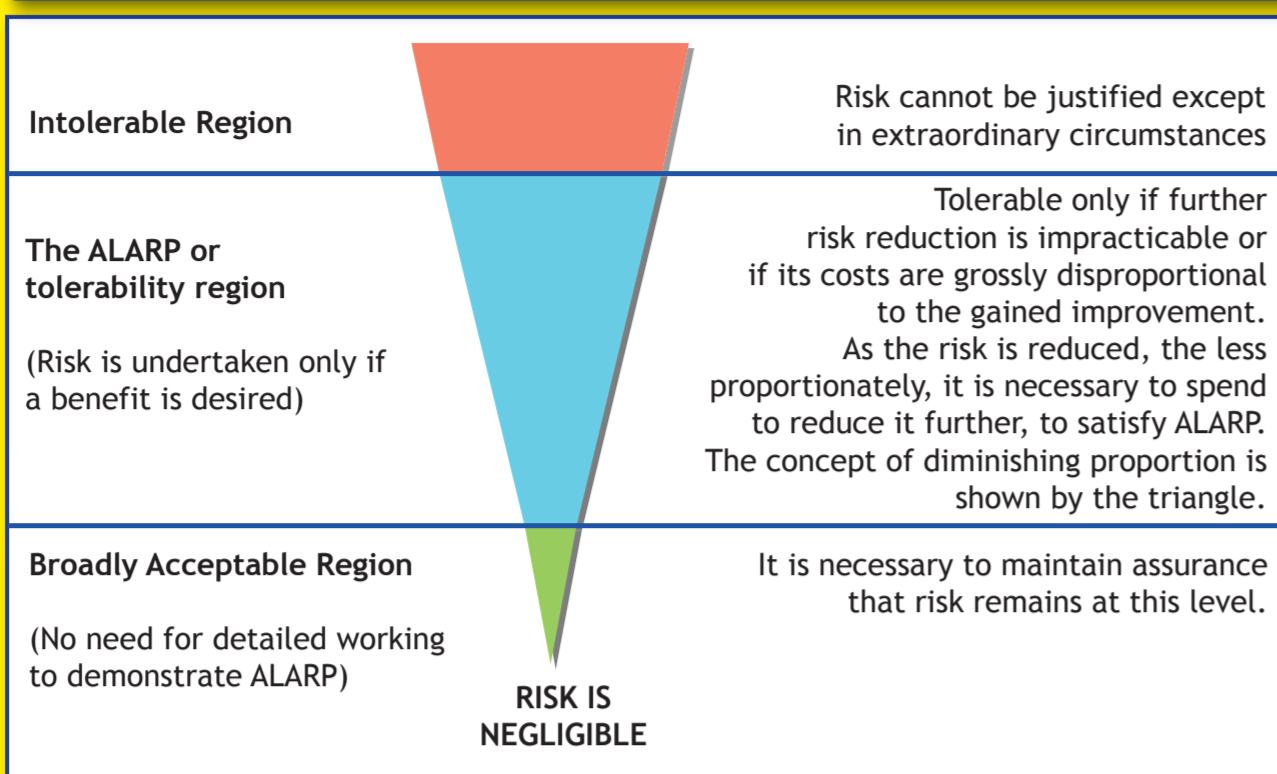
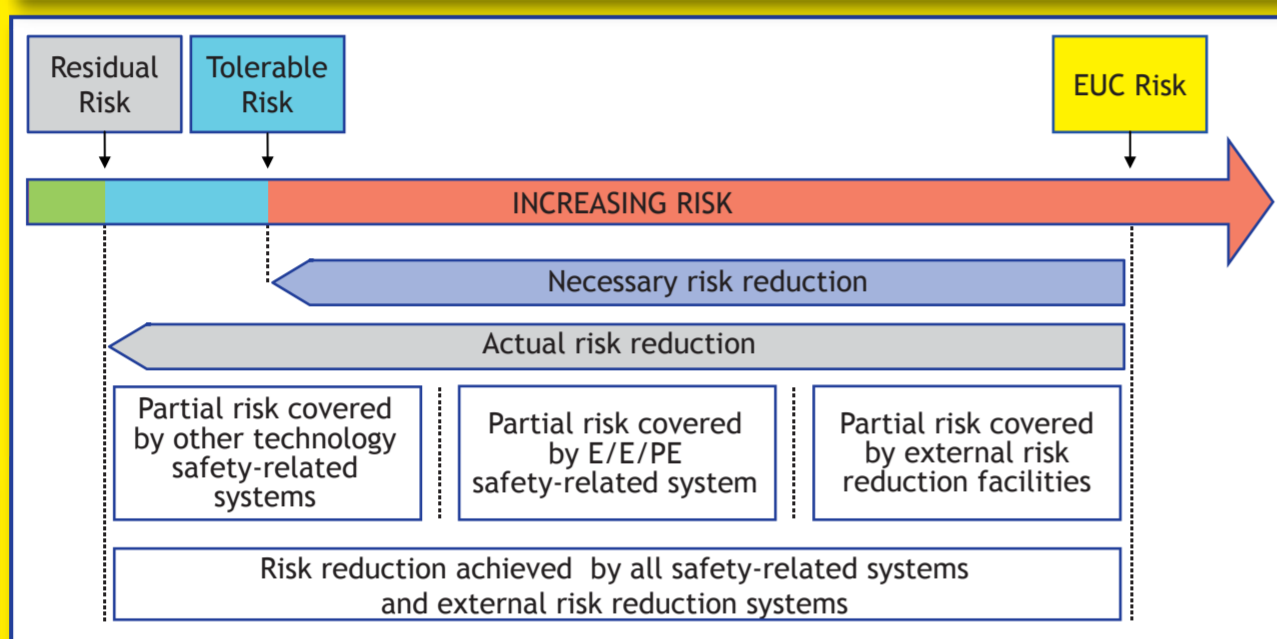


