Practical SIS Design and SIL Verification

The Institute of Measurement & Control

Manchester & Chester Local Section

29th January 2014

Functional Safety

TRAINING • CONSULTANCY • ASSESSMENT

www.silmetric.com

The Speaker...

Paul Reeve BEng CEng MIET MInstMC

Functional Safety Consultant

- **Silmetric Ltd** since 2011 providing training, consultancy and independent assessments to product and system designers in the UK, USA, Canada, Middle East and Far East
- Director of The CASS Scheme, www.cass.uk.net
- 8 years at Sira Test & Certification (part of CSA International) as the senior functional safety assessor
- 21 years in product design and development (MTL Instruments, GE Medical Systems and The BBC)

SILMETRIC is a member of:

The 61508 Association

MEMBER OF BVAA

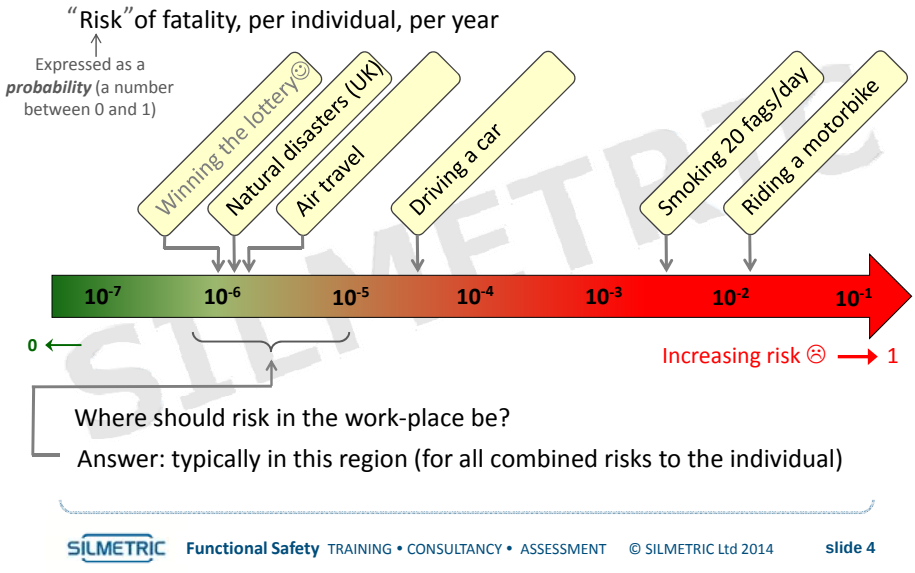
Institute of Measurement and Control COMPANION COMPANY

SILMETRIC Functional Safety TRAINING • CONSULTANCY • ASSESSMENT © SILMETRIC Ltd 2014 slide 2

Objectives of this talk...

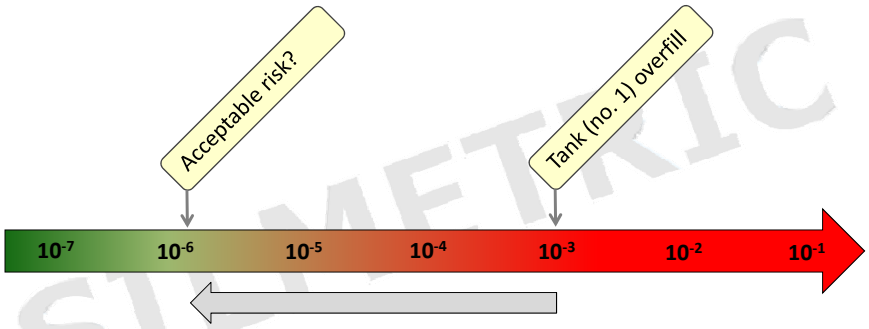
- Describe some of the key stages in designing safety instrumented systems for two common applications:
  - tank overfill protection system
  - high integrity pressure protection system (HIPPS)
- Show how the architectures can be created, PFD calculations performed and the SIL verified, following a practical approach
- Focus on the quantitative aspects of safety performance
- Use the approach in IEC 61508 and 61511 for **E**lectrical, **E**lectronic and/or **P**rogrammable **E**lectronic (E/E/PE) safety related systems
- Keep things practical, sense of reality, engineer friendly

