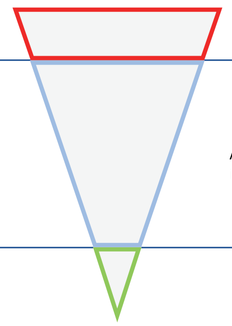
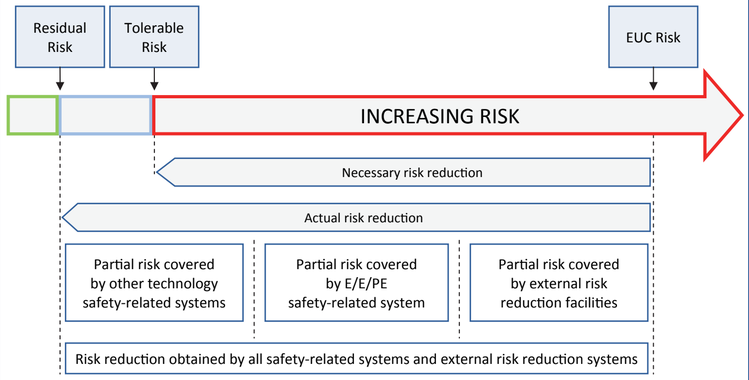
IEC 61508 — UNDERSTANDING SAFETY INTEGRITY LEVELS — IEC 61511

TOLERABLE RISKS AND ALARP (IEC 61508-5 ANNEX 'C')

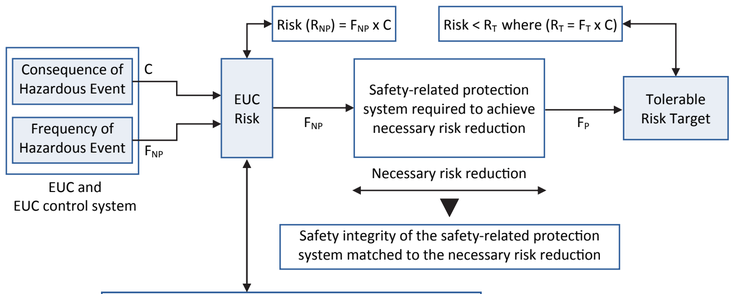


Intolerable Region	Risk cannot be justified except in extraordinary circumstances.
The ALARP or tolerability region (Risk is undertaken only if a benefit is desired)	Tolerable only if further risk reduction is impracticable or if its costs are grossly disproportional to the gained improvement. As the risk is reduced, the less proportionately, it is necessary to spend to reduce it further, to satisfy ALARP. The concept of diminishing proportion is shown by the triangle.
Broadly Acceptable Region (No need for detailed working to demonstrate ALARP)	It is necessary to maintain assurance that risk remains at this level.
RISK IS NEGLIGIBLE	

RISK REDUCTION (IEC 61508-5 ANNEX 'A')



SAFETY INTEGRITY LEVEL CALCULATION (IEC 61508-5 ANNEX 'D')



	Consequences			
Frequency	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

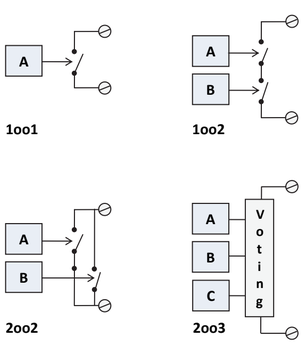
Table C.1 - Example of risk classification of accidents

1) Determine frequency (F_{NP}) and consequences (C) of hazardous event without protection.
2) Determine risk class using Table C.1.
3) Apply protections if Class = I.
4) Achieve tolerable risk target.

