IEC 61508

UNDERSTANDING SAFETY INTEGRITY LEVELS

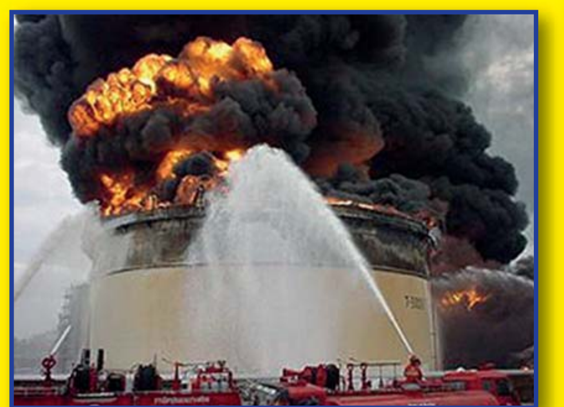
IEC 61511

SAFETY: FREEDOM FROM UNACCEPTABLE RISK

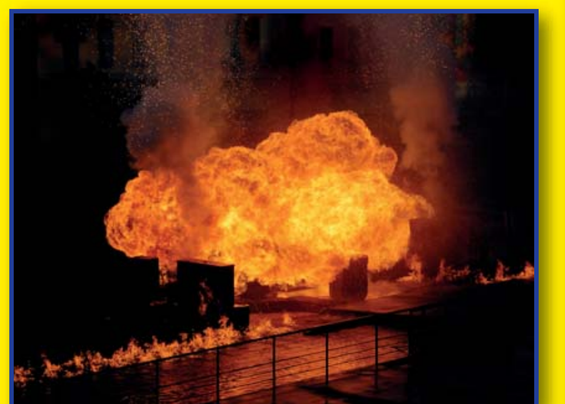
Boiling Liquid Expanding Vapor Explosion (BLEVE)

Flash Fire

Jet Fire

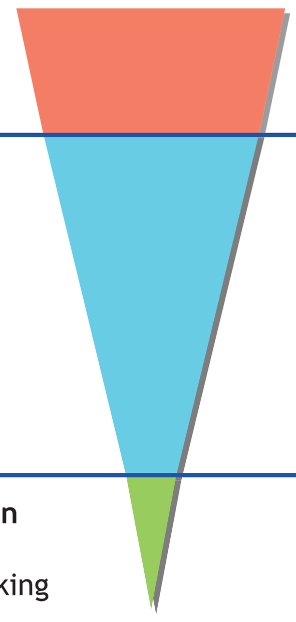


Pool Fire



Fireball

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.

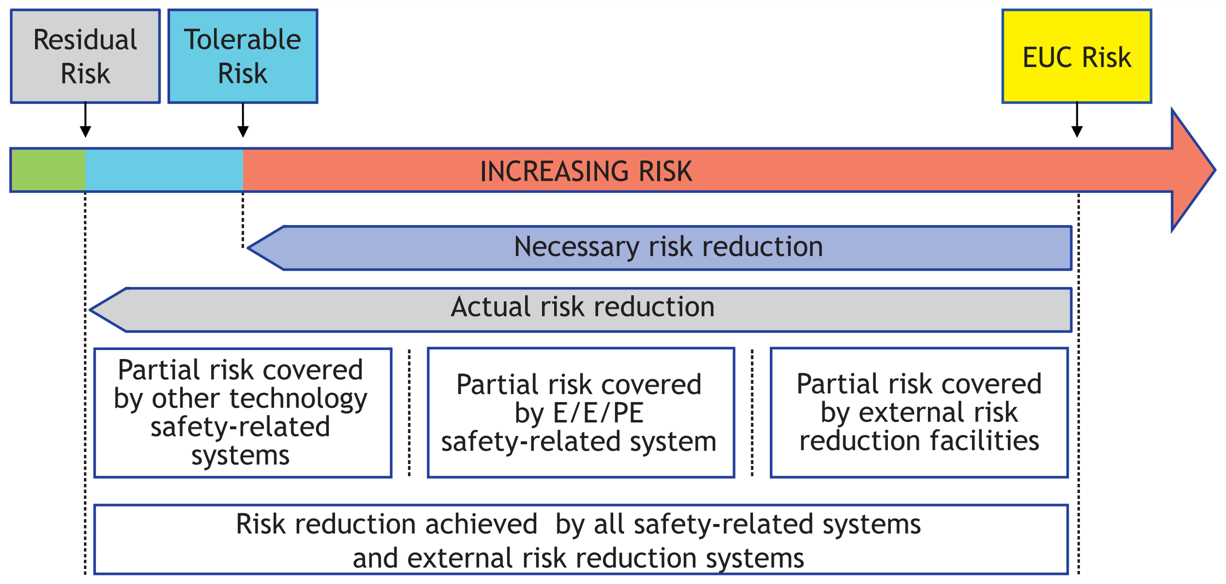
Broadly Acceptable Region

(No need for detailed working to demonstrate ALARP)

