SIL Calculations

Practical Guidance in the used of IEC 61508-6:2010

Our Members


AFK Consultancy
ANALOX
arc AWE
NUCLEAR SECURITY TECHNOLOGIES
bp
CEPHA CONTROLS
cetix
CHARTER·TECH
CLEARLINE
cml Ex
CSA GROUP
DEKRA
DIAGEO
DNV
DOW CORNING
Dräger
EATON
Powering Business Worldwide
EDF
EMERSON
Process Management
ERM
evero
ExxonMobil
FICHTNER
Consulting Engineers Limited
FRAZER·NASH
CONSULTANCY
HAZCON
Haden Freeman Ltd
hitex
EMBEDDED TOOLS & SOLUTIONS
Honeywell
I&E SYSTEMS
IC&T
its
Invertek Drives
iti
Group
LR
=M
=Method
MOORE INDUSTRIES
MUTECH
national gas transmission
P & I Design Ltd
ProcessSafety
Solutions
procon
ProSalus
SAFETY CONSULTANTS
ROAKENGINEERING
ROSAS
rotork
Schneider Electric
SELLA CONTROLS
SENSIA
SGS
Baseefa
SIEMENS
SILMETRIC
sse
TAIT
UK Atomic Energy Authority
RACE
UL Solutions
uniper
VEOLIA
VAL-FSR
Virdee Advantage Limited
WITTENSTEIN
wsp
YOKOGAWA

Who Are We?

- **We are a cross-industry group of organisations with a common interest in functional safety, particularly in applying IEC 61508 and related standards (e.g., IEC 61511, IEC 62061) correctly in order to demonstrate compliance and improve safety for all.**
- Our members include end-users (from many industry sectors), EPC companies, systems integrators, product manufacturers, consultants and certifiers. We also have active relationships with related industry organisations and safety regulators who often attend our meetings.
- We develop and publish many useful and informative guides and assessment tools which are available to all (not just our members) and are free of charge.

In This Workshop:

- We will look at the simplified formulas for the Reliability Block Diagram methodology given in IEC 61508:2010, Part 6, Annex B.
- We will then use the method to calculate the average Probability of Failure on Demand for a typical low demand example SIF from the process industry.
- We will consider the effects that imperfect testing and common cause factors have on the results of the calculations.

Assumptions

- You have an understanding of why we quantify random hardware failures in Functional Safety.
- You understand the difference between modes of operation.
- For the purpose of this workshop we will focus on Demand Mode SIFs since this is the most common mode of operation in the Process Industry sector

Mode of Operation

In Demand Mode the target failure measure is in the following format:

- Uses average Probability of Failure on Demand (PFDavg)
- Takes credit for proof testing
- Takes credit for diagnostics

Demand Mode of Operation		
SIL	**Average probability of failure on demand**	**Target risk reduction**
4	**$\geq 10^{-5}$ to $< 10^{-4}$**	**>10,000 to ≤100,000**
3	**$\geq 10^{-4}$ to $< 10^{-3}$**	**>1,000 to ≤10,000**
2	**$\geq 10^{-3}$ to $< 10^{-2}$**	**>100 to ≤1,000**
1	**$\geq 10^{-2}$ to $< 10^{-1}$**	**>10 to ≤100**

Quantifying Random Hardware Failures

IEC 61508-6:2010 Annex B:

Examples of Technique for Evaluating Probabilities of Hardware Failure

- Simplified Reliability Block Diagram
- Fault Tree
- State / Transitions approach (Markov / Petri net)

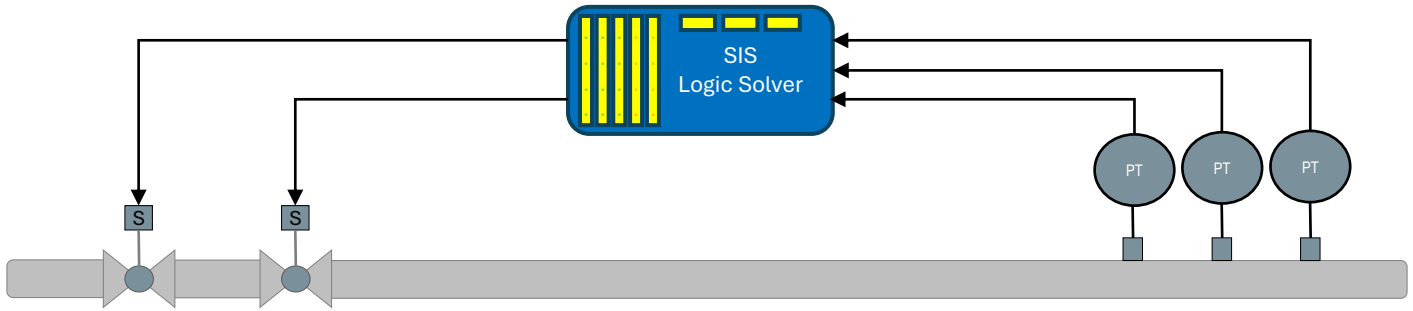
The methodology will depend on complexity

