7. SIF Design – Hardware Fault Tolerance

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

Explain the criteria for designing the architecture of a SIF

TOPICS

Redundancy – different architectures

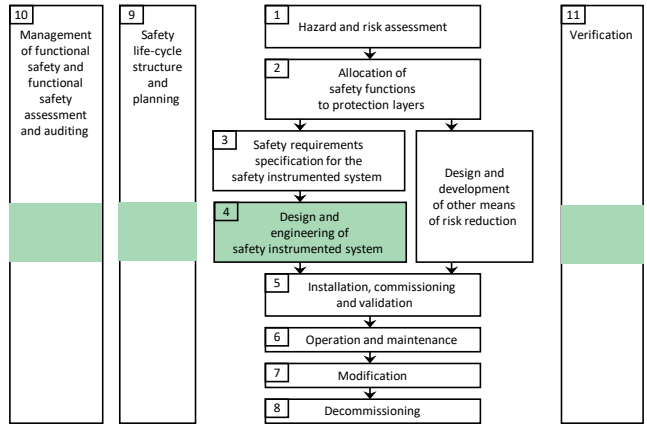
What is Hardware Fault Tolerance?

Apply IEC 61511-1 Table 6 to determine required Hardware Fault Tolerance for each subsystem.

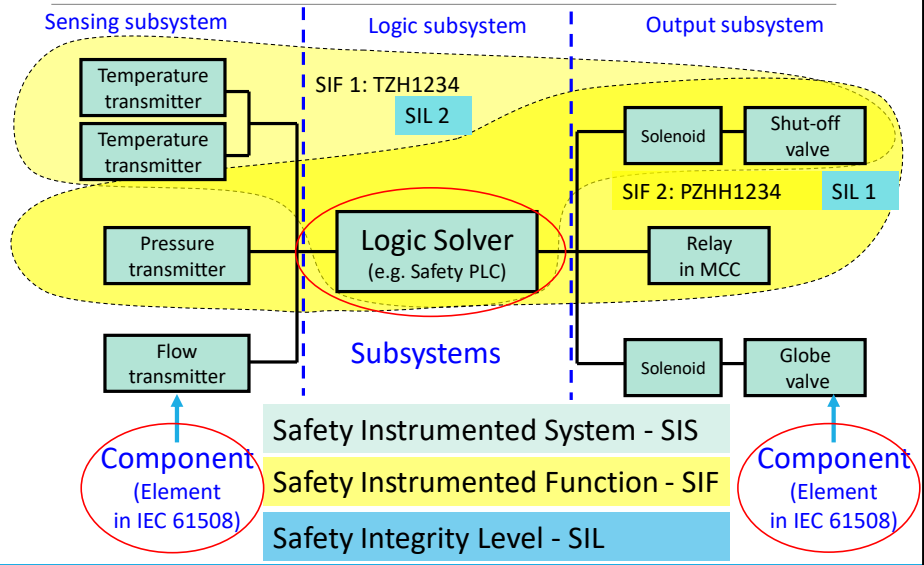
Design & Engineering

Design and implement the SIS to meet the SRS

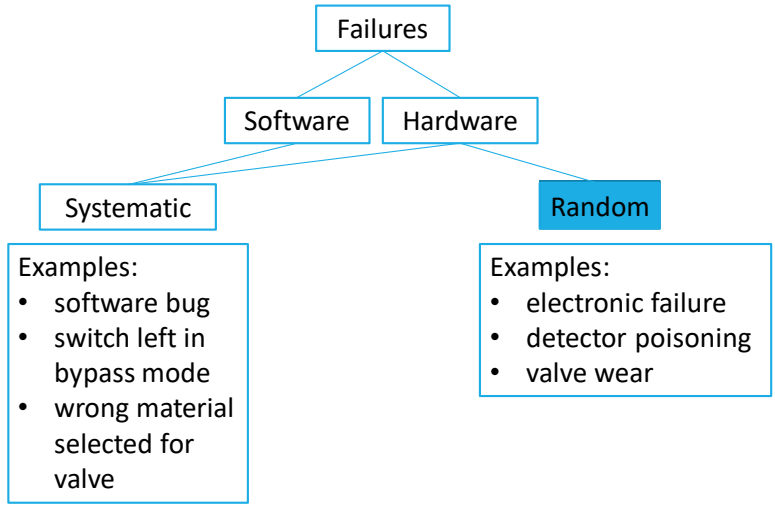
- determine the architecture (Hardware Fault Tolerance) of each SIF