SAFETY: FREEDOM FROM UNACCEPTABLE RISK

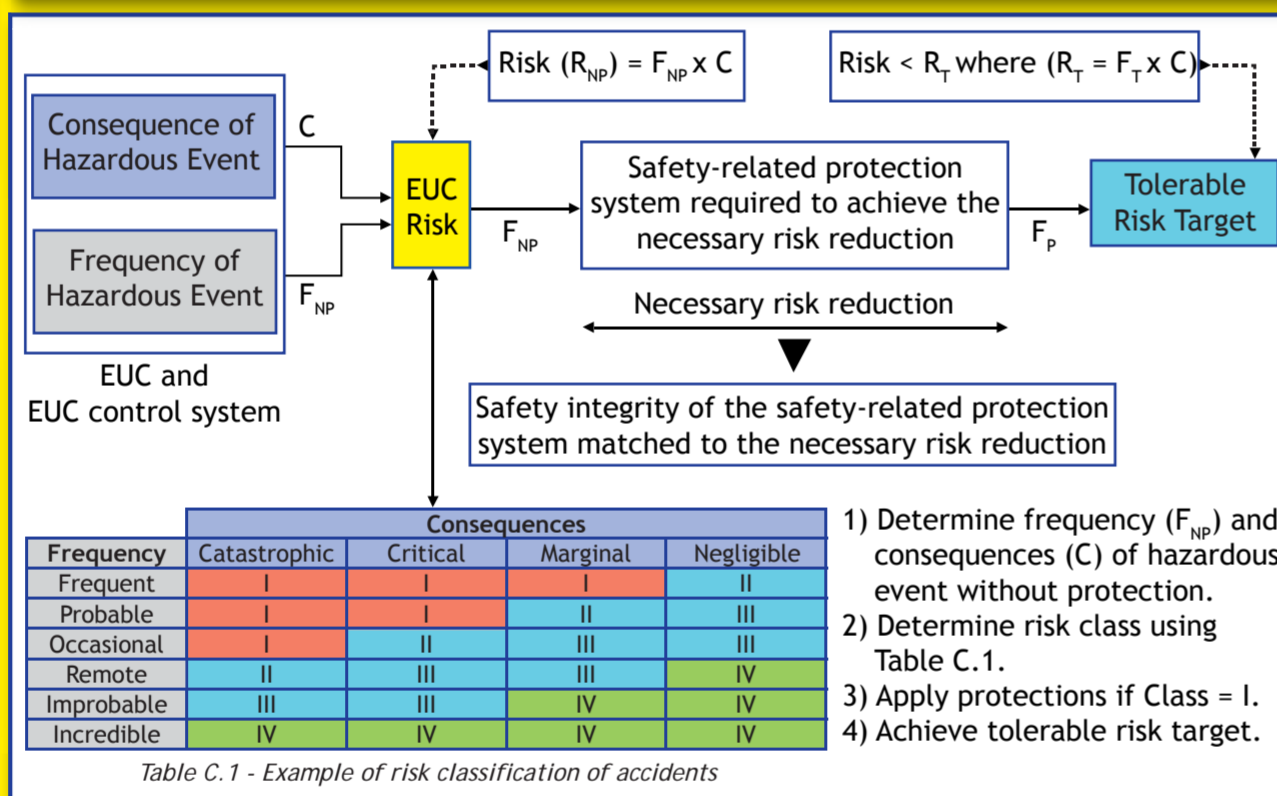
TOLERABLE RISKS AND ALARP (IEC 61508-5 Annex 'C')