More often than not, we can use the Reliability Block Diagram approach using simplified formulas to approximate PFD_{avg}

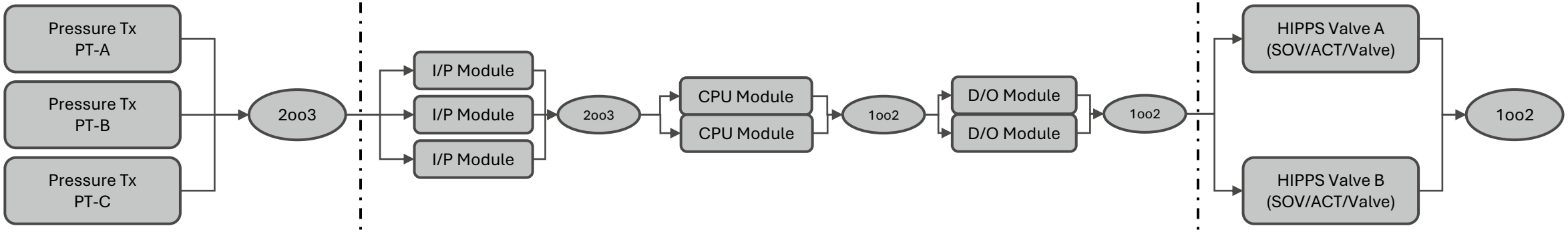
Example Using RBD

Using an example SIF we will go through the RBD methodology from IEC 61508-6 Annex B to calculate the average Probability of Failure on Demand.

1. Split the SIF into three subsystems (Initiators, Logic Solver, Final Elements)
2. Produce a simplified RBD for each subsystem complete with voting architectures
3. Apply the simplified formulas from IEC 61508-6:2010 Annex B to calculate the PFDavg of each subsystem
4. Add each subsystem PFDavg together to arrive at the total SIF PFDavg



Example RBD



Initiator Subsystem

Logic Solver Subsystem

Final Element Subsystem

Simplified Formulas

The following formula are from IEC 61508-6:2010 Annex B.3.2.

For each channel of a subsystem we need to calculate the 'channel equivalent mean down time' (t_{CE})

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

For a subsystem made up of redundant channels, we need to calculate the 'system equivalent mean down time' (t_{GE})

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Also a few other channel downtime formulas to consider for other architectures

Simplified Formulas

We then apply the channel downtime to the formula below to determine the subsystem PFD_{avg}

Subsystem Architecture	IEC 61508-6:2010 Formula
1oo1	$PFD = (\lambda_{DU} + \lambda_{DD})t_{CE}$
2oo2	$PFD = 2(\lambda_{DU} + \lambda_{DD})t_{CE}$
1oo2	$PFD = 2\left((1-\beta_D)\lambda_{DU} + (1-\beta)\lambda_{DU}\right)^2.tCE.tGE + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
2oo3	$PFD = 6\left((1-\beta_D)\lambda_{DU} + (1-\beta)\lambda_{DU}\right)^2.tCE.tGE + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$

PFD	Probability of Failure on Demand
λDU	Dangerous Undetected failure rate
λ_{DD}	Dangerous Detected failure rate
t_{CE}	Channel equivalent mean down time
t_{GE}	System equivalent mean down time
β	Common Cause Failure fraction
β_D	Common Cause Failure fraction for detected failures
MTTR	Mean Time To Restoration
MRT	Mean Repair Time
T_1	Proof Test Interval

