8. SIF Design – SIL Verification

GAS DETECTOR FUNCTIONAL SAFETY

OVERVIEW COURSE

Institute of Instrumentation Control and Automation

Mod 8 Rev 0 16 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 1

Purpose

Explains how to calculate the SIF failure probability to comply with the required SIL

TOPICS

Random failure rate

Calculating PFD_{avg}
- one component
- multiple components

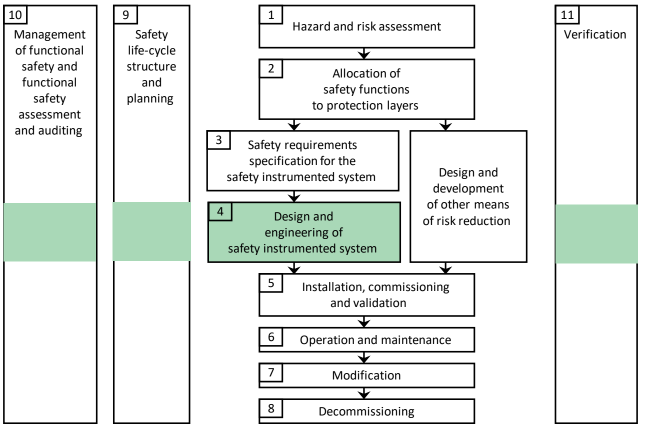
Allowing for Common Mode Failure
- what is it
- β factor model
- equations

High Demand Mode issues

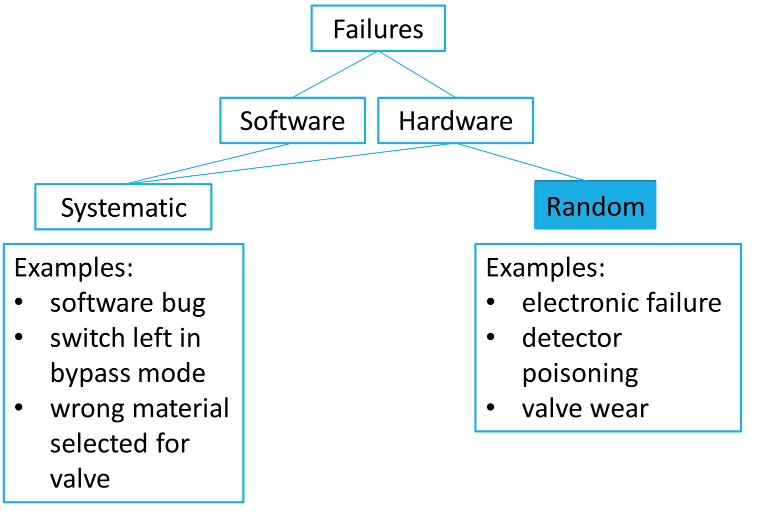
Design & Engineering

Design and implement the SIS to meet the SRS

- check if the chosen architecture of the SIF meets the target PFD_{avg} for the SIL



Different failure types



Design Process

1. Design architecture of each SIF to meet target SIL

2. Confirm that SIF meets required reliability target
   - "SIL verification"

3. Select components suitable for target SIL

4. Detailed design and engineering of the SIS (not part of this course)
   - gas detector coverage is particularly important

Some iteration around steps 1 to 3 may be required

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

- selected components must allow the SIF to meet HFT & PFD_{avg} requirements

Failure rate (λ - lambda)

Failure Rate

The number of failures per unit of time

Consider a sample of 1,000 components - over 5 years, 10 fail.

What is the average failure rate λ_{avg} (often just called λ)?