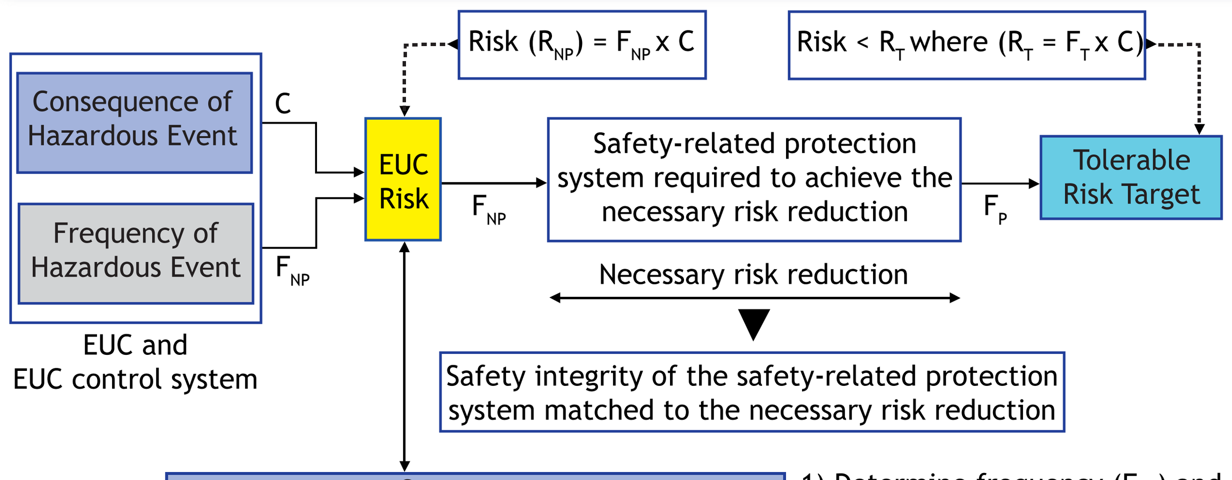
It is necessary to maintain assurance that risk remains at this level.

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.

AVAILABILITY AND RELIABILITY

Basic Concepts:

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

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

$$MTBF = MTTF + MTTR$$

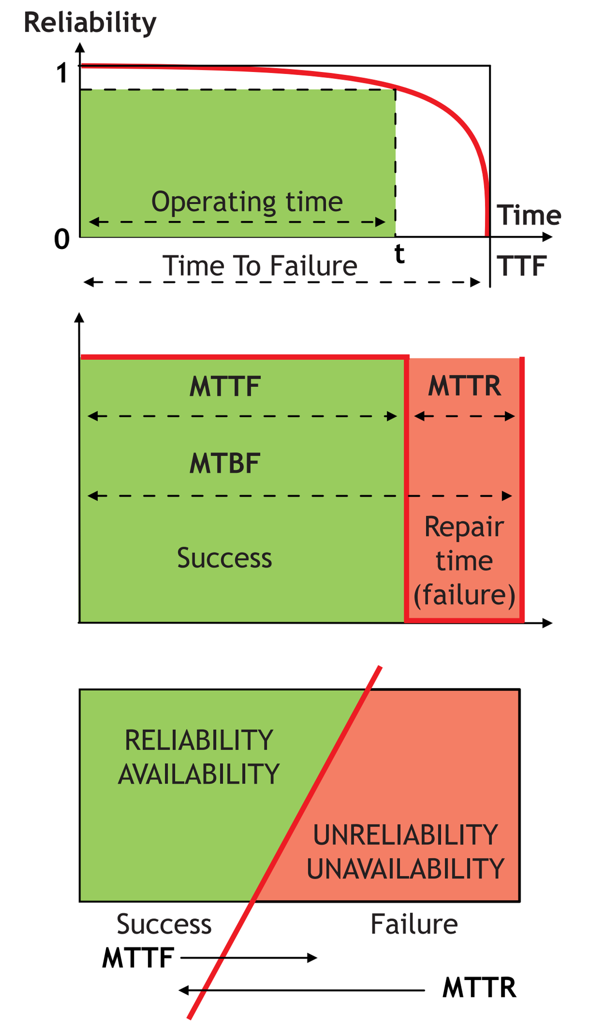
$$MTTF = MTBF - MTTR = \frac{1}{\lambda}$$

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

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

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



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

$$\text{PFDavg} = \frac{\text{Tolerable accident frequency } (F_T)}{\text{Frequency of accidents without protection } (F_{NP})} = \frac{1}{RRF}$$