Subject orientation - everyday risks



Subject orientation – risk from one process hazard

Risk of single fatality, per year, from a single hazard at a process plant



Necessary risk reduction: 10^{-3}

Some/much of this can be allocated to a safety instrumented function

 slide 5

Context – the object of the SIF

- The SIF detects the conditions for the hazard from the EUC and puts the EUC into the safe state
- If the SIF was perfect (faultless) there would be zero residual risk
- However, the SIF is not quite perfect (no engineered systems are!)
- The SIF will have a small probability of failure when a demand is placed on it, we call this the 'Probability of Failure on Demand' (PFD)
- If we can estimate the probability of the unprotected hazardous event occurring and the PFD of the SIF, we can estimate the residual risk and decide if this meets the risk criteria

 slide 6

Context...

- The Safety Instrumented Function (SIF) provides risk reduction by virtue of a PFD_{AVG} in a low demand mode

  So, if hazard rate leading to fatality with no SIF = $HAZ\_RATE_{NO\_SIF}$ then:

$HAZ\_RATE_{NO\_SIF}$ x PFD_{AVG} = $RISK_{WITH\_SIF}$ meets the Risk criteria?

Can be described as a 'Risk Reduction' figure

e.g., 10^{-4}/yr x 10^{-2} = 10^{-6}/yr ≤ Risk criteria?

Reference to IEC 61508 shows this is = SIL 2

Assumptions for this talk...

- The SIF requirements have been properly established in accordance with the standards
- Suitable instrumentation is available that complies with IEC 61508 and has verified failure data
- Systematic failures are avoided by:
  - following the prescribed realisation lifecycle
  - using design and verification 'techniques and measures' suitable for the SIL involved, e.g., from IEC 61508-2 Annex B
  - performing all the work under an appropriate functional safety management (FSM) system

BS EN 61508 / 61511 Requirements for safety integrity

Broadly speaking, the SIF (and hence SIS) must, for the SIL involved…

- Meet the requirements for:
  - PFD_{AVG}
  - 'Architectural Constraints'

HARDARE INTEGRITY

SCOPE OF THIS TALK

- Meet the requirements for:
  - Lifecycle and FSM (includes the QMS)
  - Software and hardware design
  - Use specified 'techniques and measures'

SYSTEMATIC INTEGRITY

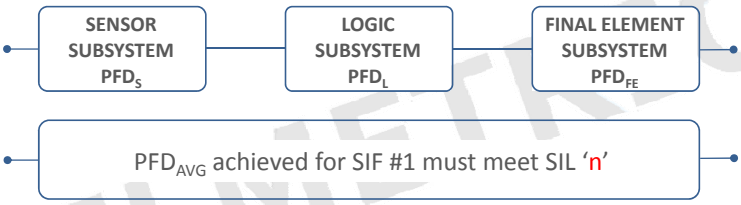
HAS BIG IMPLICATIONS ON HARDWARE AND SOFTWARE REALISATION!

 slide 9

A generic SIS

SIF #1 is specified at SIL 'n' (n = 1 to 4)

SIF #1 is implemented by the SIS comprised of subsystems:



Three basic attributes are:

1. The **architectural constraints** for each subsystem are at least SIL 'n'
2. The **systematic capability** of each subsystem is at least SC 'n'
3. The **PFD_{AVG}** is within (or <) the range for SIL 'n'

Each one of these place requirements on the elements used

 slide 10

Reference information from BS EN 61508....1

Safety Integrity Level (SIL)	Average probability of failure on demand (PFD_{AVG}) for a low demand safety function
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

IEC 61508-1 Table 2

Reference information from BS EN 61508.... 2

Safe Failure Fraction (SFF)	**Type A** element or subsystem Hardware Fault Tolerance (HFT)		
	0	1	2
<60 %	1	2	3
60 % - < 90 %	2	3	4
90 % - < 99 %	3	4	4
≥ 99 %	3	4	4

IEC 61508-2 Table 2

Type A definition: [7.4.4.1.2]

- Failure modes of all constituent components are well defined
- Behaviour of element is completely determined
- Sufficient field failure data exists to prove dangerous failure rates

