



TECHNICAL REQUIREMENTS

AUTOMATION AND INSTRUMENTATION

Document No. OL-TR-IR-000

ESD, BMS

Document No. OL-TR-IR-012

05					
04					
03					
02					
01		2019-03-14	ORLEN Lietuva	ORLEN Lietuva	ORLEN Lietuva
00	Final Issue	18-Jun-14	D ² RT' <i>engineering</i>	ORLEN Lietuva	ORLEN Lietuva
Rev.	Revision description	Date	Prep. by	Check. by	Appr. by

TABLE OF CONTENTS

TABLE OF TABLES	3
TABLE OF FIGURES	4
1. SCOPE	5
2. REFERENCES	5
3. TERMS AND DEFINITIONS	6
4. PROGRAMMABLE LOGIC CONTROLLERS (PLCs) FOR ESD	6
5. BASIC DESIGN	9
6. LOGIC ARCHITECTURE	10
7. PROGRAMMABLE ELECTRONIC SYSTEMS (PES)	10
8. DOCUMENTATION	11
9. POWER	12
10. FIELD WIRING	13
11. SENSORS	13
12. FINAL ELEMENTS	13
13. FINAL ELEMENTS – SOLENOID VALVES	14
14. ARCHITECTURES	14
15. EMERGENCY STOP (SHUTDOWN) BUTTON	14
16. SMART SENSORS FOR ESD SYSTEM	14
17. SIL CLASSIFICATION AND INTERLOCK FUNCTION IMPLEMENTATION	15
18. SAFETY REQUIREMENT SPECIFICATION	15

TABLE OF TABLES

TABLE OF FIGURES

<i>Figure 1. High Reliability SIL 1 SIS. Example</i>	17
<i>Figure 2. High Reliability SIL 2 SIS. Example</i>	17
<i>Figure 3. High Reliability SIL 3 SIS. Example</i>	17

1. SCOPE

This Specification covers requirements for ESD, BMS.

2. REFERENCES

The latest editions of the following publications are to be used with this Specification as applicable:

LST EN 60079	<i>Electrical apparatus for explosive gas atmospheres. Elektriniai aparatai, naudojami potencialiai sprogiose atmosferose</i>
LST EN 60529	<i>Degrees of protection provided by enclosures (IP code) (IEC 60529)</i>
LST EN 61508-1	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems -- Part 1: General requirements (IEC 61508-1)</i>
LST EN 61508-2	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2)</i>
LST EN 61508-3	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements (IEC 61508-3)</i>
LST EN 61508-4	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations (IEC 61508-4)</i>
LST EN 61508-5	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels (IEC 61508-5)</i>
LST EN 61508-6	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (IEC 61508-6)</i>
LST EN 61508-7	<i>Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 7: Overview of techniques and measures (IEC 61508-7)</i>
LST EN 61511	<i>Functional safety. Safety instrumented systems for the process industry sector</i>
LST EN 61511-1	<i>Functional safety. Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements (IEC 61511-1)</i>

LST EN 61511-2	<i>Functional safety. Safety instrumented systems for the process industry sector. Part 2: Guidelines for the application of IEC 61511-1 (IEC 61511-2)</i>
LST EN 61511-3	<i>Functional safety. Safety instrumented systems for the process industry sector. Part 3: Guidance for the determination of the required safety integrity levels (IEC 61511-3)</i>
LST EN 62381	<i>Automation systems in the process industry - Factory acceptance test (FAT), site acceptance test (SAT) and site integration test (SIT) (IEC 62381)</i>
LST EN 62382	<i>Electrical and instrumentation loop check (IEC 62382)</i>
NAMUR NE 43	<i>Standardization of the Signal Level for the Failure Information of Digital Transmitters (NAMUR NE 43)</i>
OL-TR-GR-000	<i>General Requirements</i>
OL-TR-IR-000	<i>Automation and Instrumentation. General</i>

3. TERMS AND DEFINITIONS

For terms and definitions see:

