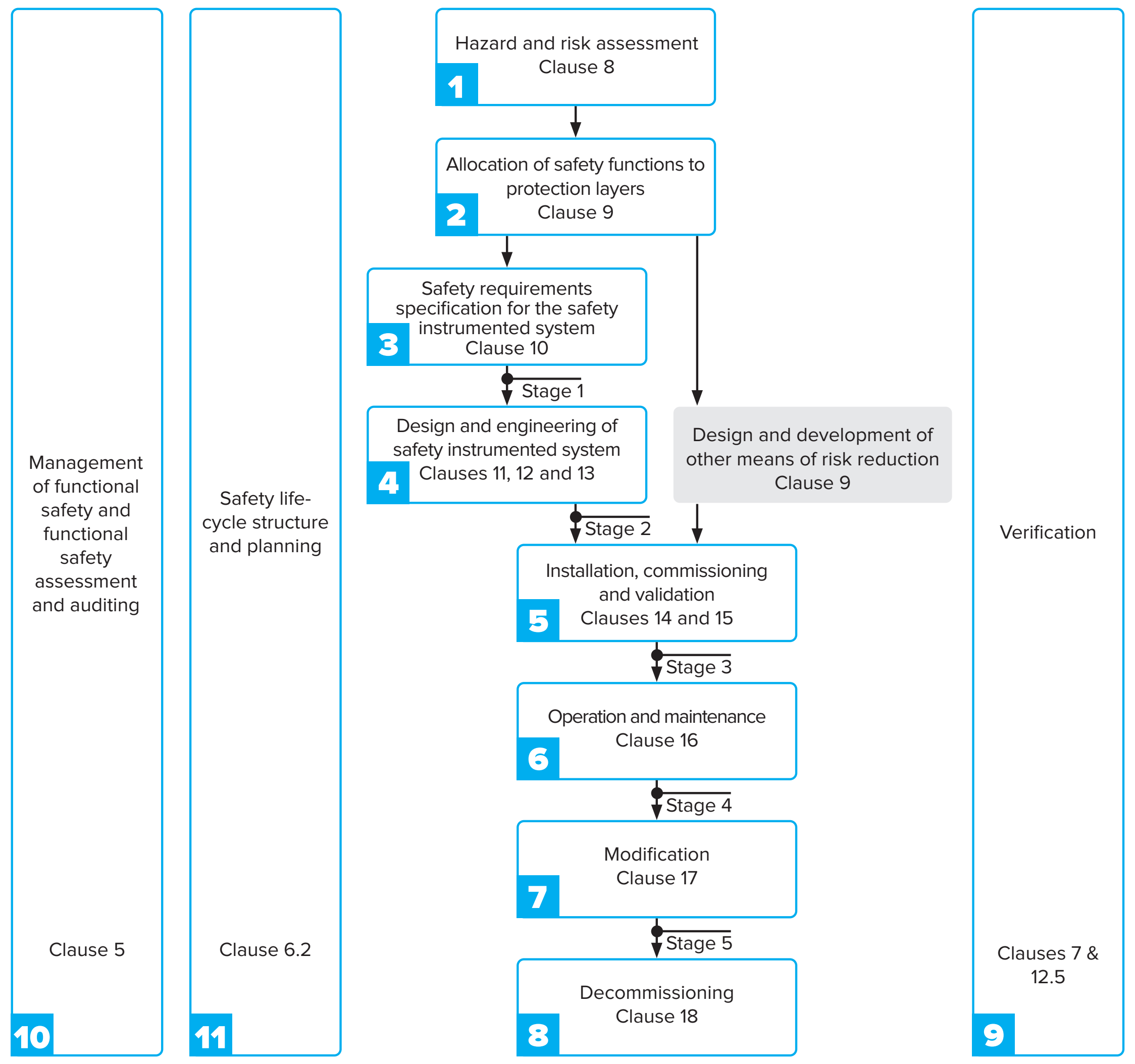
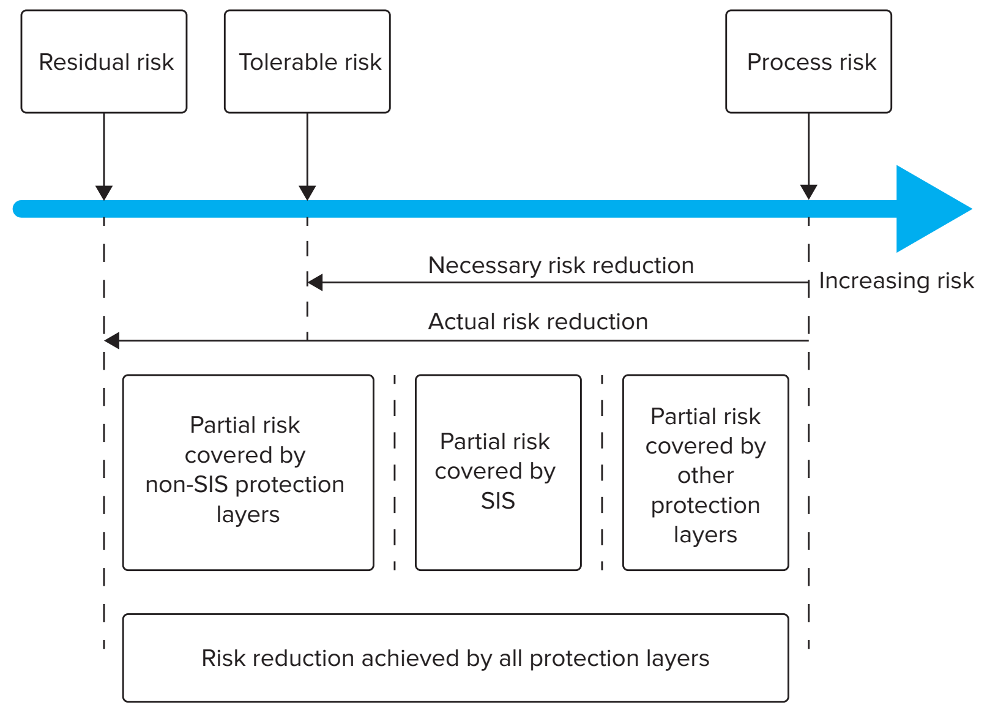
# FUNCTIONAL SAFETY FUNDAMENTALS

