9. SIF Design – Component Selection

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

Explain criteria for selecting components for a SIF

TOPICS

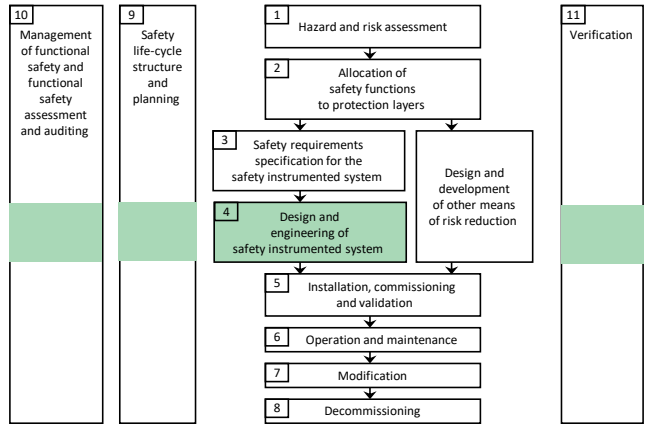
Selecting sensors and valves
- certification
- prior use

Selecting a logic solver
- relays
- standard PLCs
- safety PLCs

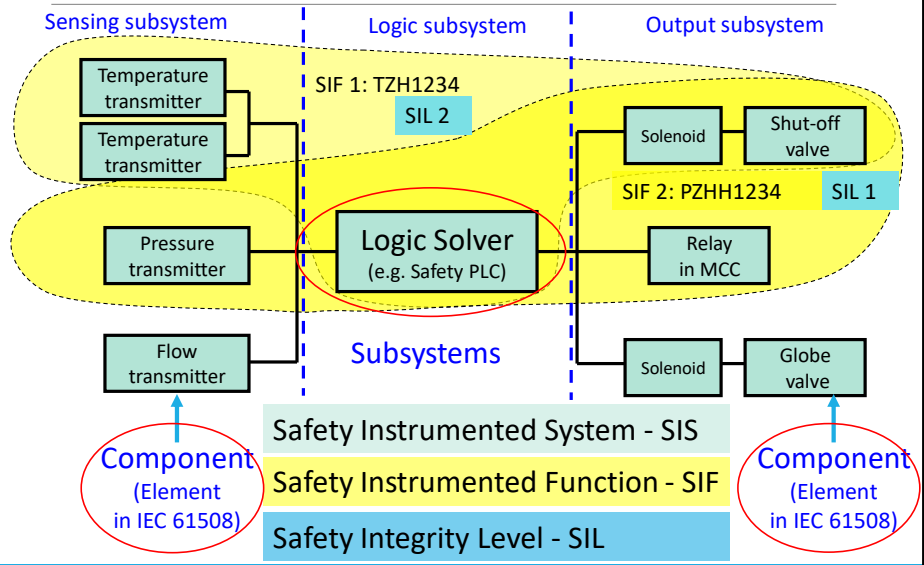
Design & Engineering

Design and implement the SIS to meet the SRS

- select appropriate components for each SIF



Reminder of Terminology



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

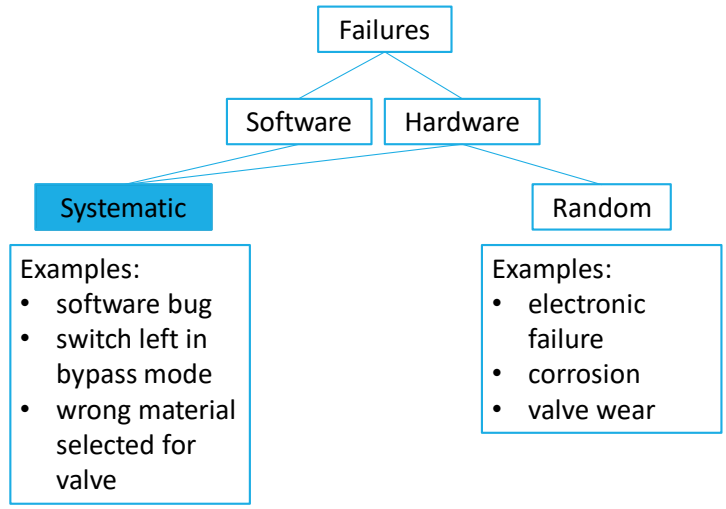
- ☑ Hardware Fault Tolerance (architectural constraints)
- ☑ Random failure rate (PFD_{avg})
- Systematic Capability of each component

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

Component selection criteria

1. Ensure component meets the engineering criteria for the application
   - good instrument engineering practice still applies
   - the instrument must be suitable for the specific fluid conditions & environment
2. Ensure that the Systematic Capability (SC) matches the SIL of the SIF
   - either through independent certification or prior use or (preferably) both
3. Ensure that the component failure rate is sufficiently low allowing for the other SIF components
   - λ_{DU} must be low enough, allowing for other components of the SIF and the proposed test interval
4. Consider the requirements for hardware fault tolerance
   - Use the IEC 61511 criteria
   - Or consider Type A or B & Safe Failure Fraction (SFF) if using Route 1H in IEC 61508

Different failure types



Why is this distinction important?

