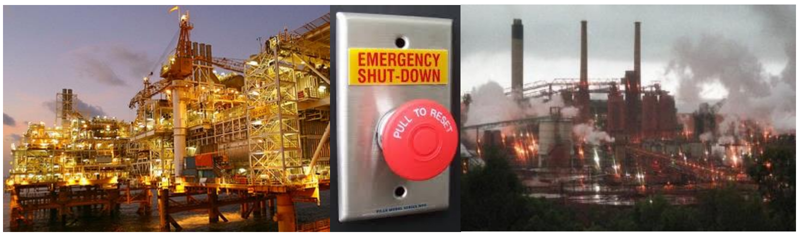


13. Summary – Case Study

GAS DETECTOR FUNCTIONAL SAFETY OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Purpose

The case study is used to summarise the lifecycle requirements from start to finish

TOPICS

Each step of the lifecycle is applied to the case study.

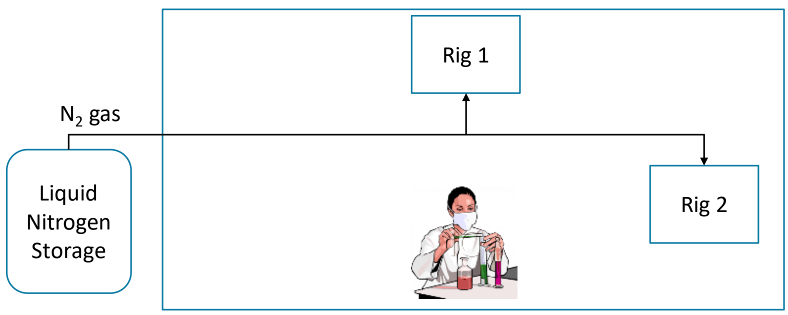
Summarises the whole course

Case Study – Nitrogen use in laboratory

A laboratory uses nitrogen for several experimental rigs; the nitrogen is piped as a vapour from a central liquid nitrogen storage vessel.

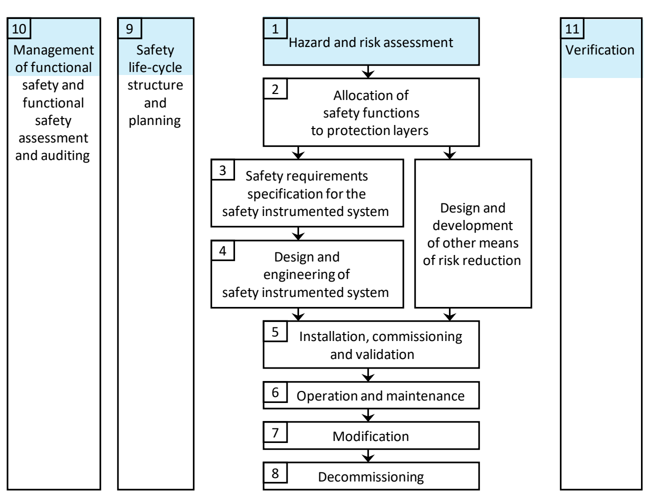
One person normally works in the laboratory when Nitrogen is in use.