## LIFECYCLE IEC61511


Hazard and risk assessment
Clause 8
1
Allocation of safety functions to protection layers
Clause 9
2
Safety requirements specification for the safety instrumented system
Clause 10
3
Stage 1
Design and engineering of safety instrumented system
Clauses 11, 12 and 13
4
Design and development of other means of risk reduction
Clause 9
Stage 2
Installation, commissioning and validation
Clauses 14 and 15
5
Stage 3
Operation and maintenance
Clause 16
6
Stage 4
Modification
Clause 17
7
Stage 5
Decommissioning
Clause 18
8
Management of functional safety and functional safety assessment and auditing
Clause 5
10
Safety life-cycle structure and planning
Clause 6.2
11
Verification
Clauses 7 & 12.5
9

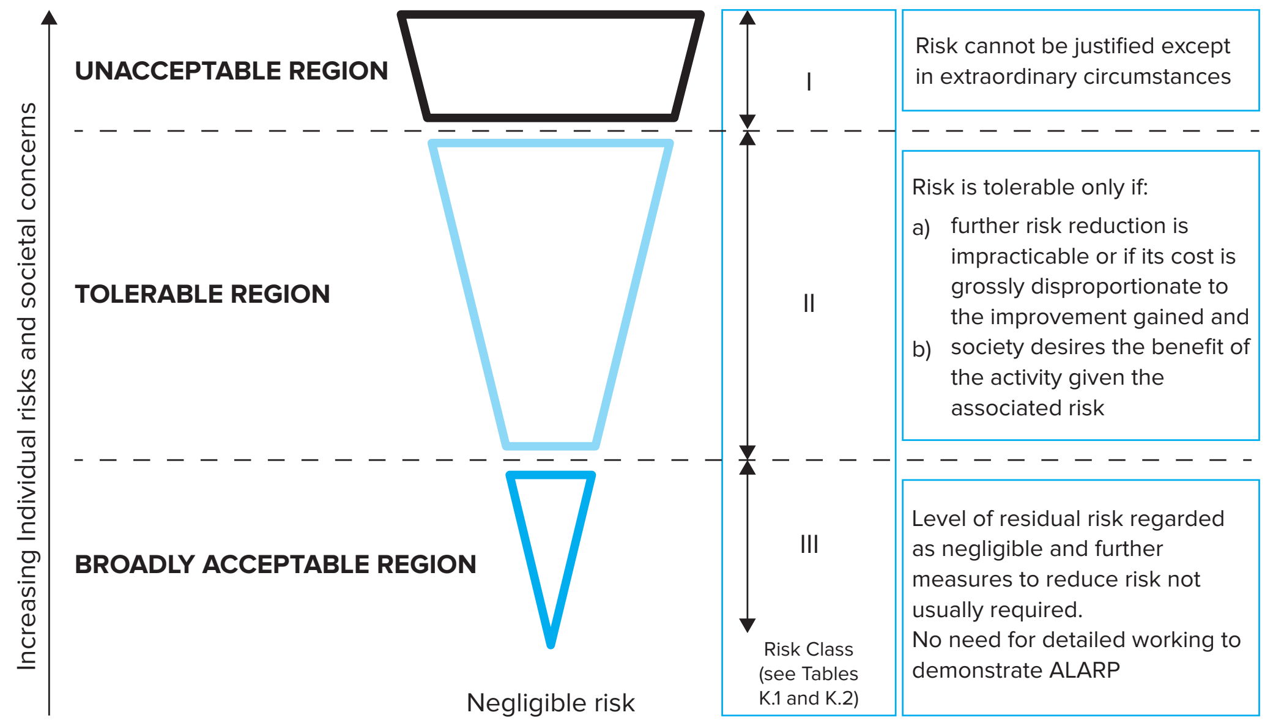
Functional Safety (FS) Management in IEC61511:2016 requires FS Assessments by a Senior independent & competent person NOT involved in the design for stage 1 - 2 & 3 and a periodic FS assessment by a Senior independent & competent person NOT involved in the operation and maintenance from the same SIS for stage 4 & 5. Furthermore, the modification phase 7 SHALL not begin before an independent FS assessment is carried out with the same conditions as for stage 5.

