Training on Functional Safety

Course 1

Functional Safety & Safety Instrumented System (SIS)

- Based on SIS life cycle of IEC61511/61508.
- The course is structured in 5 modules: Introduction, Analysis of Risks, Design & Implementation, Operation & Maintenance, and Review.
- There are several types of online courses depending on the number of hours live with the instructor.
- Optional FS Engineer certification exam.

- FS1E-WI: course for 1 participant with support by email.
- FS1E-1: course for 1 participant, includes 3 hours with the instructor.
- FS1E-2: course for 2 to 6 participants or more, includes 4 hours with the instructor.

Courses in english with 60 days of free access to the virtual classroom with the contents (PDFs, videos, Excel and Word templates, evaluation test).

Live sessions with the instructor: at the time agreed with the participants.

FS Engineer
Process Safety - IEC 61511
ID: SS-218494379
www.safetyandsis.com
Certified by FUNCTIONAL SAFETY SIS safetyandsis.com

Course 2

Design of Safety Instrumented Functions and SIL verification

- Based on SIS life cycle of IEC61511/61508 & ISA84.
- The course is structured in 7 modules with focus on the practical part with real examples from the industry.
- Includes SILcet license for SIL verification.
- There are several types of online courses depending on the number of hours live with the instructor.
- Optional FS Specialist certification exam.

- FS2E-WI: course for 1 participant with support by email.
- FS2E-1: course for 1 participant, includes 3 hours with the instructor.
- FS2E-2: course for 2 to 6 participants, includes 5 hours with the instructor.

Courses in english with 60 days of free access to the virtual classroom with the contents (PDFs, videos, Excel and Word templates, evaluation test).

Live sessions with the instructor: at the time agreed with the participants.

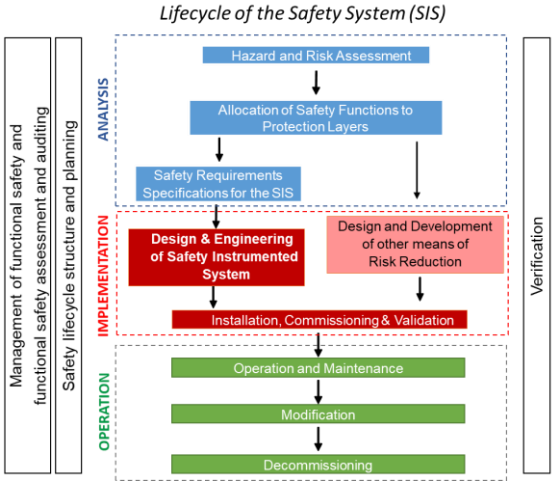
SILcet Pro Plus tool: 6 or 12 months license is included.

FS Specialist
Process Safety - IEC 61511
ID: SS-218494379
www.safetyandsis.com
Certified by FUNCTIONAL SAFETY SIS safetyandsis.com

Course 3: Cyber HAZOP Analysis (read more)

The complete functional safety training program consists of three training courses and two certification options. Our instructors have a lot of training experience in collaboration with ISA, TÜV Rheinland and TÜV SÜD.

Course 1: Functional Safety & SIS



Functional Safety in the process industry based on the Life Cycle of IEC61511. The course is structured in 5 parts:

- ✓ **Introduction**
- ✓ **Process Hazard Analysis**
- ✓ **Design & Implementation**
- ✓ **Operation & Maintenance**
- ✓ **Review**

Aimed at

Students, technicians, designers, system integrators and engineers who want to learn about Safety Instrumented Systems (SIS) in the process industry.

Course Objetive

The objective is to acquire the necessary knowledge to start working in Functional Safety. If you already have knowledge, the course will help you better understand the concepts and give you a real insight into the importance of the different phases of the life cycle.

You will benefit from the Lessons Learned and Best Practices acquired in large projects.

Methodology of online versions

Course in **english**.

Duration: 15-20 hours (depending on student experience).

There are 3 types of courses. In all of them, participants have free access to the virtual classroom (24/7) for 60 days with videos and other documents.

- FS1E-1: course for 1 participant, includes 3 hours with the instructor.
- FS1E-2: course for 2 participants, includes 4 hours with the instructor.
- FS1E-WI: course with email support.

In the live sessions the Instructor explains the main parts of the course and answers questions from the students.

Note: the schedule of the hours with the instructor to be agreed with the students. Microsoft Teams or other similar programs will preferably be used.

Documentation

- Course contents in PDF format (> 350 pages).
- Excel Templates: HAZOP, Risk Graph, LOPA and SRS.
- Word template: SIL verification report.
- Videos and instructor support (only some of the course videos can be downloaded).
- Evaluation test in each module and Certificate.

- OPTIONAL: **FS Engineer** certification exam. There is a period of 6 months for taking the exam from the beginning of the course.

Contents of Course 1

Module 1: INTRODUCTION

-Basic concepts, International Standards, What does SIF, SIS, SIL mean? Control System versus Safety Instrumented System

-Types of failures and examples. The importance of diagnostics. Types and examples.

-SIS Life Cycle: Analysis Phase, Design and Implementation Phase, Operation and Maintenance Phase

Documentation: PDFs + videos

Module 2: RISK ANALYSIS

-Risk concepts and how to reduce them with layers of protection. What is an independent protection layer (IPL)? SIS principle of independence and shared elements. Examples.

-Risk Analysis Techniques.

-HAZOP Methodology and Risk Graph

- ✓ *Definition of nodes and identification of deviations.*
- ✓ *Definition of Causes and Consequences. Evaluation of the consequences.*
- ✓ *Identification of safeguards (IPLs) and assigned credits. Is a SIS layer necessary?*
- ✓ *Determination of «SIL» with Risk Graphs.*
- ✓ *Examples with Excel template.*

-LOPA methodology

- ✓ *Identification of initiating events.*
- ✓ *Frequency of causes and conditioning modifiers.*
- ✓ *Identification of non-SIS IPLs and PFDs.*
- ✓ *Calculation of the scenario frequency.*
- ✓ *Comparison with the tolerable frequency defined by the Plant. Example of the risk matrix.*
- ✓ *Is a SIS layer necessary? SIL assigned to the SIF.*
- ✓ *Examples with Excel template.*

-Exercises: HAZOP, Risk Graph and LOPA.

