Functional Safety Demystified

BOB WEISS - FUNCTIONAL SAFETY CONSULTANT

ADAPTED FROM A PRESENTATION GIVEN TO A IICA TECHNICAL EVENING – 12TH SEPTEMBER 2019

1

Purpose

Explains how to comply with

AS IEC 61511 Ed.2

using a case study

TOPICS

What is Functional Safety?
- SIS, SIF and SIL

Standards IEC 61508 and IEC 61511

A case study demonstrates
- how to comply
- some issues and tips to address them

4 day TÜV Rheinland FSEng course in 60 minutes!

2

What is Functional Safety?

New term in IEC 61508 (introduced in 1999)

Part of Overall Safety
- freedom from unacceptable risk

Achieved by a Safety Instrumented System (SIS)
- E/E/PE Safety System in IEC 61508
- Examples:
  - Trip System
  - Emergency Shutdown System
  - Burner Management System
- Includes field devices as well as logic solver

A SIS places or maintains a process in a safe state
- Process = Equipment Under Control (EUC) in IEC 61508
- Implements Safety Instrumented Functions (SIFs)
- Each SIF achieves a Safety Integrity Level (SIL)

Acronyms to remember: SIS, SIF and SIL !.

3

AS IEC 61511-1, 2 & 3

Functional safety: Safety Instrumented Systems for the process industry sector

Part 1	Framework, definitions, system, hardware and software requirements	Normative
Part 2	Guidelines in the application of part 1	Informative
Part 3	Examples of methods for determining safety integrity in the application of hazard & risk analysis	Informative
2003	All three parts published as IEC standard	
2004	AS IEC 61511-1/2/3:2003 issued unchanged	
2016	IEC 61511-1/2/3:2016 Ed. 2 issued by IEC with part 1 corrigenda and many typos	
2017	IEC 61511-1 Ed. 2.1 published incorporating corrections	
2018	AS IEC 61511-1/2/3:2018 Ed. 2 adopts IEC Ed. 2.1	
2018	SA TR IEC61511.0:2018 issued; overview technical report	
2020	IEC TR 61511-4:2020 Part 4 issued. Tech report explaining the rationale for changes in IEC 61511-1 from Edition 1 to Edition 2	

4

IEC 61508 or IEC 61511

IEC 61508	SIS device manufacturers	SIS integrators & users SIL 1-3	SIS integrators & users SIL 4
IEC 61511		SIS integrators & users SIL 1-3	for process industries

Integrators & users in the process industries can use either IEC 61508 or IEC 61511

IEC 61511 is generally simpler to apply

2nd Ed. allows SIL 4 with many conditions

5

Why Functional Safety?

Buncefield, England 11 Dec 2005

Storage tank level gauge showed constant reading

High level switch left in test mode

Gasoline tank overflowed

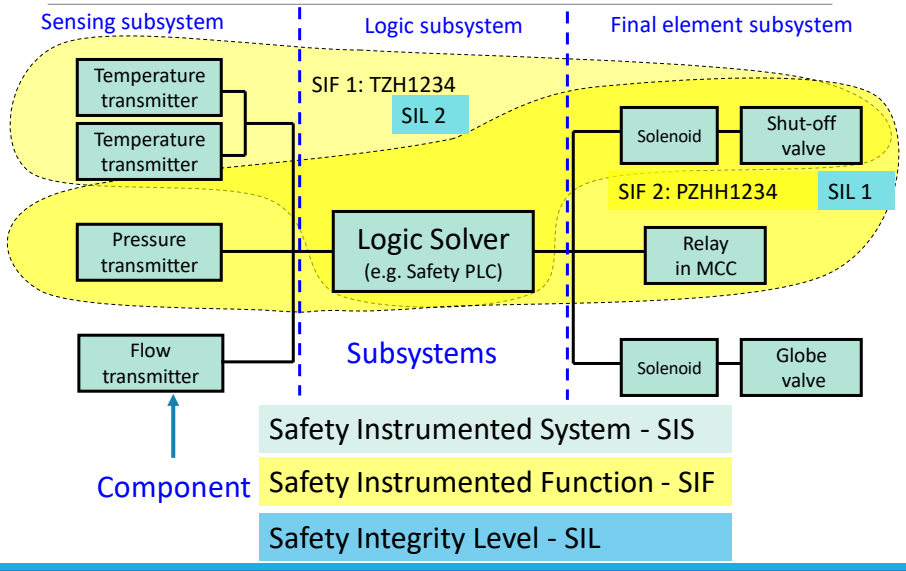
Mist exploded

- largest peacetime explosion in Europe
- 20 tanks on fire
- burned for three days
- significant environmental impact
- hundreds of millions of pounds damage

Should have complied with IEC 61511.

6

Basic Terminology



7

Safety Integrity Level vs. Risk Reduction

SIL	Risk Reduction Factor	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%
	$= 1 / PFD_{avg}$	$= 1 / RRF$	$= 100(1 - PFD_{avg})$

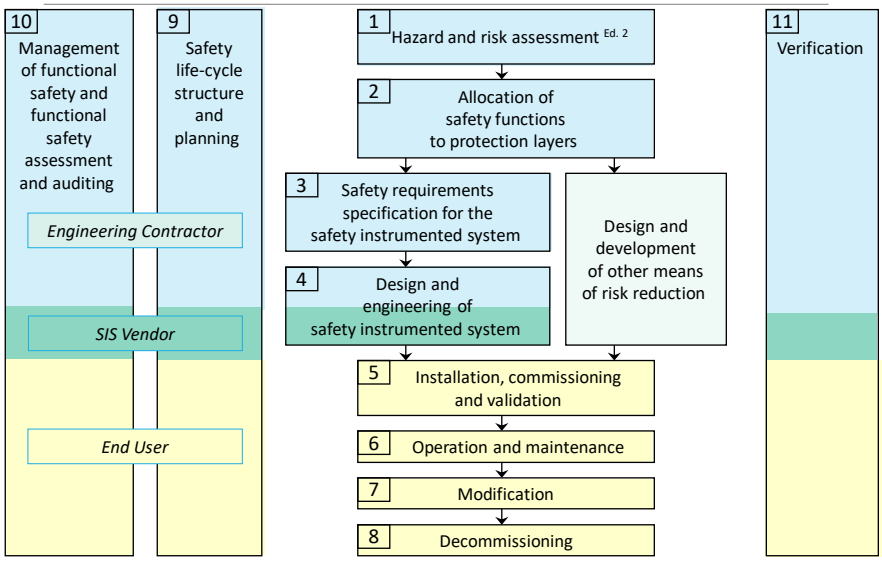
Used to specify SIL required — Used to specify SIL achieved

* Basic Process Control System

For Demand Mode SIFs only

8

Safety Lifecycle – IEC 61511



9

Complying with IEC 61511

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:

- Random failure rate (PFD_{avg})
- Hardware fault tolerance (architectural constraints)
- Systematic capability for each component
  - Field devices, logic solver, shutdown valves etc.