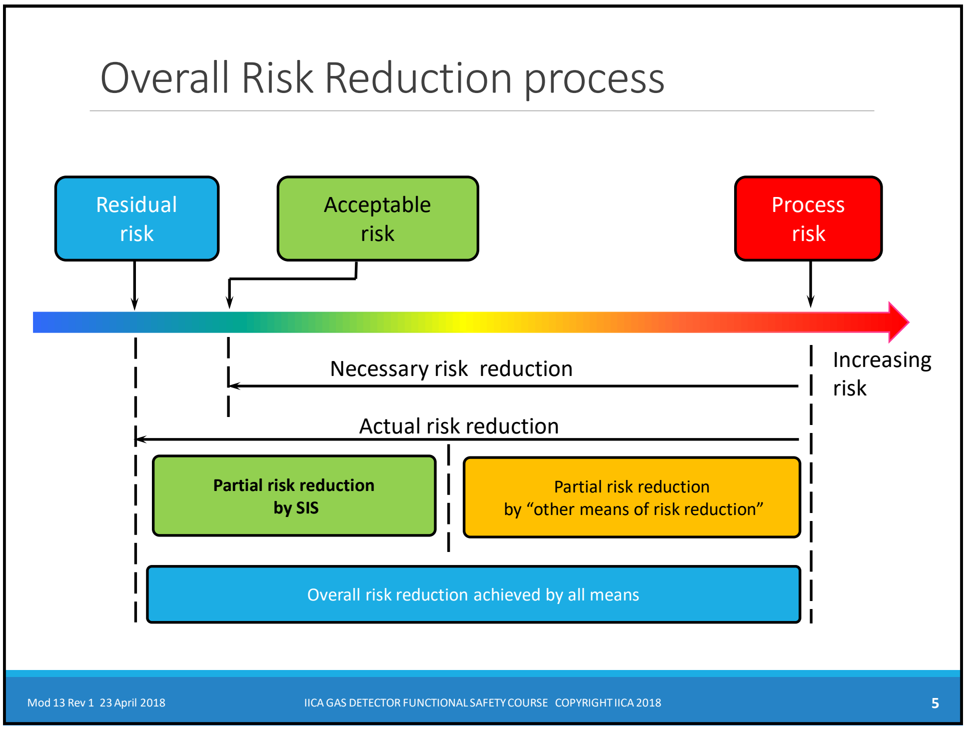
We will use this case study for the rest of the course.

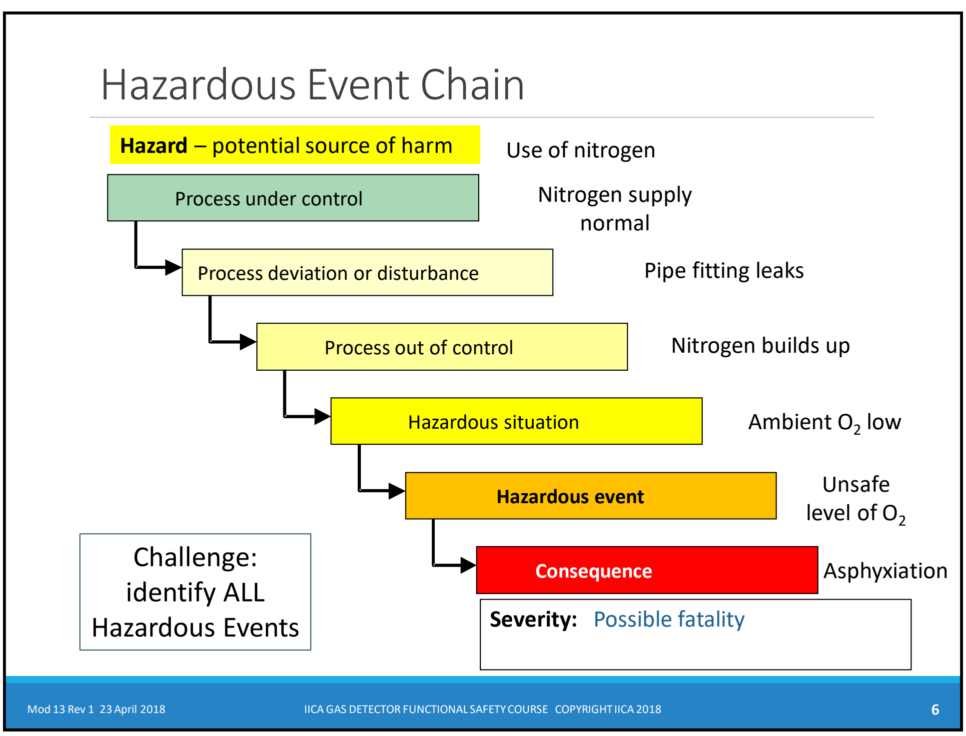


1 Hazard and Risk Assessment

Output is a list of hazardous events with their process risk and acceptable risk.