10 failures / (1,000 x 5 years)

= 2 failures per 1,000 y

= 0.002 failures/y

= $\boxed{2 \times 10^{-3} /y}$

= 0.002/y/(8760h/y)

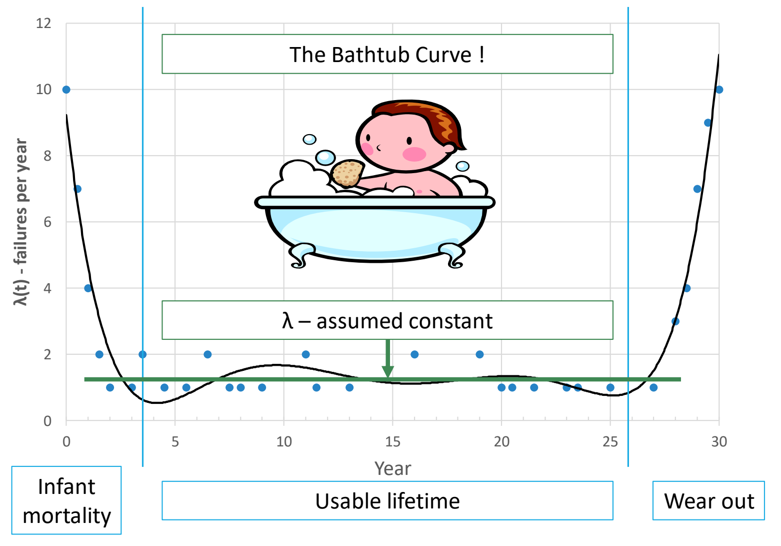
= $\boxed{2.3 \times 10^{-7} /h}$

= 230×10^{-9} /h

= $\boxed{230\ FIT}$ Failures In Time = Failures per billion hours

Be careful of the time units !

Failure Rate is not constant



Average Failure Rate

Is a property of a <u>component</u> & includes <u>all</u> failure categories

Consider a pressure transmitter used for a low pressure trip

λ

λ_S

SAFE
Loss of output

Causes spurious trip

λ_D

DANGEROUS
Frozen output

Prevents safety function

Finding Faults

Diagnostics

- automatic tests run at a high frequency to detect faults or failures in a component
- executed internal to the component or by another component
  - e.g. internal transmitter diagnostics, or comparison of transmitter outputs by control system
- to take credit, must execute at least 100 times the demand rate

Proof Tests

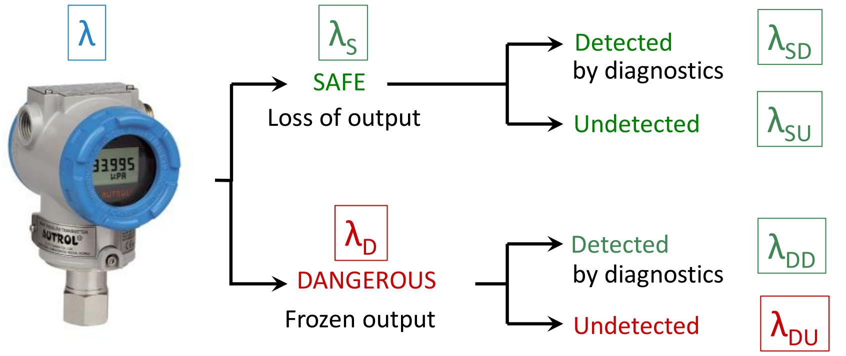
- manually initiated tests executed relatively infrequently
  - e.g. SIF function test during maintenance shutdown
- ideally restores component to as new condition
- "imperfect" proof tests are also used
  - e.g. partial valve stroke testing

Each type of test has a "coverage factor"

Add diagnostics

Smart pressure transmitter with diagnostics, used for low pressure trip

Further subdivide lambda:



Where do these numbers come from?

Failure Mode Effects and Diagnostics Analysis (FMEDA)
- extended version of FMEA

Analyses a "system"
- e.g. transmitter

Breaks down into "elements"
- each having a defined failure mode and failure rate (λ)
- e.g. resistors, op. amps, capacitors, PCB etc.