## RISK REDUCTION (IEC61511-3, ANNEX A)


Residual risk
Tolerable risk
Process risk
Necessary risk reduction
Increasing risk
Actual risk reduction
Partial risk covered by non-SIS protection layers
Partial risk covered by SIS
Partial risk covered by other protection layers
Risk reduction achieved by all protection layers

## TOLERABLE RISKS AND ALARP* (IEC61511-3 ANNEX K)

* As Low As Reasonably Practicable

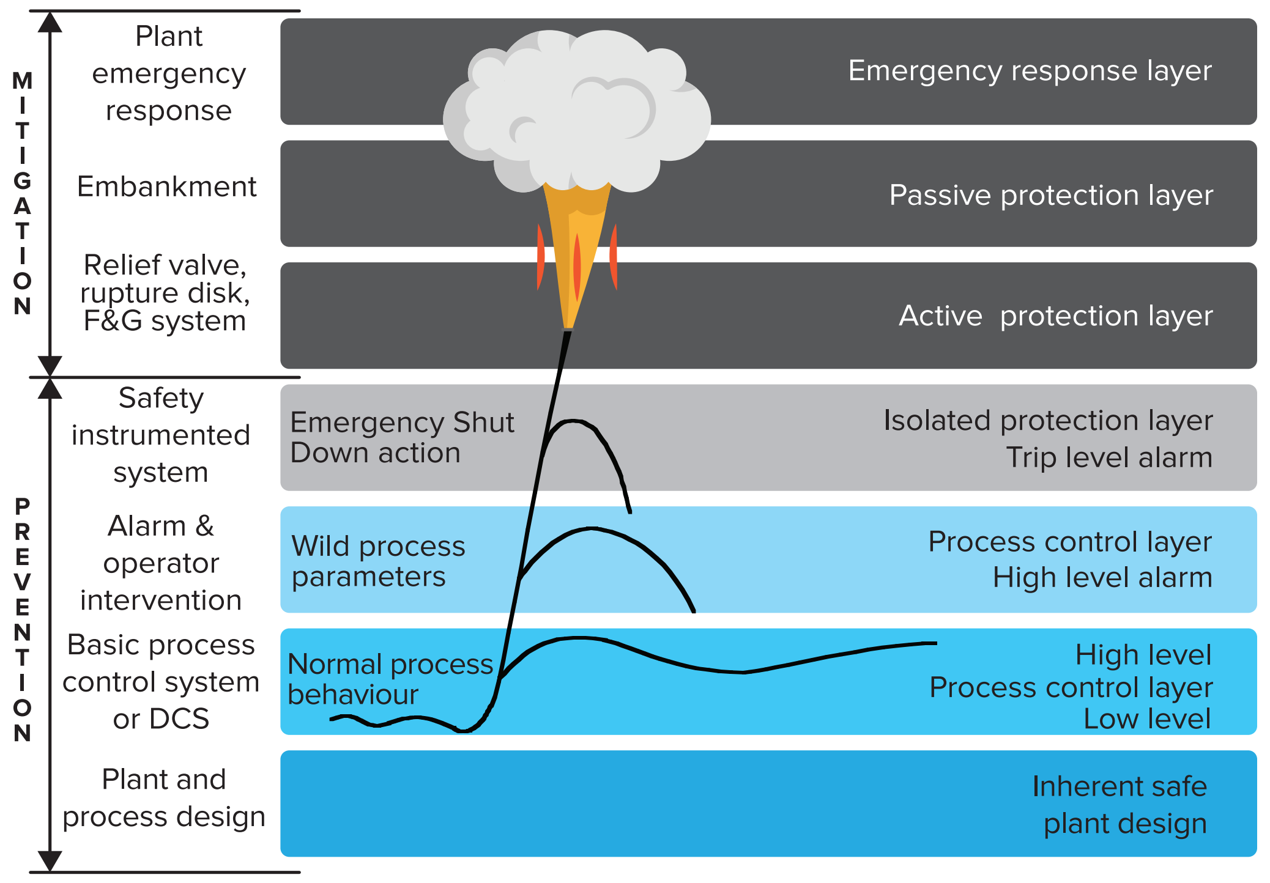