OL-TR-IR-000 *Automation and Instrumentation. General*

4. PROGRAMMABLE LOGIC CONTROLLERS (PLCs) FOR ESD

- 4.1 ESD System shall be independent from DCS System.
- 4.2 ESD System shall meet the following requirements:
 - 4.2.1 The emergency shutdown system for the process interlocks shall be based on PLC.
 - 4.2.2 The process interlock and ESD system shall be designed tested and certified according to LST EN 61508 and LST EN 61511 standards.
 - 4.2.3 The process interlock and ESD system shall have inputs and outputs separated from the inputs and outputs of the primary control and monitoring DCS system (regulatory control).
 - 4.2.4 Input and output hardware segregation for the individual interlock systems and emergency shutdown (of compressors, process sections, for instance) shall be guaranteed.
 - 4.2.5 Signal lamps and pushbuttons of ESD system shall be located on the operator console in the control room (auxiliary panel).
 - 4.2.6 Digital signals from the electric equipment shall come via interface relays. Output signals to solenoid valves and lamps shall go through the terminal strips equipped with fuses and EEx(i) separators with the line failure detection system (LFD).

- 4.2.7** Field initiators of interlocks connected to ESD system shall be Exd type of protection and shall be connected to NAMUR inputs with the line failure detection system (LFD).
- 4.2.8** The solenoid valves connected to ESD shall be Exd type of protection and powered with 24V DC. Logic digital outputs to the solenoid valves shall be transmitted through driver relays (fail safe type) located in the separated portion of the cabinet or on the output card of PLC controller and Fuse circuits.
- 4.2.9** Input signals to PLC from MCC shall be brought as the potential-free relay contacts. Output signals from PLC to MCC shall be derived as the potential-free relay contacts. The relays shall be installed in the separated relay cabinet in the cabinet room. Such solution prevents a high voltage from MCC from entering PLC of ESD system.
- 4.2.10** MOS switches (Maintenance Override Switch) will be used for testing/maintenance of the interlock initiating devices without activating of the interlock system during operation of the plant. MOS will be implemented in software and will be activated from PLC visualization screen. Visualization in DCS is preferred. Required status of MOS will be transmitted to PLC via redundant software communication connection by means of two independent pulse signals (on / off). One blinking lamp will be on the operator console (Auxiliary Panel) for the logic group of signals. The lamp will inform about use of whichever of MOS switches in the group.
- 4.2.11** During the technical design execution stage, the Vendor shall present a concept of grouping the signals. The concept will be checked and commented by the OL / User in agreed period. In addition to software, MOS there shall be a key operated switch for each equipment logic system group. These switches shall provide additional safety, so that shall the switches be open, the MOS from the PLC visualization screen cannot be operated. During Basic Engineering phase the CONTRACTOR will submit the concept of signal grouping, which will be checked and commented by OL in agreed period of time.
- 4.2.12** Switching-on of any MOS in any group as below will cause printing-out a message by the DCS alarm printer and recording that fact in the event history.
- 4.2.13** The additional switch, cable-connected to the digital input of PLC, shall be installed in the operator console (Auxiliary panel). This switch shall enable a manual switching-over of all MOS switches in a safe status (i.e. "switched-off"). This is an additional safety measure, which can be used in case of failure of the series communication between DCS and PLC.
- 4.2.14** All ESD shall be provided with at least one manual initiator (trip) connected to system logic and located at a continuously manned location (such as the operators control desk). The device shall be hardwired to the ESD and shall be protected from accidental actuation. Manual trip initiators shall lock in the tripped position when activated (push, latch, pull to reset).
- 4.2.15** HMI shall have an option to switch off/shut down all the equipment (pumps, air coolers, etc.) controlled by the electric drive by „soft pushbuttons“.
- 4.2.16** ESD with more than one initiator shall be supplied with a "first-out" alarm that provides an indication of which initiator actuated first. Where logic type is PES with data link to the DCS, each alarm shall be historized in the DCS. The first-out alarms shall be implemented by either one of the following:
a) A first-out alarm annunciator using ISA Sequence F3A-3;

b) A sequence of events functions with sufficient time resolution to determine the first event.