Not just TÜV certification

- Though it helps !

Not just meeting PFD_{avg} target.

10

Comply Throughout Lifecycle

For the rest of the presentation we'll follow the SIS lifecycle with a simple case study

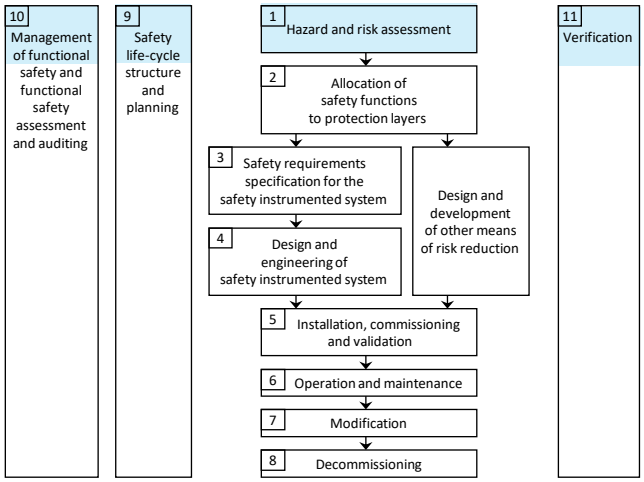
What do we need to do to comply at each stage?

Possible issues and how to address them will be explained

11

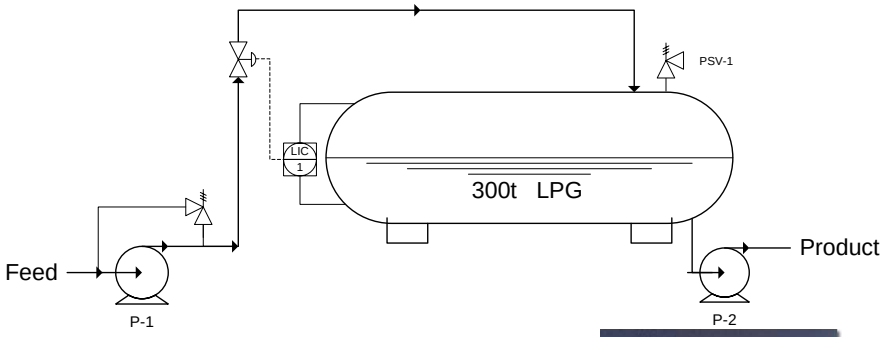
1 Hazard and Risk Assessment

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



12

A hazard



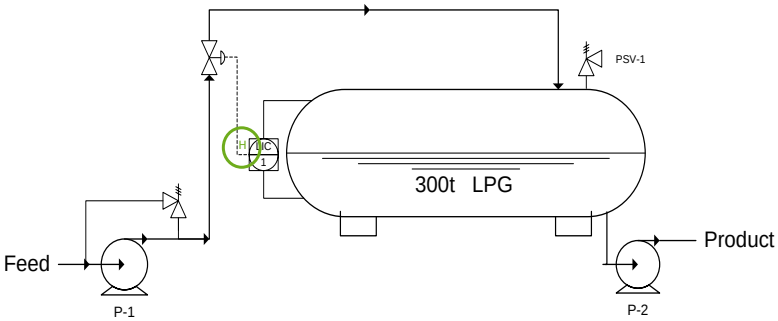
A “potential source of harm”

300t of Liquefied Petroleum Gas can potentially cause harm

Hazardous Event Example – BLEVE (video)

13

Identify Hazardous Events: HAZOP



Node: LPG Tank

Guideword: HIGH LEVEL

Consequence: High Pressure, possible tank rupture & major fire

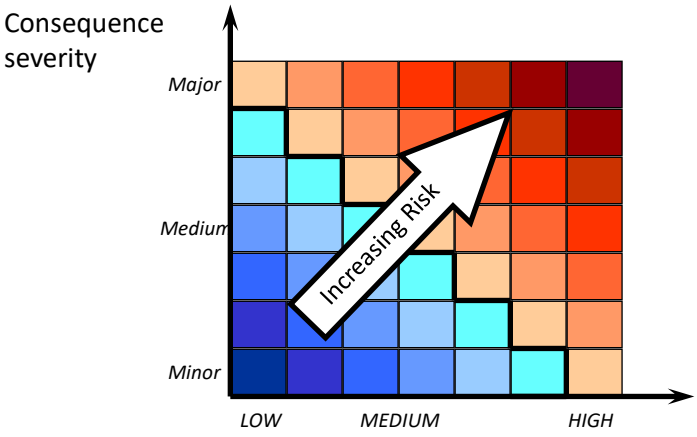
Existing Controls: Pressure Safety Valve (PSV-1)