-Safety Requirements Specification (SRS)

Documentation: PDFs + Excel templates + SRS + videos

Module 3: DESIGN & IMPLEMENTATION

-Most used architectures and examples.

-Principles of safety system design. Safety versus Availability.

-IEC requirements and key parameters to calculate the SIL.

-Formulas to calculate PFDavg and MTTFS. Data sources of failure rates.

-Examples of real industry SIFs:

- ✓ *Design assumptions (transmitter configuration, used models, architecture degradation, etc.)*
- ✓ *Example of tank level.*
- ✓ *Example of pressure vessel.*
- ✓ *Calculate the SIL achieved by Logic Solver.*

-SIL Verification Report. Example.

-IEC 61511 requirements: FAT / SAT, Validation and FSA.

Documentation: PDFs + Verification Report + videos

Module 4: OPERATION & MAINTENANCE

-Concepts and reasons for maintaining the SIS.

-Main clauses of IEC 61511:2016 on Operation & Maintenance.

-Use of the bypass and its impact. Proof Tests and their impact. Examples. Repair of the SIF and its impact. SIS modifications.

Documentation : PDFs + videos

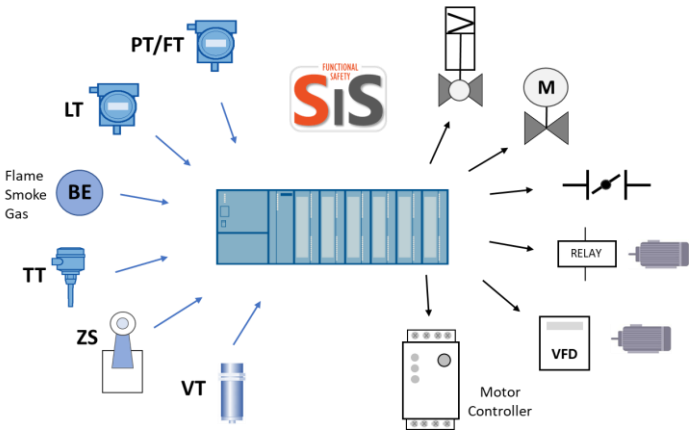
Module 5 : REVIEW

-General considerations to design the SIS.

-How to minimize hardware failures. How to minimize systematic failures.

Documentation: PDFs + videos

Course 2: Design of SIFs & SIL verification



Design of Safety Instrumented Functions and verification of SIL and MTTFS based on practical examples of safety functions in the process industry. Comparison of different designs and generation of reports. Most important parts of the Safety Instrumented System Life Cycle.

Aimed at

Technicians, designers, system integrators and engineers related to Functional Safety and Safety Instrumented Systems (SIS) of the process industry.

Course Objetive

The objective is to acquire knowledge to understand and design Safety Instrumented Functions (SIF) from a totally practical point of view. For this, all the concepts on Functional Safety are reviewed, as well as the main parameters are explained in detail. Real examples are made with the SILcet tool that allows to calculate the SIL based on the three requirements of the IEC-61511/61508 & ISA-84 Standards, as well as compare different design alternatives.

Methodology of online versions

Course in **english**.

Duration: 15-20 hours (depending on student experience).

There are 3 types of courses. In all of them, participants have free access to the virtual classroom (24/7) for 60 days with videos and other documents.

- FS2E-1: course for 1 participant, includes 3 hours with the instructor.
- FS2E-2: course for 2 to 6 participants, includes 5 hours with the instructor.
- FS2E-WI: course with email support.

In the live sessions the Instructor explains the main parts of the course and answers questions from the students.

Note: the schedule of the hours with the instructor to be agreed with the students. Microsoft Teams or other similar programs will preferably be used.

Documentation

- Course contents in PDF format (> 300 pages).
- Excel files (SILcet) with the actual calculations of the practical examples of the course
- SILcet Pro Plus tool: 12 months license for course FS2E-2, 6 months license for courses FS2E-1/WI.
- SILcet User Manual and detailed document on the formulas for calculating PFDavg and MTTFS.
- Other Excel tools: Beta factor.
- Word templates: SIL verification reports.
- Videos and instructor support (only some of the course videos can be downloaded).
- Evaluation test in each module and Certificate.
- OPTIONAL: **FS Specialist** certification exam. There is a period of 6 months for taking the exam from the beginning of the course (check conditions to get the FS Specialist Certification).

Requirements for SILcet tool: Windows 10/11, Excel 2016 or later.

Contents of Course 2

Module 1: Introduction

-Basic concepts, International Standards, What does SIF, SIS, SIL mean? Control System versus Safety Instrumented System

-Types of failures and examples. The importance of diagnostics. Types and examples.

-SIS Life Cycle: Analysis Phase, Design and Implementation Phase, Operation and Maintenance Phase

Module 2: Risk Analysis Phase

-Risk concepts and how to reduce them with layers of protection. What is an independent protection layer (IPL)? SIS principle of independence and shared elements. Examples.

-Types of Risk Analysis Techniques. Basics of HAZOP.

-Determination of «SIL» with Risk Graphs. Risk Gap concept, required SIL. Example with Risk Graph.

-Example with Safety Requirements Specification (SRS).

Module 3 : Design & Implementation Phase

-Most used architectures and examples.

-Principles of safety system design. Safety versus Availability.

-IEC requirements and key parameters to calculate the SIL.

-Formulas to calculate PFDavg and MTTFS. Data sources of failure rates.

-Simple example of SIL verification.

-Proof Tests.

Module 4: Design & SIL Verification *(SILcet is used)*

-Assumptions for the examples (configuration Low/High of the transmitter according to the architecture, online / offline tests, etc.).

-Practical exercises using the SILcet tool:

1. Tank Level (several cases)

2. Vessel under pressure (several cases): i) undefined sensor type, ii) transmitter vs switch, iii) diversity of elements, iv) credit by comparison, v) bypass impact.

3. Calculate the SIL achieved by the Logic Solver.

-21 general considerations to design the SIS.

-Examples of certificates and other documents from manufacturers of sensors, logic solver & final elements.

-Excel files included: "SILcet with the exercises solved" & Example of Safety Requirements Specification (SRS).

Module 5 : Design & SIL Verification *(SILcet is used)*

-Assumptions for the examples and SRS.