- 4.2.17** Each process initiator, except manual initiators, shall have a pre-alarm which indicates that the process has reached the point where one or more of the ESD sensors is about to cause the ESD to operate unless corrective operator action is taken. These pre-alarms shall be annunciated at a continuously manned location and shall be historized. Two separate sensors shall be used—one for the pre-alarm and one for the ESD initiator, except when redundant sensors are used.
- 4.2.18** Each ESD shall have a common non-defeatable and non-resettable flashing Priority 1 alarm indicating that a protective function of the system is bypassed. The bypass alarm shall be annunciated at the appropriate continuously manned operator console and shall be histories. This bypass alarm may also be used to indicate the presence of active bypasses on non-ESD SHE critical alarms. The alarm may be set at a low flash rate.
- 4.2.19** Each ESD shall have a common trouble alarm. ESD using voting redundancy of sensors, logic, or final elements shall indicate any fault resulting in the failure of one or more channels. ESD using a fail-no-action design shall indicate any fault that results in the loss of protection. The common trouble alarm shall have a re-flash function when any subsequent trouble alarm condition exists. The OL shall approve the alarm priority.
- 4.2.20** The failure of any environmental conditioning equipment (e.g., fans, HVAC, air filtration) required to maintain the operation of the ESD, shall be alarmed at a continuously manned location. The OL shall approve the alarm priority.
- 4.2.21** For a PES, an interface shall be provided to indicate the status of the relevant inputs, outputs, and PES application program-generated flags. This interface shall preferably be achieved by a serial data link between the PES and the DCS to allow the DCS to monitor and display all ESD parameters. Where the PES to DCS interface is not practical, the interface may be to a stand-alone PC, via a network or via a serial link. All such data display interfaces shall be 'read only' at the DCS end and shall prohibit writes from the DCS or stand-alone PC to the PES for any reason. This data interface shall be separate from any interface used as above in Item (2) or Item (3) for the 'soft pushbuttons' function and shall not be used for programming, nor shall it allow any access to the application program or affect the operation of the ESD in any way. Failure of any component(s) in the interface shall not cause a spurious shutdown, nor shall the component failure go undetected.
- 4.2.22** POS (Process Override Switch) switches shall be used for bypassing of the signals, which initiate the interlocks. It will enable start-up of the plant. Activation of POS causes de-blocking of the signal from the interlock-initiating device. The operator is informed about occurred situation with blinking lamp on the Auxiliary panel. POS shall be key operated switch. POS switches and lamps shall be located on the operator console (Auxiliary panel). Employment of POS shall be registered in the form of a message by the alarm printer for DCS and stored in the history events. The concept of use POS switches has to be agreed with and accepted by the OL.
- 4.2.23** To enable state identification of MOS and POS switches for the process operators, the dedicated graphs in DCS shall be configured to visualize status of MOS and POS switches.
- 4.2.24** The alarm of the first cause of the interlock shutdown (of the compressor, the process section, for instance) shall be configured in PLC and visualized in DCS for each interlock system.

- 4.2.25** 10% spare inputs / outputs in PLC controller shall be foreseen.
- 4.2.26** Each failure of PLC controller shall be alarmed in DCS system. Common (cumulative) alarms are allowed.
- 4.2.27** Dedicated engineer station shall be provided for maintenance of PLC controller.
- 4.2.28** PLC shall be equipped with interfaces for communication with:
a) DCS system – via redundant data transmission bus;
b) Printers;
c) Engineer station for programming and configuration of PLC controller;
d) Local arrangement / console for visualization of PLC.
- 4.2.29** Connection of DCS system to the data transmission bus shall be made using the redundant serial interface with Modbus RTU Protocol.
- 4.2.30** Delivered primary and development software (and hardware, if necessary) shall guarantee configuration (and its subsequent modification) of PLC.
- 4.2.31** The controllers shall be equipped with the hardware and software diagnostic system for the software. The system shall control operation correctness of I/O modules, processor and memory. Test results shall be printed and / or displayed on monitor. Status of inputs / outputs, clock and memory shall be accessible through dedicated computer (PC) or off-line terminal.
- 4.2.32** The software shall consist of the following parts (packages):
a) Application software;
b) Firmware;
c) Additional diagnostic software;
d) Visualization software;
e) Software for registration of the event sequence (SOER) – if required.