Reminder of Terminology



Different failure types



Design Process

1. Design architecture of each SIF to meet target SIL
2. Confirm that SIF meets required reliability target
   - "SIL verification"
3. Select components suitable for target SIL
4. Detailed design and engineering of the SIS (not part of this course)
   - gas detector coverage is particularly important

Some iteration around steps 1 to 3 may be required

Standards Compliance

Target SIL must be specified for each SIF based on hazard and risk analysis

Processes for SIS throughout lifecycle must comply

Each SIF must meet target SIL requirements for

- Hardware Fault Tolerance (architectural constraints)
- Random failure rate (PFD_{avg})
- Systematic Capability of each component

- selected components must allow the SIF to meet HFT & PFD_{avg} requirements

Redundancy – what is it?

redundancy

- more than one means for performing a required function

In functional safety, redundancy is expressed in terms of safety

- the "required function" (above) is the "safety function"

Redundancy for safety

- more than one means for performing the safety function
- at the subsystem level, refers to the role of that component in performing the safety function
- example: two pressure switches with voted outputs

channel

- a device or group of devices that independently perform(s) a specified function
- at the subsystem level "device" = "component"
- example: a pressure switch

MooN architecture

Expresses the type of redundancy between components

Usually applied within a subsystem
- but can also apply between subsystems

Functional safety architectures always represent the safety function
- beware: this often differs from the implementation voting scheme!

N= total number of channels available to perform the safety function

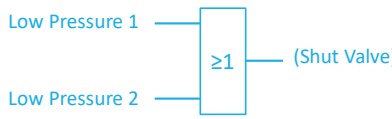
M= minimum no. of channels required to perform the safety function

An MooN configuration will tolerate N-M faults
- Hardware Fault Tolerance (HFT) = N-M

Examples:
- 1oo1 single channel only (HFT = 0)
- 1oo2 two channels; only one required to execute safety function (HFT = 1)
- 2oo2 two channels; both required to execute safety function (HFT = 0)
- 2oo3 three channels; any two required to execute safety function (HFT = 1)

1oo2 Voting

Functional Logic



Either

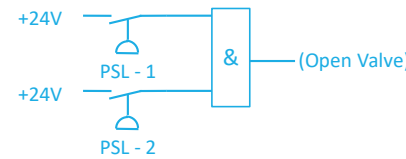
Low Pressure 1

OR

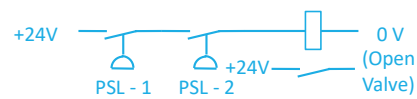
Low Pressure 2

will shut valve

Implementation
- PLC:



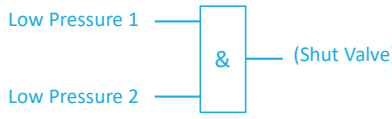
- Relays:



- both PSL-1 & PSL-2 must be energised to hold valve open

2oo2 Voting

Functional Logic



Both

Low Pressure 1

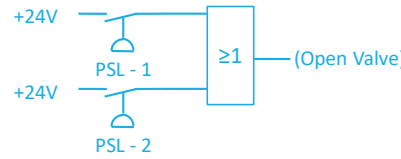
AND

Low Pressure 2

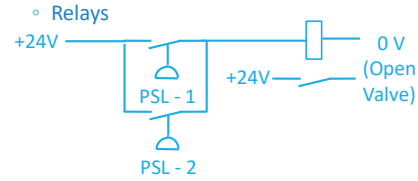
must be true to shut valve

Implementation

- PLC



- Relays



- Either PSL-1 OR PSL-2 must be energised to hold valve open

Beware !

Redundancy is based on the functional logic showing the process actions required to execute the safety function

NOT based on the logic to implement it using normally energised circuits!

- this can be very confusing!

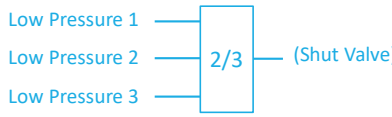
Ask

- how many channels must work correctly for the safety function to operate?

This is M.