Increasing Individual risks and societal concerns
UNACCEPTABLE REGION
TOLERABLE REGION
BROADLY ACCEPTABLE REGION
Negligible risk
I
II
III
Risk Class (see Tables K.1 and K.2)

Risk cannot be justified except in extraordinary circumstances

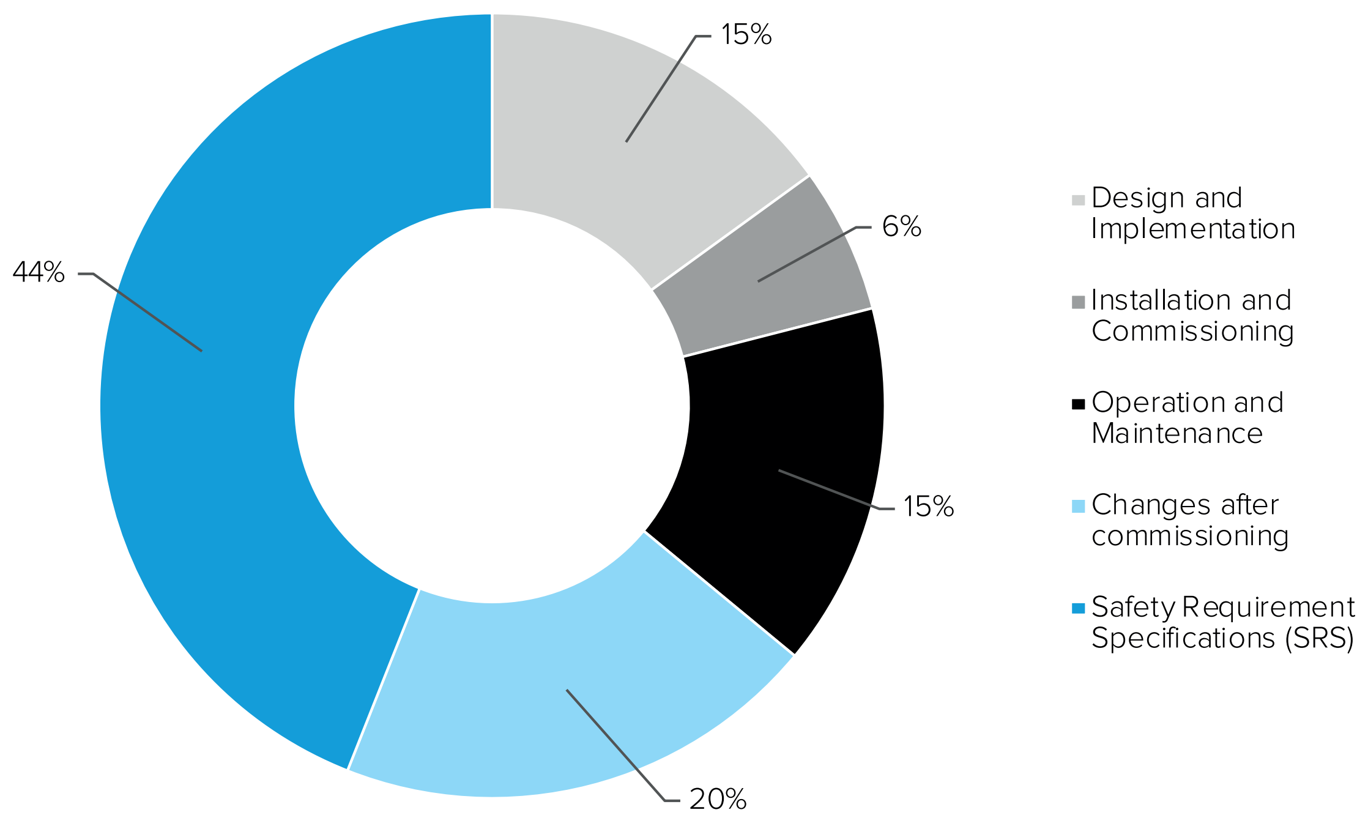
Risk is tolerable only if:
a) further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained and
b) society desires the benefit of the activity given the associated risk