5. BASIC DESIGN

- 5.1** Sharing of ESD and Control System components is allowed for certain specific applications. Where components are shared, the component shall be regarded as being part of the ESD and shall be powered from the ESD. All instances of shared components must be clearly identified in instrument records and by distinctive tag ids in the control system, so that appropriate operating, maintenance, and control applications practices are developed and used throughout the systems life cycles. Cases where sharing is permitted are as identified below. For cases not listed below, formal review and approval according to local safety policy is required.
- 5.2** Where prior engineering practice has demonstrated that shared components provide for significant cost savings with no safety impact. Specifically:
- 5.2.1** Where analog signals (devices) are required for, the ESD and the same signals (process points) are required for control by Control System. In this case, analog signals are routed to the ESD in which the shutdown logic is defined for the trip condition. Separate logic shall be used for calculating a value for the control signal and this control signal shall be sent via an analog output from the ESD to the Control System.
- 5.2.2** Where an ESD measurement is repeated to the Control System via a signal repeater for monitoring purposes only. In such cases failure of the signal repeater shall not affect the signal to the ESD.

5.2.3 Where orifice plates are used for both control measurement and ESD function: each sensor shall have separate process taps or wells. Where a single orifice plate is used for flow measurement for both control and ESD, a second set of taps on the orifice flange shall be used for the ESD. Where 2oo3 voting systems are installed on an orifice plate and the transmitter range is the same as a required DCS control transmitter, the transmitter signal shall be copied to the DCS per the Section Item a). Where the ESD transmitter ranges differ from that of the DCS sensor, four sets of taps shall be used, one each for the ESD sensors and one for the DCS sensor.

5.3 ESD shall be designed to prevent unauthorized access to the bypass or override functions and unauthorized modification of the protective function (e.g., program or set point changes).

5.4 Where there is a requirement to trip one system as a result of another system tripping, this shall be done directly using a signal from the first ESD to the second ESD. The trip of the second system shall not be inferred from cascading effects (e.g., waiting for trip initiators to react) from the results of the trip of the first system. Unless approved by the OL Representative, a trip condition shall also not be inferred from secondary or indirect measurements.

6. LOGIC ARCHITECTURE

6.1 All test facilities, including bypass switches, for the logic shall be integral to the logic equipment design. For the purpose of operator attendance, test facilities at the field device (e.g., next to a valve) are also acceptable and should normally be wired back to the PES logic solver. Sufficient information must be provided at the testing location to verify the test and ensure a safe return to service.

6.2 Any single fault in a fault-tolerant logic (e.g., 1oo2D or 2oo3 redundant) shall be alarmed but shall not initiate protective action unless required by the implementation conditions, restrictions, or requirements listed in the certifying authority approval certificate.

6.3 All electrical, electronic, and programmable electronic logic shall use time delays to avoid nuisance trips.

6.4 For relay-based systems, a 0,5 second time delay shall be applied to the final logic to prevent problems with contact bounce within the logic system. In addition, a time delay on each sensor and manual trip initiator input shall be 0,5 second unless otherwise specified.

6.5 For electronic and solid state or PES-based logic, the default 0,5 second delay shall be on the sensor and manual initiator input circuit only. Time delay on sensor inputs shall be 0,5 second unless otherwise specified.

6.6 Flame detectors for all logic types shall have a zero time delay on the sensor input.

6.7 ESD logic shall remain in its protective state after a trip until manually reset. This shall apply to a trip from any cause including loss of power source(s) even if the power source(s) and/or trip initiators return to their normal operating positions.

7. PROGRAMMABLE ELECTRONIC SYSTEMS (PES)

7.1 PES logic solvers used in Safety System applications shall be manufactured to comply with LST EN 61508. The configuration of the logic solver is determined by two requirements: (1) SIL and (2) Availability (the Spurious Trip rate). All SIS (ESD) should

be 1oo2D redundant, 2oo3 Triple Modular Redundant (TMR), Quad (2oo4), or other suitable redundant architectures shall be used. Single channel (Simplex or Single) fail-safe 1oo1D or similar system may be used with separate argument and approved by OL Representative. PES logic configurations are commonly used by Company for ESD:

7.1.1 1oo2D Redundant:

This uses a dual processor and redundant I/O modules with diagnostics to achieve high availability and fault tolerance. System shall default to 1oo1D on diagnosed failure of one channel. Either processor channel can initiate a trip, thereby meeting the high availability requirement; while a diagnosed failure of one processor channel provides for a low spurious trip rate by allowing the other channel to continue to protect the process with an appropriate alarm indicating one channel failure. Design features, which cause the single channel system to initiate a trip after a specific period of time (e.g., 72hrs), are sometimes incorporated in the operating system of the PES. These automatic trip features should normally be defeated and only an alarm used to indicate that one channel of protection has failed.

