6 Engineering
Safety Engineering Consultants
www.6engineering.co.uk
nick@6engineering.co.uk
+44 1224 460246
+44 1287 750911

6 Engineering

Your safety engineering partner

Offshore | Onshore

6 Engineering

Achieving ALARP with Safety Instrumented Systems: what does that mean?

Delivered by Nick Howard FS Eng for

The Cleveland Institution of Engineers

13 APR 2021

Achieving ALARP with Safety Instrumented Systems: what does that mean?

Agenda

1. Introductions
2. What is ALARP?
3. An example system to study
4. What is functional safety?
5. Evaluating hazards and assigning safety integrity levels
6. The international functional safety standards
7. What is a Safety Instrumented System?
8. The functional safety lifecycle (per IEC 61511)
9. Safety Requirements Specification
10. SIL calculation
11. Has ALARP been achieved?
12. Conclusions
13. Any questions?
14. Feedback

Introduction to 6 Engineering Ltd

Who we are:

Safety Engineering Consultants to the major hazard industries worldwide.

Based in North Yorkshire, offices in:

- Stokesley
- Warrington
- Aberdeen
- Cologne

What we do:

- Functional Safety
- Process Safety
- OT Cybersecurity

Disclaimer

The following information provides a brief overview and analysis of a theoretical system design and interpretation of UK legal requirements.

The information is provided as-is and does not represent a full report or conclusions; insufficient context is provided to allow any use to be made of the information under any circumstances. 6 Engineering Ltd. disclaim any responsibility in respect of any matters related to the information provided.

Speaker Introduction

Nick Howard – Safety Engineering Consultant
MSc BEng (Hons) AMIChemE FS Eng (TÜV Rheinland)

18 years experience:
- Power Generation (Conventional & Nuclear)
- Nuclear Decommissioning
- Biofuels
- Oil & Gas
- Chemicals

10 years in Process/Technical Safety

Achieving ALARP with Safety Instrumented Systems

- What is ALARP?
- What are Safety Instrumented Systems?

What is ALARP?

To explain ALARP, we need to consider the law…

2 General duties of employers to their employees.

(1) It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.

(2) …the matters to which that duty extends include in particular—

(a) the provision and maintenance of plant and systems of work that are, so far as is reasonably practicable, safe and without risks to health;

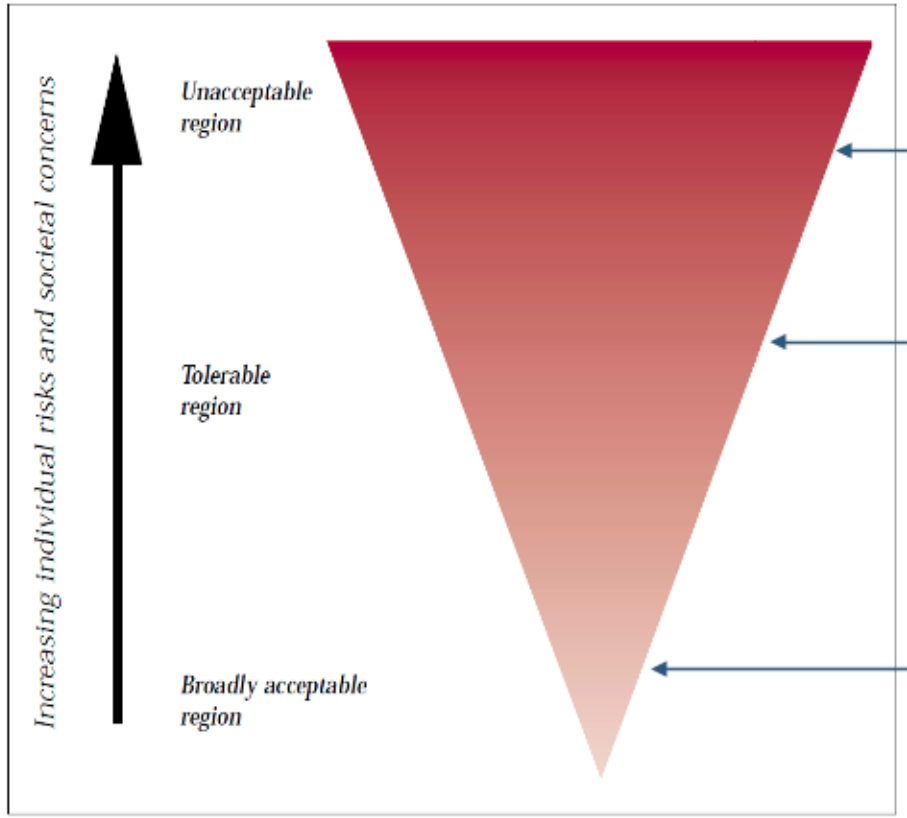
…

(e) the provision and maintenance of a working environment for his employees that is, so far as is reasonably practicable, safe, without risks to health, and adequate as regards facilities and arrangements for their welfare at work.