Overall Risk Reduction process
Residual risk
Acceptable risk
Process risk
Increasing risk
Necessary risk reduction
Actual risk reduction
Partial risk reduction by SIS
Partial risk reduction by “other means of risk reduction”
Overall risk reduction achieved by all means
Mod 13 Rev 1 23 April 2018
IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018
5


Hazardous Event Chain
Hazard – potential source of harm
Use of nitrogen
Process under control
Nitrogen supply normal
Process deviation or disturbance
Pipe fitting leaks
Process out of control
Nitrogen builds up
Hazardous situation
Ambient O_2 low
Hazardous event
Unsafe level of O_2
Consequence
Asphyxiation
Severity: Possible fatality
Challenge: identify ALL Hazardous Events
Mod 13 Rev 1 23 April 2018
IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018
6

Hazard Analysis

Identify hazards from laboratory gases

Should use a a structured process to identify all hazards
- Laboratory hazards are typically well known
- HazOp is widely used in process industries, but not so applicable for laboratories

Checklist approach is recommended
- See: https://www.acs.org/content/acs/en/about/governance/committees/chemicalsafety/hazard-assessment.html

Responsibility of laboratory management

Example hazard:

"Nitrogen used in an enclosed laboratory"

Consequence & Severity

Consequence Categories
- Safety – harm to people
- Environmental – harm to the environment
- Financial – loss of profit
- Others?

Severity grouped in bands
- safety based on likely injuries & fatalities

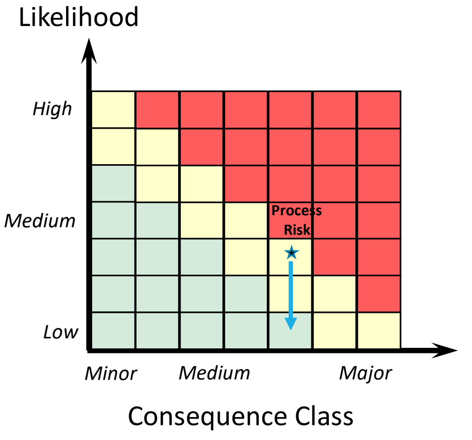
Laboratory example:

"Asphyxiation of one person. Possible fatality."

Case Study – Nitrogen use in laboratory

Hazard & Risk Analysis

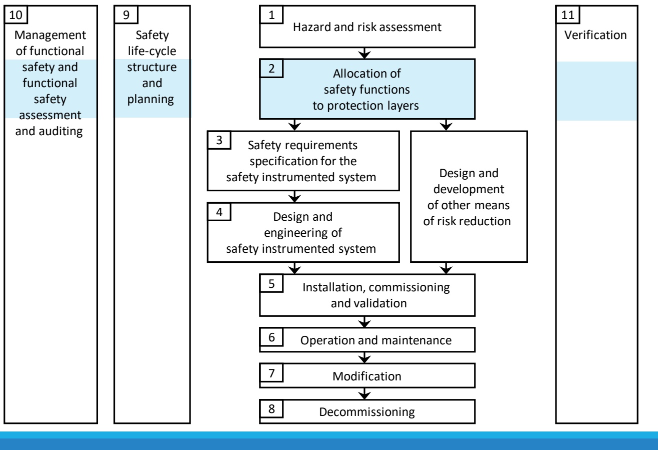
- Hazard
  - Nitrogen vapour
- Hazardous Event
  - Asphyxiation by Nitrogen in room
- Consequence
  - Possible fatality
- Likelihood of release in room
  - Unlikely (less than once per year)
- Risk reduction required



2 Allocation of Safety Functions

Often called SIL Assessment, SIL Analysis, SIL Determination or LOPA

Output is a list of Safety Instrumented Functions together with their required Safety Integrity Level.

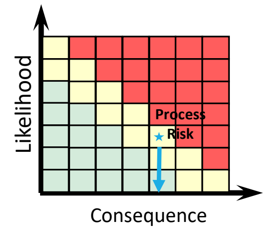


Case Study – Nitrogen SIF

Somehow we need to reduce risk

What could we do?