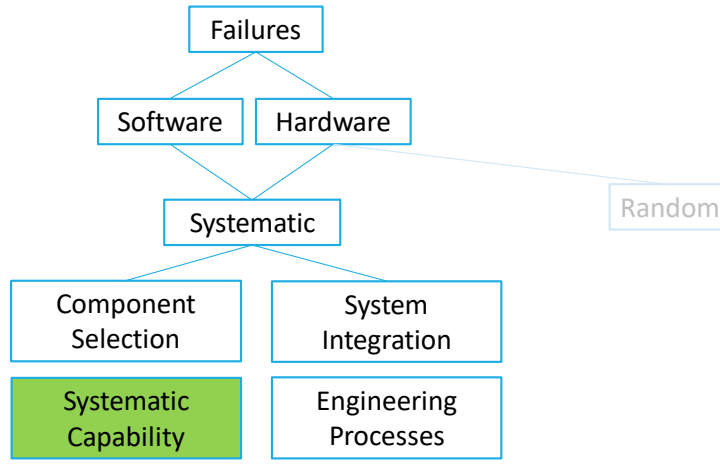
To achieve safety, BOTH random and systematic failures must be minimised

Different techniques are used for each

Quantitative measures discussed so far only apply to random failures

We need to address systematic failures separately

Minimising Systematic Failures



Systematic Capability

Definitions from IEC 61508-4

systematic safety integrity

part of the safety integrity of the SIS relating to systematic failures in a dangerous mode of failure.

systematic capability

measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL . . .

How likely is it that the component is free from systematic faults?

How to achieve Systematic Capability ?

IEC 61511 permits two approaches

1. Select components that comply with IEC 61508 parts 2 and 3
   - How do you know they comply? - independent **certification**
2. Select components based on prior use
   - specific requirements in IEC 61511
   - can also use the "proven in use" requirements of IEC 61508 (more stringent)

Best practice is to require both!

We will look at each approach

Compliance with IEC 61508

IEC 61508 Parts 2 & 3 require appropriate "techniques & measures" (Ts & Ms) to be implemented to

- avoid the introduction of systematic faults and
- control systematic faults if they occur

There are many other detailed requirements

- e.g. for development of ASICs, for communication links etc.

A user has no way of assessing the extent to which the manufacturer has complied with these requirements

Independent certification has therefore become popular for SIF components

- initially for logic solvers
- then for sensors
- more recently for valves

Example Ts & Ms – Fault Avoidance

IEC 61508-2 Ed. 2 Table B.2 – Techniques and measures to avoid introducing faults during E/E/PE system design and development (see 7.4)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Observance of guidelines and standards	B.3.1	M high	M high	M high	M high
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
	Use of well-tried components	B.3.3	R low	R low	R medium	R high
	Semi-formal methods	B.2.3, see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	– low	R low	R medium	R high
	Computer-aided design tools	B.3.5	– low	R low	R medium	R high
	Simulation	B.3.6	– low	R low	R medium	R high
	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

Certification

What is certification?

- an organisation independent of the manufacturer certifies that a device complies with the appropriate clauses of IEC 61508
- certification is paid for by the device manufacturer

Who performs certification?

- a commercial service
- in some countries, the certifying bodies must be accredited

What about TÜV ?

- TÜV stands for "technical surveillance association" in German
- originated in 1800s as state-based boiler inspection authorities
- today these have merged to become three distinct commercial organisations:
  - TÜV Rheinland
  - TÜV Süd
  - TÜV Nord

Who else ?

- exida in the US
- others ?

