven motors, safety shutoff valve for steam or combustion driven turbines, safety shutoff valve for the heat input to reboilers or direct-fired process heaters, etc.

8.1 ZV Guidelines

This section establishes the criteria for the design and selection of ZV assemblies consisting of the valve and actuator, with the associated control equipment such as limit switches, solenoid valve and positioner.

8.1.1 Mandatory requirements for applying, locating, and fireproofing power operated emergency isolation valves and their integral control components such as limit switches are provided in SAES-B-006, SAES-B-009, SAES-B-058 and SAES-B-070.

8.1.2 Valve selection guidelines in this standard are supplemental to the requirements found in SAES-L-108.

8.1.3 ZV actuator selection guidelines are provided in this standard, however for more detailed design requirements refer to 34-SAMSS-716 for pneumatic actuators, 34-SAMSS-717 for hydraulic actuators, and 34-SAMSS-718 for electric actuators.

8.2 ZV Design Criteria

8.2.1 ZVs shall be suitable for the specific application and supplied as an integrated assembly of valve and actuator, with the associated control equipment such as limit switches, solenoid valve and positioner.

8.2.2 ZVs shall meet or exceed all specified process and environmental conditions. Materials shall be carefully chosen to ensure reliable valve operation within the intended service and based on extended periods of time where the valve remains in the one position. ZV components shall not require periodic external or internal lubrication to ensure reliable operation.

8.2.3 ZVs shall move to the defined fail-safe position upon loss of ESD signal, electric power, instrument air or hydraulic supply. The fail-safe position shall be determined based on the operational impact, preliminary hazards analysis or HAZOP analysis.

8.2.4 ZVs shall be designed and installed with the ability to be tested in-service using a partial or full stroke test.

8.2.5 A full functional test of the assembled ZV (valve, actuator, and controls) shall be performed in the factory prior to shipment.

8.2.6 ZVs specified with spring return actuators do not require fire proofing of the actuator or local controls. When a ZV is located in or above a fire-hazardous zone then a fusible plug on the air signal or fusible link shall be installed within 1 meter of the spring return actuator to move the valve to the fail-safe position in the event of a fire.

8.2.7 Double-acting ZV actuators shall meet the fire-proofing requirements of SAES-B-006 when located in or above a fire-hazardous area.

8.2.8 ZVs shall be clearly identified in the field from conventional regulatory control instrumentation. An acceptable method of identification is a fixed label containing the tag description in white printed/embossed writing on a red background. It shall be obvious from a distance, to both maintenance and operations that these valves are part of the ESD system.

8.2.9 Regulatory control valves installed in series with ZVs to manipulate a fuel supply, a heat source, or a toxic fluid shall be interlocked with ZV logic such that when the ZV is commanded to close, the control valve is placed in manual and its output is forced to the fail-safe position by a command to a regulatory control software interlock.

8.3 Emergency Shutdown Valve Selection

The type of valve shall be selected based on the specific process conditions and required function. Although high performance butterfly valves (triple eccentric) have lower actuator torque and size requirements, the ZV valve selection may result in the use of axial flow, ball, or gate/globe valves depending on the service requirements.

8.3.1 Valves shall meet construction, materials requirements of SAES-L-108 and the supplemental requirements of this standard.

8.3.2 As stipulated in SAES-L-008, ZVs shall be gate, ball, high performance butterfly (flanged) or plug valves. Soft seated valves shall be fire-safe in accordance with API STD 607, API SPEC 6FA, or BS 6755 Part 2.

Metal seated valves shall meet the same requirement if they do not have graphite seals or their standard specified leakage rate exceeds that of API STD 598.

8.3.3 Metal seated valves shall meet the leakage rates specified in API STD 598 or API SPEC 6D.

8.3.4 Soft seated ZVs shall be zero leakage per API STD 598 or API SPEC 6D.

8.3.5 Valves shall be purchased from approved manufacturers listed in SAES-L-102 that have documented reliability data for the ZV components (valve and actuator). The selected valve and actuator assembly shall be proven-in-use for the intended process application.

8.3.6 Ball valves shall be trunnion mounted to minimize torque requirements and the potential for valve sticking. Refer to the applicable specification for ball valve requirements 04-SAMSS-051 and 04-SAMSS-052.

8.4 ZV Actuators

8.4.1 Fail-safe ZV actuator systems shall move the valve to the fail-safe position upon loss of ESD output signal, electrical power, instrument air or hydraulic pressure. Acceptable fail-safe actuators are spring return pneumatic actuators, spring return electric actuators (EFS MOV) and spring return hydraulic (electro-hydraulic).

