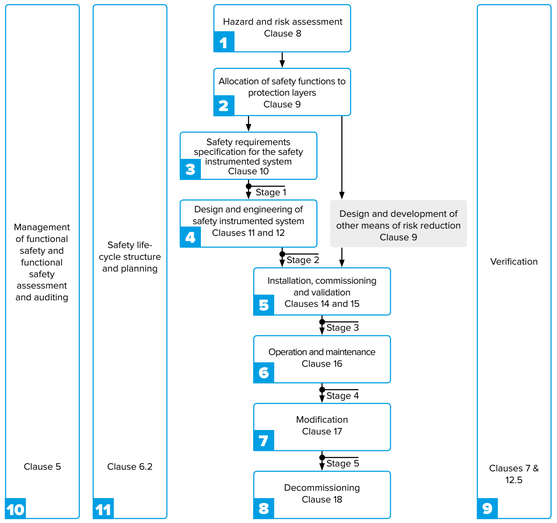
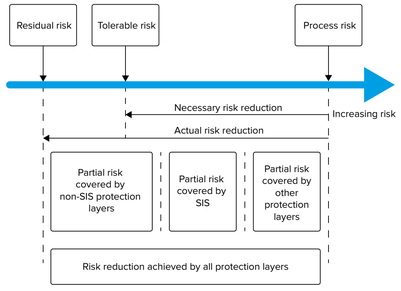
FUNCTIONAL SAFETY FUNDAMENTALS

LIFECYCLE IEC61511



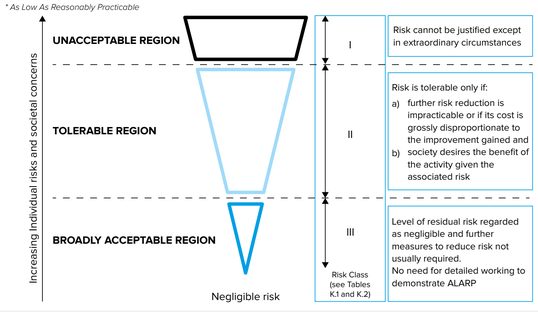
Functional Safety (FS) Management in IEC61511:2016 requires FS Assessments by a Senior independent & competent person NOT involved in the design for stage 1 - 2 & 3 and a periodic FS assessment by a Senior independent & competent person NOT involved in the operation and maintenance from the same SIS 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)

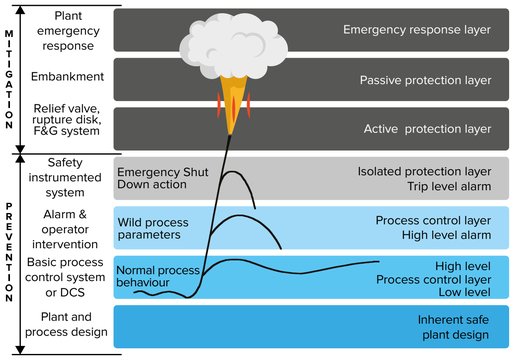


TOLERABLE RISKS AND ALARP* (IEC61511-3 ANNEX K)

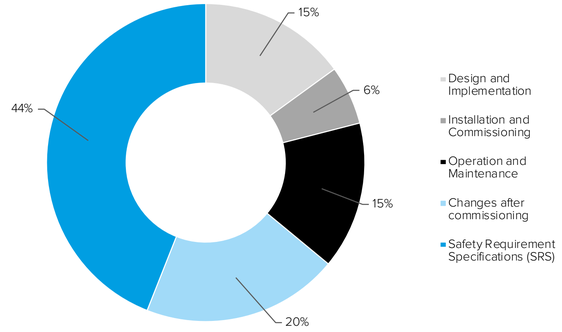
** As Low As Reasonably Practicable*



LAYERS OF PROTECTION



PRIMARY CAUSE OF FAILURE BY PHASE

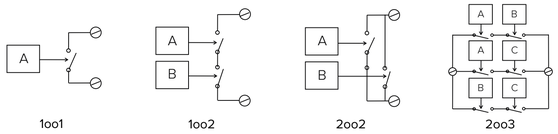


Ref: Out of control: Why control systems go wrong and how to prevent failure? (2nd edition, source: © Health & Safety Executive HSE – UK)

SIL LEVELS ACCORDING IEC 61508 / IEC 61511

SIL *Safety Integrity Level*	PFDavg *Probability of dangerous Failure on Demand per year.* Demand mode of operation (Low or High demand)	RRF *Risk Reduction Factor*	PFH *Probability of dangerous Failure per hour.* 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)

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

Failure rate categories: λ_{DD}: Dangerous Detected; λ_{DU}: Dangerous Undetected; λ_{SD}: Safe Detected; λ_{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 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 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

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

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

$$MTBF = MTTF + MTTR$$

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

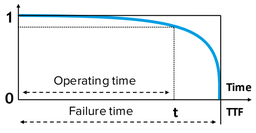
$$Availability = \frac{Operating\ Time}{Operating\ Time + Repair\ Time} = \frac{MTTF}{MTTF + MTTR} = \frac{MTTF}{MTBF} = \frac{\mu}{\mu + \lambda} = \frac{MTBM}{MTBM + MSD}$$

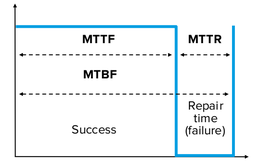
$$Unavailability = 1 - Availability = \frac{\lambda}{\mu}$$

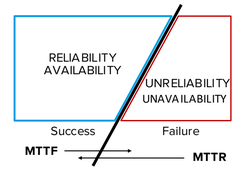
Acronyms

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

RELIABILITY





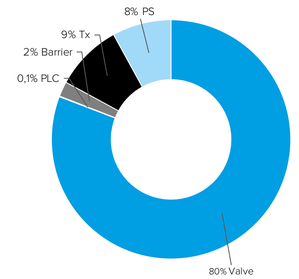


PRACTICAL APPLICATION EXAMPLE

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.

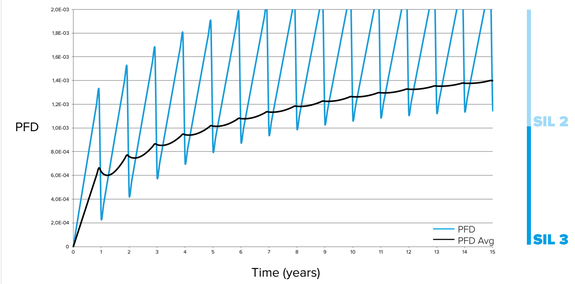
The table below contains failure data provided by the manufacturer of each sub-system.
Formulae to calculate requested values are indicated in the header.



Sub-system	λ_S per year	λ_{DD} per year	λ_{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.