PFD_{avg} Calculation

PFD_{avg} Calculation Results					
Element	Parameters				Architecture PFD_{Avg}
	Test Interval	MTTR	β factor (CCF)	β_D factor (CCF)	
Initiator Subsystem					
Pressure Transmitter	1 year	8 hours	10%	10%	2oo3 2.36E-04
Initiator Subsystem PFD_{avg} Subtotal:					**2.36E-04**
Logic Solver Subsystem					
A I/P	1 year	8 hours	2%	1%	2oo3 6.97E-07
CPU	1 year	8 hours	2%	1%	1oo2 5.34E-07
D O/P	1 year	8 hours	2%	1%	1oo2 6.68E-07
Logic Solver Subsystem PFD_{avg} Subtotal:					**1.90E-06**
Final Element Subsystem					
Valve Assembly	1 year	120 hours	10%	10%	1oo2 1.05E-03
Final Element Subsystem PFD_{avg} Subtotal:					**1.05E-03**
Total System PFD_{avg}:					**1.29E-03**
Total System RRF ($1/PFD_{avg}$):					**777**

Safety Instrumented Function Element Failure Rate Data					
Initiators	**Model**	**Data Source**	**λ_S**	**λ_{DD}**	**λ_{DU}**
Pressure Transmitter	Pressure Transmitter	SINTEF PDS Item 4.1.3	5.00E-07	8.00E-07	5.00E-07
Logic Solver	**Model**	**Data Source**	**λ_S**	**λ_{DD}**	**λ_{DU}**
Analogue Input Module	A I/P	Certificate	1.13E-06	8.86E-07	7.06E-09
Central Processing Unit	CPU	Certificate	1.31E-06	1.28E-06	4.90E-09
Digital Output Module	D O/P	Certificate	9.35E-07	8.61E-07	6.81E-09
Final Elements	**Model**	**Data Source**	**λ_S**	**λ_{DD}**	**λ_{DU}**
Solenoid Valve	Solenoid Valve	SINTEF PDS Item 4.3.5	1.90E-06	1.00E-07	6.00E-07
HIPPS Valve (incl. Actuator)	HIPPS Valve	SINTEF PDS Item 4.3.3	2.00E-06	3.00E-07	1.50E-06
Valve Assembly (sum of above)	Valve Assembly	SINTEF PDS	**3.90E-06**	**4.00E-07**	**2.10E-06**

Demand Mode of Operation		
SIL	**Average probability of failure on demand**	**Target risk reduction**
4	**$\geq 10^{-5}$ to $< 10^{-4}$**	**>10,000 to ≤100,000**
3	**$\geq 10^{-4}$ to $< 10^{-3}$**	**>1,000 to ≤10,000**
2	**$\geq 10^{-3}$ to $< 10^{-2}$**	**>100 to ≤1,000**
1	**$\geq 10^{-2}$ to $< 10^{-1}$**	**>10 to ≤100**

Beta Factor Considerations

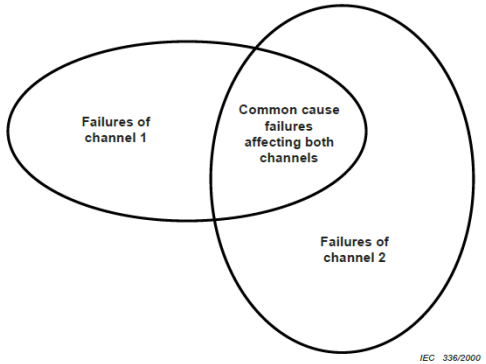


Table D.4 – Calculation of β_{int} or $\beta_{D\ int}$

Score (S or S_D)	Corresponding value of β_{int} or $\beta_{D\ int}$ for the:	
	Logic subsystem	Sensors or final elements
120 or above	0,5 %	1 %
70 to 120	1 %	2 %
45 to 70	2 %	5 %
Less than 45	5 %	10 %
NOTE 1 The maximum levels of $\beta_{D\ int}$ shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this.		
NOTE 2 Values of $\beta_{D\ int}$ lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.		

Typically we see the most conservative β values used without proper evaluation

However, from IEC 61508-6:2010 Annex D:

The β_{int} derived from Table D.4 is the common cause failure associated with a 1oo2 system. For other levels of redundancy (MooN) this β_{int} value will change as given in Table D.5 to yield the final value of β.