7.1.2 Triple Modular Redundant (TMR):

The TMR system uses three parallel processors to achieve fault tolerance and to execute a 2oo3 function on the output states, thus achieving the high availability. Similar considerations apply to the TMR system when it degrades to 1oo2 operation as apply to the 1oo2D redundant system. (i.e., no automatic trip after a time period when degrading to 1oo2 operation)

7.2 PES with voting redundancy, when degrading to single-channel operation or a dual-channel operation for a TMR system, shall sound a dedicated Priority 1 alarm.

7.3 The Priority 1 'voting degraded' alarm may be shared among a number of systems in the same physical location.

7.4 All PES shall be self-documenting. This includes the original programming of the application and any changes made after installation. As a minimum, the following shall be generated:

7.4.1 A program listing.

7.4.2 A system configuration.

7.4.3 Applications logic diagrams.

7.4.4 A cross-referenced list of equipment tag numbers and program use locations.

7.4.5 Application logic shall be implemented in one of, or a combination of, the following programming languages:

- a) Cause-Effect Matrix;
- b) Function Block Diagram;
- c) Sequential Function Chart;
- d) Ladder Diagram.

7.5 Failure of any equipment associated with external communication to the PES shall not affect safety-related functions. This includes, but is not limited to, software bypasses.

8. DOCUMENTATION

8.1 Design documentation shall include the following:

- 8.1.1 Written description of the system and its operation.
- 8.1.2 Block diagram of the system configuration.
- 8.1.3 Logic diagrams that show initiators, final elements, and the relationship between them, test and maintenance facilities, operator interface facilities, and interfaces to external devices.
- 8.1.4 Listing of the application program, including comment statements (programmable logic only). The requirements of the application logic shall be clearly defined using Cause-Effect Matrices or Functional Logic Diagrams and/or Flow Charts. Whichever method is chosen, the representation shall be kept as simple as possible to allow understanding by non-control systems specialists.
- 8.1.5 List of input and output connections with equipment tag name and physical address.
- 8.1.6 Connection and interconnection (wiring or pneumatic tubing) diagrams for troubleshooting and maintenance. System components shall be identified by OL instrument equipment tag names.
- 8.1.7 Hook-up installation drawings for sensors and final elements.
- 8.1.8 Total equipment list and bill of materials with component Vendors and model numbers.
- 8.1.9 Vendor standard documentation, including (but not limited to): specifications, site planning, installation, implementation, and operating manuals.
- 8.1.10 Recommended spare parts list for 2 years' continuous operation.
- 8.2 Design documentation shall be available for use during the project HAZOP and shall be controlled documents subject to Management of Change for the life cycle of the project.
- 8.3 Verification and validation documentation shall include the following:
 - 8.3.1 Verification test procedure(s) and test report(s) (e.g., Factory Acceptance Tests).
 - 8.3.2 Validation test procedure and test report (e.g., Site Acceptance Test).
 - 8.3.3 On-line proof testing (when required), and preventative and corrective maintenance procedures.
 - 8.3.4 The certifying authority approval certificate for the model and type of PES, specifically including the conditions for implementation, and any restrictions or requirements.
- 9. **POWER**
 - 9.1 Logic systems shall be powered from a minimum of two power supplies in a redundant configuration; each sized for full load. Failure of a single power supply due to loss of voltage or ability to support full load shall initiate a Priority 2 alarm. Field devices and related input modules shall also be powered from two power supplies, each sized for the full load, which may be the same essential power supplies.
 - 9.2 Design power supply blocks (sources) with selective SFB (SFB - Selective Fuse Breaking) technology (temporary outlet current up to 6 In) as those that power the logic.

10. FIELD WIRING

10.1 ESD shall utilize dedicated junction boxes, wiring, and termination facilities to segregate the ESD from the control system. Barriers within junction boxes and termination facilities shall clearly segregate and label wiring of different ESD. ESD alarm wiring to the main control house need not be segregated from other alarm wiring.

10.2 Only one sensor or final element shall be connected to each field circuit.

11. SENSORS

11.1 2oo3 voting of analog or numeric values shall use 'middle of three' selection with an alarm if any value falls outside a predetermined dead band above or below the middle value. Other arithmetic representations shall require OL approval (e.g., high select, average, etc.).