-Real practical exercises using the SILcet tool:

1. Low combustion air flow in Incinerator or Furnace.

2. Stop of high pressure pumps by partial closure of the suction.

3. Gas valve closure due to flame loss.

4. Emergency depressurization in a reactor: action on several lines when the temperature is excessive (Reactor Bed Temperature).

5. How to solve a SIF with two Logic Solvers (Safety PLCs).

6. SIF with shared elements (Control System and SIS).

7.Example with Partial Valve Stroke Test.

8.Examples with Complex Architectures.

- Excel file included: "SILcet with the exercises solved" & Example of Safety Requirements Specification (SRS).

Module 6: SIL Verification Report

-How to prepare a SIL Verification Report.

-Main document with MS-Word Template.

-Annex of parameters, graphs and results (PFDavg, PFH, MTTFS) generated by SILcet.

-Example of report with the exSILentia tool.

Module 7: Design & SIL Verification *(SILcet is used)*

Note: Other additional exercises that are delivered resolved to the participants at the end of the course.

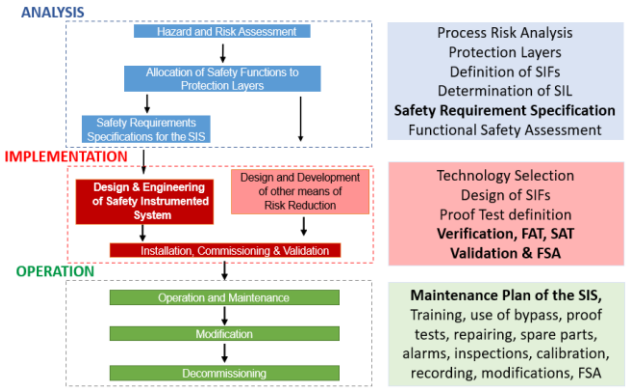
-Assumptions for the exercises.

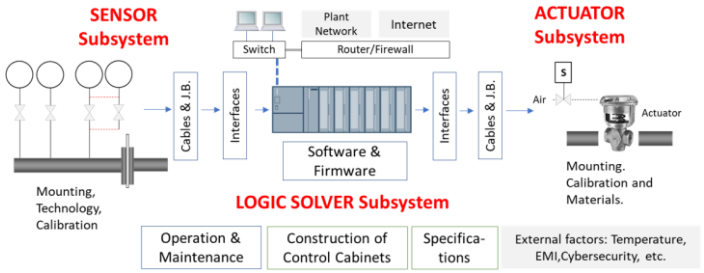
-Real practical exercises using the SILcet tool (in each case there are several possible configurations):

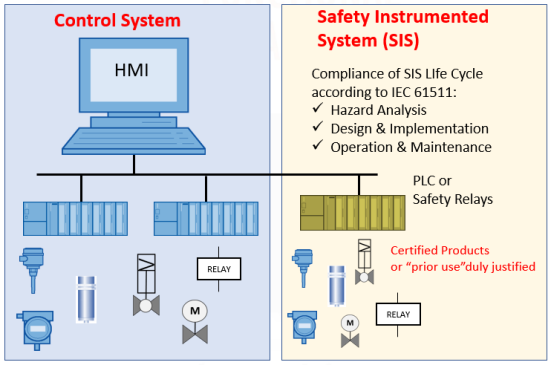
- *Turbine Trip Valve Hydraulic System.*
- *High Integrity Pressure Protection System*
- *Pressure vessels (different cases).*
- *Others: Solutions with high availability, Fire & Gas System, Protection of a Silo.*

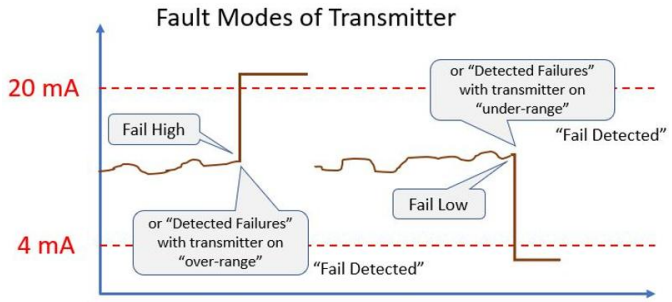
- Excel file included: "SILcet with the exercises solved".

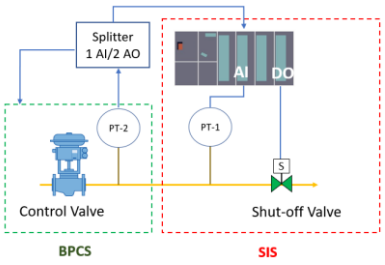
Some diagrams, tables and graphs used in the courses are shown below.