Beta Factor Considerations

Beta Factor for systems with levels of redundancy greater than 1oo2 should be changed with multiplication factors given in IEC 61508-6:2010 Annex D, Table D.5

MooN		N			
		2	3	4	5
M	1	β_{int}	0,5 β_{int}	0,3 β_{int}	0,2 β_{int}
	2	-	1,5 β_{int}	0,6 β_{int}	0,4 β_{int}
	3	-	-	1,75 β_{int}	0,8 β_{int}
	4	-	-	-	2 β_{int}

Beta Factor Considerations

PFD_{avg} Calculation Results Including β Factor Multiplications					
Element	Parameters				Architecture PFD_{Avg}
	Test Interval	MTTR	β factor (CCF)	β_D factor (CCF)	
Initiator Subsystem					
Pressure Transmitter	1 year	8 hours	15%	15%	2oo3 3.44E-04
Initiator Subsystem PFD_{avg} Subtotal:					**3.44E-04**
Logic Solver Subsystem					
A I/P	1 year	8 hours	3%	2%	2oo3 1.04E-06
CPU	1 year	8 hours	2%	1%	1oo2 5.34E-07
D O/P	1 year	8 hours	2%	1%	1oo2 6.68E-07
Logic Solver Subsystem PFD_{avg} Subtotal:					**2.24E-06**
Final Element Subsystem					
Valve Assembly	1 year	120 hours	10%	10%	1oo2 1.05E-03
Final Element Subsystem PFD_{avg} Subtotal:					**1.05E-03**
Total System PFD_{avg}:					**1.40E-03**
Total System RRF ($1/PFD_{avg}$):					**717**

β x 1.5

β x 1.5

≈8.5% Reduction in RRF

PFD_{avg} Calculation Results					
Element	Parameters				Architecture PFD_{Avg}
	Test Interval	MTTR	β factor (CCF)	β_D factor (CCF)	
Initiator Subsystem					
Pressure Transmitter	1 year	8 hours	10%	10%	2oo3 2.36E-04
Initiator Subsystem PFD_{avg} Subtotal:					**2.36E-04**
Logic Solver Subsystem					
A I/P	1 year	8 hours	2%	1%	2oo3 6.97E-07
CPU	1 year	8 hours	2%	1%	1oo2 5.34E-07
D O/P	1 year	8 hours	2%	1%	1oo2 6.68E-07
Logic Solver Subsystem PFD_{avg} Subtotal:					**1.90E-06**
Final Element Subsystem					
Valve Assembly	1 year	120 hours	10%	10%	1oo2 1.05E-03
Final Element Subsystem PFD_{avg} Subtotal:					**1.05E-03**
Total System PFD_{avg}:					**1.29E-03**
Total System RRF ($1/PFD_{avg}$):					**777**

Other Considerations

IEC 61508-6:2010, Annex B.3 - Reliability block diagram approach is based on some assumptions listed in Clause B.3.1. These include:

B.3.1 Underlying hypothesis

The calculations are based on the following assumptions:

– the channels in a voted group all have the same failure rates and diagnostic coverage;

– for each safety function, there is perfect proof testing and repair (i.e. all failures that remain undetected are detected by the proof test),

IEC 61511-1:2016, Clause 11.9.2 also states:

11.9.2 The calculated failure measure of each SIF due to random failures shall take into account all contributing factors including the following:

h) the coverage of any periodic proof tests, the associated proof test procedure and the reliability for the proof test facilities and procedure;

Simplified Formulas with PTC

Fortunately, IEC 61508-6:2010 Annex B.3.2.5 includes formulas considering 'non-perfect proof tests'.

These introduce the concept of Proof Test Coverage (PTC).

- PTC is a measure of how effective the proof test is at revealing Undetected Dangerous Failures.
- Undetected Dangerous Failures that can not be revealed by proof testing remain until the equipment is returned to its 'As New' condition.
- A second test interval (T_2) is introduced as the time interval when the equipment is returned to 'As New'.

Simplified Formulas with PTC

The ‘channel equivalent mean down time’ (t_{CE}) considering PTC is now:

$$t_{CE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{2} + MRT\right)\frac{\lambda_{DD}}{\lambda_D}MTTR$$

The ‘system equivalent mean down time’ (t_{GE}) considering PTC is now:

$$t_{GE} = \frac{\lambda_{DU}(PTC)}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DU}(1-PTC)}{\lambda_D}\left(\frac{T_2}{3} + MRT\right)\frac{\lambda_{DD}}{\lambda_D}MTTR$$

Simplified Formulas with PTC

With the simplified PFDavg formulas now:

Subsystem Architecture	IEC 61508-6:2010 Formula
1oo1	$PFD = (\lambda_{DU} + \lambda_{DD})t_{CE}$
2oo2	$PFD = 2(\lambda_{DU} + \lambda_{DD})t_{CE}$
1oo2	$PFD = 2\left((1-\beta_D)\lambda_{DU} + (1-\beta)\lambda_{DU}\right)^2 . tCE . tGE + \beta_D . \lambda_{DD} . MTTR + \beta . \lambda_{DU}(PTC)\left(\frac{T_1}{2} + MRT\right) + \beta . \lambda_{DU}(1-PTC)\left(\frac{T_2}{2} + MRT\right)$
2oo3	$PFD = 6\left((1-\beta_D)\lambda_{DU} + (1-\beta)\lambda_{DU}\right)^2 . tCE . tGE + \beta_D . \lambda_{DD} . MTTR + \beta . \lambda_{DU}(PTC)\left(\frac{T_1}{2} + MRT\right) + \beta . \lambda_{DU}(1-PTC)\left(\frac{T_2}{2} + MRT\right)$

What PTC to Use?