11.2 Sensors, or switches, that have a selectable failure direction will require a decision on failure mode and will normally be set consistent with a fail-no-action design philosophy with failure alarm at a continuously manned location.

Voting Table

1oo1		1oo2			2oo2			2oo3			
Input	Trip status	Input		Trip status	Input		Trip status	Input		Trip status	
OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
TRIP	TRIP	TRIP	OK	TRIP	TRIP	OK	OK	TRIP	OK	OK	OK
FAIL	TRIP	TRIP	TRIP	TRIP	TRIP	TRIP	TRIP	TRIP	TRIP	OK	TRIP
		MOS	OK	OK	MOS	OK	OK	TRIP	TRIP	TRIP	TRIP
		MOS	TRIP	TRIP	MOS	TRIP	TRIP	MOS	OK	OK	OK
		MOS	MOS	OK	MOS	MOS	OK	MOS	TRIP	OK	OK
		FAIL	OK	OK	FAIL	OK	OK	MOS	TRIP	TRIP	TRIP
		FAIL	TRIP	TRIP	FAIL	TRIP	TRIP	MOS	MOS	OK	OK
		FAIL	FAIL	TRIP	FAIL	FAIL	TRIP	MOS	MOS	TRIP	TRIP
		MOS	FAIL	TRIP	MOS	FAIL	TRIP	MOS	MOS	FAIL	TRIP
								MOS	MOS	MOS	OK
								FAIL	OK	OK	OK
								FAIL	TRIP	OK	TRIP
								FAIL	TRIP	TRIP	TRIP
								FAIL	FAIL	OK	OK
								FAIL	FAIL	TRIP	TRIP
								FAIL	FAIL	MOS	TRIP
								FAIL	FAIL	FAIL	TRIP
								MOS	FAIL	OK	OK
								MOS	FAIL	TRIP	TRIP

Remarks:

OK	Sensor (-s) available
TRIP	Process exceed limit value
MOS	Sensor (-s) bypassed from the process and voting (maintenance issues)
FAIL	Sensor (-s) failure simulation signal (signal < 3,6 mA or > 21,2 mA)

12. FINAL ELEMENTS

- 12.1** Final elements shall remain in their protective state after a trip or loss of power source (e.g., electrical, air, or hydraulic) until manually reset, even if any trip initiators return to their normal operating positions. All ESD final elements require manual reset at the final element, unless otherwise specified. Manual reset can be accomplished by an electrical switch installed for this specific purpose.
- 12.2** ESD valves shall not have hand wheels.
- 12.3** ESD valves shall be designed and installed such that flow through the valve shall tend to force the valve in the required failure direction (flow tending to close or open).
- 12.4** Where the ESD valve is also required to be fire safe, the valve shall be fire tested. For fire safe valves, a graphite packing system is required. Where soft-seated valves are used in fire safe service, the valve shall be of fire safe approved design, which forces metal-to-metal backup seating upon loss of the soft seat.
- 13. FINAL ELEMENTS – SOLENOID VALVES**
- Solenoid valves used in fail-no-action ESD shall use 1oo2 voting redundancy. Voting redundancy for solenoid valves used in fail-action ESD shall be use 2oo2 voting. Where 2oo2 solenoids are used to minimize spurious trips, facilities shall be installed at the solenoids to allow testing of the individual solenoids by an operator. Other configurations are available (e.g., 2oo3) and should be evaluated to achieve the required Availability and Reliability (AT and STR). Where a solenoid bypass is provided, it shall be car sealed in safe position and shall activate the bypass alarm when it is not in safe position. Position may be detected by a limit switch or pressure switch.
- 14. ARCHITECTURES**
- For examples of architectures see Figures 1., 2. and 3. The other architecture concepts shall be approved by OL.
- 15. EMERGENCY STOP (SHUTDOWN) BUTTON**
- 15.1** Manual means that are independent of both the SIS logic solver and DCS system may be provided to allow the operator to initiate a shutdown in an emergency. The requirements for manual shutdown are normally defined in the SRS.
- 15.2** The emergency stop may be connected to the SIS PE logic solver (for example, when a sequenced shut down is required) provided that it is necessary and deemed appropriate by the H and RA team.
- 15.3** Emergency STOP (shutdown) button must comply with OL requirements
- 16. SMART SENSORS FOR ESD SYSTEM**
- 16.1** Smart sensors shall be write-protected (mechanical switches designed for that purpose or introduction of limited software access) to prevent inadvertent modification from remote location, unless appropriate safety review allows the use of read/write. The review should take into account human factors such as failure to follow procedures.
- 16.2** All transmitters for ESD systems must be certificated according LST EN 61508.
- 16.3** All on/off valves must be approved with OWNER regarding certification according LST EN 61508.