What is ALARP?

…and the guidance on interpreting it:

ALARP: As Low As Reasonably Practicable



The risk of fatality per annum:

- $>10^{-3}$ intolerable*
- 10^{-3} to 10^{-6} Tolerable if ALARP
- $<10^{-6}$ Broadly Acceptable

*except for specific categories where risk cannot be reduced.

Some rules around ALARP

- ALARP cannot be used to justify not implementing relevant good practice (RGP).
  - RGP is contained within Approved Codes of Practice (ACoP) issued by HSE or industry standards.
- A Cost Benefit Analysis (CBA) cannot form the sole argument of an ALARP decision.
- ALARP is for circumstances where:
  - established good practice does not exist or is out of date, or
  - the situation is complex and the relevance of individual good practices is questionable (e.g. the combination of discrete hazards is not foreseen in the good practice documents)

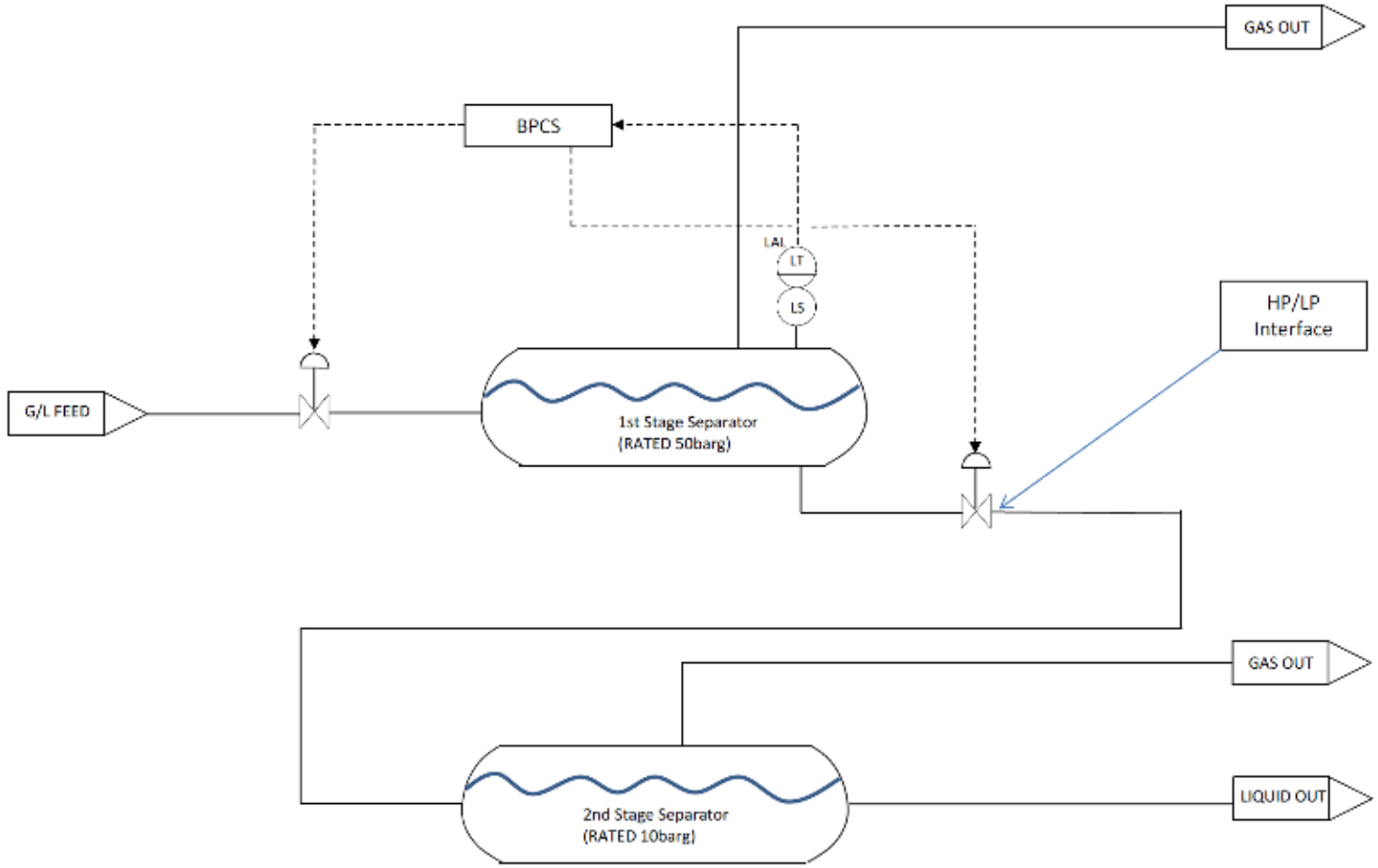
Story time…

- Once upon a time, there was a process plant, designed for a specific set of process variables, such as pressure, temperature, gas/liquid ratio…