Identifies impact of local failures on system failure modes
- e.g. failure of resistor open circuit -> transmitter fails low

Identifies the % of these failures that are detected by diagnostics

The lambdas are then grouped and summed to get λ_{DU}, λ_{DD}, λ_{SU}, λ_{SD}

Diagnostic Coverage (DC) and Safe Failure Fraction (SFF) can then be calculated from these values

Data from certificate

Produkt (2)	MSC2/MGC2 & SC2-34XX (brennbare Gase) (flammable gases)	MSC2/MGC2 & SC2-11XX (toxische Gase) (toxic gases)
Sicherheitsfunktion Safety Function	Vom Gas am Eingang bis zu den Relaisausgängen From gas at inlet to relay output	
Messbereich measuring range	0 – 100 % UEG 0 – 100 % LEL	Abhängig von Gasart Depending on the type of gas
SIL	2	
HFT	0	0
PFD	$6{,}37 \times 10^{-4}$	$1{,}690 \times 10^{-7}$
~~SFF~~	~~91,92 %~~	~~91,55 %~~
λ_{DU}	$1{,}350 \times 10^{-7}$ (per h)	$1{,}690 \times 10^{-7}$ (per h)
λ_{DD}	$4{,}490 \times 10^{-7}$ (per h)	$4{,}460 \times 10^{-7}$ (per h)
λ_{SU}	$1{,}089 \times 10^{-6}$ (per h)	$1{,}380 \times 10^{-6}$ (per h)
λ_{SD}	$4{,}810 \times 10^{-9}$ (per h)	$6{,}910 \times 10^{-9}$ (per h)
Proof test interval	≤ 1 Jahr / year	
MTTR	72 Stunden / hours	

Beware of numbers!

λ_{DU} on certificates is often very optimistic because it is:

- theoretical
- does not allow for the application e.g. sensor coverage
- may not include all the mechanical components e.g. sampling system

Example: 1.35 x 10^{-7} per hr on previous slide is 1 failure per 845 y

For gas detection you must include detector coverage, as it will dominate reliability

- see: ISA-TR84.00.07-2010 Guidance on the Evaluation of Fire and Gas System Effectiveness
- new edition about to be published
- this report applies to process industry (normally open air situations) rather than laboratories, but the principles are similar
- are there any guidelines on this for laboratories?

Mod 8 Rev 0 16 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 15

Failure probability

Mod 8 Rev 0 16 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 16

Finding Faults

Diagnostics

- automatic tests run at a high frequency to detect faults or failures in a component
- to take credit, must execute at least 100 times the demand rate
- increasing Diagnostic Coverage reduces λ_{DU}

Proof Tests

- manually initiated tests executed relatively infrequently
  - e.g. SIF function test during maintenance shutdown
- ideally restores component to as new condition
- directly influences PFD_{avg}

Proof tests are critical for demand mode SIFs

PFD average formula

If a component of a SIF fails when asked to operate:

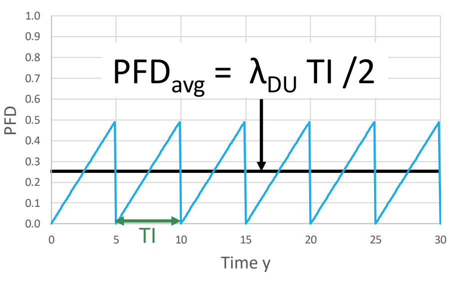
- it must have failed dangerously
  - safe failures will cause a spurious trip
- the failure must not have been detected by diagnostics
  - if detected, it is assumed corrective action will have been taken
- hence we are concerned with <u>dangerous undetected</u> failures
- λ_{DU} is the appropriate failure rate to use

If at t = TI, we test the component
and repair it if faulty,
PFD is reset to 0

$$\boxed{PFD_{avg} = \lambda_{DU}\ TI/2}$$

Example:
$PFD_{avg} = 0.1 \times 5/2 = 0.25$

Certificate example:
$1.35 \times 10^{-7} \times 8760/2 = 5.9 \times 10^{-4}$



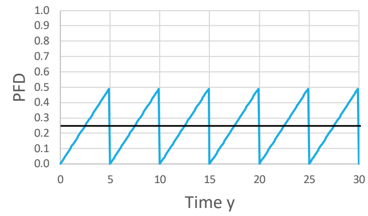
Proof Test Interval

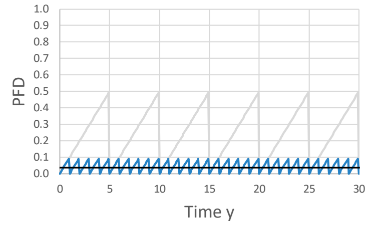
PFD_{avg} is directly proportional to proof test interval (TI)