New Controls: Add High Level Alarm

14

Risk

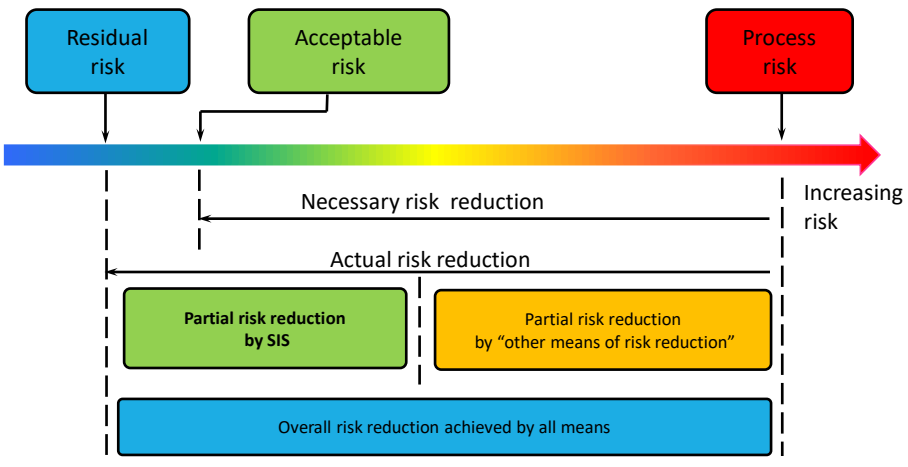
The product of severity and likelihood



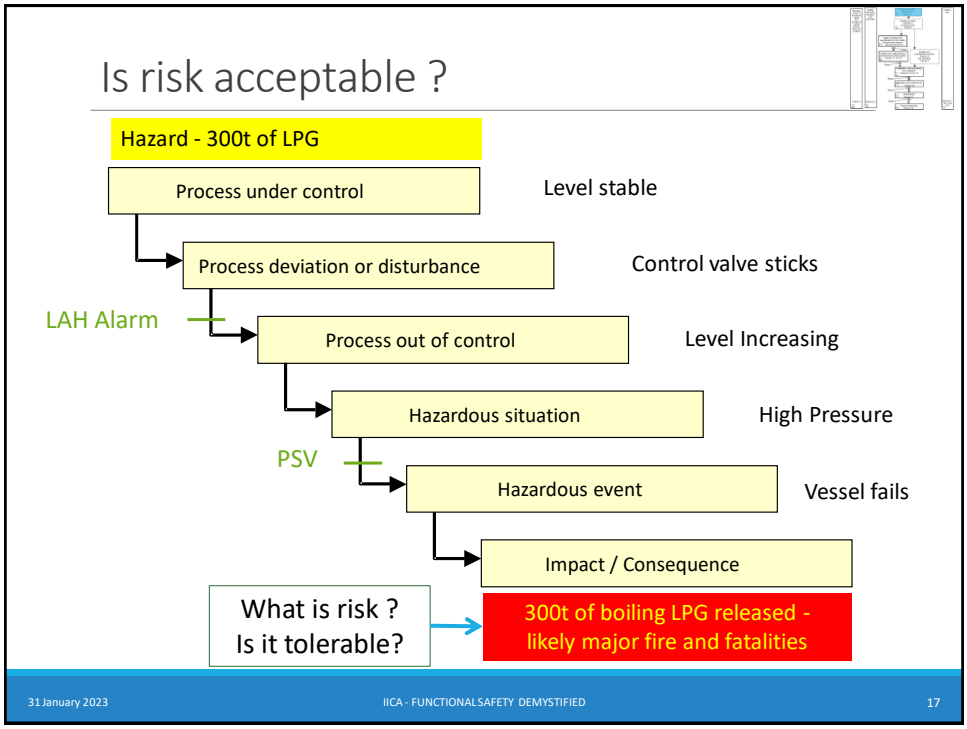
"The expected value of loss"

15

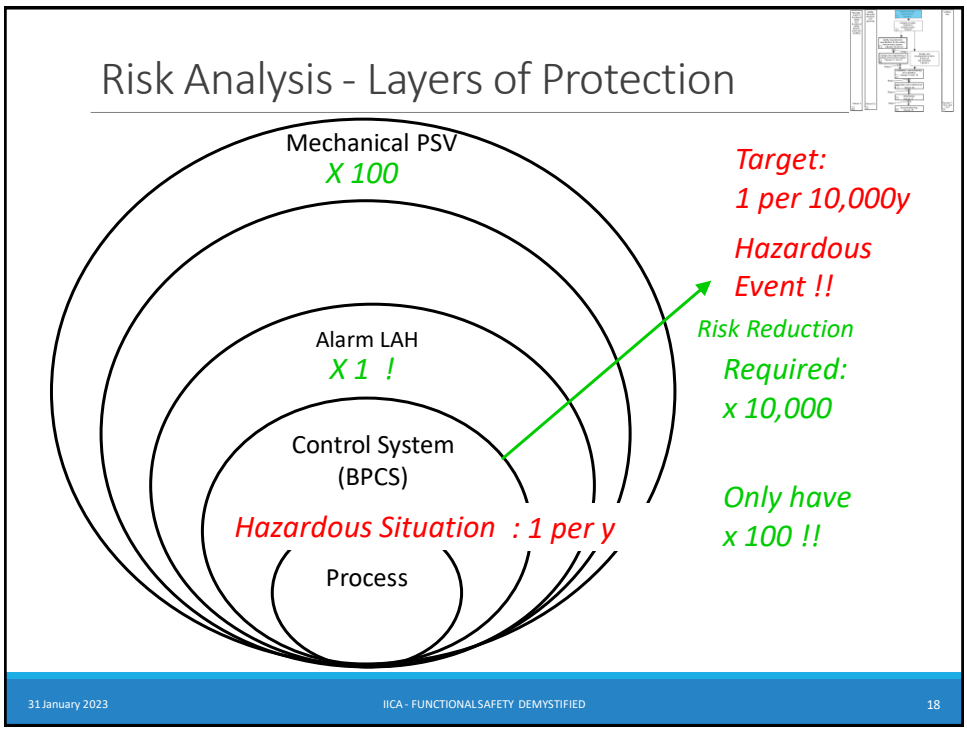
Risk reduction concept



16


Is risk acceptable ?
Hazard - 300t of LPG
Process under control
Level stable
Process deviation or disturbance
Control valve sticks
LAH Alarm
Process out of control
Level Increasing
Hazardous situation
High Pressure
PSV
Hazardous event
Vessel fails
Impact / Consequence
What is risk ?
Is it tolerable?
300t of boiling LPG released - likely major fire and fatalities
31 January 2023
IICA - FUNCTIONAL SAFETY DEMYSTIFIED
17

17


Risk Analysis - Layers of Protection
Mechanical PSV
X 100
Alarm LAH
X 1 !
Control System
(BPCS)
Hazardous Situation : 1 per y
Process
Target:
1 per 10,000y
Hazardous
Event !!
Risk Reduction
Required:
x 10,000
Only have
x 100 !!
31 January 2023
IICA - FUNCTIONAL SAFETY DEMYSTIFIED
18

18

Hazard & Risk Analysis - Issues

Must identify ALL potential Hazardous Events & their causes
- Need HAZID as well as HAZOP
- HAZard Identification
  - Top down process identifying hazards
- HAZard and Operability Study
  - Bottom up process starting from deviations
  - If hazards not identified, impact of deviations may be missed

HAZOP is a review process, not a design process
- The standards gloss over this

Today HAZOP often includes at least a qualitative risk assessment
- May be used to identify which deviations or protective functions need LOPA