Let's decide to:
- measure ambient O_2 using gas detectors
- raise alarm when O_2 getting low
- if O_2 very low isolate nitrogen supply
- if O_2 critically low raise evacuation alarm



The automated isolation of the supply is a potential SIF
- **"If % O_2 < 17% then close nitrogen shut-off valve."**

An alarm without automatic action should not normally be a SIF as human response is unreliable

Alarms should be independent of the automated shutdown SIF
- e.g. use a separate sensor where possible

Case Study – SIL Determination

Likely consequence:
- one fatality (C2)

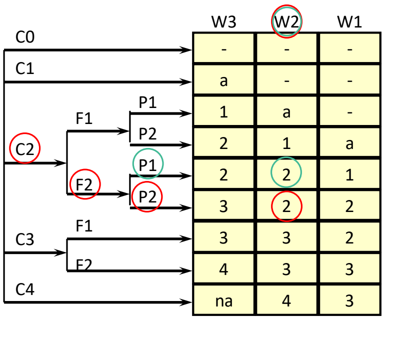
Probability of persons present:
- normally occupied when nitrogen in use, so assume > 90% (F2)

Possibility to avoid the hazard
- if no independent warning alarm 0%. (P2)
- if independent warning alarm 90% (P1)

Frequency of occurrence
- frequency of leak > 1 per 10 y (W2)

Required protection
- SIL 2

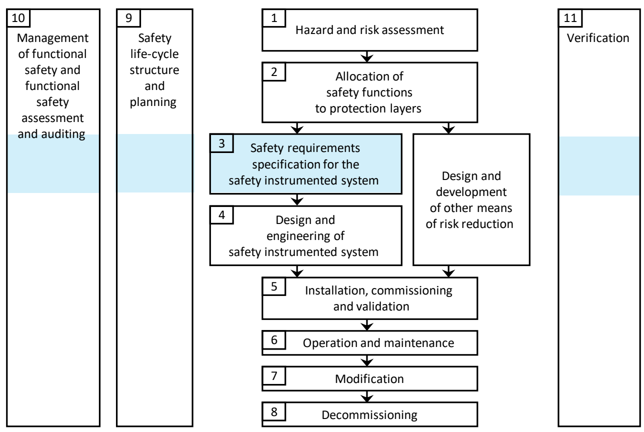
Note if likely consequence >1 fatality need
- SIL 3
- unless occupied < 10% of time and frequency < 1 per 10y



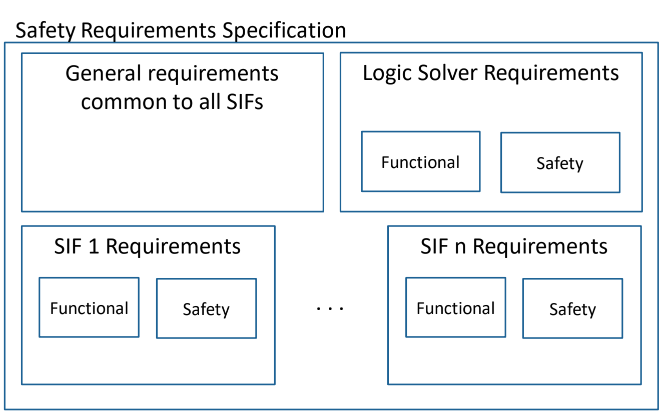
3 Safety Requirements Specification - SRS