MEAN TIME TO SPURIOUS FAILURE

MTTFs	
1oo1	$\frac{1}{\lambda_S}$
1oo2	$\frac{1}{2\lambda_S}$
2oo2	$\frac{1}{2\lambda_S^2 \times MTTR}$
2oo3	$\frac{1}{6\lambda_S^2 \times MTTR}$

SYSTEM ARCHITECTURES



G.M. INTERNATIONAL S.R.L
Via San Fiorano, 70
20852 Villasanta (MB) - ITALY
phone: +39 039 2325038
info@gmintsrl.com
www.gmintsrl.com

SIL LEVELS ACCORDING IEC 61508 / IEC 61511

SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand mode)	RRF Risk Reduction Factor	PFDavg Average probability of failure on demand per hour (high demand or continuous mode)
SIL 4	**≥ 10^{-5} and < 10^{-4}**	**100000 to 10000**	**≥ 10^{-9} and < 10^{-8}**
SIL 3	**≥ 10^{-4} and < 10^{-3}**	**10000 to 1000**	**≥ 10^{-8} and < 10^{-7}**
SIL 2	**≥ 10^{-3} and < 10^{-2}**	**1000 to 100**	**≥ 10^{-7} and < 10^{-6}**
SIL 1	**≥ 10^{-2} and < 10^{-1}**	**100 to 10**	**≥ 10^{-6} and < 10^{-5}**

AVERAGE PROBABILITY OF FAILURE ON DEMAND

$$\frac{\text{Tolerable accident frequency}}{\text{Frequency of accidents without protections}} = \frac{1}{RRF}$$

Simplified equations

PFDavg	Without common causes	With common causes (Beta factor)
1oo1	$\lambda_{DU} \times \frac{TI}{2}$	-
1oo2 1oo2D	$\lambda_{DU_1} \times \lambda_{DU_2} \times \frac{TI^2}{3}$	$\frac{[(1-\beta)\times(\lambda_{DU}\times TI)]^2}{3} + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
1oo3	$\lambda_{DU_1} \times \lambda_{DU_2} \times \lambda_{DU_3} \times \frac{TI^3}{4}$	$\frac{[(1-\beta)\times(\lambda_{DU}\times TI)]^3}{4} + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
2oo2	$(\lambda_{DU_1} + \lambda_{DU_2}) \times \frac{TI}{2}$	$[(1-\beta)\times(\lambda_{DU}\times TI)] + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
2oo3	$[(\lambda_{DU_1}\times\lambda_{DU_2}) + (\lambda_{DU_1}\times\lambda_{DU_3}) + (\lambda_{DU_2}\times\lambda_{DU_3})] \times \frac{TI^2}{3}$	$[(1-\beta)\times(\lambda_{DU}\times TI)]^2 + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
1oo1 (Et ≠ 100%)	$\lambda_{DU}\left[\left(Et\times\frac{TI}{2}\right) + (1-Et)\frac{SL}{2}\right]$	TI: Proof Test Time Interval Et: Test Effectiveness λ_{DU}: Dangerous Undetected Failures

SAFE FAILURE FRACTION (IEC 61508-2 CLAUSE 7.4)

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

	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	SIL3
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	SIL2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
> 99 %	SIL 3	SIL 4	SIL 4

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

AVAILABILITY AND RELIABILITY

Basic Concepts:

Failure Rate:

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

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

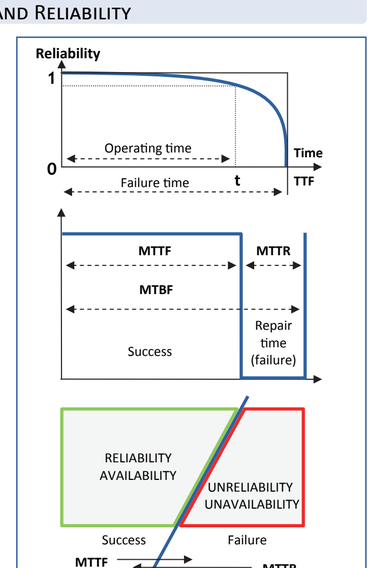
$$MTBF = MTTF + MTTR$$

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

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

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

Acronyms:
MTBF: Mean Time Between Failures
MTTF: Mean Time To Failure
MTTR: Mean Time To Repair
MTBM: Mean Time Between Maintenance
MSD: Expected Mean System Downtime
λ: Failure rate
μ: Repair rate