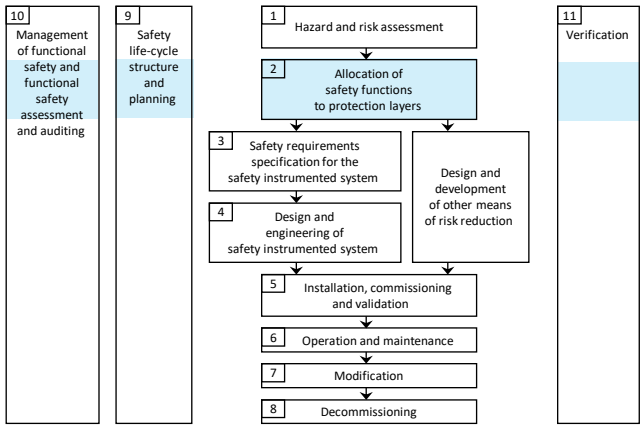
Team composition is critical
- Balance between design and operations is essential

19

2 Allocation of Safety Functions

Often called SIL Assessment, SIL Analysis or SIL Determination

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



20

Risk is unacceptable - reduce further

Hazard - 300t of LPG

Process under control — Level stable

Process deviation or disturbance — Control valve sticks

LAH Alarm

Process out of control — Level Increasing

LZHH Trip

Hazardous situation — High Pressure

PSV

Hazardous event — Vessel fails

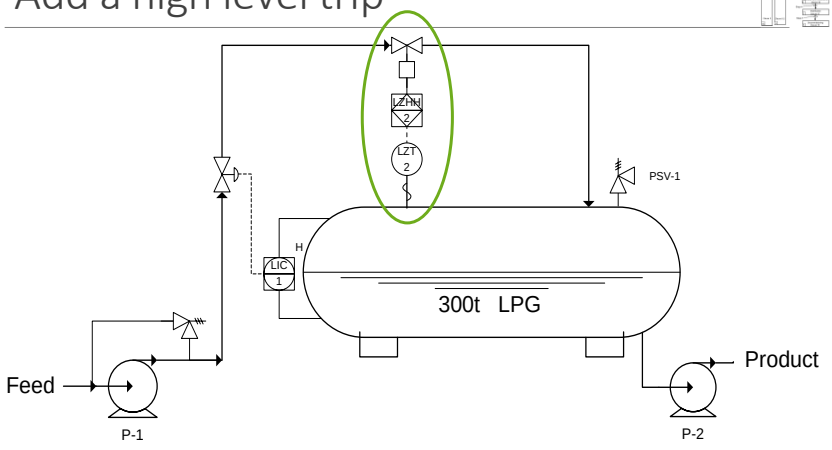
How do we reduce risk further?

Impact / Consequence

300t of boiling LPG released - likely major fire and fatalities

21

Add a high level trip

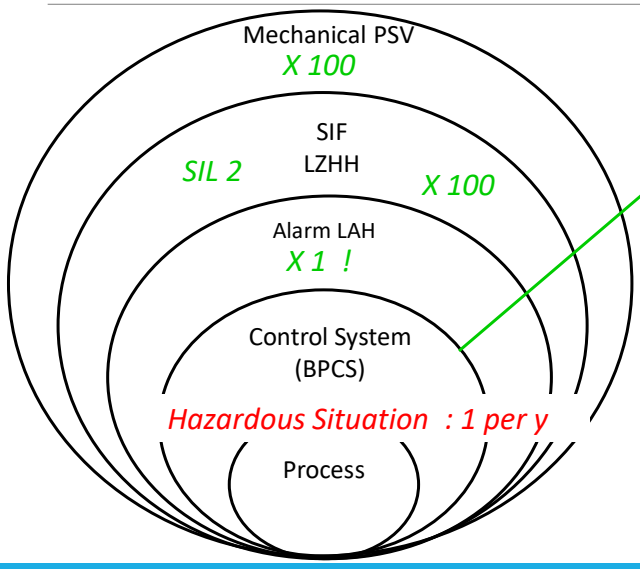


High Level Trip LZHH2 added

- Shuts off flow when High High level reached

22

Layers of Protection – SIL assessment



Target:
1 per 10,000y

Hazardous Event !!

Risk Reduction Required:
x 10,000

SIF must reduce risk by 10,000/100 = 100

23

Safety Integrity Level vs. Risk Reduction

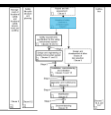
SIL	Risk Reduction Factor	Probability of Failure on Demand (PFD_{avg})	Safety Availability
4	> 10,000	$\geq 10^{-5}$ < 10^{-4}	> 99.99%
3	> 1,000 ≤ 10,000	$\geq 10^{-4}$ < 10^{-3}	> 99.9 ≤ 99.99%
2	> 100 ≤ 1,000	$\geq 10^{-3}$ < 10^{-2}	> 99 ≤ 99.9%
1	> 10 ≤ 100	$\geq 10^{-2}$ < 10^{-1}	> 90 ≤ 99%
BPCS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

Used to specify SIL required — Used to specify SIL achieved

For Demand Mode SIFs only

24

Phase 1 & 2 Compliance Achieved !



☑ 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 (PFDavg)
- Systematic Capability of each component

25

SIL Assessment - Issues

Layer of Protection Analysis (LOPA) has become the standard tool
- CCPS has excellent guidance books
- IChemE runs training in Australia
- Ensuring Protection Layers are independent can be difficult

The standard doesn't necessarily mirror actual practice
- Some overlap between phases 1 and 2

Sensible determination of tolerable risk is important
- May be difficult in immature safety cultures
- MUST be set by the operating company, not a consultant
- How to use alongside ALARP and SFAIRP?

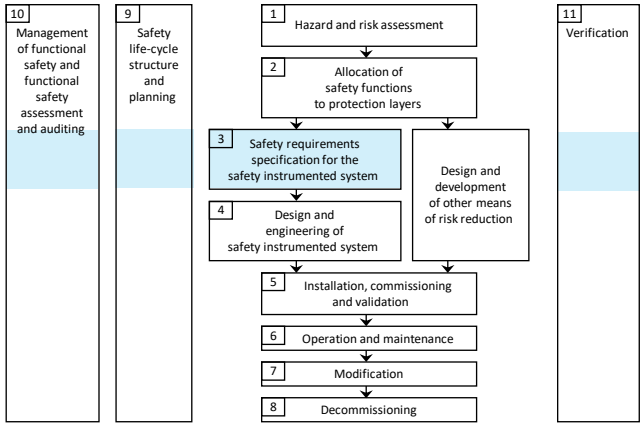
Justification for reliability data is often not done well
- See HSE report reviewing actual LOPAs in the UK
  - HSE Research Report RR716 *A review of Layers of Protection Analysis (LOPA) analyses of overfill of fuel storage tanks* Health and Safety Executive 2009

26

3 Safety Requirements Specification - SRS

Defines functional and integrity requirements of SIS

Output is a set of documents ready for detail design.