8.4.2 Double-acting actuators with back up air supply tanks shall only be considered when spring return fail-safe actuators cannot be used (due to valve size and torque requirements) or when fail-steady action is required.

8.4.3 Motor operated ZV actuators which do not utilize spring-return mechanisms in the event of loss of power, or electrical component failure, are not considered to be fail-safe and shall only be used in ESD applications requiring a fail-steady response. ESD commands shall override all integral MOV selector switch signals except when the integral MOV selector switch is switched to its 'off' position. When used as a ZV, a MOV shall provide an 'off-line' signal to the ESD system when its local selector switch is located in its 'off' position.

8.4.4 ZVs shall have open and close position indication mounted on the valve actuator which is clearly visible to an operator located near the valve.

8.4.5 ZVs shall be equipped with open and closed limit switches. The ZV limit switches shall be hardwired as inputs to the ESD logic when they are required to verify ESD close and open commands or provide an

interlock to other ESD logic. The ZV limit switch position shall be annunciated to the operator's console HMI.

8.4.6 ZV actuators shall be provided with integral hand-wheels or hydraulic hand pumps for manual (open/close) operation. Manual hand-wheels or backup hydraulic operators shall be capable of being locked out or car-sealed. Automatic operation of the actuator shall not overrule manual actuator operation. Chain-wheel operation shall not be used. Refer to SAES-B-058.

8.4.7 ZV closure speed shall be as rapid as is practical for the specific process application. Refer to SAES-B-058 and SAES-B-064 for specific valve closure requirements. Careful attention shall be given to pipeline applications in order to avoid potential surge and or water hammer effects resulting from sudden valve closure.

8.5 Power Sources for Alternative ZV Actuators

When a fail-safe spring-return actuator is not used, an independent and reliable backup energy source shall be provided. The alternative power sources in this section are considered to be reliable and independent:

8.5.1 Compressed air stored in a dedicated, separate air storage drum, located in close proximity to a double-acting, piston-operated emergency isolation valve, sourced to an instrument air header via double non-return, check valves.

8.5.1.1 An air storage drum shall be sized to move the ZV from the normal operating position to the fail-safe position, return the ZV to the normal operating position, and move the ZV to the fail-safe position (three strokes). The tank shall be sized based on a starting air pressure of 690 kPa (100 psig) and a final pressure of 415 kPa (60 psig).

8.5.1.2 Only one emergency isolation valve (ZV) shall be connected to an air storage drum.

8.5.1.3 Safety relief valves (PZVs) are not required for air storage drums provided they are sized for a fire case and the instrument air is dry with maximum dew point of -20°C. (Refer to SAES-J-600).

8.5.1.4 Air storage drums shall incorporate a drain valve, redundant series inlet check valves and a local pressure gauge. If the media is not dry instrument air or gas, a rechargeable drier or

filter separator assembly shall be included upstream of the drum inlet.

8.5.2 Hydraulic fluid reservoir capable of moving the ZV to the fail-safe operating upon loss of utility supply, providing there is a reliable power source, hand-pump, or power pack available for re-charging the hydraulic system.

8.5.3 Process gas or other suitable compressed gas supplies shall be used only in remote locations where no other alternatives are possible. Where gas cylinders are used, provision shall be made to monitor cylinder outlet/header pressure, with a local or remote indicator to alert operations personnel of low pressure.

8.6 ZV Local Control

8.6.1 ZVs shall be provided with local control and testing features as outlined in 34-SAMSS-634.

8.6.2 Smart ZVs shall be used to provide local control and test facilities for pneumatically operated ZVs unless there is a technical limitation for the application that requires the use of electric-pneumatic local ZV shutdown cabinets.

8.6.3 ZVs shall be provided with a means to initiate and complete a partial or full stroke test on the valve. The partial or full stroke test shall be initiated from the local control panel. The test may also be initiated via an ESD hand-held communicator (via HART protocol), or using a laptop computer with vendor specified valve testing and diagnostic software.

8.6.4 The ZV shall remain in-service during a partial or full stroke test. In the event that a shutdown signal is initiated during testing, the ZV shall move to the defined failure position (closed, open or steady).

8.6.5 The local control station shall provide the means to close a normally open ZV in the field and re-open a fail-closed ZV after an ESD system reset.

8.6.6 Resetting ESD system logic shall not cause a ZV or other equipment to automatically move to the normal operating position. Local operator intervention is required at a ZV's local control station to re-open a ZV following a trip.

8.7 Block and Bypass Valves

The installation of a full bypass valve in parallel with a ZV shall be determined

on a case-by-case basis with mutual agreement between the Proponent Operations, Loss Prevention Department and P&CSD.