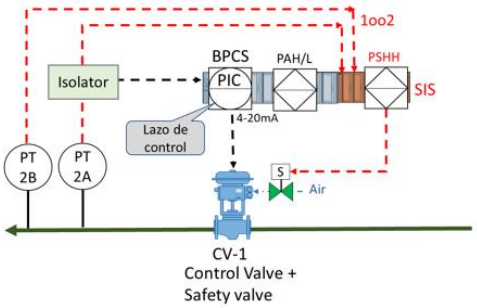


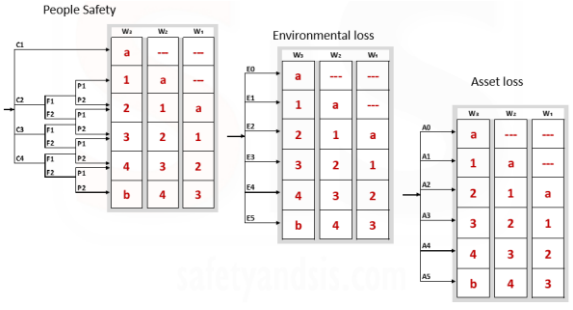


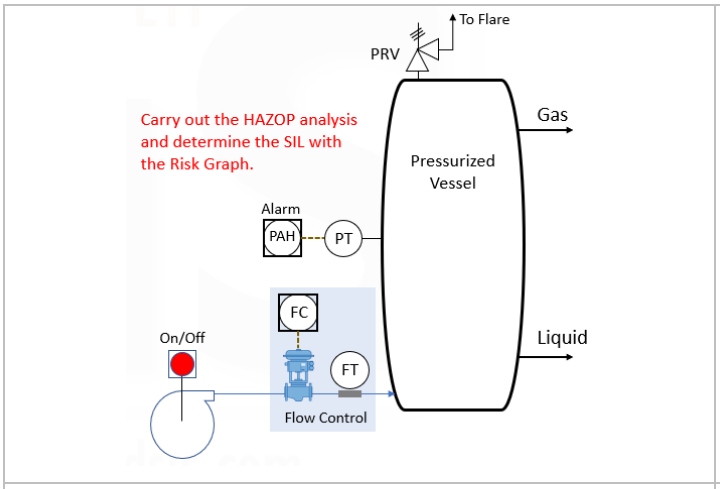


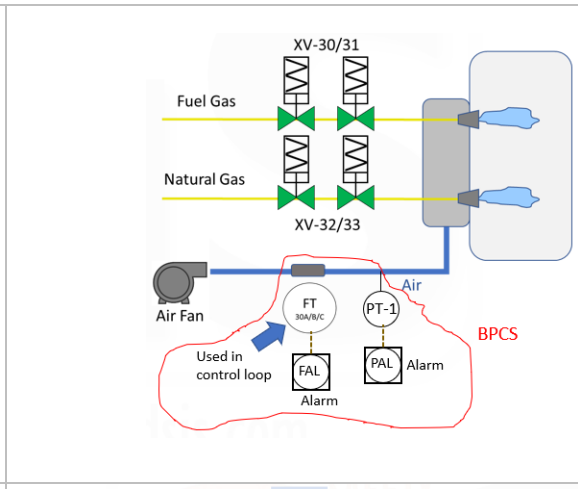
Risk Matrix

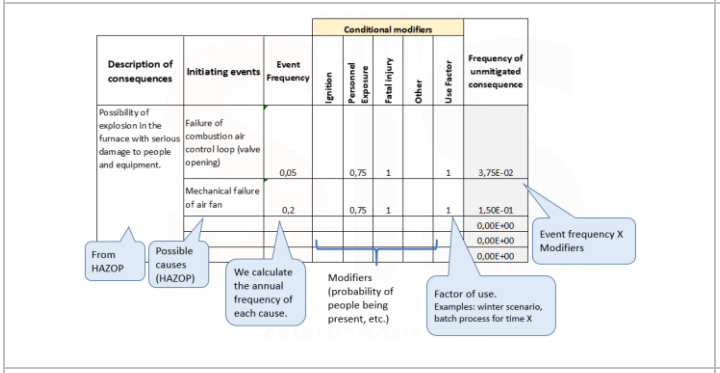
Frequency(1/year)	Categories of Consequences 1	2	3	4	5	6
> 1	HIGH	HIGH	HIGH	VERY HIGH	VERY HIGH	VERY HIGH
$1 - 10^{-1}$	HIGH	HIGH	HIGH	VERY HIGH	VERY HIGH	VERY HIGH
$10^{-1} - 10^{-2}$	LOW	HIGH	HIGH	VERY HIGH	VERY HIGH	VERY HIGH
$10^{-2} - 10^{-3}$	LOW	LOW	HIGH	HIGH	VERY HIGH	VERY HIGH
$10^{-3} - 10^{-4}$	LOW	LOW	LOW	HIGH	HIGH	VERY HIGH
$10^{-4} - 10^{-5}$	LOW	LOW	LOW	LOW	HIGH	HIGH
$10^{-5} - 10^{-6}$	LOW	LOW	LOW	LOW	MEDIUM	HIGH
$10^{-6} - 10^{-7}$	LOW	LOW	LOW	LOW	LOW	MEDIUM

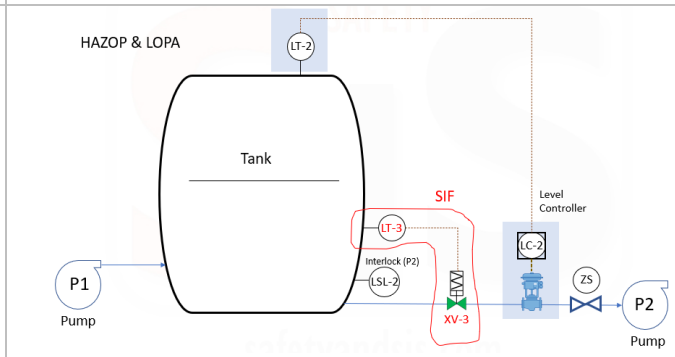


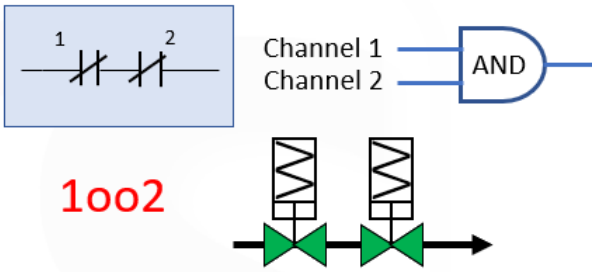


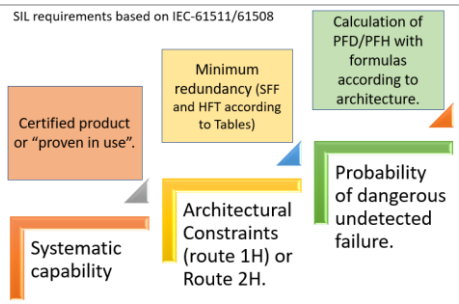

To Flare
PRV
Carry out the HAZOP analysis and determine the SIL with the Risk Graph.
Gas
Pressurized Vessel
Alarm
PAH
PT
FC
On/Off
FT
Liquid
Flow Control

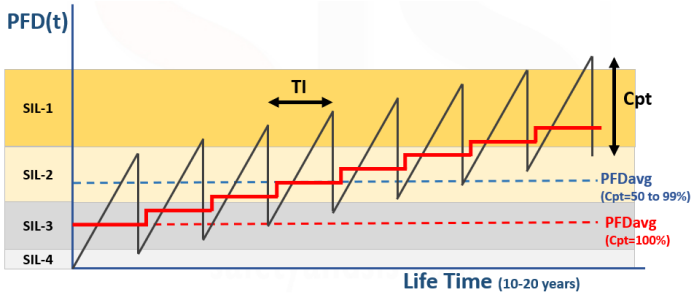

XV-30/31
Fuel Gas
Natural Gas
XV-32/33
Air
Air Fan
FT
PT-1
BPCS
Used in control loop
FAL
PAL
Alarm
Alarm