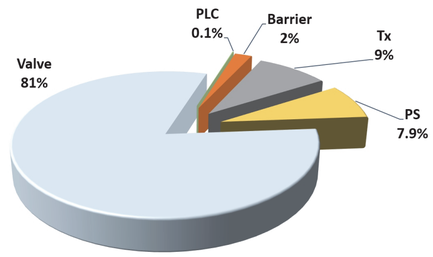


A PRACTICAL APPLICATION

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

INFLUENCE OF PERIODIC TEST DURATION AND EFFECTIVENESS ON PFDAVG (1OO1)

MANUAL PERIODIC TEST DURATION

The duration of a manual proof test can have a significant impact on the overall SIS performance.
In 1oo1 architectures, during the test, the system must be taken offline, and its availability is zero.
The original simplified formula is modified into:

$$PFDavg = \lambda_{DU} \times \frac{TI}{2} + \frac{TD}{TI}$$

where TI is the proof test interval and TD the test duration.

Note: The average probability of failure is strictly related to test interval (TI); increasing time between tests directly leads to higher probability of failures and therefore lower SIL levels.

Example:
λ_{DU}= 0.002 / yr; TI = 1 yr (= 8760 hrs); TD = 8 hrs
We obtain: PFDavg = 0.001 + 0.0009 = 0.0019; RRF = 1/0.0019 = 526 (suitable for SIL 2 level)

MANUAL PERIODIC TEST EFFECTIVENESS

The effectiveness of a periodic proof test indicates the percentage of dangerous failures detected by the test.
If effectiveness is lower than 100%, the proof test does not bring the probability of failure of the system back to zero ("as new"), therefore PFDavg progressively increases in time.
In this case the system not always maintains the original SIL level throughout its lifetime.
The formula for calculating PFDavg when effectiveness is lower than 100% is:

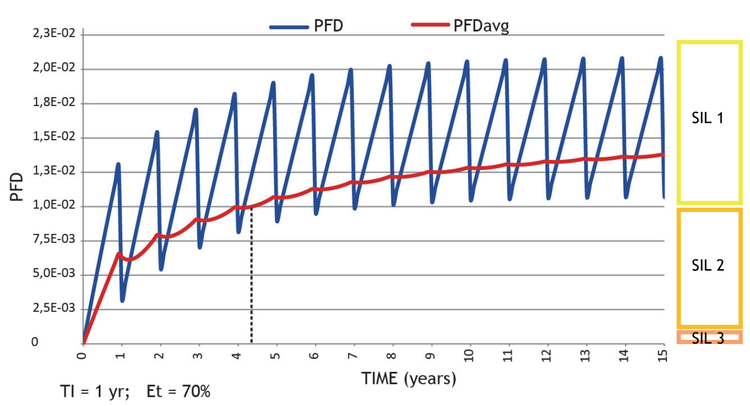
$$PFDavg = (Et \times \lambda_{DU} \times \frac{TI}{2}) + [(1 - Et) \times \lambda_{DU} \times \frac{SL}{2}]$$

where:
Et: periodic test effectiveness to reveal dangerous failures (e.g. 90%)
SL: system lifetime. It is equal to the time until the system is completely tested (100%) or replaced. If this never happens, SL is equal to the lifetime of the whole plant.

The complete formula for calculating PFDavg taking **both influences** into account is:

$$PFDavg = (Et \times \frac{\lambda_{DU}}{2}) + \frac{TD}{TI} + [(1 - Et) \times \lambda_{DU} \times \frac{SL}{2}]$$

The following graph shows an example of PFD and PFDavg variations in case T-proof test is carried out once a year with 70% effectiveness: SIL 2 level is maintained only for about 4 years; the SIF then downgrades to SIL 1.



TI = 1 yr; Et = 70%

When dealing with SIFs, safety engineers should pay special attention to the selection of sub-systems, the time interval between periodic tests 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 G.M. International.

FOR SAFETY TECHNOLOGY