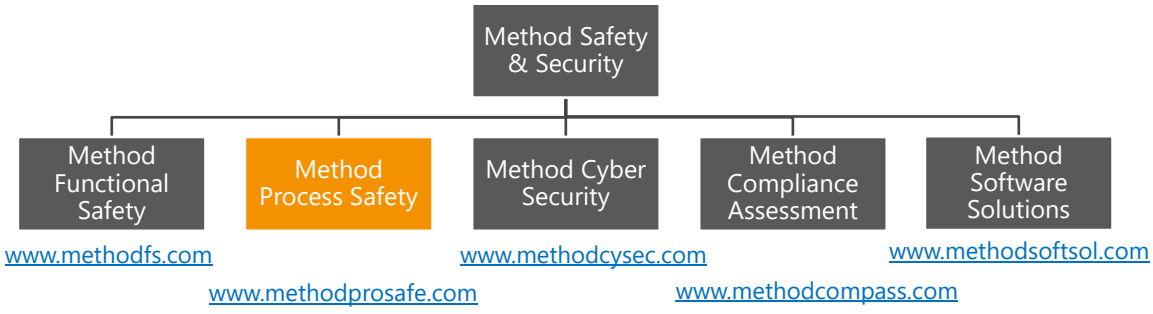
What Process Engineers Should Know About Functional Safety

IChemE Irish Members Group & Engineers Ireland, August 2025

=Method

Who We Are:

=Method are functional safety and process safety consultants and trainers.



=Method

What is Process Safety?

Safety:

- "Freedom from risk which is not tolerable" – IEC61511

Process Safety (CCPS definition):

- Process safety deals with the prevention and control of incidents that have the potential to release hazardous materials or energy.
- Such incidents can cause toxic effects, fire or explosion and could ultimately result in serious injuries, property damage, lost production and environmental impact.

=Method

What is Functional Safety?

"Part of the overall safety relating to the process & the BPCS which depends on the correct functioning of the SIS & other protection layers" - IEC61511

So functional safety is a key thing we do in order to achieve overall process safety, i.e. freedom from intolerable risk.

=Method

Basic Process Control System (BPCS)

- The main purpose of the BPCS is to provide continuous control of the process.
- The BPCS is the main plant DCS or PLC/SCADA system.

=Method

The Functional Safety Standards

IEC61508 – "Functional safety of electrical/electronic/programmable electronic safety-related systems"

This is the "basic safety standard" from which others are derived.

IEC61511 is a version of IEC61508 which has been simplified for the process industries

IEC62061
Machinery Safety

IEC61513
Nuclear Safety

IEC61511
The Process Industries

ISO 26262
automotive software

Etc!

=Method

The Legal Status of IEC61511

- The Health & Safety at Work Act requires you to reduce risk "so far as is reasonably practicable".
- This means you must have systems in place to assess and manage risk.
- IEC61511 is "Recognised as Good Practice" by the HSE for achieving functional safety.
  - Its use is not mandatory, but in practice, it is the easiest (only?) way to demonstrate compliance.

Safety Instrumented Functions (SIFs)

- A protection layer whose objective is to achieve or maintain a safe state of the process when a specific dangerous event occurs.
- Each SIF will have a sensor, a logic solver and a final element.

SENSOR
(input)

LOGIC SOLVER
(makes a decision)

FINAL ELEMENT
(output – takes action)

- These must operate **independently** from the BPCS

Safety PLC photo credit www.hima.com

Safety Instrumented Functions (SIFs)

- Each SIF will have a calculated **reliability**, called a **Safety Integrity Level** (SIL)

SIL	Probability of Failure on Demand (PFDavg)		Risk Reduction Factor (RRF)	
	From	From	To	To
1	0.1	0.01	10	100
2	0.01	0.001	100	1,000
3	0.001	0.0001	1,000	10,000
4	0.0001	0.00001	10,000	100,000