- Then…

- There was a modification planned!
  - First, there was a HAZOP; deviations from the design intent were identified
  - These deviations could result in fatalities, thus the risk profile was established
  - Then, it was determined there was a significant risk reduction required
  - The design team looked at different options; each had its own pros and cons
  - They selected an approach, evaluated it using LOPA and decided that one aspect of this approach was to use a Safety Instrumented System (SIS), with a Safety Integrity Level (SIL) of 1.
  - And the plant manager lived happily ever after. The end… or maybe not…

An Example System



An Example Risk Matrix

			LIKELIHOOD					
			1E-7/yr to 1E-6/yr	1E-6/yr to 1E-5/yr	1E-5/yr to 1E-4/yr	1E-4/yr to 1E-3/yr	1E-3/yr to 1E-2/yr	1E-2/yr to 1E-1/yr
			1	2	3	4	5	6
SEVERITY	>10 Fatalities	E	1E	2E	3E	4E	5E	6E
	4-10 Fatalities	D	1D	2D	3D	4D	5D	6D
	1-3 Fatalities or 4-10 serious injuries	C	1C	2C	3C	4C	5C	6C
	1-3 Serious inujries or 4-10 minor injuries	B	1B	2B	3B	4B	5B	6B
	1-3 minor injuries	A	1A	2A	3A	4A	5A	6A

Key:

	Intolerable - risk reduction must be implemented irrespective of cost or complexity
	HSE criterion: Tolerable if ALARP for a single fatality - risk reduction must be implemented if there is sufficient risk benefit
	Broadly Acceptable - additional risk reduction should be considered where it is simple and low-cost

An Example HAZOP Worksheet

Node 1	First and second stage separators
Node details	Reservoir fluids containing oil and gas at 20C are fed into the first stage separator operating at 48 barg where the more volatile components flash off to join the vapour stream. The liquid stream is fed to the second stage separator, operating at 5 barg where the remaining volatile components are flashed off.
Fluid State	Liquid & Gas
Flow	500bbl/hr
Pressure	48barg
Temperature	20C
Drawings	P&ID1
Notes	First stage separator design pressure is 50barg Second stage separator design pressure is 10barg

Item No.	Deviation	Cause	Risked Event	Risk			Safeguards	Action	Actionee	Target Date
				Severity	Freq.	Risk				
1.1	Level less	Level control valve on liquid line ex first stage separator opens wider than required.	Level in first stage separator drops allowing gas blowby through liquid line and overpressure of second stage separator by 5 times design pressure leading to loss of primary containment, potential ignition and up to 4 fatalities	D	6	6D	1. None	Provide a means of protecting the HP/LP interface between the first and second stage separators in the event of a lower than required level in the first stage separator.	ABC	1st Jan 2021

What do we need to achieve?

- We need to implement engineered risk reduction measures to reduce risk:

			LIKELIHOOD					
			1E-7/yr to 1E-6/yr	1E-6/yr to 1E-5/yr	1E-5/yr to 1E-4/yr	1E-4/yr to 1E-3/yr	1E-3/yr to 1E-2/yr	1E-2/yr to 1E-1/yr
			1	2	3	4	5	6
SEVERITY	>10 Fatalities	E	1E	2E	3E	4E	5E	6E
	4-10 Fatalities	D	1D	2D	3D	4D	5D	6D
	1-3 Fatalities or 4-10 serious injuries	C	1C	2C	3C	4C	5C	6C
	1-3 Serious inujries or 4-10 minor injuries	B	1B	2B	3B	4B	5B	6B
	1-3 minor injuries	A	1A	2A	3A	4A	5A	6A