Level of residual risk regarded as negligible and further measures to reduce risk not usually required.
No need for detailed working to demonstrate ALARP

## LAYERS OF PROTECTION



## PRIMARY CAUSE OF FAILURE BY PHASE

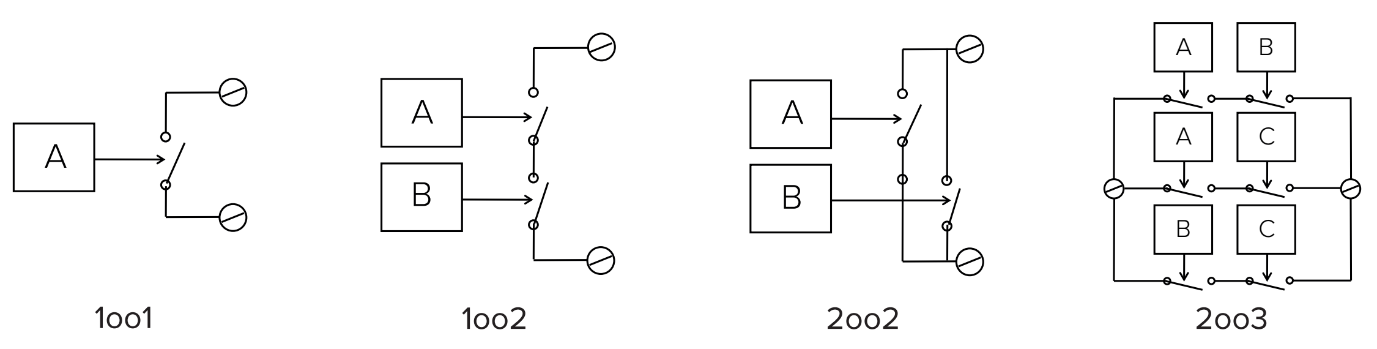


*Ref.: Out of control: Why control systems go wrong and how to prevent failure? (2nd edition, source: © Health & Safety Executive HSE – UK)*

## SIL LEVELS ACCORDING IEC 61508 / IEC 61511

| **SIL**<br>*Safety Integrity Level* | **PFDavg**<br>*Probability of dangerous Failure on Demand per year.*<br>Demand mode of operation (Low or High demand) | **RRF**<br>*Risk Reduction Factor* | **PFH**<br>*Probability of dangerous Failure per hour.*<br>Continuous mode or High demand mode |
|---|---|---|---|
| **SIL 4** | $\geq 10^{-5}$ and $< 10^{-4}$ | > 100000 to ≤ 10000 | $\geq 10^{-9}$ and $< 10^{-8}$ |
| **SIL 3** | $\geq 10^{-4}$ and $< 10^{-3}$ | > 10000 to ≤ 1000 | $\geq 10^{-8}$ and $< 10^{-7}$ |
| **SIL 2** | $\geq 10^{-3}$ and $< 10^{-2}$ | > 1000 to ≤ 100 | $\geq 10^{-7}$ and $< 10^{-6}$ |
| **SIL 1** | $\geq 10^{-2}$ and $< 10^{-1}$ | > 100 to ≤ 10 | $\geq 10^{-6}$ and $< 10^{-5}$ |

## SYSTEM ARCHITECTURES



*All contacts are considered in open (De-energize to trip) condition.*

## SAFE FAILURE FRACTION (IEC 61508-2 CLAUSE 7.4)

$$\text{SFF: } \frac{\sum\lambda_{DD}+\sum\lambda_{SD}+\sum\lambda_{SU}}{\sum\lambda_{DD}+\sum\lambda_{DU}+\sum\lambda_{SD}+\sum\lambda_{SU}} = 1 - \frac{\sum\lambda_{DU}}{\sum\lambda_{TOT}}$$

Failure rate categories: $\lambda_{DD}$: Dangerous Detected; $\lambda_{DU}$: Dangerous Undetected; $\lambda_{SD}$: Safe Detected; $\lambda_{SU}$: Safe Undetected.