← Works at least 9 times out of 10

← Works at least 99 times out of 100

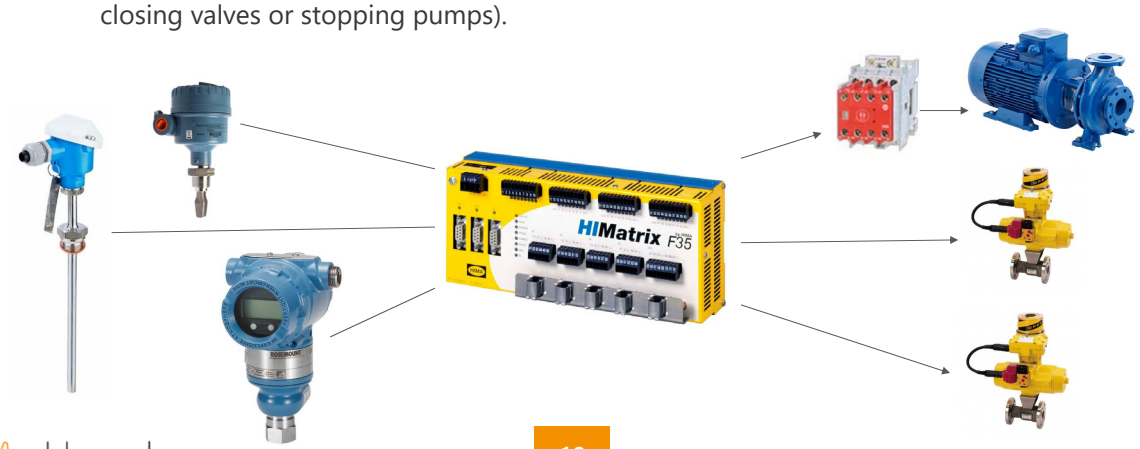
Etc.....

- We usually use LOPA (layer of protection analysis) to decide what SIL is required

=Method

Safety Instrumented System (SIS)

- An independent system, whose function is only to maintain safety.
- **A SIS is usually made up of several SIFs**
- The SIS usually remains passive until there is a process upset that the BPCS does not or cannot deal with, and then acts to bring the process to a safe state (e.g. by closing valves or stopping pumps).



=Method

Instrument photo credit www.emerson.com

The Functional Safety Lifecycle

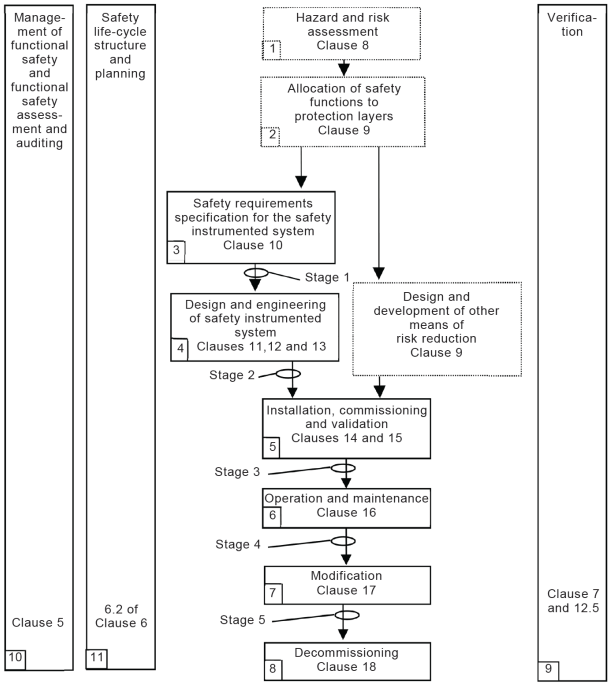


Diagram from
PD IEC TR 61511-0 Fig 1

=Method

The Real Basics

1) Assess your risks
2) Decide what safety functions you need (if any)
3) Design and implement them
4) Keep them well maintained
5) Ensure everything is:
   - Managed well, in accordance with the standard
   - Done by competent people
   - Checked by competent people

=Method

The Role of Process Engineers

- Process engineers have a key role in carrying out hazard & risk assessment (usually using HazOp), and "allocation" (usually using LOPA).
  - It's usually Process Safety Engineers who lead these studies.
- Process engineers must work with ECI engineers to define the SIS
  - Our knowledge of process operation and process hazards is vital in getting this right.

The Role of Process Engineers

SENSOR
(input)

LOGIC SOLVER
(makes a decision)

FINAL ELEMENT
(output – takes action)

ECI Engineers' SIF Description:

"The purpose of this SIF is to close valve X if the temperature goes above 100°C"

The Role of Process Engineers

SENSOR
(input)

LOGIC SOLVER
(makes a decision)

FINAL ELEMENT
(output – takes action)

Process Engineers' SIF Description:

"The purpose of this SIF is to prevent an unventable runaway reaction leading to vessel rupture and up to two fatalities, by closing thermal oil valve X if a malfunction of the BPCS causes the temperature inside the vessel to approach the runaway onset temperature of 120°C"

Defining Safety Instrumented Functions:

A useful acronym is "SLATS":	**Example:**
○ **S**ensing	Measure the reactor temperature using TT01
○ **L**ogic	If TT01 > 100°C THEN
○ **A**ctuate	Close valve x to stop the thermal oil flow
○ **T**iming	Within 30 seconds
○ **S**afety integrity (SIL)	And do it to SIL 1 reliability with a PFD of 0.05

Some Things to be Aware of

- Chemical industry SIFs are generally “low demand mode”
  - i.e. we expect them to operate less than **once** per year.
  - If your SIFs are activating more often than that, it is important that you investigate why and fix the underlying process.