8.7.1 A bypass valve installed for the purpose of in-service testing of a ZV shall be capable of being car-sealed closed and meet shut-off and fire-safety requirements of SAES-L-108.

8.7.2 Bypass or equalizing valves around ZVs shall be equipped with a sealed, proximity type limit switch, monitoring the valve "closed" position and providing an alarm remotely to the operator when the bypass valve is not closed. Local pressure and differential pressure gauges and/or transmitters shall be provided where pressure equalization is required prior to opening a ZV.

8.7.3 Unless otherwise prohibited an upstream block valve shall be provided for ZVs which fail-open such as for vapor depressuring and liquid pull down systems. The purpose of the upstream block valve is to permit in-service testing of the ZV.

8.7.4 An upstream block valve on a fail-open ZV shall be capable of being car-sealed open and be equipped with a sealed, proximity type limit switch, monitoring the 'open' position and providing an alarm remotely to the operator when the block valve is not open.

9 Documentation and ESD Validation

Documentation shall completely describe ESD functions and be kept up-to-date at all times.

9.1 Design Validation

9.1.1 A Safety Requirements Specification (SRS) shall be developed for each ESD system and consist of the documentation as listed in this section. The SRS shall be reviewed and concurred to by the Saudi Aramco Proponent Operating Department, Chief Fire Prevention Engineer, Loss Prevention Department and the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

9.1.2 SIL assignments for ESD loops shall be reviewed and verified during detailed engineering design. Verification of ESD SIL assignments shall be by calculation of the Probability of Failure on Demand (PFD) for each ESD loop.

9.1.3 SIL-3 applications shall include a quantitative analysis that examines the probability of failure on demand for the particular process application.

Prior to implementation, this analysis shall be reviewed and approved by the Saudi Aramco Proponent Operations, Chief Fire Prevention Engineer, Loss Prevention Department and the Manager, Process & Control Systems Department of Saudi Aramco, Dhahran.

9.2 Design Documentation (Ref. SAES-J-005)

The following documents shall be developed during project proposal or design phases and form the basis for the development, validation and testing of new or revised ESD application logic:

9.2.1 HAZOP analysis identifying or verifying the type, function and trip settings of protective instruments which function as required emergency shutdown inputs and outputs.

9.2.2 The ESD Safety Requirements Specification (SRS) consisting of the safety functional requirements and the safety integrity level assignment for each ESD loop. Information required in the SRS includes:

1. The list of all ESD Loops (Safety Instrumented Functions) and the corresponding SIL assignment.
2. The list of ESD I/O with device description, the trip setting and the defined fail-safe position or state.
3. A written description of each ESD loop which defines the required safety function with each input device and the corresponding shutdown trip setting. The written description shall provide sufficient detail to develop Boolean and application logic for the system.
4. A Cause-and-Effect matrix diagram which correlates ESD output actions (by device description and tag number) in response to process shutdown inputs (by instrument tag number, device descriptor and shutdown trip setting).
5. A Boolean or function block type logic diagram graphically showing ESD inputs, outputs and internal logic using conventional ANSI/ISA S5.2 logic elements as required by SAES-J-005.
6. The requirements for energize-to-trip and de-energize to trip functions.
7. The requirements for manual shutdown, resets and input bypasses.
8. Requirements for filters and timers.
9. Functional requirements in addition to the system material specification.
10. An ESD system block diagram.

10 Application Logic

10.1 The application logic and system configuration for programmable controller based systems shall consider the specific requirements documented by the manufacturer's safety installation guidelines and system alerts.

10.2 ESD logic shall be simple and understandable. Comments shall be inserted within ESD logic to explain the function of each network and be descriptive enough to allow maintenance and engineering to perform trouble shooting without having to revert to separate logic narrative.

10.3 Logic shall be grouped by plant, unit, area, equipment and equipment protection system. Logic shall be segregated for individual pumps, turbines, compressors, and process interlocks which are grouped together in a defined process configuration into different networks or files. Identical logic structures and elements (except for tag names and addresses) should be used for identifying ESD logic of equipment operating in parallel trains, or which are controlled in a similar manner.

10.4 The logic developer must be consistent in selecting and applying logic elements and developing a network structure which is consistent between similar types of application programs.

10.5 Soft copies of the latest version of the application programs, cross reference tables and other source code shall be stored in a secure location. A written procedure shall be in place at each operating facility detailing the backup requirements of the ESD system applications.

10.6 The assignment of input and output addresses shall minimize or prevent a potential failure of one module adversely affecting more than one critical piece of equipment of a parallel process train. The assignment of inputs to separate modules also applies to multiple ESD input devices that are voted in a 1oo2, 2oo2 or 2oo3 manner when more than one input module is available.