### ROUTE 1 H

*(for further information see 61508-2 Clause 7.4.4.2)*

| | Hardware Fault Tolerance 0 | Hardware Fault Tolerance 1 | Hardware Fault Tolerance 2 |
|---|---|---|---|
| **TYPE A Components**<br>Simple devices with well-known failure modes and a solid history of operation | | | |
| < **60 %** | SIL 1 | SIL 2 | SIL 3 |
| **60 % - < 90 %** | SIL 2 | SIL 3 | SIL 4 |
| **90 % - < 99 %** | SIL 3 | SIL 4 | SIL 4 |
| > **99 %** | SIL 3 | SIL 4 | SIL 4 |
| **TYPE B Components**<br>Complex components with potentially unknown failure modes | | | |
| < **60 %** | Not allowed | SIL 1 | SIL 2 |
| **60 % - < 90 %** | SIL 1 | SIL 2 | SIL 3 |
| **90 % - < 99 %** | SIL 2 | SIL 3 | SIL 4 |
| > **99 %** | SIL 3 | SIL 4 | SIL 4 |

### ROUTE 2 H

*(for further information see 61508-2 Clause 7.4.4.3)*

| SIL | Mode of operations | Minimum Hardware Fault Tolerance |
|---|---|---|
| 1 | any mode | 0 |
| 2 | low demand mode | 0 |
| 2 | high demand or continuous mode | 1 |
| 3 | any mode | 1 |
| 4 | any mode | 2 |

## AVAILABILITY AND RELIABILITY

### BASIC CONCEPTS

$$\lambda = \frac{\text{Failures per unit time}}{\text{Components exposed to functional failure}}$$

$$1\ \text{FIT} = 1 \times 10^{-9}\ \text{Failures per hour}$$

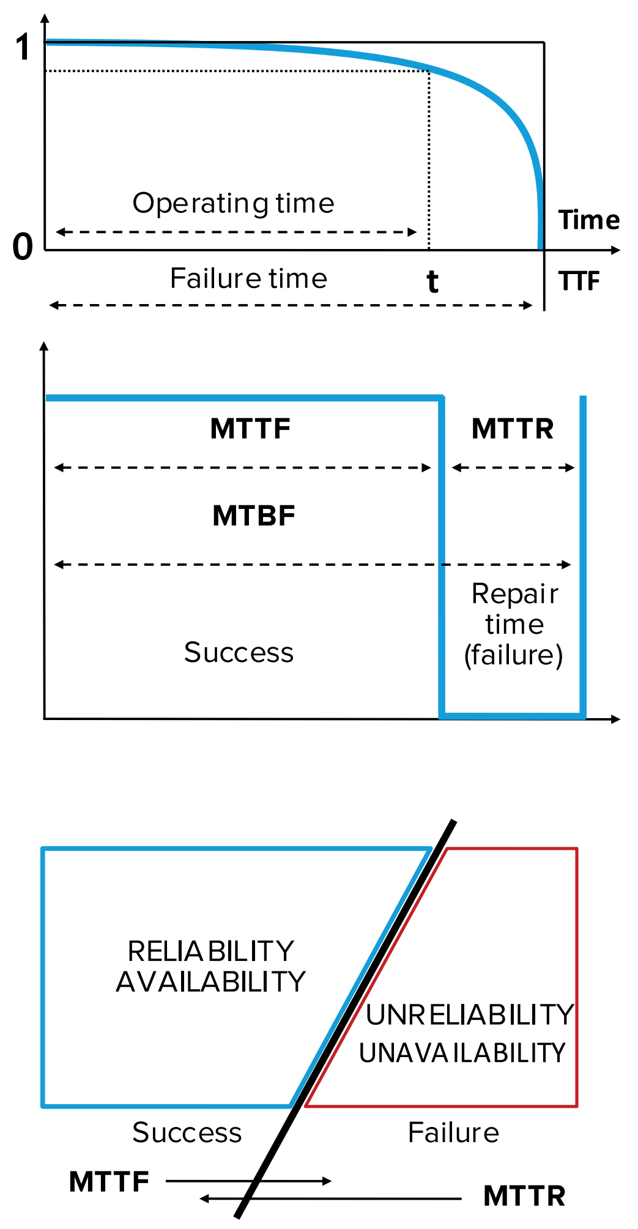
$$\text{MTBF} = \text{MTTF} + \text{MTTR}$$