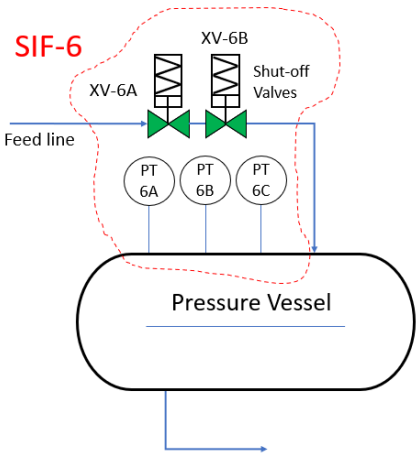

Conditional modifiers
Description of consequences
Initiating events
Event Frequency
Ignition
Personnel Exposure
Fatal injury
Other
Use Factor
Frequency of unmitigated consequence
Possibility of explosion in the furnace with serious damage to people and equipment.
Failure of combustion air control loop (valve opening)
0,05
0,75
1
1
3,75E-02
Mechanical failure of air fan
0,2
0,75
1
1
1,50E-01
0,00E+00
0,00E+00
0,00E+00
From HAZOP
Possible causes (HAZOP)
We calculate the annual frequency of each cause.
Modifiers (probability of people being present, etc.)
Factor of use. Examples: winter scenario, batch process for time X
Event frequency X Modifiers

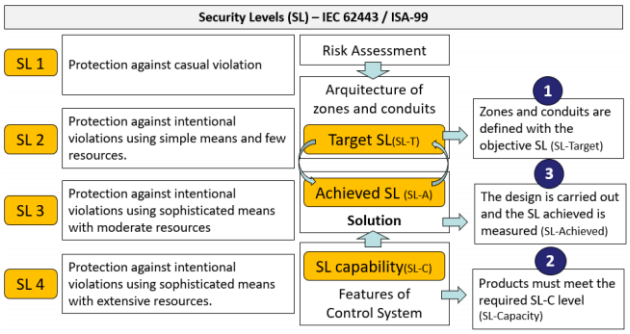

HAZOP & LOPA
LT-2
Tank
SIF
LT-3
Level Controller
LC-2
Interlock (P2)
LSL-2
XV-3
ZS
P1
Pump
P2
Pump

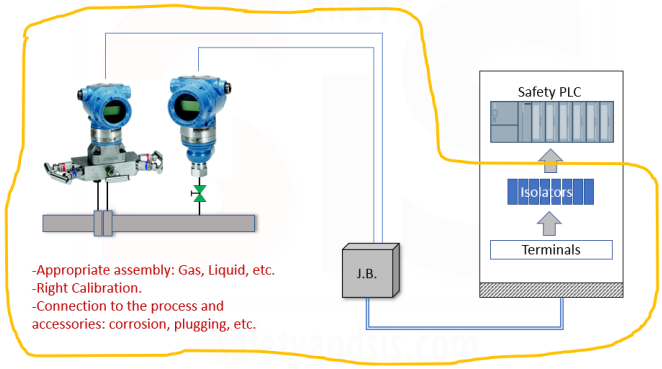

1
2
Channel 1
Channel 2
AND
1oo2

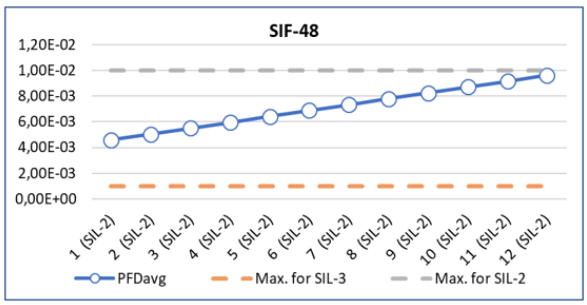

SIL requirements based on IEC-61511/61508
Calculation of PFD/PFH with formulas according to architecture.
Minimum redundancy (SFF and HFT according to Tables)
Certified product or "proven in use".
Probability of dangerous undetected failure.
Architectural Constraints (route 1H) or Route 2H.
Systematic capability

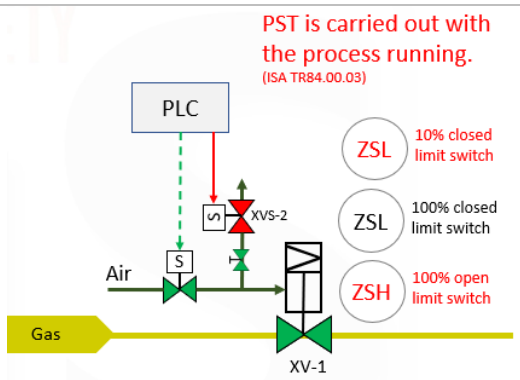

PFD(t)
SIL-1
TI
Cpt
SIL-2
PFDavg
(Cpt=50 to 99%)
SIL-3
PFDavg
(Cpt=100%)
SIL-4
Life Time (10-20 years)