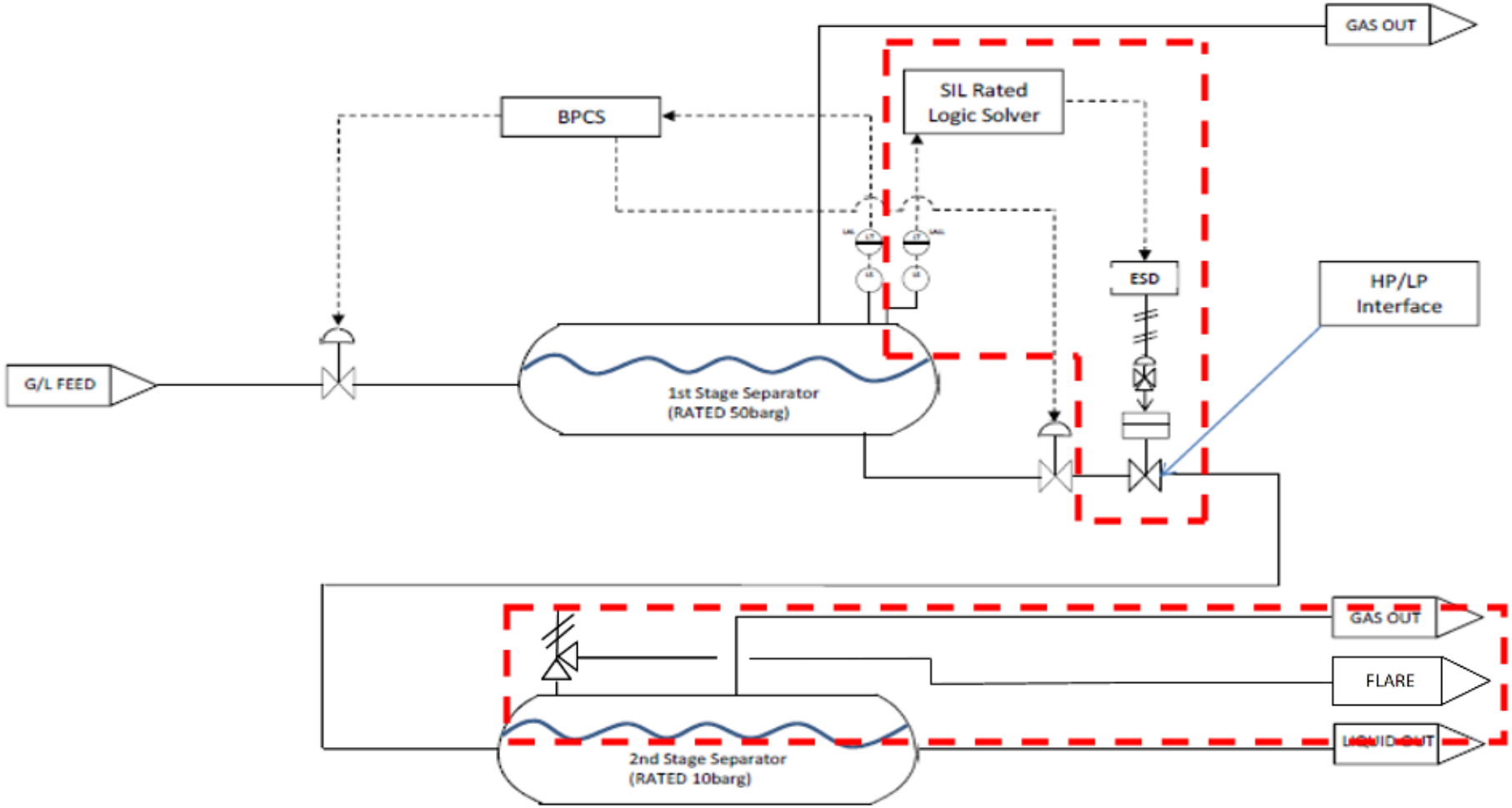
Key:

	Intolerable - risk reduction must be implemented irrespective of cost or complexity
	HSE criterion: Tolerable if ALARP for a single fatality - risk reduction must be implemented if there is sufficient risk benefit
	Broadly Acceptable - additional risk reduction should be considered where it is simple and low-cost

What engineered risk reduction measures can we suggest?