Reduce TI from 5 years

to 1 year

PFDavg reduces from 0.25 to 0.05





Safety Integrity Level vs. PFD_{avg}

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

Used to specify SIL <u>required</u>

Used to specify SIL <u>achieved</u>

* Basic Process Control System

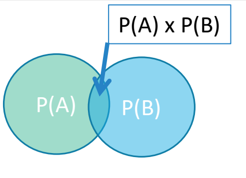
For Low Demand Mode SIFs only

PFD_{avg} for multiple devices

Boolean Algebra - AND

Applies to <u>independent</u> events A and B
- P(A & B) = P(A) x P(B)

Events are independent if P(B) does not depend on P(A) and vice versa
- e.g. successive coin tosses



Example
- P(channel A will fail) = 0.1
- P(channel B will fail) = 0.1

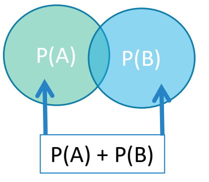
1oo2 architecture
- both A AND B have to fail to lose safety function
- P(A & B fail) = 0.1 x 0.1 = 0.01

Basis for most fault tree and reliability block diagram calculations
- BUT not accurate for combining PFD_{avg} in 1oo2 architecture (or similar)
  - use formulas on later slide

Boolean Algebra - OR

Applies to independent events A and B

- P(A or B) = P(A) + P(B) – P(A) x P(B)
  - subtract intersection to avoid double counting



Example

- P(channel A will fail) = 0.1
- P(channel B will fail) = 0.1

2oo2 architecture

- either A OR B have to fail to lose safety function
- P(A or B fail) = 0.1 + 0.1 – 0.1 x 0.1 = 0.19 ≈ 0.2
  - ignore "x" term generally if P < 0.1

Basis for most fault tree and reliability block diagram calculations

- also OK to use for combining multiple PFD_{avg} in 2oo2 architecture

PFD_{avg} combinations summary

	PFD_{avg}	$MTTF_S$	(Mean Time between safe failures)
1oo1	$\lambda_{DU} \cdot TI / 2$	$1/\lambda_S$	
1oo2	$(\lambda_{DU} \cdot TI)^2 / 3$	$1/(2\lambda_S)$	
2oo2	$\lambda_{DU} \cdot TI$	$1/(2(\lambda_S)^2 \cdot MTTR)$	
2oo3	$(\lambda_{DU} \cdot TI)^2$	$1/(6(\lambda_S)^2 \cdot MTTR)$	

Example:

1oo1	0.1	5y	
1oo2	0.013	2.5y	
2oo2	0.2	625y	MTTR = 1 wk = 0.02 y say
2oo3	0.04	208y	

Which is safest and least safe ?

Which has the best and worst time between spurious trips?

Which is the best compromise?

Summary of Architectures

Safest to least safe ◦ best to worst	Lowest to Highest spurious trip rate ◦ best to worst
1oo2	2oo2
1oo2D)	2oo3)
2oo3)	1oo2D)
1oo1D (safety)	1oo1D (availability)
1oo1	1oo1
2oo2	1oo1D (safety)
1oo1D (availability)	1oo2

Common practice
- 1oo1 for HFT = 0
- 2oo3 for HFT = 1

For simplified formulae for all architectures see:
PDS Reliability Prediction Method for Safety Instrumented Systems (SINTEF 2013)

Common Mode Failures

Common Mode Failures

common mode failures (IEC 61511-1 Ed. 2 3.2.7.2)
- concurrent failures of different devices characterized by the same failure mode (i.e. identical faults)
- Common Mode Failures are often assumed to be Common Cause Failures and are abbreviated "CCF"

Examples:
- high temperature results in cards failing open circuit
- contaminated instrument air causes solenoid valves to stick open