$$\text{MTTF} = \text{MTBF} - \text{MTTR} = \frac{1}{\lambda} \qquad \mu = \frac{1}{\text{MTTR}} \qquad \lambda = \frac{1}{\text{MTTF}}$$

$$\text{Availability} = \frac{\text{Operating Time}}{\text{Operating Time} + \text{Repair Time}} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} = \frac{\text{MTTF}}{\text{MTBF}} = \frac{\mu}{\mu + \lambda} = \frac{\text{MTBM}}{\text{MTBM} + \text{MSD}}$$

$$\text{Unavailability} = 1 - \text{Availability} = \frac{\lambda}{\mu}$$

### RELIABILITY



**Acronyms**

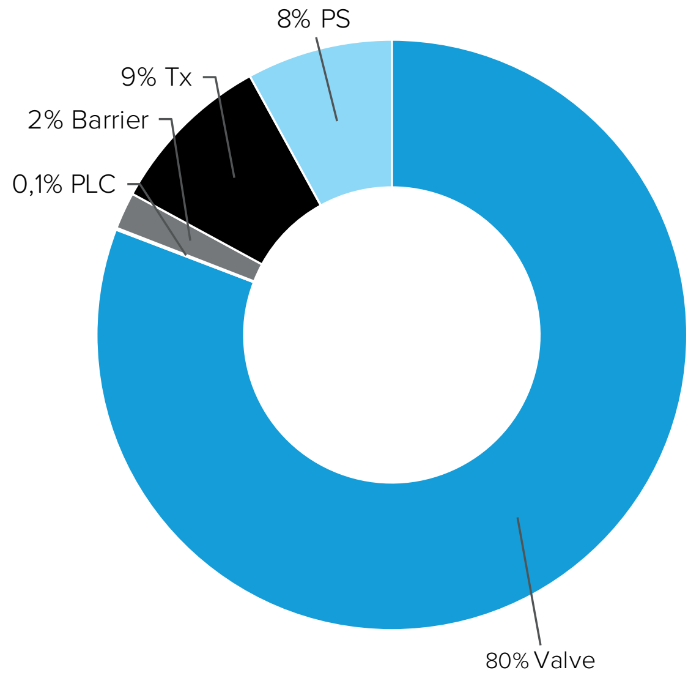
| | |
|---|---|
| MTBF | Mean Time Between Failures |
| MTTF | Mean Time To Failure |
| MTTR | Mean Time To Restoration |
| MTBM | Mean Time Between Maintenance |
| MSD | Expected Mean System Downtime |
| λ | Failure rate |
| μ | Repair rate |

## PRACTICAL APPLICATION EXAMPLE

Calculate MTBF, MTBFs, PFDavg, RRF, and possible SIL level of the following SIF, which includes a transmitter, a barrier, a safety PLC, and a valve as final element, in 1oo1 architecture.
T-proof test is carried out once a year with 100% effectiveness.

The pie chart on the right shows percentages of the single sub-systems on the total PFD of the Safety Function.