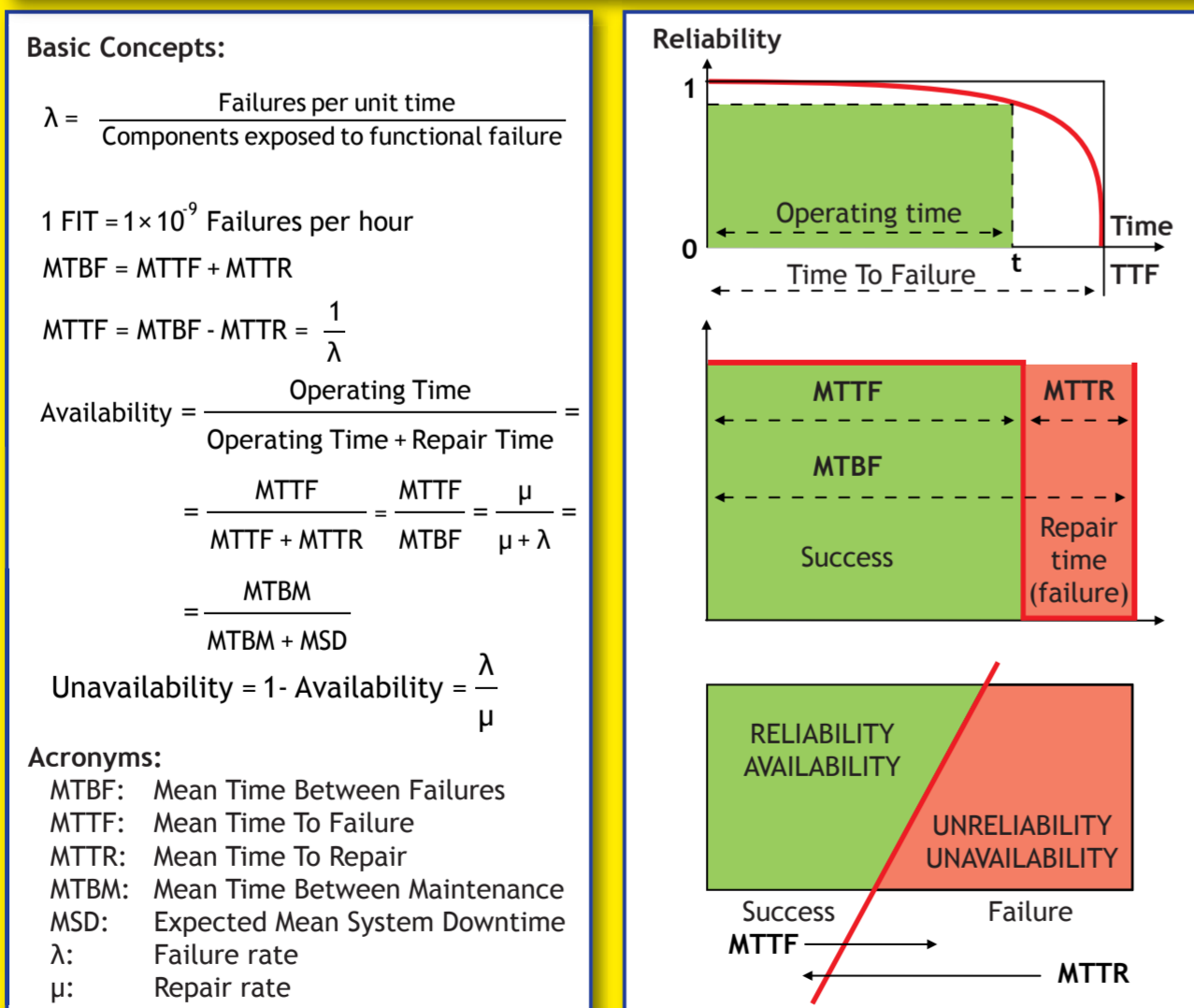
RISK REDUCTION (IEC 61508-5 Annex 'A')