Defines functional and integrity requirements of SIS

Output is a set of documents ready for detail design



SRS Contents



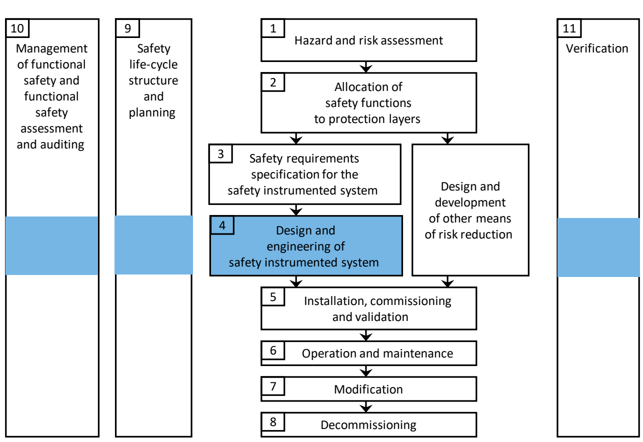
Case Study – SRS for oxygen SIF

SIF ID:	01
Name:	Laboratory low ambient oxygen
Protects against:	Possible asphyxiation; single fatality
Likely cause(s):	Nitrogen leak and ventilation failure
SIF Function:	When oxygen concentration falls below 17% isolate oxygen supply by closing shut-off valves
Other protection:	Independent alarms at 19% and 16% oxygen Ventilation system
Required SIL:	SIL 2
Time between demands:	1 to 10y
Operating Mode:	Low demand
Other requirements:	. . .
References:	. . .

4 Design and Engineering

SIS vendor or contractor for logic solver

EPC contractor or end-user for field hardware

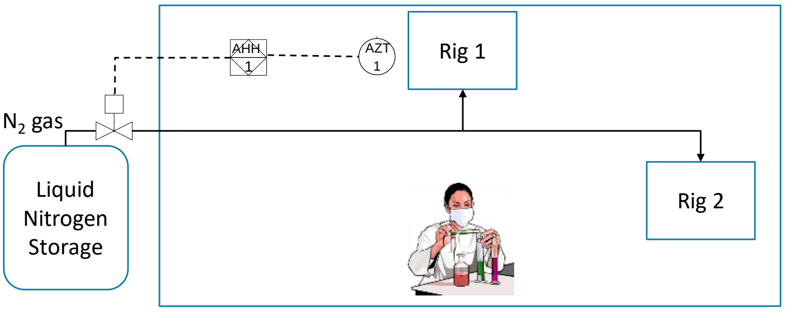


Design a SIF- single detector (Q1)

A laboratory uses nitrogen for several experimental rigs; the nitrogen is piped as a vapour from a central liquid nitrogen storage vessel.

One person normally works in the laboratory when Nitrogen is in use.

Option 1 – Single detector covers entire area.

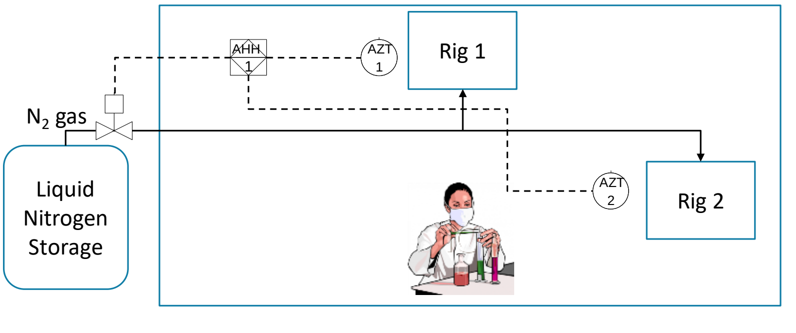


Design a SIF – multiple detectors (Q2)

Option 2 – Two detectors needed to cover entire area.

Note that either only one detector may detect leak depending on where leak occurs. This is still 1oo1 architecture for calculation purposes.

Following answers assume only one detector is required.



Required Hardware Fault Tolerance (Q2, 3)

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

(Q2) Minimum HFT = 0
- one gas detector (minimum) per area covered; one shut-off valve

(Q3) 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

Reference Information

Reliability data λ_{DU}:
- Detector: 0.0667 /y including control unit (gas to relay output)
- Valve: 0.0167 /y

Test Interval:
- 1 year

β factor:
- 5%

Equations:

1oo1 $PFD_{avg} = \lambda_{DU}\, TI/2$

1oo2 $PFD_{avg} = (\lambda_{DU}\, TI)^2/3 + \beta\, \lambda_{DU}\, TI/2$

2oo3 $PFD_{avg} = (\lambda_{DU}\, TI)^2 + \beta\, \lambda_{DU}\, TI/2$

Calculate PFD_{avg} for SIF (Q4)

$PFD_{avg} = \lambda_{DU}$ TI /2

Detector including controller

PFD_{avg} = 0.0667 x 1 /2 = 0.0333

Solenoid valve (assume directly operated, no intermediate relays etc.)