17. SIL CLASSIFICATION AND INTERLOCK FUNCTION IMPLEMENTATION

- 17.1** Interlock functions implementation in ESD controller as well as quality and quantity selection of field instrumentation will be done prior to the results of SIL (Safety Integrity Level) analyze performed earlier.
- 17.2** The Contractor will perform SIL analysis based on methodology based upon LST EN 61511 standard requirements.
- 17.3** SIL is a numerical means of quantifying the design requirements of a Safety Instrumented System to match the Risk imposed by process. The SIL of an SIF (Safety Instrumented Function) is a means of quantifying the relative reduction in risk associated with the correct operation of that SIF or SIS (Safety Instrumented System). SIL implies a numeric designation of PFD (Probability of Failure on Demand) and Availability, as shown in the Table 1.

Table 1. SIL – PFD Range - Availability

Safety Integrity Level (SIL)	PFD Range	Availability
1	10^{-1} to 10^{-2}	90.00 % to 99.00 %
2	10^{-2} to 10^{-3}	99.00 % to 99.90 %
3	10^{-3} to 10^{-4}	99.90 % to 99.99 %
4	10^{-4} to 10^{-5}	99.99 % to 99.999 %

- 17.4** SIL analysis will be performed with cooperation with OWNER representatives and final report and proposed technical solutions must obtain an acceptance from E&A OL.
- 17.5** CONTRACTOR will provide to OWNER HAZOP report procedure and calculations of SIL, P&I diagrams and instrumentation basic data in two weeks before commencing of works.

18. SAFETY REQUIREMENT SPECIFICATION

A safety requirement specification (SRS) shall be developed to ensure that all safety criteria conceived prior to the detailed engineering phase of the project are completely addressed. Although specifically aimed at Safety, the SRS will also include consideration of all identified protective functions. The SRS is key to a successful design and implementation and shall be included in any project plan checklist. For modifications to existing ESD or small site projects, the need for an SRS and/or the level of detail covered in the SRS shall be reviewed with the OWNER'S Representative. For large projects, minimum requirements shall include the following:

- 18.1.1** The SRS shall be approved by the Risk OWNER as determined by the site practice. OWNER'S Representative referred to in this GP shall be the Risk OWNER designee to monitor compliance with the SRS or steward additions and exceptions throughout the detailed engineering of the ESD.
- 18.1.2** The SRS shall include a description showing required protective functions, along with their respective risk as determined by Risk Assessment.
- 18.1.3** The time interval between two FST (full stroke test or **proof test interval PTI**) should be not less than 6 years, or other term agreed with customer.
- 18.1.4** The system must be designed to minimize the probability of spurious trip.

- 18.1.5 Mean time to spurious trip** (MTTF spurious) should be once in minimum 50 years for the SIF and minimum 200 years for the PES (ESD).

Mission time (SIF is expected to be operational) a 15 years as minimum. The period of time between when the SIF (or device) is put into service and when it is replaced or completely refurbished to “as-new” condition.

MTTR (Mean Time to Repair / Restoration) - the average time between the occurrence of a failure and the completion of the repair of that failure. This includes the time needed to detect the failure, initiate the repair and fully complete the repair.

- sensor part 8H,
- logic solver part 12H,
- final elements 24H.

Startup time - 24H. In the Startup Time field you can list the number of hours it takes to restart the process after a shutdown.

Beta Factor - Beta factor, indicating common cause susceptibility. The fraction of total failure rate that is attributed to a single cause in common with other units in the group. A **common cause failure** (CCF) will result in all units with the group failing simultaneously.

Typical ranges for common cause are as follows.

- logic solvers = 0.5% to 5%
- sensors and final elements = 1% to 10%

In lower SIL applications there is a reduced emphasis on common cause due to the limited use of redundancy. In these cases the assumed levels of common cause is as follows:

- between similar final elements in the same group 10%
- between different final elements in the same group 5%
- between similar final elements in different groups 5%
- between different final elements in different groups 2%

Maintenance Capability Index (MCI) – the effectiveness of the repair processes in place at a specific site.