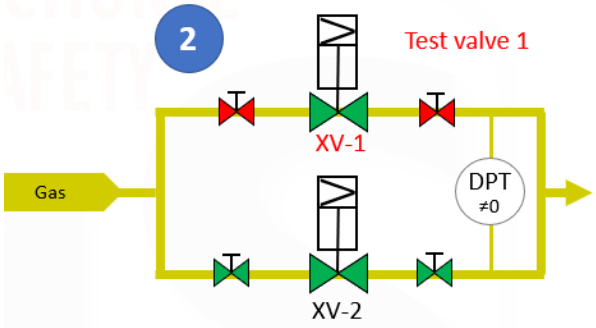

SIF-6
XV-6B
XV-6A
Shut-off Valves
Feed line
PT 6A
PT 6B
PT 6C
Pressure Vessel

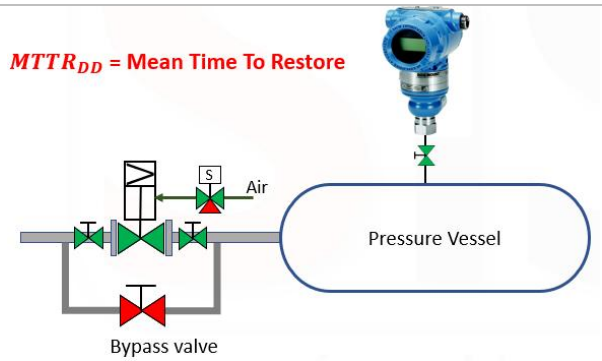

Security Levels (SL) – IEC 62443 / ISA-99
SL 1
Protection against casual violation
SL 2
Protection against intentional violations using simple means and few resources.
SL 3
Protection against intentional violations using sophisticated means with moderate resources
SL 4
Protection against intentional violations using sophisticated means with extensive resources.
Risk Assessment
Arquitecture of zones and conduits
Target SL(SL-T)
Achieved SL (SL-A)
Solution
SL capability(SL-C)
Features of Control System
1
Zones and conduits are defined with the objective SL (SL-Target)
3
The design is carried out and the SL achieved is measured (SL-Achieved)
2
Products must meet the required SL-C level (SL-Capacity)

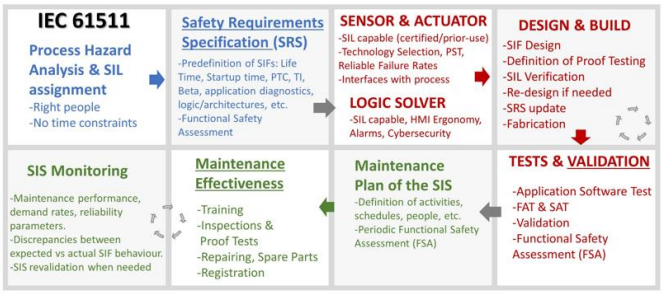

Safety PLC
Isolators
Terminals
J.B.
-Appropriate assembly: Gas, Liquid, etc.
-Right Calibration.
-Connection to the process and accessories: corrosion, plugging, etc.

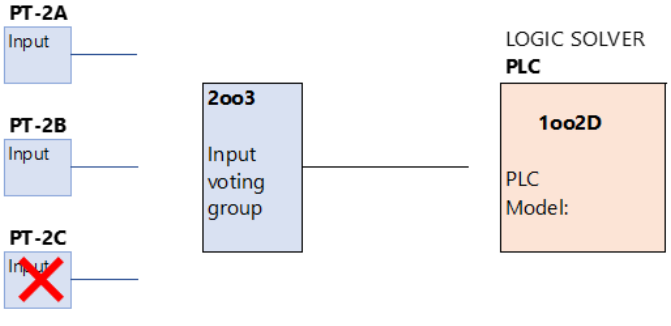

SIF-48
1,20E-02
1,00E-02
8,00E-03
6,00E-03
4,00E-03
2,00E-03
0,00E+00
1 (SIL-2)
2 (SIL-2)
3 (SIL-2)
4 (SIL-2)
5 (SIL-2)
6 (SIL-2)
7 (SIL-2)
8 (SIL-2)
9 (SIL-2)
10 (SIL-2)
11 (SIL-2)
12 (SIL-2)
PFDavg
Max. for SIL-3
Max. for SIL-2

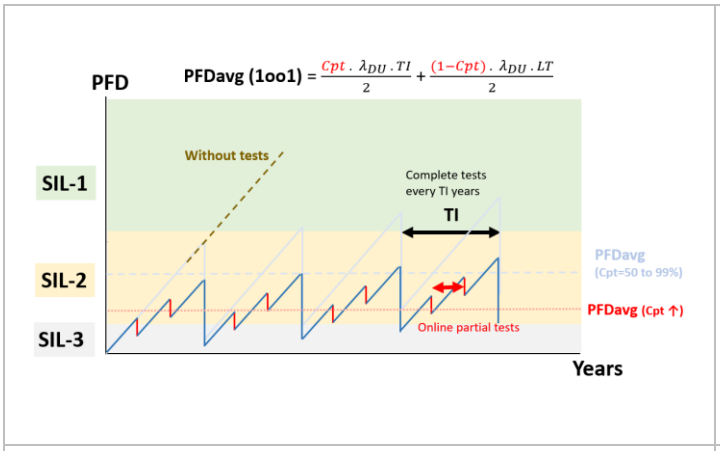

PST is carried out with the process running.
(ISA TR84.00.03)
PLC
ZSL
10% closed limit switch
ZSL
100% closed limit switch
ZSH
100% open limit switch
XVS-2
S
Air
Gas
XV-1