PFD_{avg} = 0.0167 x 1 /2 = 0.00835

Total SIF: PFD_{avg} = 0.0333 + 0.00835 = 0.0417

OK for SIL 1 only

Safety Integrity Level vs. PFD_{avg}

SIL	Risk Reduction Factor (RRF)	Probability of Failure on Demand (PFD_{avg})	Safety Availability
4	> 10,000	$\geq 10^{-5}$ < 10^{-4}	> 99.99%
3	> 1,000 ≤ 10,000	$\geq 10^{-4}$ < 10^{-3}	> 99.9 ≤ 99.99%
2	> 100 ≤ 1,000	$\geq 10^{-3}$ < 10^{-2}	> 99 ≤ 99.9%
1	> 10 ≤ 100	$\geq 10^{-2}$ < 10^{-1}	> 90 ≤ 99%
BPCS*	≤ 10	$\geq 10^{-1}$	≤ 90%
	= 1 / PFD_{avg}	*= 1 / RRF*	*= 100(1 – PFD_{avg})*

Used to specify SIL required

Used to specify SIL achieved

* Basic Process Control System

For Low Demand Mode SIFs only

To meet SIL 2 – Option 1 (Q5, 6)

PFD_{avg} = 0.04 > 10^{-2} so only SIL 1 – need SIL 2

Option 1: test detectors before each 1 week experiment (say)

Assume TI = 1/52 y

$PFD_{avg} = \lambda_{DU}$ TI /2

Detector including controller

PFD_{avg} = 0.0667 x 1/52 /2 = 0.00064

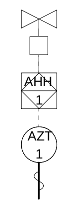
Solenoid valve (assume directly operated, no intermediate relays etc.)

PFD_{avg} = 0.0167 x 1 /2 = 0.00835

Total SIF: PFD_{avg} = 0.00064 + 0.00835 = 0.0090

OK for SIL 2 (just)

Clearly OK for SIL 2 if valve is also tested prior to each experiment (PFD_{avg} = 0.0008)



To meet SIL 2 – Option 2 (Q5, 6)

Option 2: Add redundant detector and valves, each in 1oo2 configuration

Assume TI = 1 y

1oo2 $PFD_{avg} = (\lambda_{DU}\,TI)^2/3 + \beta\,\lambda_{DU}\,TI/2$

Detector including controller

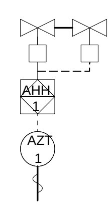
PFD_{avg} = $(0.0667 \times 1)^2$ /3 + 0.05 * 0.0667 /2
= 0.00148 + 0.0016
= 0.00315

Solenoid valve

PFD_{avg} = $(0.0167 \times 1)^2$ /3 + 0.05 * 0.0167 /2
= 9.30 x 10^{-5} + 0.0004175
= 0.00051

Total SIF: PFD_{avg} = 0.00315 + 0.00051 = 0.00366

OK for SIL 2



Component selection (Q7)

The components selected should:

1. Be certified as complying with IEC 61508
   - having Systematic Capability SC2 or greater
   - or "Suitable for SIL 2"
   - see example certificate

and/or

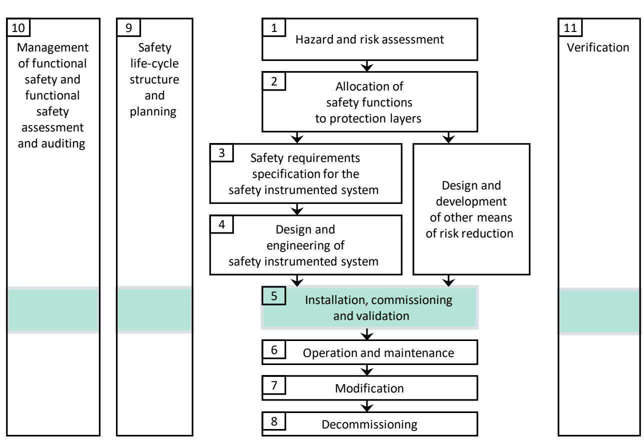
2. Meet prior use requirements
   - sufficient experience gained of clearly identified "identical" components in a similar operating environment
   - manufacturer has a quality system

Best practice is to have both!