27

Safety Requirements Specification

Functional Requirements

- desired behaviour of each SIF
- behaviour in response to faults
- timing requirements
- human machine interface
- normal and abnormal modes of operation
- bypass requirements
- etc.

Safety Integrity Requirements

- Safety Integrity Level for each SIF
- basis for SIL
- testing requirements
- special requirements to maintain SIL
- etc.

AS 61511 Ed.2 has a greatly expanded checklist

28

Cause-and-Effect Diagram

SIFs commonly documented by Cause and Effect diagrams

Should link to SIFs via SIF ID or similar:

SIF ID provides traceability to SIF documentation

Tag#	Description	SIF	CLOSE VALVE LZV-02	CLOSE VALVE UV-03A	CLOSE VALVE UV-03B	OPENS VALVE UV-03C	Set LIC1 to MAN, OP=0
			14 21	13	13	-	-
BS-01	Burner Loss of Flame	13		1	1	X	
PSL-01	Fuel Gas Pressure Low			1	1	X	
LZHH-02	LPG Tank High High Level	14	2	SIL?			X

29

Safety Requirement Spec. - Issues

The SRS sets the foundation for rest of lifecycle
- But must evolve with the design and with modifications

Ensure it is presented so that it can be updated
- Not just a consultant's report!

Avoid duplication of data
- To aid modification

Assign SIF IDs early
- To allow traceability

Can evolve into a "SIF Dossier"
- Contains all information about the SIF, either directly or via links

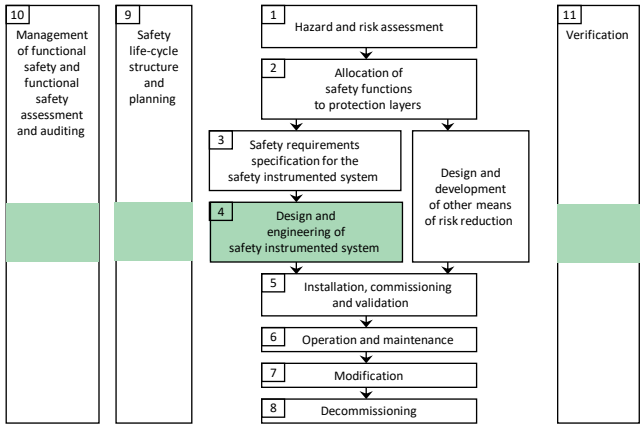
How to manage documents across lifecycle?
- Evolving – needs adapted Document Management System

30

4 Design and Engineering

SIS vendor or contractor for logic solver

EPC contractor or end-user for field hardware



31

Standards Compliance

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

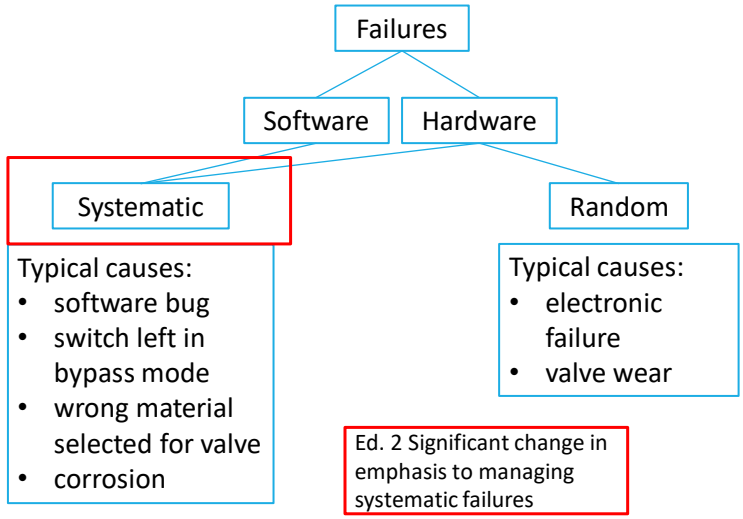
Processes for SIS throughout lifecycle must comply

Each SIF must meet target SIL requirements for:

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

32

Failure types



33

Are failures Systematic or Random?

Meant Time to Fail for a typical pressure transmitter (bigger is better!)

Source	$MTTF_{du}$ y
Device certificate (from FMEDA analysis)	2,854
SIL Solver Database (SIS Tech)	149
OREDA Offshore Reliability Database	22

Two orders of magnitude variation !

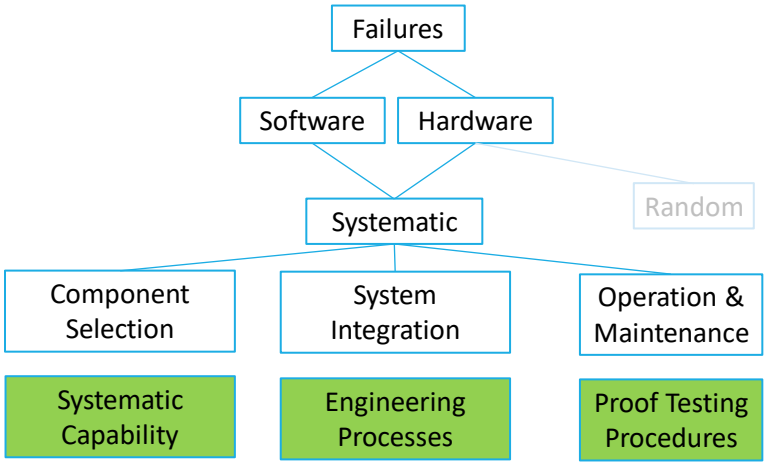
The certificate value is purely theoretical
- Failure Mode Effects and Diagnostics Analysis (FMEDA) during design
- Excludes process connections

OREDA is based on actual observations
- Includes process connections
- Includes environmental influences and systematic failures (i.e. human error)

Human error has a strong influence on single component failures !