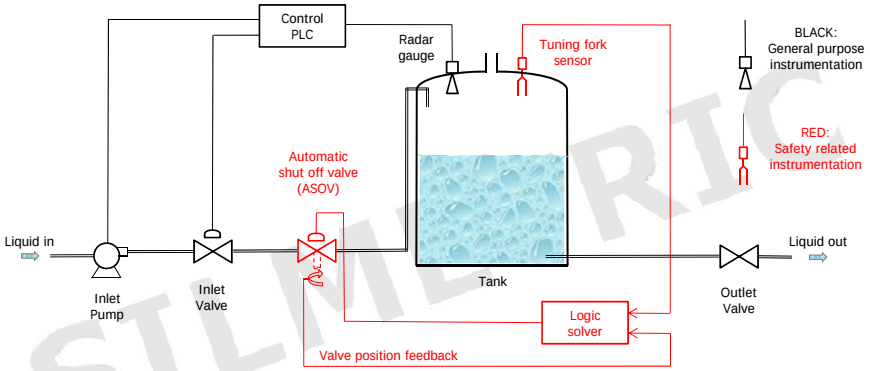
Safe Failure Fraction (SFF)	**Type B** element or subsystem Hardware Fault Tolerance (HFT)		
	0	1	2
<60 %	NO	1	2
60 % - < 90 %	1	2	3
90 % - < 99 %	2	3	4
≥ 99 %	3	4	4

IEC 61508-2 Table 3

Type B definition: [7.4.4.1.3]

- an element where any one of the three Type A requirements cannot be met

Example 1 – tank overfill protection (SIL 2)



Hazard #1: *Loss of containment (tank overfill) of hazardous liquid*

SIF #1: *Shut off ASOV if level reaches > 95% of tank capacity;* ***SIL 2***

Example failure data and methodology

For this example, we shall assume the following elements with their respective functional safety data are available:

Parameter	Level sensor	Safety Trip Alarm	Actuated Valve
Dangerous detected failure rate, λ_{DD} (hr^{-1})	1.4E-07	1.7E-07	5.6E-07
Dangerous undetected failure rate, λ_{DU} (hr^{-1})	2.5E-08	8.6E-08	2.8E-07
Safe failure rate, λ_S (hr^{-1})	1.3E-07	6.6E-07	4.5E-07
Safe failure fraction, SFF	90% to <99%	90% to <99%	60% to <90%
Type, A/B	Type A	Type B	Type A
Systematic capability, SC	SC2	SC3	SC2

Example of product failure data (full version!)

FUNCTIONAL SAFETY DATA DECLARATION (IEC 61508-2)	
Product identification:	Position Sensor, part no. XXX-YYYY-ZZ
Element safety function:	To provide a 4-20mA signal corresponding to position measured
Architectural parameters:	Type B; HFT=0; SFF = 74%; category 2 [ISO 13849]
Random hardware failures:	λ_{DD} = 3.25E-06; λ_{DU} = 2.15E-06; λ_{SD} = 2.20E-08; λ_{SU} = 2.81E-06
PFD_{AVG}:	9.44E-03
MTTFd:	53 years [ISO 13849]
Performance Level:	PL c [ISO 13849]
Diagnostic coverage:	60%
Diagnostic test interval:	<1 second
Restrictions in use:	Digital communications are not assessed for safety related use
Hardware safety integrity compliance:	Route 1_H
Systematic safety integrity compliance:	Route 1_S
Systematic Capability:	SC 2
Environment limits:	Operational temp: -20 to +70°C
Lifetime/replacement limits:	10 years
Proof Test requirements:	Refer to safety manual, document no. xyz, rev 1.3
Maintenance requirements:	Refer to I, O & M manual, document no. xyz, rev 1.1
Repair constraints:	Refer to I, O & M manual, document no. xyz, rev 1.1

Just a note about failure data...

2.137	failures per million hours
2.137 x 10^{-6}	failures per hour
2.137E-06	failures per hour
2137 FIT	failures per 10^{-9} hour (Failures In Time)

These all mean the same

But how *precise* are failure rate estimations?