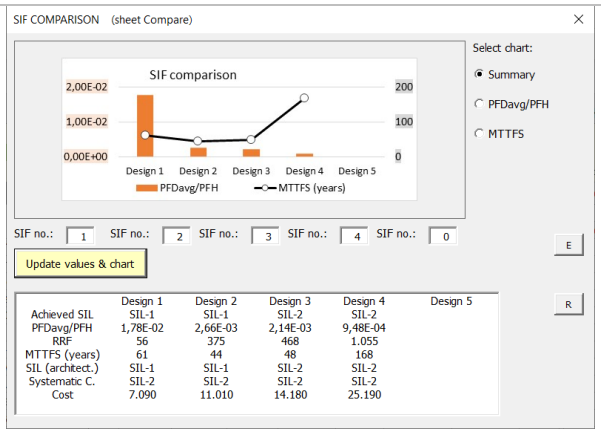

2
Test valve 1
XV-1
Gas
DPT
≠0
XV-2

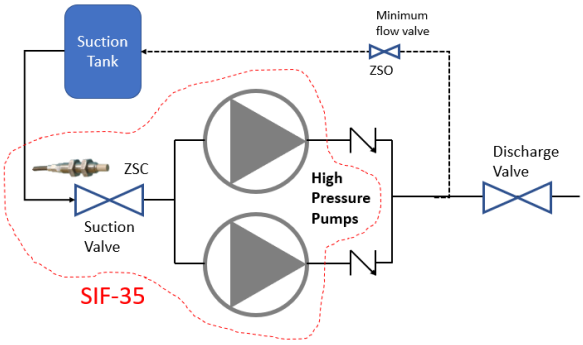

$MTTR_{DD}$ = Mean Time To Restore
S
Air
Pressure Vessel
Bypass valve

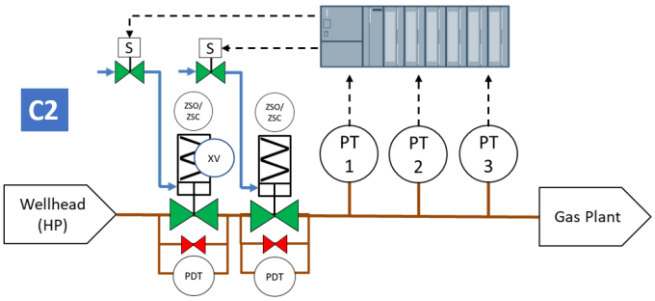

IEC 61511
Process Hazard Analysis & SIL assignment
-Right people
-No time constraints
Safety Requirements Specification (SRS)
-Predefinition of SIFs: Life Time, Startup time, PTC, TI, Beta, application diagnostics, logic/architectures, etc.
-Functional Safety Assessment
SENSOR & ACTUATOR
-SIL capable (certified/prior-use)
-Technology Selection, PST, Reliable Failure Rates
-Interfaces with process
LOGIC SOLVER
-SIL capable, HMI Ergonomy, Alarms, Cybersecurity
DESIGN & BUILD
-SIF Design
-Definition of Proof Testing
-SIL Verification
-Re-design if needed
-SRS update
-Fabrication
TESTS & VALIDATION
-Application Software Test
-FAT & SAT
-Validation
-Functional Safety Assessment (FSA)
Maintenance Plan of the SIS
-Definition of activities, schedules, people, etc.
-Periodic Functional Safety Assessment (FSA)
Maintenance Effectiveness
-Training
-Inspections & Proof Tests
-Repairing, Spare Parts
-Registration
SIS Monitoring
-Maintenance performance, demand rates, reliability parameters.
-Discrepancies between expected vs actual SIF behaviour.
-SIS revalidation when needed

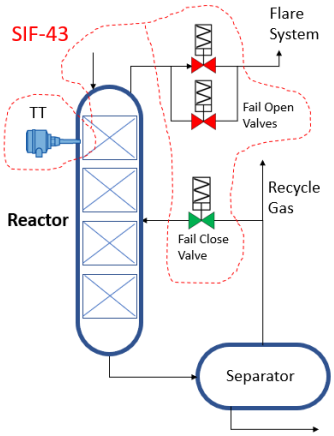

PT-2A
Input
PT-2B
Input
PT-2C
Input
2oo3
Input voting group
LOGIC SOLVER
PLC
1oo2D
PLC Model:

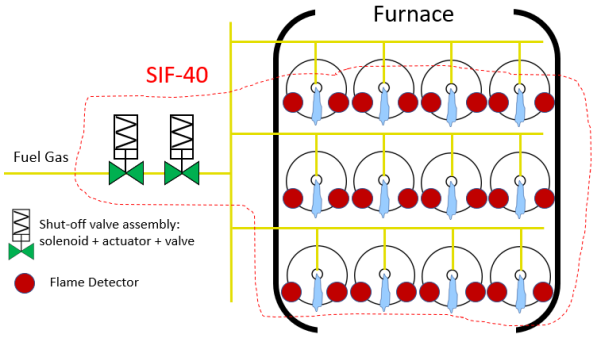

PFD
PFDavg (1oo1) = $\frac{Cpt \cdot \lambda_{DU} \cdot TI}{2} + \frac{(1-Cpt) \cdot \lambda_{DU} \cdot LT}{2}$
Without tests
Complete tests every TI years
TI
SIL-1
SIL-2
SIL-3
PFDavg (Cpt=50 to 99%)
PFDavg (Cpt ↑)
Online partial tests
Years

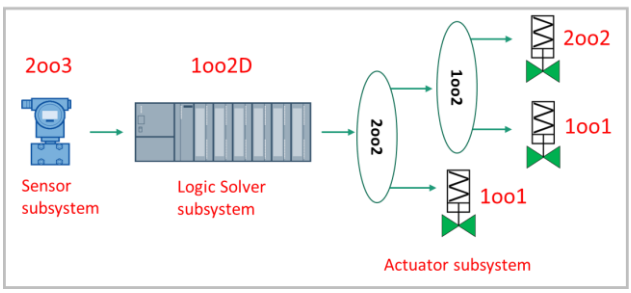

SIF COMPARISON (sheet Compare)
SIF comparison
2,00E-02
1,00E-02
0,00E+00
200
100
0
Design 1
Design 2
Design 3
Design 4
Design 5
PFDavg/PFH
MTTFS (years)
Select chart:
Summary
PFDavg/PFH
MTTFS
SIF no.: 1
SIF no.: 2
SIF no.: 3
SIF no.: 4
SIF no.: 0
Update values & chart
E
R
Achieved SIL SIL-1 SIL-1 SIL-2 SIL-2
PFDavg/PFH 1,78E-02 2,66E-03 2,14E-03 9,48E-04
RRF 56 375 468 1.055
MTTFS (years) 61 44 48 168
SIL (architect.) SIL-1 SIL-1 SIL-2 SIL-2
Systematic C. SIL-2 SIL-2 SIL-2 SIL-2
Cost 7.090 11.010 14.180 25.190

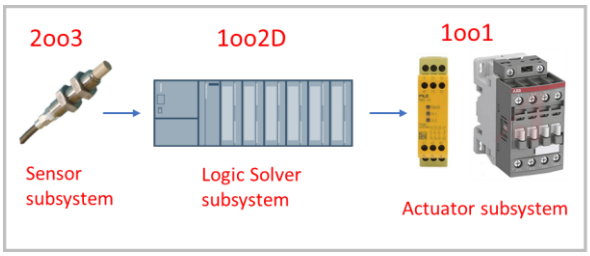

Suction Tank
Minimum flow valve
ZSO
ZSC
Suction Valve
High Pressure Pumps
Discharge Valve
SIF-35