34

Minimising Systematic Failures



35

Control of systematic failures

For integration of components into a system (SIS):

- Functional Safety Management System (FSMS)
  - for all phases of lifecycle including operation
  - quality system for SIS
- verification, validation, audit and assessment
- can comply with either IEC 61511 or IEC 61508

Within each component:

- ensure quality design in accordance with IEC 61508
- ensure appropriate techniques and measures from IEC 61508 used for the SIL of the target SIF
- measured by the term “systematic capability”
  - SC 1 to 4 corresponding to SIL 1 to 4
  - Formerly called “SIL x Capability”
- independent certification or “prior use”

36

Functional Safety Management System

Quality system with safety aspects

Safety management system that includes:

- policy and strategy to achieve safety
- responsible persons, departments, organizations
- relationship between those responsible and allocation to safety lifecycle phases
- selected “techniques and measures”
- references to the deliverables
- the functional safety assessment process (Functional Safety Assessment Plan)
- procedures for ensuring prompt follow-up of actions from hazard and risk analysis, verification, validation etc.
- configuration and change management
- . . .

37

Functional Safety Management - Issues

Extension of engineering/operations management system

Needs to be given adequate emphasis

- Limited understanding by management
- More important than many of the technical aspects

Not well handled in many existing facilities

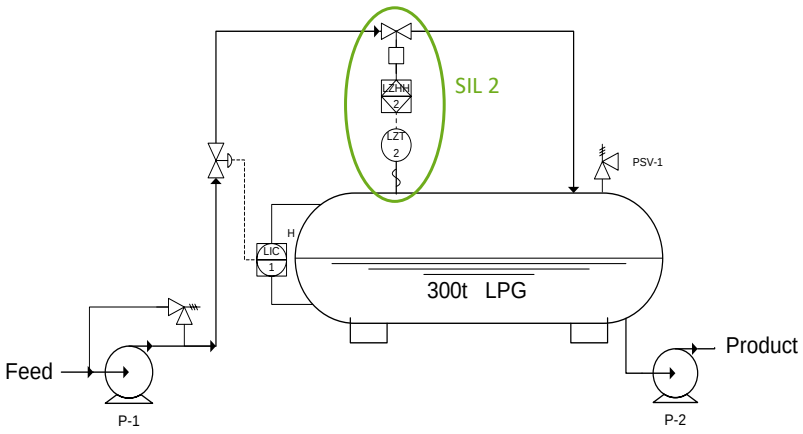
- Often not formalised
- Document management not extended to SRS & SIF documents

Assessment activities often not done well

- Especially documentation of verification and validation
- Functional Safety Assessments patchy
- See also later slides

38

SIL Verification



Does the design of SIF LZHH2 meet SIL 2?

39

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 (PFDavg)
- Systematic Capability of each component

40

Hardware Fault Tolerance

"Architectural constraints" in IEC 61508

Aim is to avoid unrealistic claims for random failure rates
- from single components

Use Table 6 in IEC 61511-1 2016 Ed. 2 (Major change from Ed. 1)
- simplified, relaxes previous unrealistic restrictions
- based on IEC 61508 Route 2H
- see next slide

Or use IEC 61508-2 (Route 1H) constrains SIF architecture based on:
- Safe Failure Fraction
- complexity of device ("Type A" or "Type B")
- target SIL

Outcome is required minimum Hardware Fault Tolerance (HFT)
- no. of voted devices minus no. required to perform safety function
  - For MooN architecture, HFT = N - M

41

Case Study: Hardware Fault Tolerance

HFT IEC 61511 Ed. 2 Table 6

Radar gauge, smart device assumptions
- Diagnostic Coverage > 60%
- We know λ_{DU} with confidence limit > 70%
- SIF operates in Low Demand mode

For SIL 2 min HFT = 0 (see below)
- Only one device required
- If operating mode is High Demand, HFT =1 (what if mode changes in future?)

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

42

Hardware Fault Tolerance - Issues

IEC 61511 requires reliability data to be known to a confidence level of 70%

- How do we know this?
- Does most reliability data achieve this?

What if SIL 2 SIF mode changes from Low to High Demand?

- Required HFT increases from 0 to 1

IEC 61508 Route 1H needs the "Safe Failure Fraction (SFF)"

- How well do we know this?
- Does it include process connections?
- How do we allow for variations between processes?

43

Standards Compliance

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

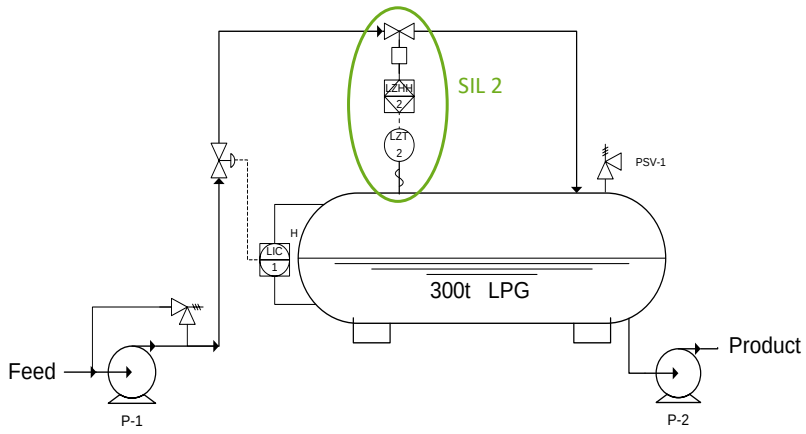
☑ Processes for SIS throughout lifecycle must comply

☑ Each SIF must meet target SIL requirements for:

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

44

SIL Verification



What is calculated "PFD_{avg}" for SIF LZHH-2?

45

Safety Integrity Level vs. Risk Reduction

SIL	Risk Reduction Factor	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

For Demand Mode SIFs only

46

Case Study: PFD Calculation

Test interval = 1 y

Reliability data:

- Valve: λ_{DU} = 1/20y (= 0.05 y^{-1})
- Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
- Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})

$PFD_{avg} = \lambda_{DU} \times TI / 2$
= 0.05 x 1 / 2 = 0.025 for valve
0.001 x 1 / 2 = 0.0005 for logic solver
0.01 x 1 / 2 = 0.005 for transmitter
Total PFD_{avg} = 0.025 + 0.0005 + 0.005 = 0.0305

Calculated SIL = 1 (PFD_{avg} range 0.01 – 0.1)

Required SIL = 2 Not OK!

How can this be fixed?

47

Case Study: Adjust Test Interval

Test interval = 1 month

Reliability data:

- Valve: λ_{DU} = 1/20y (= 0.05 y^{-1})
- Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
- Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})

$PFD_{avg} = \lambda_{DU} \times TI / 2$
= 0.05 / 12 / 2 = 0.002 for valve
0.001 / 12 / 2 = 0.00004 for logic solver
0.01 / 12 / 2 = 0.0004 for transmitter
Total PFD_{avg} = 0.002 + 0.00004 + 0.0004 = 0.00244

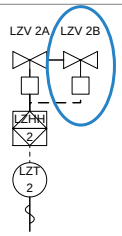
Calculated SIL = 2 (PFD_{avg} range 0.001 – 0.01)

Required SIL = 2 OK

BUT operations object to monthly testing !