We are engineers, so let's be realistic ☺

(The "-06" is the most useful quantity, the "2" is useful, the rest of the figures aren't warranted)

Simplified procedure to meet the SIL requirements

1. Select and arrange the elements in each subsystem to meet the **architectural constraints** for the SIL

2. Ensure each subsystem meets the **systematic capability** (SC) of the SIL

3. Calculate the **PFD_{AVG}** for each subsystem and ensure the sum meets (or is <) the target **PFD_{AVG}** for the SIF and hence meets the SIL

$PFD_S + PFD_L + PFD_{FE} = PFD_{SIF}$

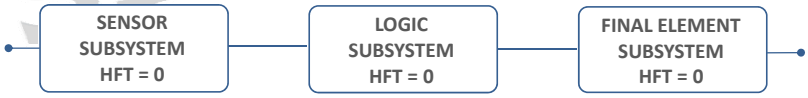
Refer to simplified PFD equations in BS EN 61508-6

 slide 17

Step 1: Architectural constraints

Compare the element data provided with the architectural constraints (AC) tables in BS EN 61508-2. Use the minimal Hardware Fault Tolerance (HFT) required to satisfy the SIL.

Subsystem	Data provided	Conclusion with reference to BS EN 61508-2 table 2/3
Sensor	Type A SFF = 90 – 99%	Up to SIL 3 with HFT = 0
Logic	Type B SFF = 90 – 99%	Up to SIL 2 with HFT = 0
Final element	Type A SFF = 60 - 90%	Up to SIL 2 with HFT = 0

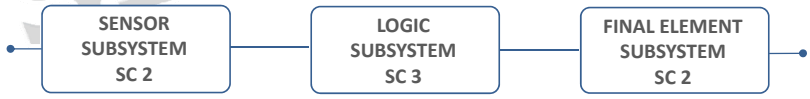


 slide 18

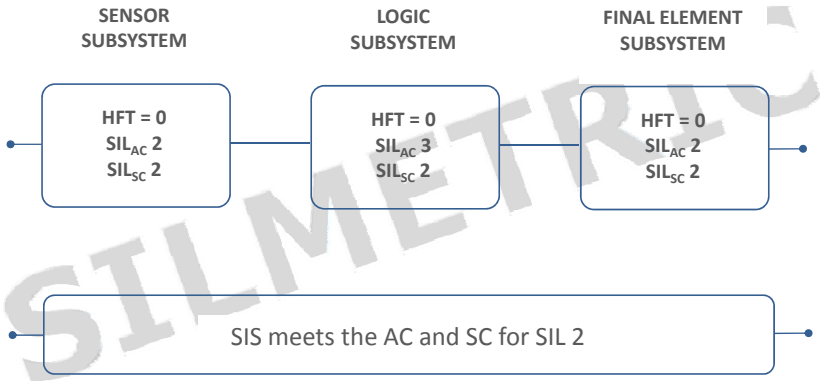
Step 2: Systematic capability

Compare the element data provided with the SC requirements for the subsystem. Increase the HFT if necessary to satisfy the SIL.

Subsystem	Data provided	Conclusion (SC 'n' = SIL 'n')
Sensor	SC 2	SIL 2
Logic	SC 3	SIL 3
Final element	SC 2	SIL 2



Conclusion of Steps 1 & 2



Step 3: PFD_{AVG} for each subsystem (1oo1)

$$PFD_{AVG} = (\lambda_{DU} + \lambda_{DD})\, t_{CE}$$

Equations from IEC 61508-6 (informative)

$$\text{Where } t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

For this example, we shall assume the following values (which must be confirmed by the operator):

- Proof test interval, T_1 = 8,760 hrs (= 1 yr)
- Mean time to repair, MTTR = 8 hrs