The resultant failure modes in each channel are in the same direction

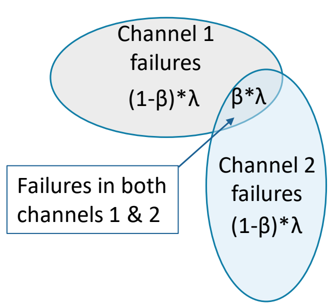
The failures occur within a short time of each other
- this may still allow a failure in one channel to be corrected before the other channel fails

Channel 1 Fault	Fails open circuit
Channel 2 Fault	Fails open circuit

The β-factor model

β is the probability that if one channel fails, ALL channels will fail in the same way

Typical values: 0.01 to 0.1 (usually a percentage 1% to 10%)



PFD_{avg} with common mode

	PFD_{avg}
1oo1	$\lambda_{DU} \cdot TI / 2$
1oo2	$(1-\beta) \cdot (\lambda_{DU} \cdot TI)^2 / 3 + \beta \cdot \lambda_{DU} \cdot TI / 2$
2oo3	$(1-\beta) \cdot (\lambda_{DU} \cdot TI)^2 + \beta \cdot \lambda_{DU} \cdot TI / 2$
2oo2	$\lambda_{DU} \cdot TI$

Use these formulas!

Usually assume 1 - β ≈ 1

Example PFD_{avg} with typical β = 5%

Must include β !

	without β	β term	total with β=5%	β term/total
1oo1	0.01	-	0.01	-
1oo2	0.00013	0.0005	0.00063	81%
2oo3	0.0004	0.0005	0.00088	57%
1oo3	2×10^{-6}	0.0005	0.000502	99.6%

What value for β?

Suggested default values

- field devices – measurement
  - e.g. transmitters, pressure switches separate tapping points — 2%
  - with shared tapping points — 10%
- field devices – final elements
  - e.g. solenoid valves, block valves — 5%
- electronics in equipment room
  - e.g. logic solvers, relays — 1%

If PFD_{avg} close to SIL boundary or β dominates PFD_{avg} calc

- determine β more rigorously (e.g. using IEC 61508-6 Annex D)

Common causes of common mode failures

Temperature

Contamination

Water ingress

Corrosion

Electromagnetic noise or interference

Vibration

Power supply quality

Air or hydraulic fluid quality

Errors in design / selection / software / maintenance

Are these random or systematic failures?

What can be done to mitigate each of these?

Mod 8 Rev 0 16 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 31

Diversity

Redundancy using identical components does not reduce common mode failures

To reduce common mode, use diverse channels

Example: Protection against runaway exothermic reaction

- In order of increasing diversity, and decreasing β
  - three identical temperature transmitters
  - temperature switch & 2 different brand transmitters
  - 2 different brand temperature transmitters and a pressure transmitter

See IEC 61508-6 Table D.1 for a useful checklist of items to reduce β

- note that although reducing β reduces random failures, this is achieved by reducing systematic failures

Mod 8 Rev 0 16 April 2018 IICA GAS DETECTOR FUNCTIONAL SAFETY COURSE COPYRIGHT IICA 2018 32

High Demand Mode

More than one demand per year and cannot guarantee sufficiently frequent proof testing

If SIF operates in High Demand Mode

- PFD_{avg} cannot be used
- probability of failure per hour (for a component = λ_{DU}) must be used

For OR gates, can add λ_{DU} values

- 2oo2 PFH = 2 x λ_{DU}

For AND gates and more complex architectures more complex formulas apply

- 1oo2 PFH = λ_{DU}^2 x TI + ß x λ_{DU}
- 2oo3 PFH = 3 x λ_{DU}^2 x TI + ß x λ_{DU}
- Note that TI is still relevant for redundant architectures
- From *PDS Reliability Prediction Method for Safety Instrumented Systems* (SINTEF 2013) Table 9

Summary

The probability that the SIF will fail must be low enough to comply with the required SIL

Random failure rate λ_{DU}

Calculating PFD_{avg}

- one component: $PFD_{avg} = \lambda_{DU} * TI/2$
- multiple components: See formulas

Allowing for Common Mode Failure

- failure of all channels from a common cause
- β factor model allows for this
- use the equations with β

High Demand Mode

- measure is Probability of Failure per Hour (PFH)
- see formulas

Questions?