48

Case Study: Duplicate Block Valves



Test interval = 1 year

Reliability data:

- Valve: λ_{DU} = 1/20y (= 0.05 y^{-1})
- Logic solver: λ_{DU} = 1/1000y (= 0.001 y^{-1})
- Sensor: λ_{DU} = 1/100y (= 0.01 y^{-1})

For 2 valves 1oo2 voting: PFD_{avg} = 0.0020 (was 0.025)

PFD_{avg} = 0.0020 + 0.0005 + 0.005 = 0.0075

Calculated SIL = 2 (PFD_{avg} range 0.001 – 0.01)

Required SIL = 2 OK

Common Cause Failures

Increasing Hardware Fault Tolerance (HFT) reduces random failure rate

But must allow for Common Cause Failures (CCF)

- represented by β – the probability that if one channel fails, all will fail

Is β important?

Architecture	PFD_{avg} without β-term	Total PFD_{avg} with β = 5%	β-term/total
1oo1	10 E-3	10 E-3	-
1oo2	0.13 E-3	0.63 E-3	81%
2oo3	0.40 E-3	0.88 E-3	57%
1oo3	0.002 E-3	0.050 E-3	99.6%

CCF (β) quickly dominates !

Must include β in PFD_{avg} calculations !

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.

How likely is it that each component is free from systematic faults ("bugs") ?

51

PFD_{avg} Calculation - Issues

Strictly speaking PFD_{avg} only addresses random failures
- But systematic failures dominate accident causes

How good is the data?
- Result is only good to an order of magnitude (i.e one SIL)
- Don't get bogged down on accuracy
- Focus on the parts that really matter

Common Mode Failure often dominates for redundant components
- Impact must be assessed!
- Calculation only addresses random failures, though.

52

Control of systematic failures

For integration of components into a system (SIS):

- functional safety management system
  - for all phases of lifecycle including operation
- verification, validation, audit and assessment
- can comply with either IEC 61511 or IEC 61508

Within each component:

- ensure quality design in accordance with IEC 61508
- ensure appropriate techniques and measures from IEC 61508 used for the SIL of the target SIF
- measured by the term "systematic capability"
  - SC 1 to 4 corresponding to SIL 1 to 4
  - formerly called "SIL Capability"
- independent certification or "prior use"

53

Case Study: Transmitter Selection

Must control systematic faults

Transmitter selected must comply with IEC 61508 and IEC 61511

Must either:

be designed and manufactured in accordance with IEC 61508

- confirmed by independent certificate (e.g. by a "TÜV" or exida)
- Systematic Capability from 1 to 4
  - i.e. techniques and measures are suitable for SIL 1 to 4

OR

meet requirements for Prior Use (or "proven in use"):

- sufficient experience gained in a comparable application

Best practice: require BOTH prior use and certification

54

Component Certification

An independent organisation certifies that the component meets the requirements of IEC 61508 for a particular SIL

- not only “TÜV” !!!

Parts 2 and 3 contain numerous “techniques and measures” required to avoid and control faults

- the rigour required increases with SIL

The aim is to reduce the likelihood of systematic faults to an acceptably low level relative to the SIL

The result is expressed as “Systematic Capability” or SC from 1 to 4

- corresponding to SIL 1 to 4
- was previously called “SIL Capability”

The certificate also usually also includes failure data and whether the component is “Type A” or “Type B”

- details are in a companion report

55

Transmitter TÜV Certificate

TÜV NORD

Certificate

Honeywell International Inc.
Industrial Measurement & Control
1100 Virginia Dr.
Fort Washington, PA 19034, USA

The safety related
ST3000 Pressure Transmitter
meets the requirements listed in the following standard

IEC 61508-1:1998; IEC 61508-2:2000; IEC 61508-3:1998; Functional safety of electrical/electronic/programmable electronic safety-related systems
SIL 2 capability for single transmitter use
SIL 3 capability for multiple transmitter use

based on report no. SAS-128/2006T in the valid version.
This certificate entitles the holder to use the certification mark:

Certificate-Register-No.: SAS-1399/06, Vers. 1.0, Augsburg, 2006-Dec-12
File reference: 2.4-115/06
Valid to: 2011-Dec-12

TÜV NORD SysTec GmbH & Co. KG

56

Transmitter TÜV Certification

57

Prior Use (IEC 61511)

Requires that appropriate evidence is available that the component is suitable based on consideration of:

- the manufacturer's quality systems
- adequate identification of the devices
- demonstration of performance in similar operating environments
- the volume of operating experience

Focus is on demonstrating freedom from systematic faults (new in Ed. 2)

IEC 61508 term is "Proven in Use"

- more rigorous requirements

58

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
- Design now complies

59

Component Selection - Issues

Certification gives some confidence in manufacturer's systems
- Easy to use!
- Reliability data is usually very optimistic

Prior use gives confidence in suitability for your application environment
- Easy to abuse!
- Including systematic failures, not just random failures
- Dataset is usually too small to give accurate reliability data

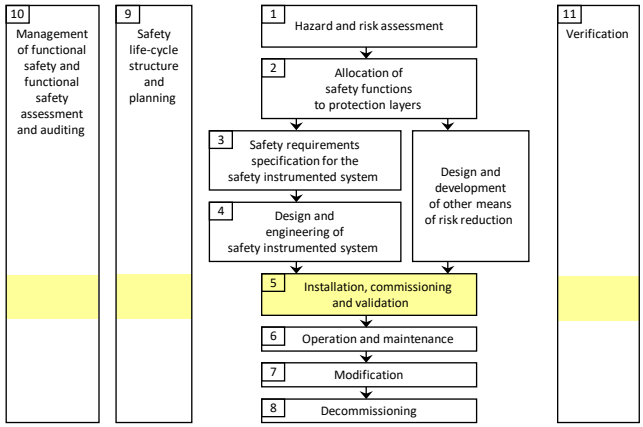
Try to use both Certification and Prior Use justification

60

5 Installation, Commissioning, Validation

Logic Solver installed with field equipment

Includes loop checking, validation and final functional safety assessment.