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



AVAILABILITY AND RELIABILITY



SIL LEVELS ACCORDING IEC 61508 / IEC 61511

SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand)	RRF Risk Reduction Factor	PFDavg Average probability of failure on demand per hour (high demand)
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 $< 10^{-5}$

AVERAGE PROBABILITY OF FAILURE ON DEMAND

PFDavg = $\frac{\text{Tolerable accident frequency (F}_T\text{)}}{\text{Frequency of accidents without protection (F}_{np}\text{)}} = \frac{1}{\text{RRF}}$

	Without common causes	With common causes (Beta factor)
1001	$\lambda_{DU} \times \frac{TI}{2}$	not applicable
1002 1002D	$\lambda_{DU1} \times \lambda_{DU2} \times \frac{TI^2}{3}$	$\frac{[(1-B) \times (\lambda_{DU} \times TI)]^2}{3} + \frac{(B \times \lambda_{DU} \times TI)}{2}$
1003	$\lambda_{DU1} \times \lambda_{DU2} \times \lambda_{DU3} \times \frac{TI^3}{4}$	$\frac{[(1-B) \times (\lambda_{DU} \times TI)]^3}{4} + \frac{(B \times \lambda_{DU} \times TI)}{2}$
2002	$(\lambda_{DU1} + \lambda_{DU2}) \times \frac{TI}{2}$	$[(1-B) \times (\lambda_{DU} \times TI)] + \frac{(B \times \lambda_{DU} \times TI)}{2}$
2003	$\left[\frac{(\lambda_{DU1} \times \lambda_{DU2}) + (\lambda_{DU1} \times \lambda_{DU3})}{(\lambda_{DU2} \times \lambda_{DU3})} \right] \times \frac{TI^2}{3}$	$[(1-B) \times (\lambda_{DU} \times TI)]^2 + \frac{(B \times \lambda_{DU} \times TI)}{2}$
1001 (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	Hardware Fault Tolerance	Hardware Fault Tolerance
	0	1	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

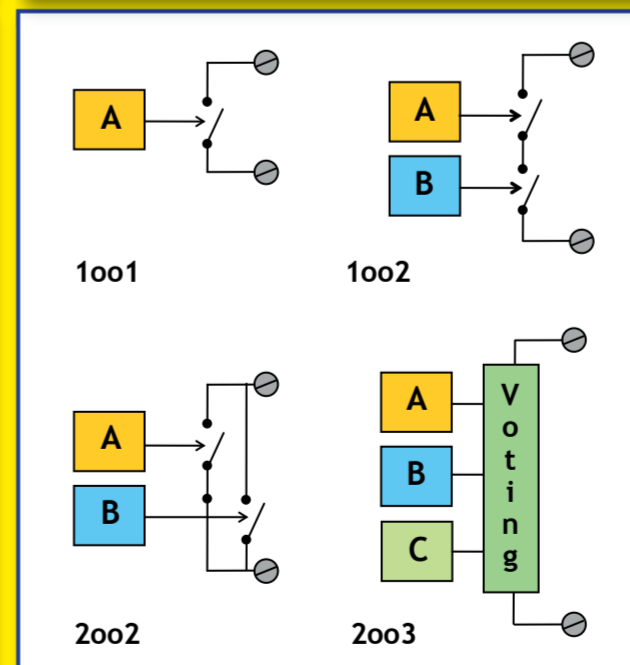
Failure rates categories: λ_{DD} : Dangerous Detected; λ_{DU} : Dangerous Undetected
 λ_{SD} : Safe Detected; λ_{SU} : Safe Undetected