- Sensor and final elements – 90%. Good repair. Repair actions are always performed, tool calibration is not always up to date, maintenance crew does not always completely fix original problem.
- Logic solver – 99%. Almost perfect repair. Repair actions are always performed, tool calibration is always update, a minor maintenance mistake is hardly ever made.

- 18.1.6** The SRS shall include any site or industry regulations to be applied to the design.
- 18.1.7** The SRS shall include for each SIF and overall system, the required Availability Target (AT), spurious trip rate, and proof testing proposals, including the consequences of spurious trip events and site-specific design criteria relating to unit turnaround (TA) timings and site system testing requirements and practices (on-line or TA testing).
- 18.1.8** The SRS shall identify whether double block valve and/or redundant sensor designs are required to achieve the required Availability Target and Spurious Trip Rate. The SRS shall indicate the basic configuration of the hardware system design, addressing issues of redundancy, shared components, communication, location of components and system boundaries.

- 18.1.9** The SRS shall prescribe all ESD generated alarms and preferred alarm display method.
- 18.1.10** It is not expected that the availability target of any Company process will require a SIL-4 system.

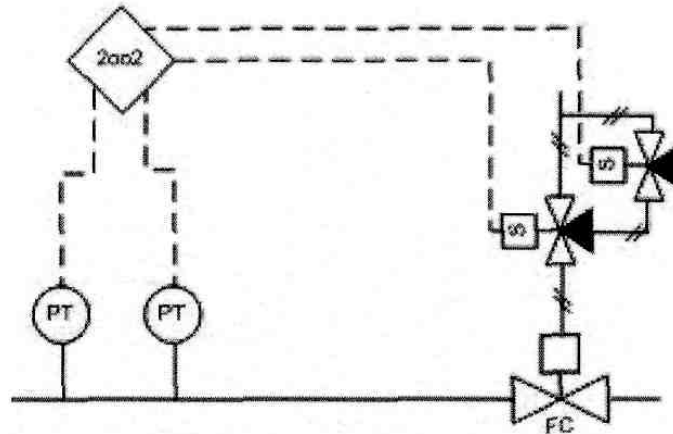


Figure 1. High Reliability SIL 1 SIS. Example

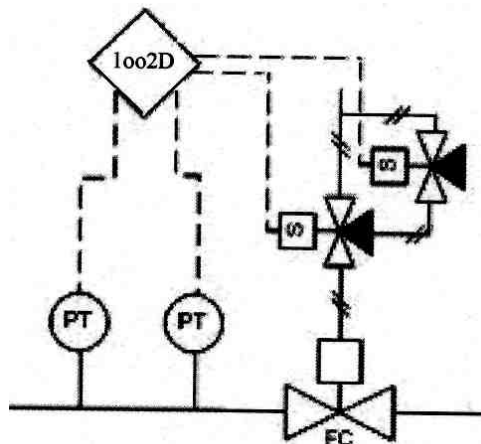


Figure 2. High Reliability SIL 2 SIS. Example

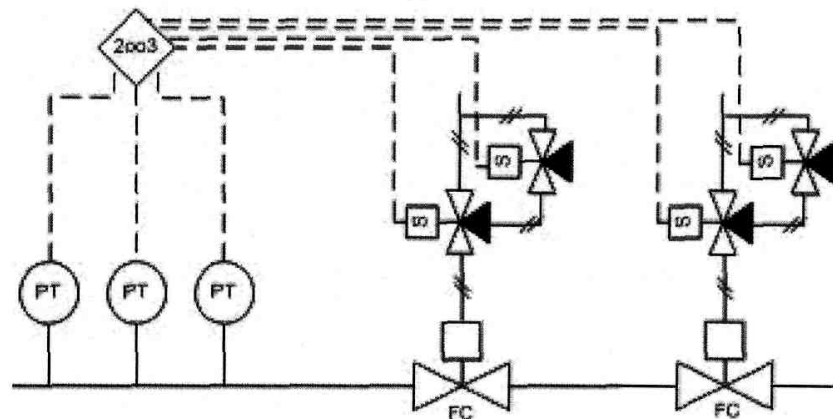


Figure 3. High Reliability SIL 3 SIS. Example