This depends on the Proof Tests being performed.

For modern, SIL certified initiators (e.g. electronic transmitters) the Safety Manual usually details proof test procedures and the PTC that can be claimed.

Usually a good start point but you must consider this is the context of the specific application.

Logic Solver – Usually left at 100% due to the difficulty in testing for the very small dangerous undetected failures. I consider 98% to allow for testing inconsistencies or human errors.

What PTC to Use?

SIF Final Elements (typically valves) do not usually have detailed proof test procedures with corresponding PTC due to the varying applications they are used in.

FMEDA + designed proof test procedures

Compare the proof test procedures against failure modes of an equivalent valve from a generic data source such as OREDA.

OREDA Based Valve Test Coverage Analysis - ESDV (Taxonomy 4.4.5.1)			
Failure Mode	**Failure %**	**Proof Test Method**	**Complete in PT?**
Delayed operation	11	Timed operation	Y
Failure to close	32	Stroke test	Y
Internal Leakage	15	Leak test	N
Structural Deficiency	24	Visual inspection + Stroke Test	Y
other	18	Assumed visual inspection	Y
Proof Test Coverage	***85 %***		

Effect on Overall PFDavg

PFD_{avg} Calculation Results Considering PTC and β MooN multiplications						
Element	Parameters					Architecture PFD_{Avg}
	Test Interval	MTTR	β factor (CCF)	β_D factor (CCF)	PTC	
Initiator Subsystem						
Pressure Transmitter	1 year	8 hours	10%	10%	90%	2oo3 6.76E-04
					Initiator Subsystem PFD_{avg} Subtotal:	**6.76E-04**
Logic Solver Subsystem						
A I/P	1 year	8 hours	2%	1%	98%	2oo3 1.21E-06
CPU	1 year	8 hours	2%	1%	98%	1oo2 6.12E-07
D O/P	1 year	8 hours	2%	1%	98%	1oo2 7.76E-07
					Logic Solver Subsystem PFD_{avg} Subtotal:	**2.60E-06**
Final Element Subsystem						
Valve Assembly	1 year	120 hours	10%	10%	85%	1oo2 2.71E-03
					Final Element Subsystem PFD_{avg} Subtotal:	**2.71E-03**
					Total System PFD_{avg}:	**3.39E-03**
					Total System RRF ($1/PFD_{avg}$):	**295**

PFD_{avg} Calculation Results Including β Factor Multiplications					
Element	Parameters				Architecture PFD_{Avg}
	Test Interval	MTTR	β factor (CCF)	β_D factor (CCF)	
Initiator Subsystem					
Pressure Transmitter	1 year	8 hours	15%	15%	2oo3 3.44E-04
				Initiator Subsystem PFD_{avg} Subtotal:	**3.44E-04**
Logic Solver Subsystem					
A I/P	1 year	8 hours	3%	2%	2oo3 1.04E-06
CPU	1 year	8 hours	2%	1%	1oo2 5.34E-07
D O/P	1 year	8 hours	2%	1%	1oo2 6.68E-07
				Logic Solver Subsystem PFD_{avg} Subtotal:	**2.24E-06**
Final Element Subsystem					
Valve Assembly	1 year	120 hours	10%	10%	1oo2 1.05E-03
				Final Element Subsystem PFD_{avg} Subtotal:	**1.05E-03**
				Total System PFD_{avg}:	**1.40E-03**
				Total System RRF ($1/PFD_{avg}$):	**717**

Any Questions?

Presenter: Ian Dolan – Principal Consultant
Contact Details: idolan@sellacontrols.com

What's next....

Slot	Start Time	Paper	Workshop	Finish Time
11	16:00	Slot A-11: Functional Safety and Communication Links	Slot B-11: Discussion on Difference Between ISO 26262 and IEC 61508	16:30
-	16:30	Close / Informal Post Symposium Question / Discussion		17:30

We would be more than happy to discuss membership with you (https://61508.org/membership/)