Solution	Pros	Cons
Bursting disk (Risk reduction factor ~100)	Passive device Provides reliable protection No periodic maintenance Easy to specify	Single use item Requires periodic replacement Designed for a specific pressure More likely to be used for the fire protection case
Pressure Relief Valve (Risk reduction factor ~100)	Passive device Provides reliable protection Once used, resets Set pressure may be adjustable	Requires periodic inspection & maintenance
Safety Instrumented System (e.g. low level trip) (Risk reduction factor dependent on design; offers up to 100,000)	Provides reliable protection Once used, resettable and reusable Can be easily designed to meet the required RRF	Active device Requires periodic inspection & maintenance & testing Requires rigorous design, installation and validation activities (i.e. paperwork heavy)

Proposed Risk Reduction Measures: SIF & Relief Valve



Evaluating the proposed risk reduction measures (using LOPA)

Asset:	Plant A		Date:	10/04/2021	
Project:	Separator System		Loop Tag:	LALL-1SS01	
Scenario:	Overpressure of second stage separator, loss of primary containment, ignition and up to 5 fatalities.				
Category:	Safety	TMEL:	1.00E-05	Severity Level:	D

Ref	Description	Frequency	Reference
Initiating Cause 1	Level control valve on liquid line ex first stage separator open more than required	1.00E-01	HAZOP ref Node 1, Item 1.1. BPCS Loop failure
Initiating Cause 2			
Initiating Cause 3			
Enabling Event 1			
Initiating Event Frequency		1.00E-01	SIF Required

	IC1	IC2	IC3		Description/Justification
Safeguard 1	1				New LL level trip on first stage separator at HP/LP interface with second stage separator (not credited)
Safeguard 2	0.01				Pressure relief valve
CM1					
CM2					
IEL for each IC	1.00E-03	0.00E+00	0.00E+00		
Intermediate Event Likelihood				1.00E-03	
RRF				100	SIL 1

Severity Level		TMEL	Description
	E	1.00E-06	>10 fatalities
	D	1.00E-05	4 to 10 fatalities
	C	1.00E-04	1 to 3 fatlities
	B	1.00E-03	Multiple major injuries
	A	1.00E-02	Single major injury

How is RRF related to SIL?

Risk Reduction Factor (RRF)	Safety Integrity Level (SIL
10 - <=100	1
>100 - <=1000	2
>1000 - <=10,000	3
>10,000 – <=100,000	4

BS EN 61511-1:2017 + A1 2017 Table 4

Our target

What Is SIL?

- Safety Integrity Level (SIL) is a rating from 1 (lowest) to 4 (highest) of the amount of risk reduction provided by a safeguard.

Safety Integrity Level (SIL)	Risk Reduction Factor (RRF)	Average Probability of Failure on Demand (PFDavg) (Low Demand Systems)	Approximate Range of Mean Time to Failure (years) (high demand) (RRF)*	Probability of Failure per Hour (PFH) (High/Continuous Demand Systems)
1	> 10 to ≤ 100	$\geq 10^{-2}$ to $< 10^{-1}$	$10^{2} \geq$ MTTF> 10	$\geq 10^{-9}$ to $< 10^{-8}$
2	> 100 to ≤ 1 000	$\geq 10^{-3}$ to $< 10^{-2}$	$10^{3} \geq$MTTF$> 10^{2}$	$\geq 10^{-8}$ to $< 10^{-7}$
3	> 1 000 to ≤ 10 000	$\geq 10^{-4}$ to $< 10^{-3}$	$10^{4} \geq$ MTTF$> 10^{3}$	$\geq 10^{-7}$ to $< 10^{-6}$
4	> 10 000 to ≤ 100 000	$\geq 10^{-5}$ to $< 10^{-4}$	$10^{5} \geq$ MTTF$> 10^{4}$	$\geq 10^{-6}$ to $< 10^{-5}$

https://www.wildeanalysis.co.uk/wp-content/uploads/2016/07/white_paper_methods_determining_safety_integrity_level_gulland_4sight_consulting.pdf

Relevant Good Practice which our design can follow:

- BS EN 61508:2010 Parts 1-7
  - Functional safety of electrical/electronic/programmable electronic safety-related systems
  - Aimed at designers and manufacturers of equipment/devices destined for use in functional safety systems

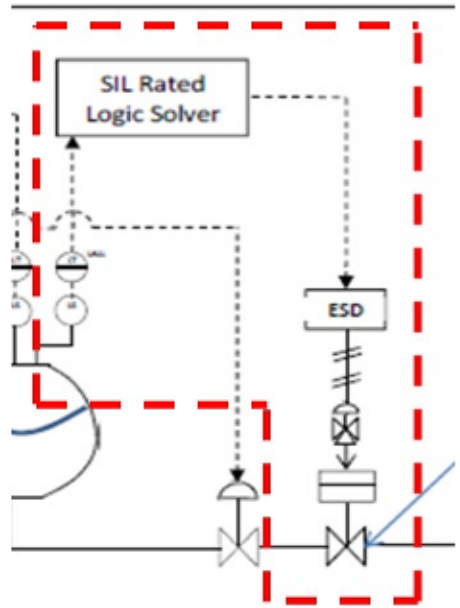
- BS EN 61511:2016 Parts 1-3 (as amended)
  - Functional safety – Safety instrumented systems for the process industry sector
  - Aimed at designers, integrators and users of process plants