Example Certificate

Issuing Body

Manufacturer

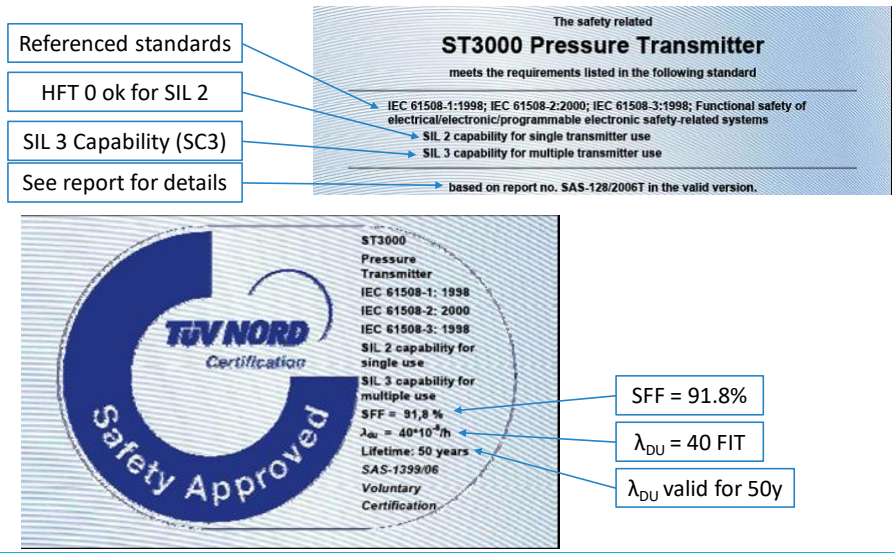
Certified device

See next slide for details

Certificate No.

Expiry Date

Certificate Details



Certification challenges

Make sure you understand exactly what the certificate covers
- see Sample certificates
- each component certified against IEC 61508 Ed.2 2010 requires a Safety Manual (furnished by the supplier)

Understand the constraints in the Safety Manual
- environmental limits
- usage restrictions e.g. usually only apply to “de-energise to trip” usage
- what firmware revisions are covered?

Is the certifying authority accredited (e.g. by DaakS or ANSI)?

Interpret the failure rate figures with great care
- do they reflect your operating environment?
- do they include process connections, filters etc.?

Claiming Prior Use (IEC 61511)

Main aim is to gather evidence that likelihood of dangerous systematic faults is sufficiently low

May also provide reliability data based on actual use, provided that sample size is large enough

IEC 61511-1 11.5.3 key points

- appropriate evidence shall be available that the devices are suitable for use in the SIS
- level of detail depends on the device complexity
- must be in a similar operating environment, but can be in non-safety applications

Evidence required

Manufacturer's quality systems

- how does the user judge this?
- some "prior use" certificates are available that assess this independently
  - is ISO 9000 certification sufficient ?

Devices must be identified adequately

- same model, same software version etc.

Operating environment must be similar

- does not have to be in safety applications
- may be across organisations

Volume of operating experience

- user's approved equipment list
- extensive history of satisfactory performance with unsatisfactory devices eliminated
- may be challenging to identify if operating environments are sufficiently similar

Prior use challenges

Is sample size sufficient?

How similar are operating environments?

How similar are the devices (e.g. firmware revisions)?

Have all failures been documented?

Would the written evidence stand up in court?

Certification vs Prior Use

Certification

- simple to use !
- based on assessment of the manufacturer's design, manufacturing and management processes
  - difficult for user to do
- theoretical distribution of failure rates and diagnostic coverage, based on FMEDA
  - independent of no. of units in service
- theoretical failure data may not reflect your planned usage environment or include process elements
- does not assess systematic errors in actual use
  - maintenance & operating environment

Prior Use

- simple to abuse!
  - tempting to claim without sufficient evidence
- based on actual achieved performance
  - failure data reflects real world usage
- difficult to obtain sufficiently large sample size
  - new devices
  - small companies
- if claimed appropriately reflects actual application and maintenance environment

Best practice

Use both certification and prior use

Certification
- provides assurance of vendor's processes
- provides useful distribution of failure modes

Prior Use
- reflects performance under real-world conditions
- reflects actual environment
  - process fluids
  - weather
  - maintenance
  - management
  - etc.

Large companies are pooling actual performance data anonymously to overcome some limitations of prior use
- e.g. OREDA, FARADIP, PERD databases

Logic Solvers

Types of Logic Solvers

Relays
- traditional electromechanical logic
- up to SIL 3

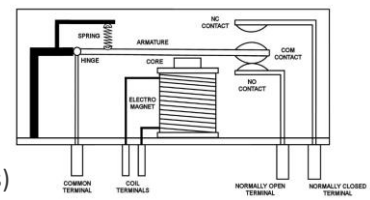
Solid State Logic
- passive or active logic
- up to SIL 4

Standard PLCs
- need to be “safety configured”
- up to SIL 2 with prior use claim

Safety PLCs
- independently certified
- up to SIL 3

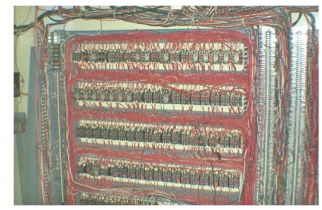
Relays - characteristics

Discrete electromechanical devices
- historically the only choice until the mid 1970s



Programmed by wiring
- do you know what is actually installed?