MEAN TIME TO SPURIOUS FAILURE

MTTFs

1001	$\frac{1}{\lambda_S}$
1002	$\frac{1}{2\lambda_S}$
2002	$\frac{1}{2\lambda_S^2 \times \text{MTTR}}$
2003	$\frac{1}{6\lambda_S^2 \times \text{MTTR}}$

SYSTEM ARCHITECTURES

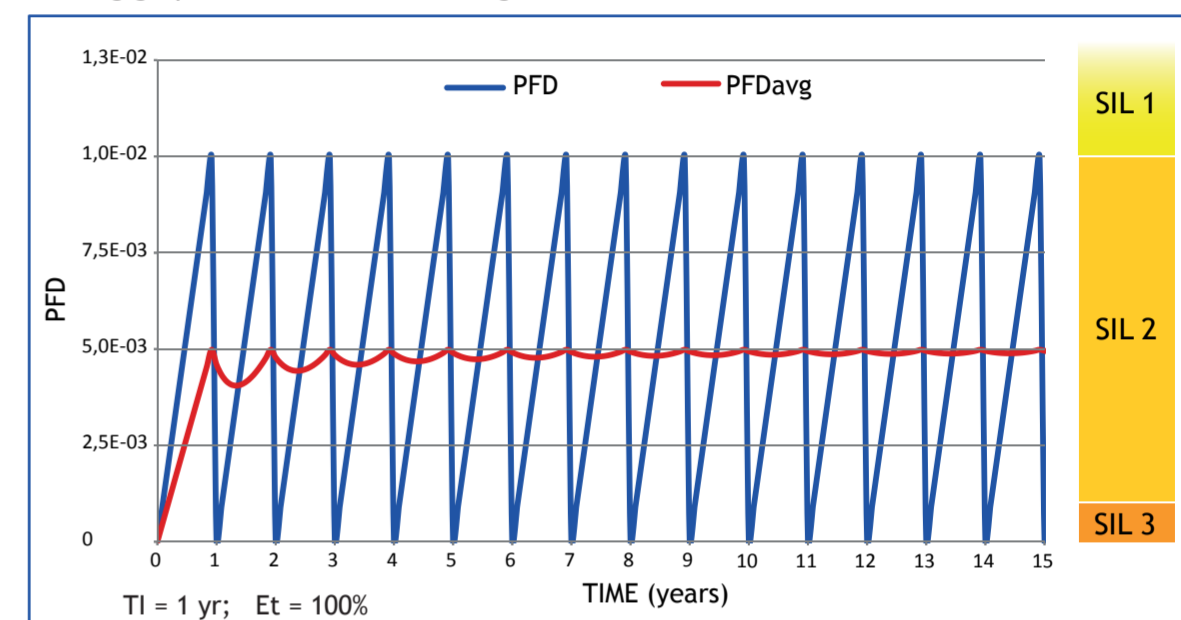


A PRACTICAL APPLICATION

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 1001 architecture. T-proof test is carried out once a year with 100% effectiveness. 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	MTBF = 1/λ (yrs)	λ = 1/MTBF (per year)	MTBFs = 1/λ _s (yrs)	λ _s per year	λ _{DO} per year	λ _{DU} per year	PFDavg 1001 = λ _{DU} /2	% of total PFDavg	RRF = 1/PFDavg	SFF	SIL Level
Tx	102	0.00980	125	0.00800	0.0010	0.00080	0.000400	8 %	2500	91.8 %	SIL 2
Barrier	314	0.00318	629	0.00159	0.0014	0.00019	0.000095	1.9 %	10526	94.0 %	SIL 3
PLC	685	0.00146	741	0.00135	0.0001	0.00001	0.000005	0.1 %	200000	99.3 %	SIL 3
Valve	30	0.03330	60	0.01660	0.0083	0.00830	0.004100	83 %	244	73.8 %	SIL 2
Power Supply	167	0.00600	189	0.00530	0.0000	0.00070	0.000350	7 %	2857	88.3 %	SIL 3
Total (SIF)	18.8	0.053	40.8	0.0245	0.019	0.01	0.005	100 %	200	-	SIL 2

The following graph shows PFD and PFDavg variations in time:



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.

INFLUENCE OF PERIODIC TEST DURATION AND EFFECTIVENESS ON PFDavg (1001)

MANUAL PERIODIC TEST DURATION

The duration of a manual proof test can have a significant impact on the overall SIS performance. In 1001 architectures, during the test, the system must be taken offline, and its availability is zero. The original simplified formula is modified into:

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

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

Example:
 $\lambda_{DU} = 0.002$ / 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 increases progressively 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:

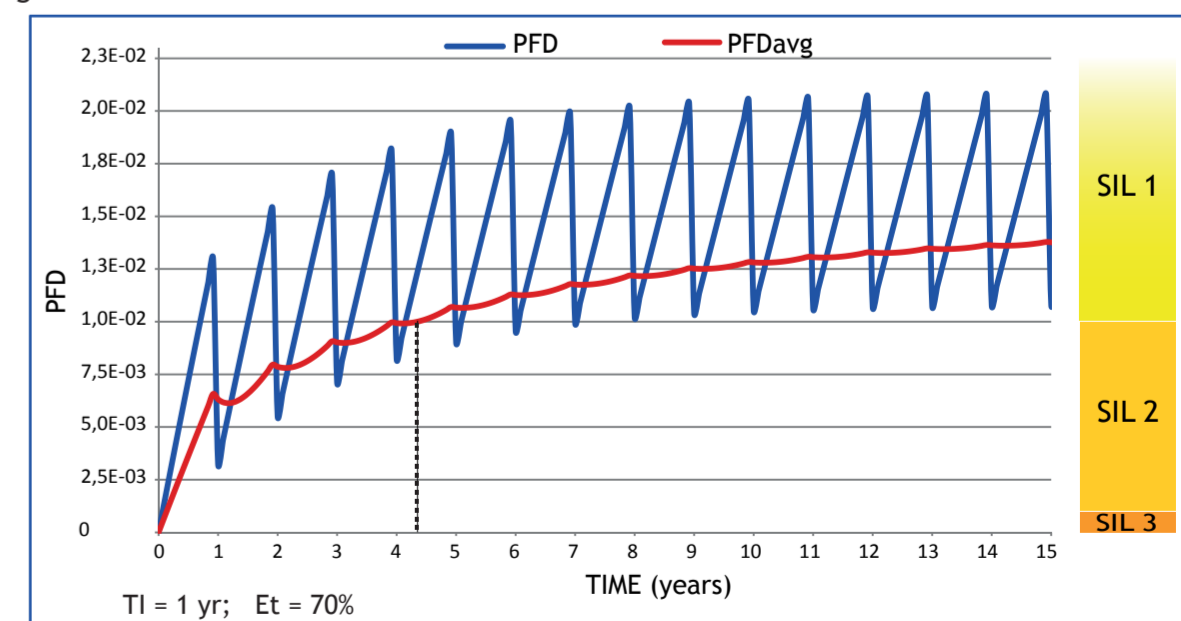
$$\text{PFDavg} = (Et \times \lambda_{DU} \times \frac{TI}{2}) + [(1-Et) \times \lambda_{DU} \times \frac{SL}{2}]$$

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:

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

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.



When dealing with SIFs, safety engineers should pay special attention to the selection of the 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.