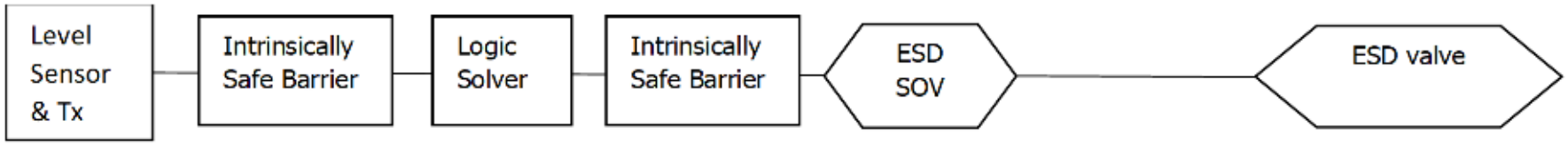
- NAMUR Recommendation NE43
  - Standardization of the Signal Level for the Failure Information of Digital Transmitters

What is a Safety Instrumented System (SIS)?

- Designed to detect a hazardous process variable
- Electrical/electronic/programmable electronic systems
  - Made up of one or more Safety Instrumented Functions (SIFs)
  - Can be made up of one or more microprocessor-based logic solvers, termed a 'Node'
  - Can be made up of relays to execute the logic
  - Some use a switch to send a signal that a trip point has passed
  - Some use a sensor to give a live reading of the process variable being measured and use programmable logic to initiate a trip
  - Some move a valve to put the process in the safe state
  - Some alarm to alert the operator to take action
  - Some open a relay to trip a pump
- Can be used to fill the risk reduction gap
- Have a quantum of risk reduction formally assigned to them
- Require formal ongoing management & testing

What does our SIS look like?