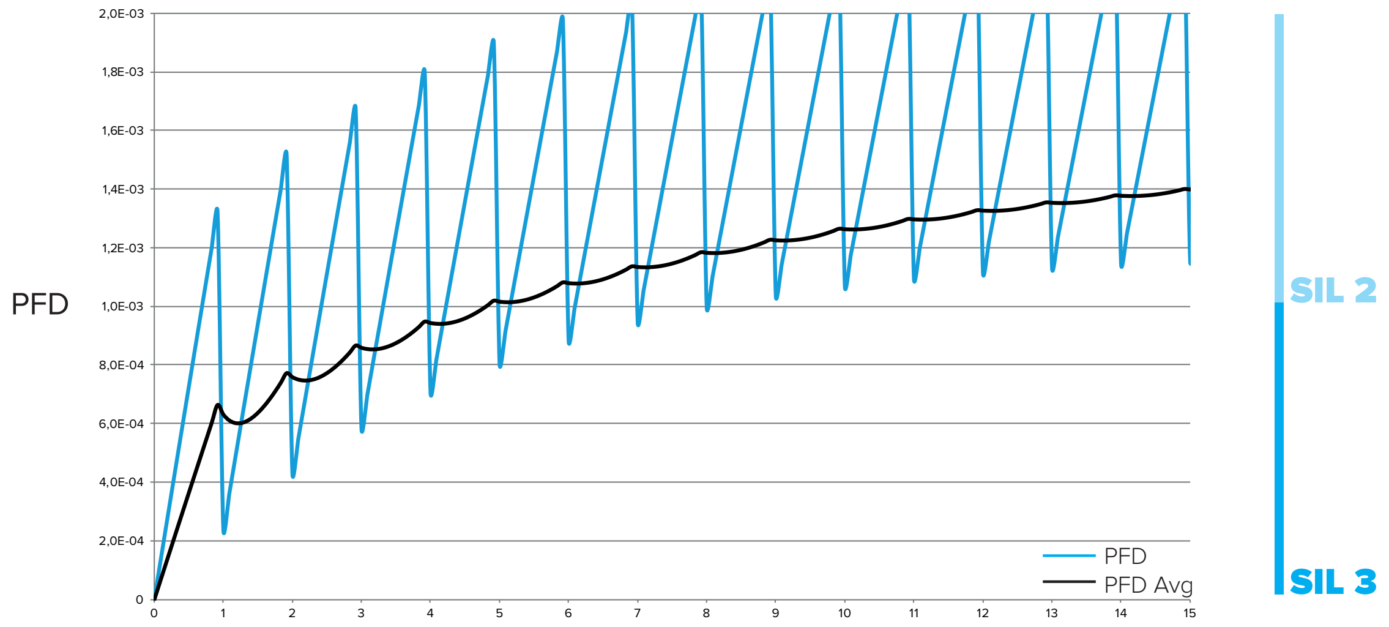
The table below contains failure data provided by the manufacturer of each sub-system.
Formulae to calculate requested values are indicated in the header.



| Sub-system | $\lambda_s$ per year | $\lambda_{DD}$ per year | $\lambda_{DU}$ per year | λ per year= 1/MTBF | MTBF (yrs) | MTBFs= $1/\lambda_s$ (yrs) | PFDavg 1oo1=$\lambda_{DU}/2$ | % of Total PFDavg | RRF= 1/PFDavg | SFF | SIL |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Tx | 0.00800 | 0.0010 | 0.00080 | 0.00980 | 102 | 125 | 0.000400 | 9 % | - | 91.8 % | 2 |
| Barrier | 0.00159 | 0.0014 | 0.00019 | 0.00318 | 314 | 629 | 0.000095 | 2 % | - | 94.0 % | 3 |
| PLC | 0.00135 | 0.0001 | 0.00001 | 0.00146 | 685 | 741 | 0.000005 | 0.1 % | - | 99.3 % | 3 |
| Valve | 0.01370 | 0.0066 | 0.00720 | 0.02750 | 36 | 73 | 0.003602 | 81 % | - | 73.8 % | 2 |
| Power Supply | 0.00530 | 0.0000 | 0.00070 | 0.00600 | 167 | 189 | 0.000350 | 7.9 % | - | 88.3 % | 3 |
| **Total (SIF)** | **0.02994** | **0.0091** | **0.00890** | **0.04794** | **21** | **33** | **0.004452** | **100 %** | **225** | **-** | **2** |

## PROOF TEST

The following graph shows an example of PFD and PFDavg variations in case T-proof test is carried out once a year with 80% effectiveness: SIL 3 level is maintained only for about 5 years; the SIF then downgrades to SIL 2.



When dealing with SIFs, safety engineers should pay special attention to the selection of sub-systems, the time interval between periodic proof test with achievable coverage factor and the system architecture. A wise choice of these three key elements is what it takes to achieve the required SIL level. For more details on any of the subjects in this poster, refer to “Safety Instrumented Systems” manual by GM International.

Information presented in this poster is for the general education of the reader. GM International does not have control over the use of the information by the readers therefore GM International disclaims any and all liability of any kind arising out of such use. Examples are provided as simple illustrations of the topics and, as such, are not intended as a guide to manage plant safety. The readers should use and apply only the guidance provided in the standards pertaining to their applications. The reproduction by any means, partial or total, of the poster and its content is prohibited without making a clear reference to the original source.

SIL

# Functional Safety Fundamentals

gmi
technology for safety