Step 3: PFD_{AVG} for the SIF

$$PFD_{AVG}\ (SIF) = PFD_S + PFD_L + PFD_{FE}$$

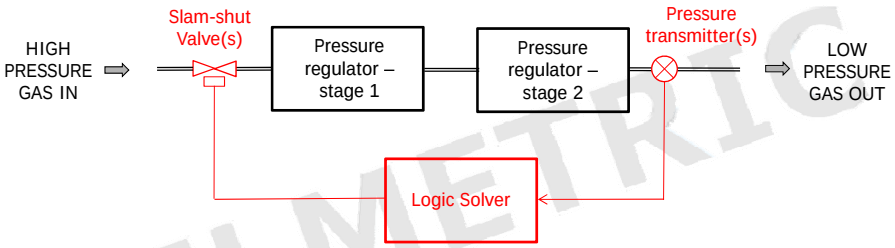
$$= 1.1E\text{-}04 + 3.8E\text{-}04 + 1.2E\text{-}03$$

$$= 1.7E\text{-}03$$

Referring to BS EN 61508-1 table 2 shows this is comfortably in the SIL 2 range (10^{-3} to 10^{-2}).

SIL	PFD_{AVG}
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

High Integrity Pressure Protection System (HIPPS)



Hazard #1: *Overpressure and rupture of downstream pipeline*

SIF #1: *Shut off gas supply if outlet pressure > 2bar;* ***SIL 3***

 slide 23

Example failure data and methodology

For this example, we shall assume the following elements with their respective functional safety data are available:

Parameter	Pressure Transmitter	Safety Trip Alarm	Actuated Valve
Dangerous detected failure rate, λ_{DD} (hr^{-1})	3.4E-07	1.7E-07	5.6E-07
Dangerous undetected failure rate, λ_{DU} (hr^{-1})	3.4E-08	8.6E-08	2.8E-07
Safe failure rate, λ_S (hr^{-1})	6.2E-07	6.6E-07	4.5E-07
Safe failure fraction, SFF	90% to <99%	90% to <99%	60% to <90%
Type, A/B	Type B	Type B	Type A
Systematic capability, SC	SC3	SC3	SC2

 slide 24

Example 2 – HIPPS (SIL 3)

For this example, we shall assume that the user requirements specification has an additional **availability** requirement that necessitates **2oo3 voting in the sensor subsystem** (very typical for HIPPS)

We follow the same method as before to define, for each subsystem, the:

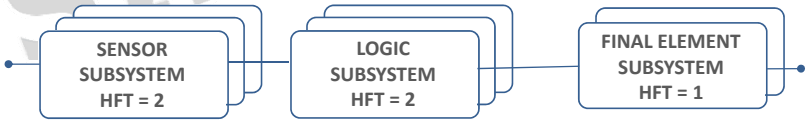
1. Architectural constraints
2. Systematic capability
3. PFD_{AVG}

And finally the PFD_{AVG} of the SIF to verify the SIL achieved

Step 1: Architectural constraints

Compare the element data provided with the architectural constraints (AC) tables in BS EN 61508-2. Use the minimal Hardware Fault Tolerance (HFT) required to satisfy the SIL (or the Availability, if higher).

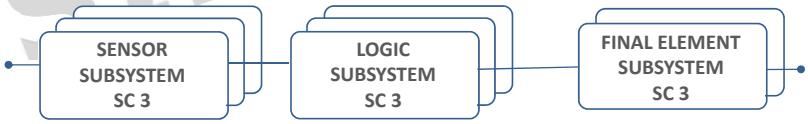
Subsystem	Data provided	Conclusion with reference to BS EN 61508-2 table 2/3
Sensor	Type B SFF = 90 – 99%	SIL 3 requires HFT = 1 But HFT = 2 for availability
Logic	Type B SFF = 90 – 99%	SIL 3 requires HFT = 1 But HFT = 2 for availability
Final element	Type A SFF = 60 - 90%	SIL 3 requires HFT = 1



Step 2: Systematic capability

Compare the element data provided with the systematic capability required for the SIL. Increase the SC of the subsystem if required to satisfy the SIL.

Subsystem	Data provided	Conclusion (SC 'n' = SIL 'n')
Sensor	SC 3	SIL 3
Logic	SC 3	SIL 3
Final element	SC 2	need to increase to SIL 3



Systematic capability and redundancy

There are limits to what SIL capability can be claimed for a combination of multiple (redundant) elements *in respect of systematic capability*.