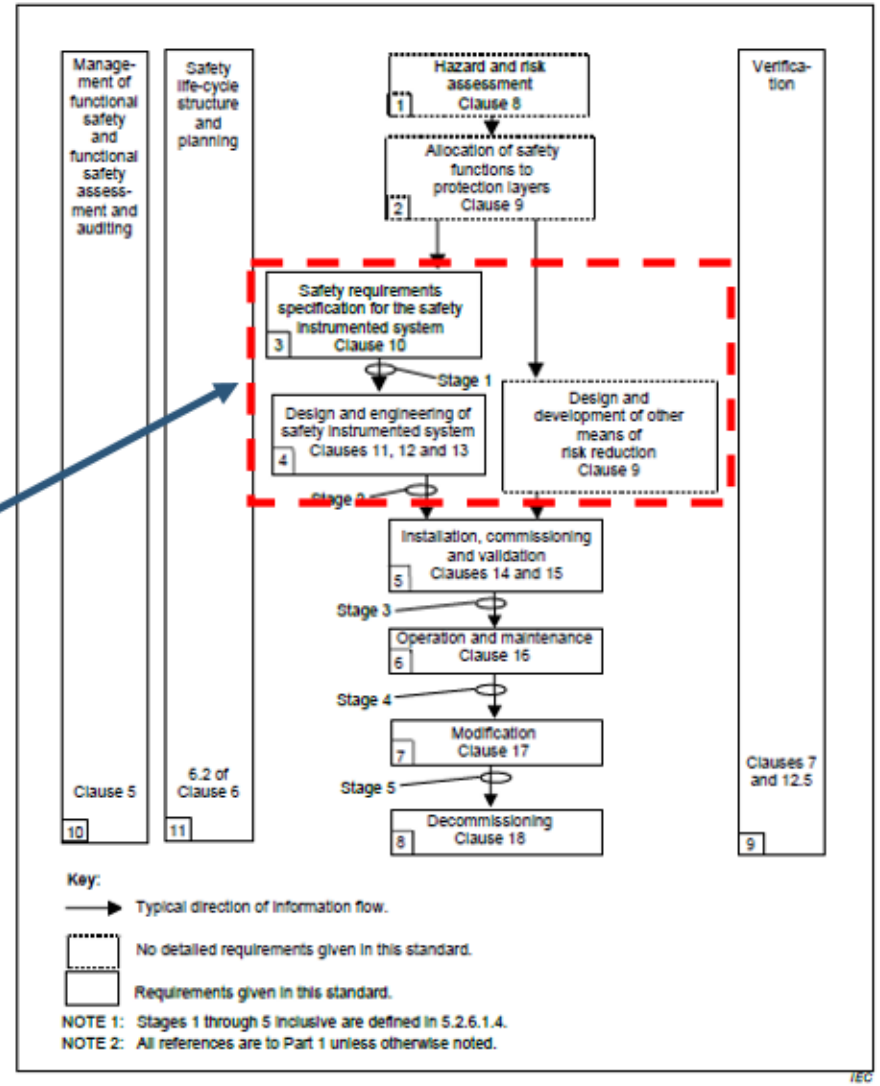




A 1oo1 (1 out of 1), or 'simplex' architecture

The Functional Safety Lifecycle

Where we are



From BS EN 61511-1:2016

Safety Requirements Specification

1. BS EN 61511-1 clause 3.2.72 states that a safety requirements specification is a:
   - specification containing the functional requirements for the SIFs and their associated safety integrity levels
2. Clause 10 deals with the SIS Safety Requirements Specification. It lists 29 separate requirements which must be presented, including:
   1. a description of all the SIF necessary to achieve the required functional safety
   2. a list of the plant input and output devices related to each SIF which is clearly identified by the plant means of equipment identification
   3. the assumed sources of demand and demand rate on each SIF
   4. response time requirements for each SIF to bring the process to a safe state within the
   5. process safety time
   6. the required SIL and mode of operation (demand/continuous) for each SIF
   7. a description of SIS process measurements, range, accuracy and their trip points

Simplified SIL Calculation Formulae

Architecture	Simplified Formula
1oo1	$\frac{1}{2}\lambda_d T_i$
1oo2	$\frac{1}{3}\lambda_d^2 T_i^2$
2oo2	$\lambda_d T_i$
2oo3	$\lambda_d^2 T_i^2$

λ= dangerous failure rate
Ti= test interval

Note that it is common to find failure rates expressed as failures in time; i.e. per billion hours.
The full formulae can be found in IEC 61508-6.

Schutzfunktion/Safety Function	Überfüllsicherung/overfill protection
SIL	2
Prüfinterval/Proof test interval	≤ 1 Jahr/year
Gerätetyp/Device type	B
HFT	0
SFF	94 %
PFD_{avg} [1]	0,01x10-2
λ_{du}	30 FIT
λ_{dd}	1,3 FIT
λ_{su}	426 FIT
λ_{sd}	138 FIT
$MTBF_{tot}$ [2]	190 Jahre/years

Hardware Fault Tolerance (HFT) SIL

- Achieved HFT is determined by architecture, component type and safe failure fraction (SFF):
  - Greater redundancy = better HFT
  - SFF is the proportion of all failures which fail to a safe state
- There are two types of component from a HFT perspective, Type A & Type B. Briefly:
  - Type A – all the failure mechanisms are known
    - e.g. switches, relays, valves
  - Type B – all the failure mechanisms are not known
    - e.g. programmable controllers & sensors

SIL RATING	MINIMUM REQUIRED HFT
1 (Any mode)	0 (no redundancy required)
2 (Low demand mode)	0 (no redundancy required)
2 (Continuous mode)	1 (100% redundancy required)
3 (High demand mode)	1 (100% redundancy required)
4 (any mode)	2 (200% redundancy required)

HFT SIL

- BS EN IEC 61508-2 Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

	HARDWARE FAULT TOLERANCE (TYPE A DEVICES)		
Safe Failure Fraction	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% to <90%	SIL 2	SIL 3	SIL 4
90% to <99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

HFT SIL

- BS EN IEC 61508-2 Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

	HARDWARE FAULT TOLERANCE (TYPE B DEVICES)		
Safe Failure Fraction	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% to <90%	SIL 1	SIL 2	SIL 3
90% to <99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

SIL Calculation results

Our chosen test interval (every 2 months)

Component	Type	Test Interval (yr)	Dangerous Failure Rate (per yr)	Configuration	PFDavg	HFT	SFF	A or B	HFT SIL
Initiating Element(s)									
		0.166666667			10				
LNS1280	Endress & Hauser Liquiphant		3.68E-04	1oo1	3.07E-04	0	95	B	2
Tx	Endress & Hauser FTL57		N/A						
ISB	Endress & Hauser FTL325P		N/A						
Processing Element(s)									
Logic Solver	Hima-Sella		1.28E-05	1oo1	1.07E-05	0	99.86	B	3
Final Element(s)									
ISB	Pepperl & Fuchs KFD2-SL2-EX2.B		2.91E-03	1oo1	2.42E-03	0	100	A	3
SOV	Burkert 6518C		1.87E-03	1oo1	1.56E-03	0	69	A	2
V1207K1	Norbro 30-RDB40-1SD1EO-D		4.67E-03	1oo1	3.89E-03	0	54.9	A	1
PFDavg target:	1.00E-02	PFDavg Achieved:	8.19E-03	PFDavg SIL:	2	Target HFT SIL	1	Overall HFT SIL	1
Target Met/Exceeded	YES					Target Met?	YES	Overall SIL	1

Our achieved failure rate

Our achieved SIL by failure rate

Our achieved Hardware Fault tolerance SIL

Our target failure rate

Our target Hardware Fault tolerance SIL

Our overall SIL achieved

What Can Affect Failure Probability?