Well-defined failure modes (“Type A” devices)
- but not perfectly “fail safe” as many assume!
- SFF typically around 70%



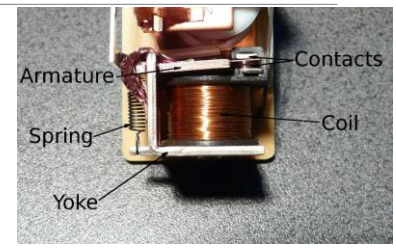
Low cost for small systems

Immune to interference

High speed

Easy interfacing to on/off devices
- not so straightforward for timers, analogue devices

Relays - Issues



Consider failure modes
- contacts may not all operate together
- contacts may weld
- nuisance trips
- no diagnostics

Communication with operator
- only via hardwired inputs

Complexity increases rapidly with size
- especially adding reliable timers and interfaces to transmitters

Difficult to detect undocumented modifications (e.g. bridges !)

Low initial cost, but high overall cost of ownership

Relays - tips

Use force-guided relays where contacts are to be monitored
- ensures all contacts move together – if one welds others don't move
- use separate relays to provide redundancy
  - series wiring of 2 contacts on the same relay does not improve safety!
- by themselves, they do not improve safety!

Consider using "safety relays" for monitoring, especially for SIL 3
- designed for machine protection to Categories 1 to 4
- ensures all single failures are detected

IEC 61508 certified relays are available
- more commonly certified for machine protection to EN 50205
- beware of certification based solely on high use cycle applications

Ensure contact circuits are protected from overcurrent
- currents limited to < 50% of contact rated current
- install diodes across inductive loads (e.g. solenoid valves)

Microprocessor based - PLCs

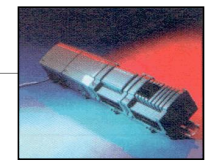
"Programmable Logic Controllers"

Two flavours
- standard industrial, "safety configured"
- safety certified

Programmed in ladder logic or function block languages
- "limited variability languages"

Modular Input/Output (I/O) modules (or "shoebox" for small systems)

PLC - Advantages



Very flexible and scalable

Compact

Easy communication with human machine interface (DCS or SCADA)
- particularly for "integrated" systems

Self documenting
- can easily view the actual logic in use
- online monitoring of dynamic behaviour aids troubleshooting

Excellent control of "forces"

Readily accept analogue inputs from transmitters as well as digitals
- permits improved safety integrity over use of switches

More complex logic does not influence random reliability
- timers and analogue signal processing are easy to implement

PLC - disadvantages

Software based
- assuring software quality requires discipline and skill
- ensuring security can be difficult

Failure modes are complex and can be obscure

Common mode failure of all SIFs can occur
- unlike relays and solid state logic, which are distributed
- but distributed SISs are becoming more common

Effort to "safety configure" standard PLCs is considerable
- not generally warranted

Safety certified PLCs are relatively expensive to purchase
- particularly for small systems
- but lifecycle cost may be lower

What is "safety configured" ?

IEC 61511-1 permits "safety configured" industrial PLCs up to SIL 2

Must satisfy the requirements for prior use (see previous module)

To use a safety configured PLC, you must:
- understand the unsafe failure modes
- configure the system to address the identified unsafe failure modes
- ensure that the embedded software has a good history of use in safety applications
- protect the system against unauthorised modifications

For SIL 2 applications a formal assessment is required
- see 11.5.5.6 for checklist of items

Significant effort is required to fully comply
- not generally warranted
- for significant sized systems a safety PLC will generally be better value

Safety PLCs

PLCs designed specifically for safety applications

Combination of redundancy and high level of diagnostics ensures low probability of a dangerous failure

Require much less configuration of diagnostics by the user
- often only the response to diagnostics needs to be configured
- architecture is transparent
  - e.g. application loaded once to three processors

Can get very low spurious trip rates or pay less if that is not so important
- in some architectures

Purchase cost is greater than standard PLCs

Implementation cost is much less compared to "proper" safety configured PLCs
- but more if safety configuration is ignored !!

Safety PLC architectures

"Triple Modular Redundant" (2oo3D) – Triconex

1oo2D/2oo4D – most other systems
- new systems are mostly 2oo4D

Architectures are complex
- all use voting plus diagnostics
- fault degradation mechanisms vary

Best to rely on certification reports and safety manuals to assess alternatives
- beware of marketing simplifications!

Certification to IEC 61508 is essential
- very reliable, so prior use data usually insufficient

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

Summary

SIF components must be certified and/or meet criteria for prior use

Selecting sensors and valves

- certification measures component "quality"
- prior use measures actual performance in your environment
- best to require both

Selecting a logic solver

- relays
  - for small systems
  - prior use justification is commonly made
- standard PLCs
  - must be safety configured
  - to SIL 2 max
- safety PLCs
  - certified up to SIL 3
  - simpler to apply
  - cost effective for larger systems
  - rely on certification to IEC 61508

Questions?