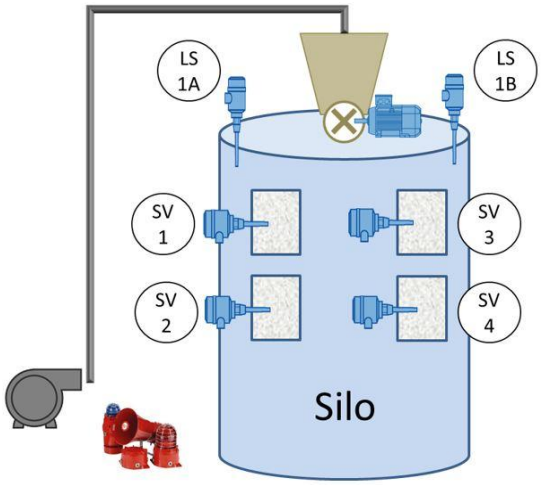

C2
S
S
ZSO/ ZSC
ZSO/ ZSC
XV
PT 1
PT 2
PT 3
Wellhead (HP)
Gas Plant
PDT
PDT

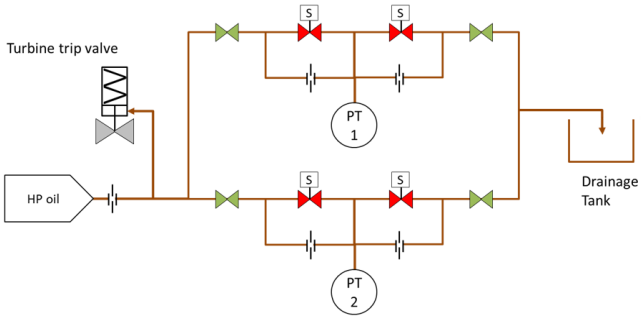

SIF-43
Flare System
TT
Fail Open Valves
Recycle Gas
Reactor
Fail Close Valve
Separator

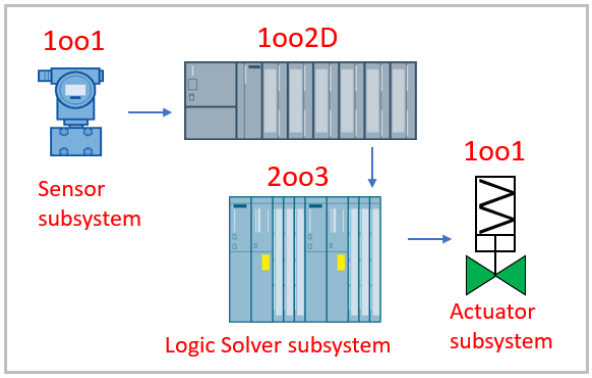

Furnace
SIF-40
Fuel Gas
Shut-off valve assembly: solenoid + actuator + valve
Flame Detector

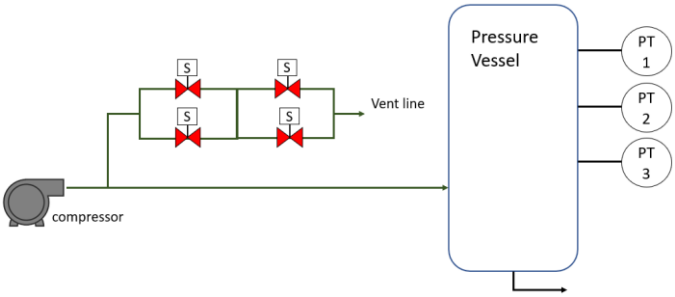

2oo3
1oo2D
2oo2
1oo2
2oo2
1oo1
1oo1
Sensor subsystem
Logic Solver subsystem
Actuator subsystem

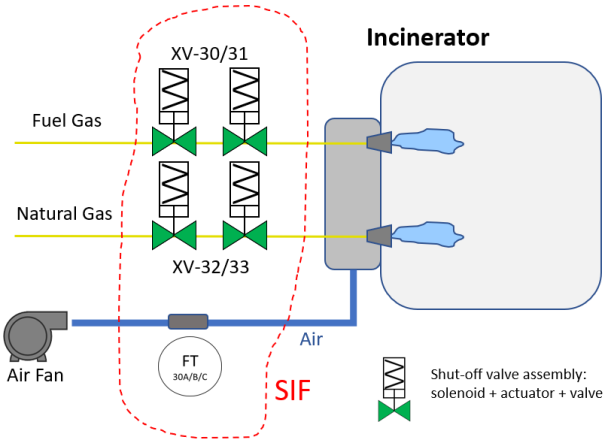

2oo3
1oo2D
1oo1
Sensor subsystem
Logic Solver subsystem
Actuator subsystem

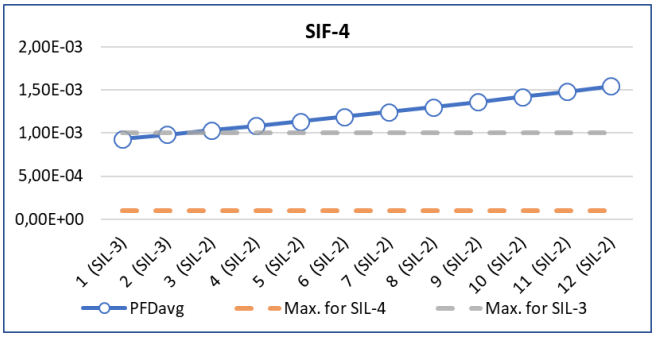

LS 1A
LS 1B
SV 1
SV 2
SV 3
SV 4
Silo


Turbine trip valve
HP oil
PT 1
PT 2
Drainage Tank


1oo1
1oo2D
Sensor subsystem
2oo3
1oo1
Logic Solver subsystem
Actuator subsystem


Pressure Vessel
Vent line
compressor
PT 1
PT 2
PT 3


Incinerator
XV-30/31
Fuel Gas
Natural Gas
XV-32/33
Air
Air Fan
FT
SIF
Shut-off valve assembly: solenoid + actuator + valve


SIF-4
2,00E-03
1,50E-03
1,00E-03
5,00E-04
0,00E+00
1 (SIL-3)
2 (SIL-3)
3 (SIL-2)
4 (SIL-2)
5 (SIL-2)
6 (SIL-2)
7 (SIL-2)
8 (SIL-2)
9 (SIL-2)
10 (SIL-2)
11 (SIL-2)
12 (SIL-2)
PFDavg
Max. for SIL-4
Max. for SIL-3