- Failure probability is affected by a number of things:

1. System architecture: 1oo2 is less likely to fail than 1oo1 (redundancy)
2. Proof test interval: the more frequent the testing, the lower the failure rate
3. Mean time to repair: this does have an effect, albeit usually minor
4. Diagnostic coverage: smart instruments & position sensors can detect otherwise undetected failures
5. Proof test coverage: the more thorough the test, the higher the failure mode coverage

Systematic Capability

BS EN 61511-1 clause 3.2.80 states that systematic capability is a:

- measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual.
- The device safety manual should be inspected to ensure that it is not used in a SIF above its SIL capability, for example:

Areas of application:
Overfill prevention device or operating maximum detection of all types of liquids in tanks or piping to satisfy particular safety systems requirements to IEC 61508 or DIN V 19250.

The measuring system fulfils the requirements concerning
- Functional safety according to IEC 61508 and DIN V 19250
- Explosion protection by intrinsic safety
- EMC to NAMUR Recommendations

Benefits at a glance
- For overfill prevention up to SIL 2/AK 4, in redundant versions up to SIL 3/AK 5&6
  Certified by TUEV Rheinland/ Berlin Brandenburg
  TUEV Anlagentechnik GmbH
  Automation, software and IT to IEC 61508
- Permanent self-monitoring
- No calibration
- Protected against outside vibration by optimised drive
- Space-saving switching unit
- Measuring system test by pressing a test-button
- Fail-safe by PFM technology

Extract from Endress & Hauser Liquiphant Safety Manual

Has ALARP been achieved?

- We had a risk reduction target of 10,000 to bring us down to a likelihood of 1E-05/yr
- The guidance states that risk should be reduced to broadly acceptable (1E-06/yr) so far as is reasonably practicable
- How can we determine whether we should provide additional risk reduction?
- Use ICAF: the implied cost of averting a fatality:

$$\text{ICAF}=\frac{C.GDF}{L(\Delta PLL)}$$

Where:

C = cost of implementing measure (£); * by a Gross Disproportionation Factor (GDF)

L = Estimated Lifetime of plant (years; assumed to be 20)

ΔPLL = Change in Potential Loss of Life (PLL) following implementation of a risk reduction measure (fatalities per year) = 5E-05 -5E-06 = 4.5E-05

Has ALARP been achieved?

Cost of Risk Reduction Measure	ICAF
£1000	£2.78m
£10,000	£27.78m
£100,000	£277.78m

1. The statistical cost of a human life was around £1.8m in 2019
2. Gross Disproportionation Factor used is 3.
3. It can be concluded that it is highly unlikely that further risk reduction is reasonably practicable.

Conclusions

1. Safety Instrumented Systems are a valid method of achieving ALARP, either on their own or in conjunction with other risk reduction measures.

2. The more risk reduction required, the more rigorous the design of the SIS, and hence more paperwork.

3. Reducing risks to broadly acceptable levels is not always reasonably practicable.

4. To avoid undertaking a cost-benefit analysis on each design, it is useful to set tolerability parameters, such as the Tolerable Mitigated Event Likelihood in LOPA.

5. Although the proposed design solution achieves the required risk reduction, bi-monthly proof testing is unlikely to be practical for the facility; therefore the design may need some redundancy (or better equipment).

6. If in doubt, ask for expert support.

Further reading…

- https://www.hse.gov.uk/managing/theory/index.htm
- https://www.hse.gov.uk/research/misc/vectra300-2017-r03.pdf
- https://www.61508.org/
- https://webcommunities.hse.gov.uk/gf2.ti/f/22306/676101.1/PDF/-/CDOIF_Guideline__Installed_SIS_v1_0_Stakeholder_Comments__WG_Final.pdf

Any Questions?

- Go ahead, ask away!

Feedback

- If you like what we do, tell others! If you don't, tell us!

- We appreciate feedback, it helps us improve.
  - You can give it in person
  - You can call +44 1224 460246 /+44 1287 750911
  - You can email us info@6engineering.co.uk