SC N (N=1,2,3) is the Systematic Capability of an element determined by the systematic integrity measures used (e.g., software, lifecycle, FSM, documentation, etc)

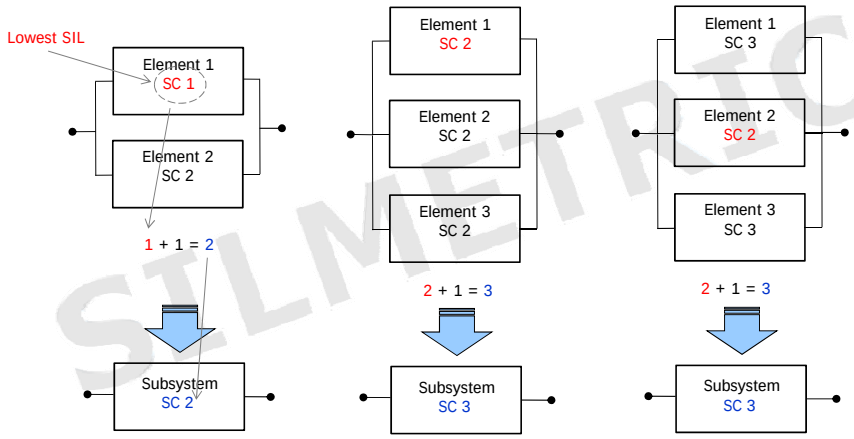
Rule: The SC of a combination of elements (arranged in redundancy) is limited to the lowest SC (1, 2, 3) of the elements +1, *providing there is sufficient independence between the multiple elements* [7.4.3.2]

The SC claimed for the combination can only be SC N+1 at most, regardless of how many elements are used in the combination [7.4.3.3]

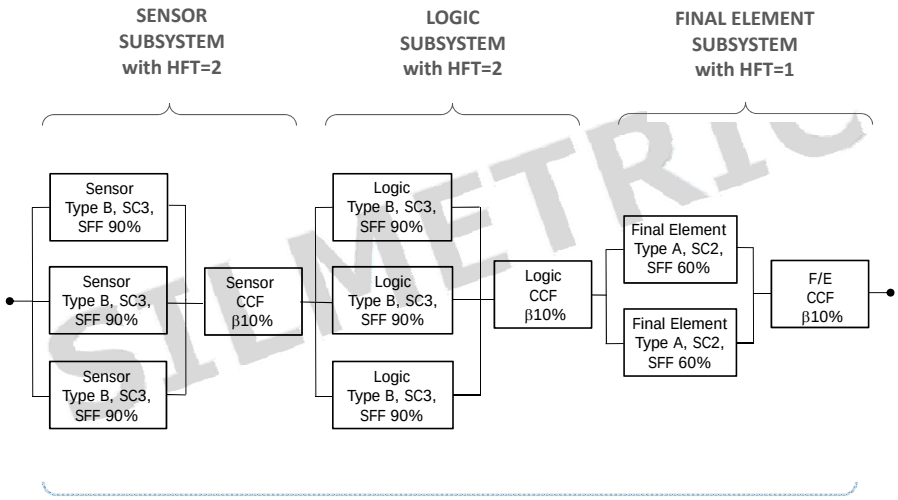
Note that 'sufficient independence' should be justified by common cause failure analysis and be commensurate with SIL involved [7.4.3.4]

Systematic capability and redundancy (cont.)

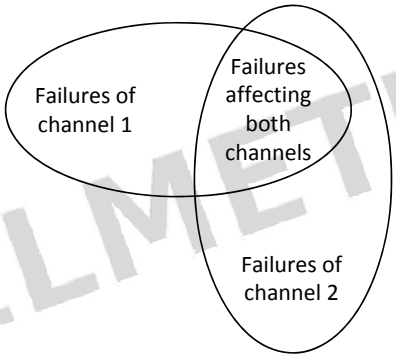
Examples of systematic capability using a combination of elements...