Some Things to be Aware of

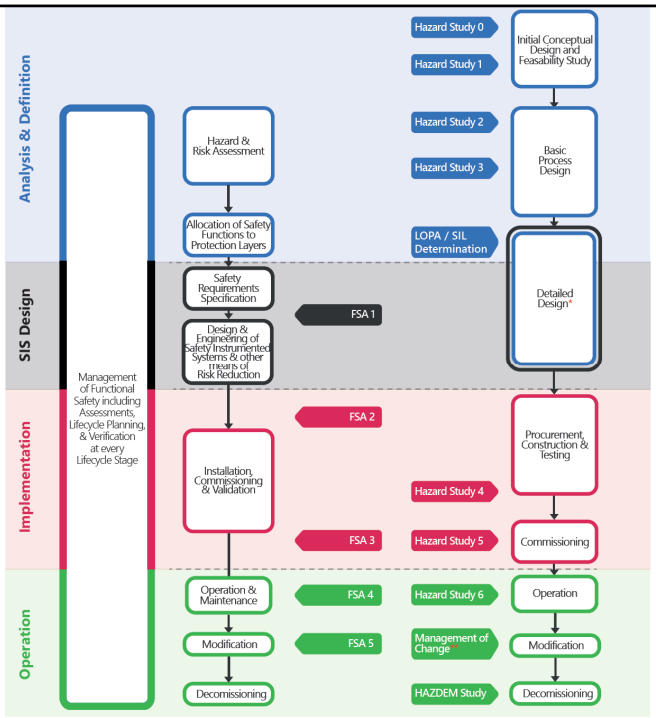
- HazOp and LOPA are functional safety lifecycle stages, so they need functional safety management (FSM)

  To be compliant……
  - Plan what you’re doing in advance
  - Ensure everybody is trained and competent
  - Ensure everything is independently verified (checked)

Tying the PS and FS Lifecycles Together:

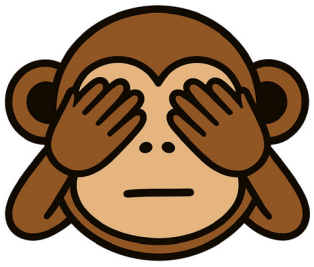
Activities:
- **Analysis and Definition**
- **SIS Design**
- **Implementation**
- **Operation**

* It is also usual for the hazard study 3 to be reviewed and revised during the detailed design phase, especially for large projects.
** Management of change (MOC) usually includes a review of the Hazard Study 3 (HazOp). However, depending on the change being made, other hazard studies may also have to be revised.



MA001.003 v2.2

SHAMELESS PLUG ALERT!



Relevant Method Training Courses

=Method Hazard Study Leaders & Team Members Courses

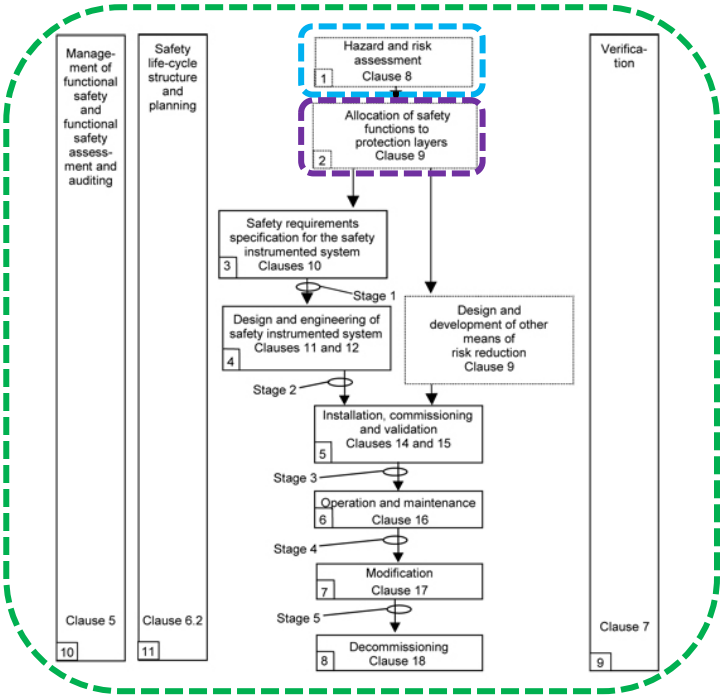
=Method LOPA Leaders Course

=Method TÜV Certified Functional Safety Training Course and Examination in IEC61508 or IEC61511

=Method Process Safety Management Training Course

=Method "Achieving ALARP" Training Course

=Method



QR Code for IChemE Survey:

What Process Engineers should know about Functional Safety - 19th Aug 25

Link for Details of Training Courses:

Process Safety:

https://www.methodprosafe.com

Functional Safety:

https://www.methodfs.com