2oo3 Voting

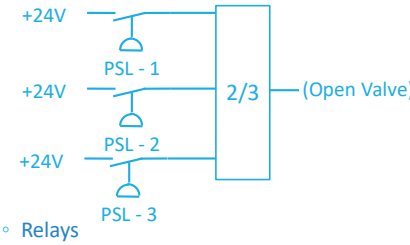
Functional Logic



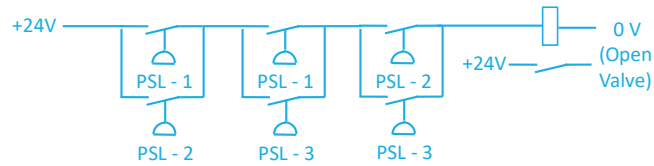
- any 2 pressure switches detecting low pressure will shut valve

Implementation

- PLC



- Relays



- any 2 PSLs must be energised to hold valve open

Hardware Fault Tolerance

Definition

- the number of dangerous random hardware faults that can occur in a subsystem without jeopardising the correct operation of the safety function
  - for MooN architecture, HFT = N - M

IEC 61511 requires a minimum HFT for each SIL

- to avoid unrealistic claims for reliability of a single component
- protects against random hardware failures only

Different rules may be used:

- IEC 61511 Ed. 2 - a modified version of IEC 61508 Route 2H
- IEC 61508-2 Ed. 2 Route 1H
- IEC 61508-2 Ed. 2 Route 2H
- IEC 61511 Ed. 1 –superseded by Ed. 2 which relaxes requirements

We will use IEC 61511 Ed. 2 – preferred approach for process industries

IEC 61508 Ed. 2 Route 1H is also often used (needs SFF and Type A or B)

Required HFT – IEC 61511 Ed. 2

IEC 61511-1 2016 (Ed. 2) 9.2.7 Table 6 and IEC 61508-2 2010 (Ed. 2) 7.4.4.3

Required HFT based on SIL & Mode only

SIL	Mode	Minimum required HFT
1	Any	0
2	Low demand	0
2	High demand or continuous	1
3	Any	1
4	Any	2

IEC 61511 Ed.2 requirements:

- reliability data confidence level must be 70%
- programmable devices must have Diagnostic Coverage > 60%
- reduces HFT by 1 for SIL 2 – 4 compared to Ed. 1

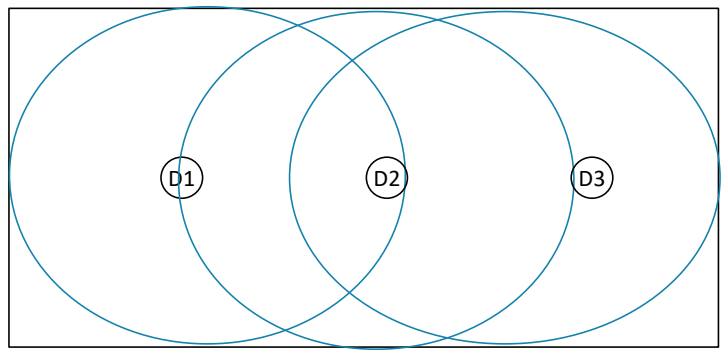
IEC 61508 Ed. 2 Route 2H requirements:

- based on field feedback
- collected in accordance with ISO 14224 or equivalent
- with a statistical confidence level of 90%

HFT for Gas Detectors

Sufficient detectors must be provided to ensure entire area is covered

HFT applies to any point in area e.g. HFT=1 means two detectors can "see" any point in the coverage area:



Case study – Hardware Fault Tolerance

SIF must meet SIL 2

Assume:
- Low Demand mode
- Diagnostic coverage > 60%
- Well understood failure data

Apply IEC 61511-1 Table 6 requirements:

SIL	Mode	Minimum required HFT
1	Any	0
2	Low demand	0
2	High demand or continuous	1
3	Any	1
4	Any	2

Minimum HFT = 0
- one gas detector (minimum) per area covered; one shut-off valve

Note if High Demand mode or SIL 3, need HFT 1: 1oo2 or 2oo3 architecture
- multiple detectors, any 2 can detect low oxygen; 2 shut-off valves in series

Summary

Explained redundancy and the criteria for designing the architecture of a SIF

Redundancy expressed as MooN in terms of safety function
- N = number of channels required to perform safety function
- M = total number of channels required

Hardware Fault tolerance (HFT) = N - M

IEC 61511-1 requires a minimum HFT based on
- SIL required
- mode of operation

One of three criteria to be satisfied
- with PFD_{avg} and Systematic Capability

Questions?