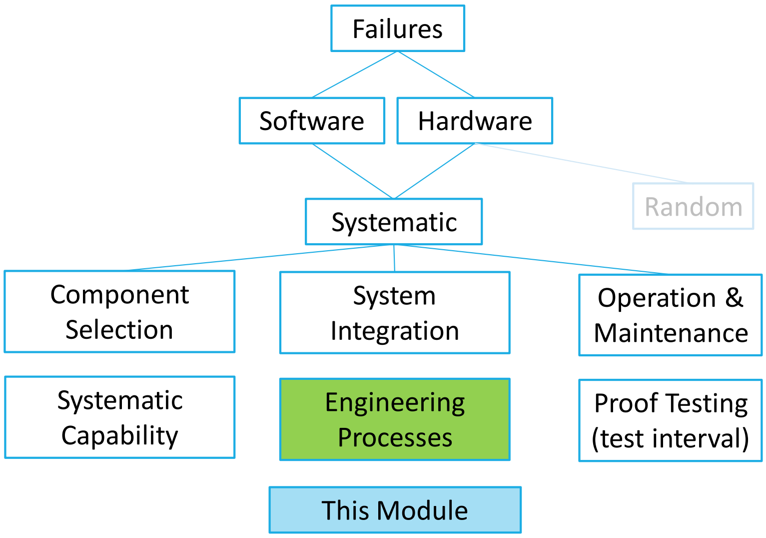
5 Installation, Commissioning, Validation

Logic Solver installed with field equipment

Includes loop checking, validation and final functional safety assessment



Minimising Human Error



Functional Safety Management System

The "Quality System" that manages all the aspects of Functional Safety

May be part of another management system
- quality management system
- process safety management system
- project management system
- etc.

Pulls together all the requirements to manage Functional Safety
- in a coherent system
- based on written procedures aligned with the lifecycle

Based on a "lifecycle" for all the functional safety activities in that organisation
- corporate
- site
- project

Assurance techniques

verification: "build the product right"
- confirms that each step is correct
- performed at each step

validation: " build the right product"
- confirms that the installed SIS meets the Safety Requirements Specification
- just prior to start-up (as a minimum)
- software often validated in Factory Acceptance Test

audit
- confirms that the procedures are appropriate and are being followed

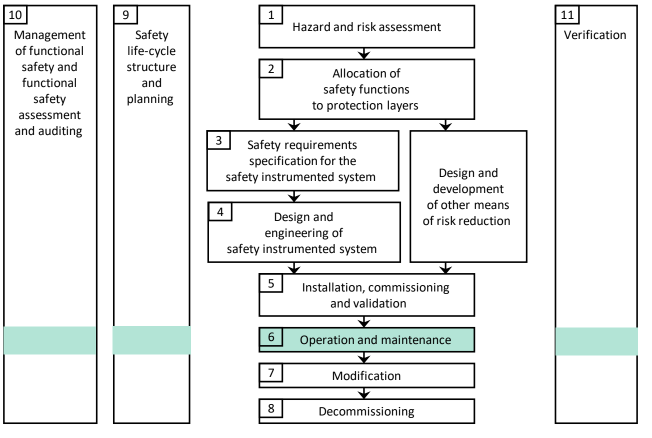
functional safety assessment
- judgement as to whether the required safety is being met

All must be planned & documented

Appropriate independence required

Operations and Maintenance

Operate and maintain the SIS to preserve functional safety as per SRS



Operations' responsibilities

Train operators & maintainers
- what the SIS does
- how to use/maintain the SIS

Manage "bypasses" ("overrides") responsibly
- only for designated purposes for limited time

Proof test each SIF
- at frequency based on SIL verification
- promptly fix any faults found (!)