61

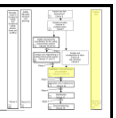
Standards Compliance

- ☑ 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

Verification, Validation, Functional Safety Assessment

62

Case Study: Verification and Validation



Project Verification and Validation Plan required
- Consider level of independence required (i.e. independent engineer)
- Define responsibilities

Verify each phase e.g.
- Safety Requirements Specification
- Verify hardware design documents
- Verify functional specifications etc
- Implement code walkthrough

Logic Solver Factory Acceptance Test (2nd Ed. clause is now normative)
- Complete integration test validates application software on target hardware

Logic Solver Site Acceptance Test
- Power up test on site

Safety Function Testing
- SIS validation

Functional Safety Assessment

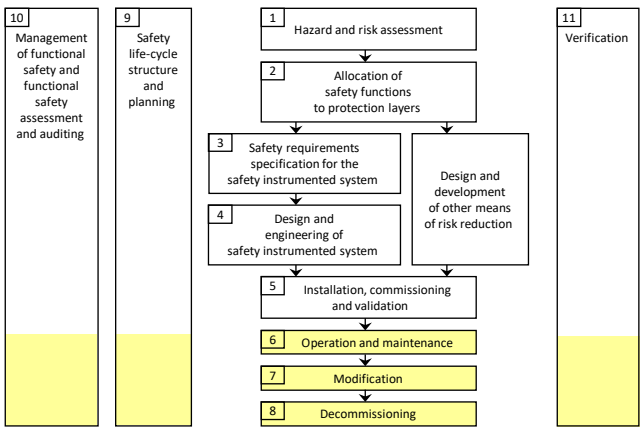
Note that terminology is from the ISO9000 discipline
- Some disciplines swap the meanings of "verification" and "validation"!

63

6 Operations, Maintenance and Modification

The Cinderella Phases !

User must follow a Functional Safety Management System for the life of the SIS.



64

Ops and Maintenance Obligations

Train operators & maintainers

Proof test each SIF at specified interval

Monitor design assumptions
- demand rates
- component reliability

Adjust test interval to suit

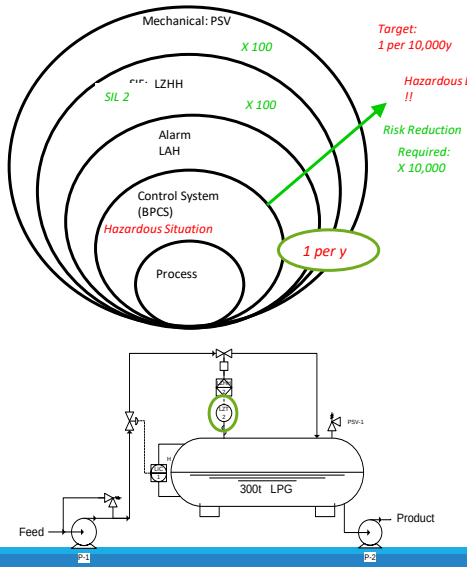
Control modifications

Ensure Maintenance and Operational Overrides are used as designed

Monitor and promptly follow-up diagnostics

65

Case Study: Operation and Maintenance



Risk analysis assumed:
- demand on SIF once per year
- what happens in practice?

SIL verification assumed:
- transmitter failure rate 0.01 y^{-1}
- what happens in practice?

Etc etc . . .

Must verify actual performance against assumptions and adjust testing as required

Documentation of assumptions is critical

66

Operations & Modification - Issues

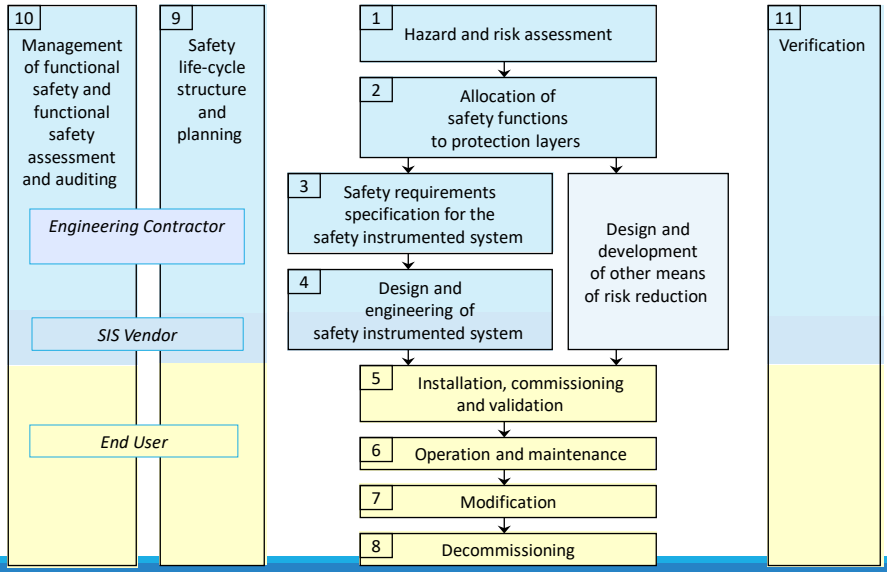
SIF testing at adequate intervals can be challenging
- Especially valves, including overhaul
- Must be considered during design

Online testing is ok
- But what if SIF fails test? Shut down to fix?

Management of Change is challenging
- What process or equipment changes impact SIFs and their required SIL?
- Use checklists spawned from main MOC checklist
- Must formally manager protection layers

67

Summary 1 – The SIS Lifecycle



68

Summary 2 – Focus on systematic failures

Systematic failures dominate functional safety

Don't get distracted by accurate quantification of random failures

Razor sharp focus required on reducing systematic failures
- including competent instrument selection and design
- this will also reduce random failures

Examples:
- **designers**: specify the requirements for lifetime management of systematic failures in a Safety Manual e.g. periodic overhauls of valves
- **operators**: follow up all failures of devices or organisation – are they symptomatic of common mode failure?
- **researchers**: how can we link systematic and random failure rates?

69

Summary 3 – Requirements

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

☑ 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.

Not just TÜV certification
- though it helps !

Not just meeting PFD_{avg} target

Don't forget spurious trip rate!

70

Need more?

IICA runs the following courses:

TÜV Rheinland Functional Safety Engineer course

- For those with 3+ years experience in functional safety
- Leads to Functional Safety Engineer (TÜV Rheinland) qualification
- Face-to-face courses in Melbourne, Brisbane and Sydney
- Online courses and inhouse courses also available

See https://iica.org.au/events/ for schedule and further details or email training@iica.org.au for further information

71