11 Testing

11.1 Emergency shutdown systems shall be designed so as to permit functional testing of field input devices, internal logic, and output devices without forcing a shutdown or the complete bypassing of the ESD system in order to accomplish the task.

11.2 Functional Test

A full functional test shall verify:

1. The operation, calibration and trip setting of all ESD input devices.
2. The logic associated with each ESD loop including input device, manual shutdown, reset bypasses and final control elements.
3. The logic associated with voted inputs.
4. Alarm functions, first out alarming and sequence of events.
5. The correct firmware version and the latest application program.
6. The requirements for manual shutdown buttons, reset buttons and input bypasses.
7. The correct function and installation of all hardware including I/O modules, main processors, communication modules, power supplies and grounding.
8. The correct function and installation of interfaces and communications to the regulatory control system.

11.3 Testing During Project Execution

11.3.1 A full functional test is required during the factory acceptance test and site acceptance test/commissioning.

11.3.2 A full functional test shall verify that the programmed application logic controls the action of inputs and outputs as per the logic defined in the Safety Requirements Specification.

11.3.3 ESD functional tests shall be witnessed and verified by representatives from the respective proponent engineering, maintenance and operating departments.

11.3.4 Project records shall be kept and forwarded to Operations, Maintenance and Engineering Departments which document the ESD logic, input device and final element testing, test results and exception item resolutions.

11.4 Periodic Testing of Shutdown Logic

11.4.1 ESD systems shall be periodically validated against their functional requirements specifications. The validation will typically be performed during the unit turnaround and consist of a verification of the ESD I/O and shutdown logic.

11.4.2 The ESD system may be omitted from a periodic test of the shutdown logic if there have been no major changes made to the logic (such as performing a download all), the operating shutdown logic program has

been compared to the control copy and is identical, and there has been no addition of ESD I/O into the logic since the last functional test on the shutdown logic.

11.5 Periodic Testing of I/O

11.5.1 Analog devices (such as transmitters, transducers, or trip amplifiers) used as ESD inputs shall be physically and functionally tested every 12 months by simulating a process input over the calibrated range of the device, and verifying the appropriate ESD logic and response to the final shutdown element.

11.5.2 Discrete ESD inputs such as process switches shall be physically and functionally tested every 6 months by simulating a shutdown signal by applying the appropriate process media.

11.5.3 ZV assemblies shall be partially stroked 10% to 20% of valve movement every 3 months to verify that the pneumatic, electrical, and mechanical components are correctly functioning.

11.5.4 ZV assemblies shall be fully stroked on a yearly basis when it is practical to do so, i.e., when a full ZV bypass is available, the process or equipment is spared or the process operations can be maintained. Test procedures shall confirm that the valve closes fully when the shutdown signal is initiated.

11.5.5 Calibration records and test results for ESD input devices or sensors, final elements, and internal ESD logic shall be documented and archived for permanent record. These records shall be made available for periodic plant maintenance audits and Loss Prevention Compliance Reviews.

12 Management of Change

12.1 A written procedure shall be in place at each operating facility detailing the requirements for the review and approval of all changes made to an ESD system.

12.2 Proposed changes to installed ESD systems, including the replacement of existing devices with different instruments, shutdown trip setting or logic changes or final control device modifications shall be subjected to thorough review and approval by qualified personnel from Operations, Engineering, Maintenance, Inspection, and Loss Prevention, with assistance from P&CSD, if necessary.

12.3 Proposed changes shall undergo simulation, or emulation, validation and testing before being commissioned and placed in-service.

12.4 The following steps shall be carried out prior to implementing any change within an existing ESD system:

12.4.1 HAZOP analysis of the process unit, equipment or process, identifying the intent and effect of the change to the existing ESD system. ESD loops shall be verified for instrument type, function, failure modes, trip setting and that the loop meets the assigned SIL.

12.4.2 Modification of the cause-and-effect matrix diagram which correlates ESD output actions (by device description and tag number) in response to process shutdown inputs (by instrument tag number, device descriptor and shutdown trip setting).

12.4.3 Preparation of the written description of each ESD loop which defines the required safety function with each instrument/device and the corresponding shutdown trip setting. The written description shall provide sufficient detail to develop a Boolean and application logic for the system.

12.4.4 Development of a Boolean or function block type logic diagram graphically showing ESD inputs, outputs and internal logic using and/or, timer, or counter logic elements with basic logic statements, comment blocks, tag numbers and device descriptions imbedded in the diagram which describe the intended functionality.

12.4.5 A written description of the work and steps involved in implementing the change, including any steps that might pose a risk to personnel, process equipment, to the environment, or to the local community.

Revision Summary

29 June 2005 Major revision.