Conclusion of Steps 1 & 2



Common cause failure



Addressing common cause failure (β-factor)

Some issues that affect common cause failure are:

- separation (location, distance apart, etc)
- diversity in technology or unit type
- complexity (more complex often leads to higher CCF
- environment control or testing
- operational and maintenance procedure
- other human factors (e.g., competence)

Step 3: PFD_{AVG} for the 1oo2 subsystem

$$PFD_{AVG} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MTTR\right]$$

Where

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

β= common cause factor (CCF) for dangerous undetected failures

β_D = CCF for dangerous detected failures

We make the same assumptions as previous example for T_1 and MTTR

 slide 33

Step 3: PFD_{AVG} for the 2oo3 subsystem

$$PFD_{AVG} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left[\frac{T_1}{2} + MTTR\right]$$

Where

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{2} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left[\frac{T_1}{3} + MTTR\right] + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

β, β_D, T_1 and MTTR as explained earlier

 slide 34

Step 3: PFD_{AVG} for the SIF

$$PFD_{AVG}\ (SIF) = PFD_S + PFD_L + PFD_{FE}$$

$$= 1.5E\text{-}05 + 3.8E\text{-}05 + 1.2E\text{-}04$$

$$= 1.8E\text{-}04$$

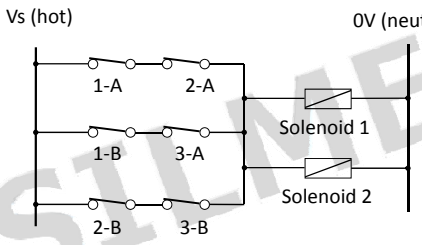
Referring to BS EN 61508-1 table 2 shows this is comfortably in the SIL 3 range (10^{-4} to 10^{-3}).

SIL	PFD_{AVG}
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$

 slide 35

2oo3 voting

Assumes each logic solver has two output relays (A and B) that can be connected as follows:



Ch1	Ch2	Ch3	TRIP
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

 slide 36

Summary and final thoughts...

- Be realistic about the precision of failure data
- Check intended environment and conditions carefully against equipment specs – if in doubt specify more frequent proof tests
- The proof test procedure needs careful preparation, especially when HFT > 0 is involved
- Ensure independence between the BPCS and the SIS
- Keep things simple where possible
- Check the actual proof test and MTTR values being used and re-calculate PFDs if different figures are used to those assumed in the analysis

Comments and points raised after the talk (29/01/14)...

1. There can be a tendency to be over cautious during the risk assessment / SIL determination phase, thus resulting in an inflated risk reduction requirement leading to increased cost for the engineering and of ownership (higher SIL to maintain). We should aim to use more realistic figures during SIL determination.
2. Determining whether an element (or subsystem) is type A or B can make a significant difference to the complexity and cost of the final system. There was a suggestion that manufacturers could have an interest in stating type B in order to sell more products! On the other hand, manufacturers' marketing people might want to state type A so that the product is seen to be suitable in higher SIL applications. Motivation aside, the judgement is difficult depending on how you interpret the type A/B criteria. (Maybe more justification from the manufacturer, rather than just a statement, would be helpful to enable an integrator/user to make a final judgement for the application).

Comments and points raised after the talk (29/01/14)...

3. The site log is importance to record all trips (spurious and real) in order to verify the demand rate assumptions made during initial risk assessment. The use of the log should feature in the site procedures and operator training programme.
4. Examples have been seen involving a 2oo3 valve configuration, where all three measurements share a common tapping or sampling point. Inadvertent isolation of this would bypass the whole system. As for the isolation valve there was no clear indication what was the open and the closed position!
5. What happens when a demand occurs just as you are proof testing / servicing one of the devices in a 2oo3 system? How is such a system configured to respond on reset (as a 2oo3 or as a 1oo2)? The functionality should be considered in the safety requirements specification and covered in the proof testing procedure.

 slide 39

Comments and points raised after the talk (29/01/14)...

6. Can valve position feedback (tank overfill example) be routed back to the control system (non-SIS) for indication/diagnostics in the cases when a hardware logic solver (e.g., trip amp) is used rather than a safety PLC? The answer will depend on whether the BPCS / SIS independence is compromised and how much reliance (in terms of risk reduction) is placed on the feedback.
7. The principle of "keep control separate from safety" is recommended.

 slide 40

That's the end of this talk...

ARE THERE ANY (MORE) QUESTIONS?

SILMETRIC

Thanks for listening

Functional Safety
TRAINING • CONSULTANCY • ASSESSMENT
www.silmetric.com