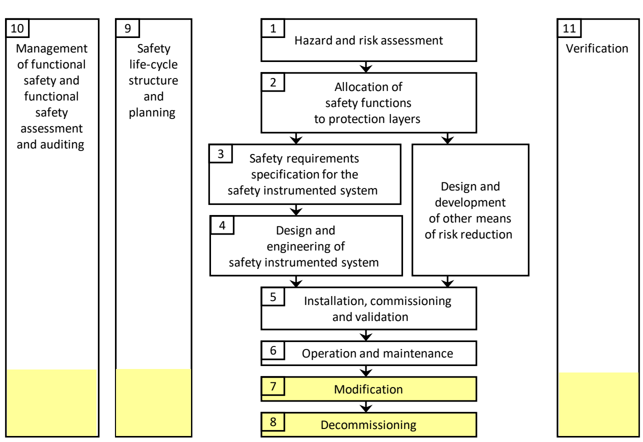
Control modifications to the SIS
- to maintain functional safety at all times

Monitor design assumptions for each SIF
- demand rate
- reliability data
- then update test intervals (or more) if required

Modification & Decommissioning

Ensure functional safety is retained during and after modifications

Ensure decommissioned SIS or SIFs does not reduce functional safety



Aim of control of modifications

Also called Management of Change (MOC)

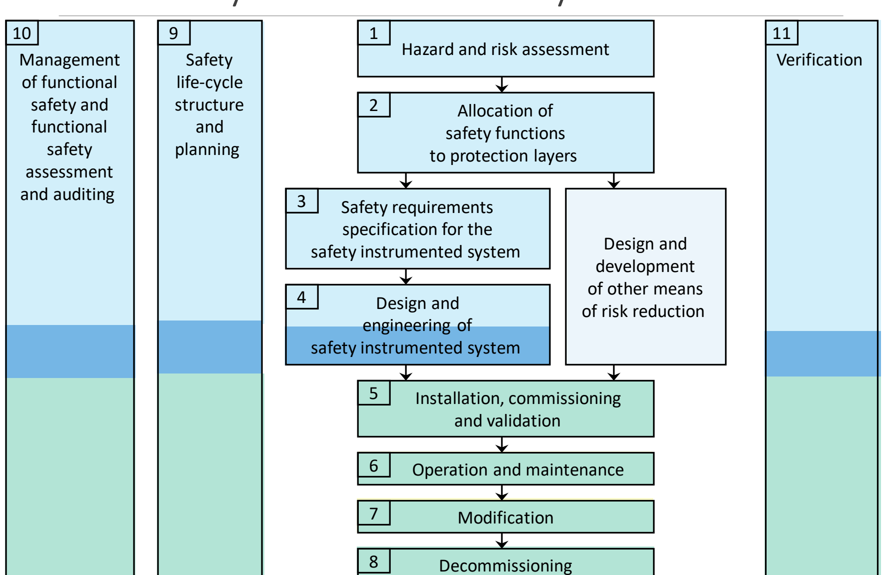
Must preserve functional safety after modification
- how does the proposed modification impact functional safety?
- what measures are needed to ensure the required functional safety is achieved?

Must preserve functional safety during modification
- modification must be planned
- Functional Safety Assessment must be performed prior to undertaking the modification (IEC 61511 Ed.2 new requirement - see 17.2.3, 17.2.6, 5.2.6.1.9)

Applies to:
- SIS hardware
- SIS software
- BPCS that may impact demand rates on SIS or SIS diagnostics
- process changes that may impact SIS including demands

Similar requirements for controlling decommissioning

Summary 1 – The SIS Lifecycle



Summary 2 - 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

Mod 13 Rev 1 23 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 35

Summary

The case study is used to summarise the lifecycle requirements from start to finish

Each step of the lifecycle was used to summarise the whole course

Thanks for your attention!

Questions?