	Simplified equations: Without common causes	Simplified equations: With common causes (Beta factor)
1oo1	$\lambda_{DU} \times \frac{TI}{2}$	*not applicable*
1oo2 / 1oo2D	$\lambda_{DU_1} \times \lambda_{DU_2} \times \frac{TI^2}{3}$	$\frac{\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2}{3} + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
1oo3	$\lambda_{DU_1} \times \lambda_{DU_2} \times \lambda_{DU_3} \times \frac{TI^3}{4}$	$\frac{\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^3}{4} + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
2oo2	$\left(\lambda_{DU_1} + \lambda_{DU_2}\right) \times \frac{TI}{2}$	$\left[(1-\beta)\times(\lambda_{DU}\times TI)\right] + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
2oo3	$\left[\left(\lambda_{DU_1}\times\lambda_{DU_2}\right)+\left(\lambda_{DU_1}\times\lambda_{DU_3}\right)+\left(\lambda_{DU_2}\times\lambda_{DU_3}\right)\right] \times \frac{TI^2}{3}$	$\left[(1-\beta)\times(\lambda_{DU}\times TI)\right]^2 + \frac{(\beta\times\lambda_{DU}\times TI)}{2}$
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)

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

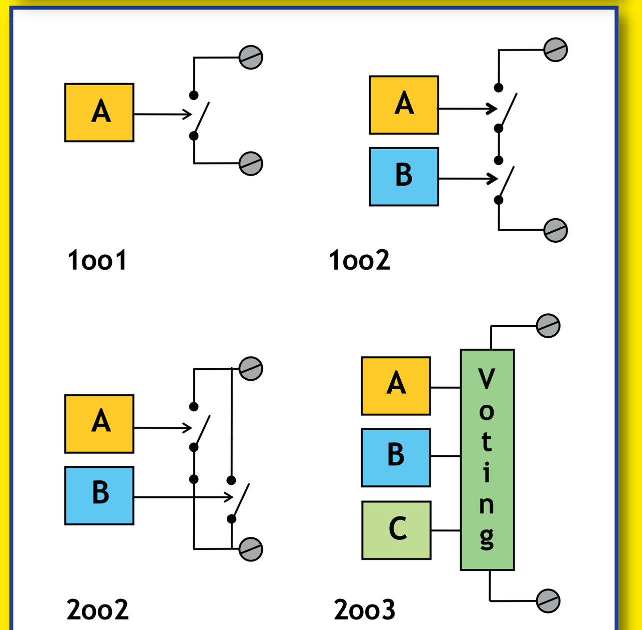
SFF	Hardware Fault Tolerance 0	Hardware Fault Tolerance 1	Hardware Fault Tolerance 2
TYPE A Components – Simple devices with well-known failure modes and a solid history of operation			
< 60%	SIL 1	SIL 2	SIL 3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4
TYPE B 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

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
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

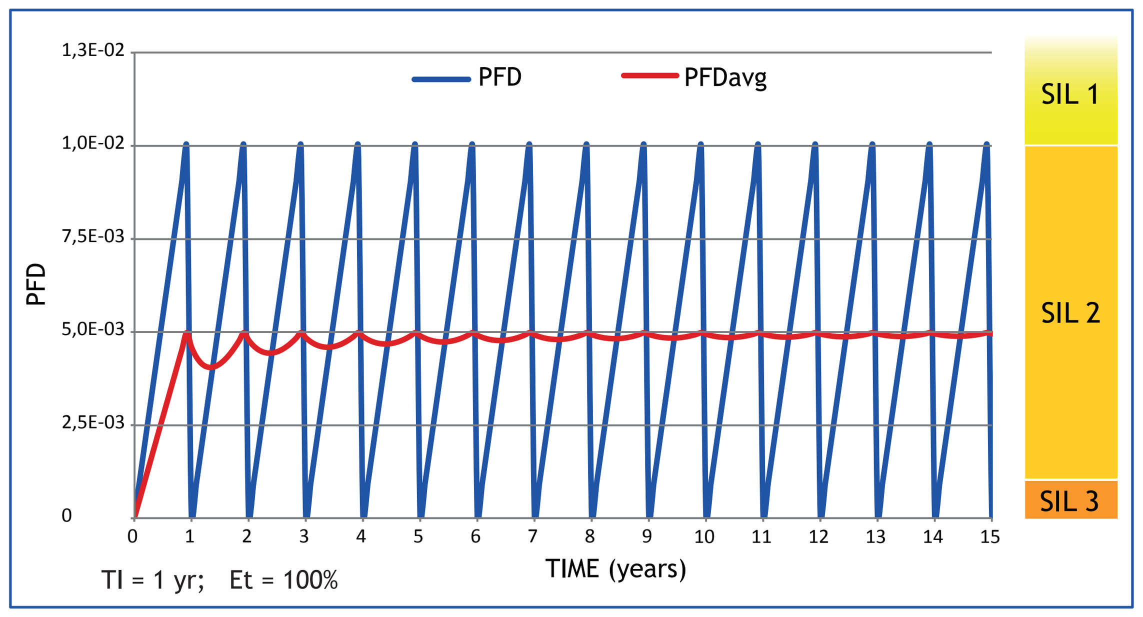


A PRACTICAL APPLICATION

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 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 $=1/\lambda$ (yrs)	λ per year $=1/MTBF$	MTBFs $=1/\lambda_S$ (yrs)	λ_S per year	λ_{DD} per year	λ_{DU} per year	PFDavg 1oo1 $=\lambda_{DU}/2$	% 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 (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:

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

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

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 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:

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

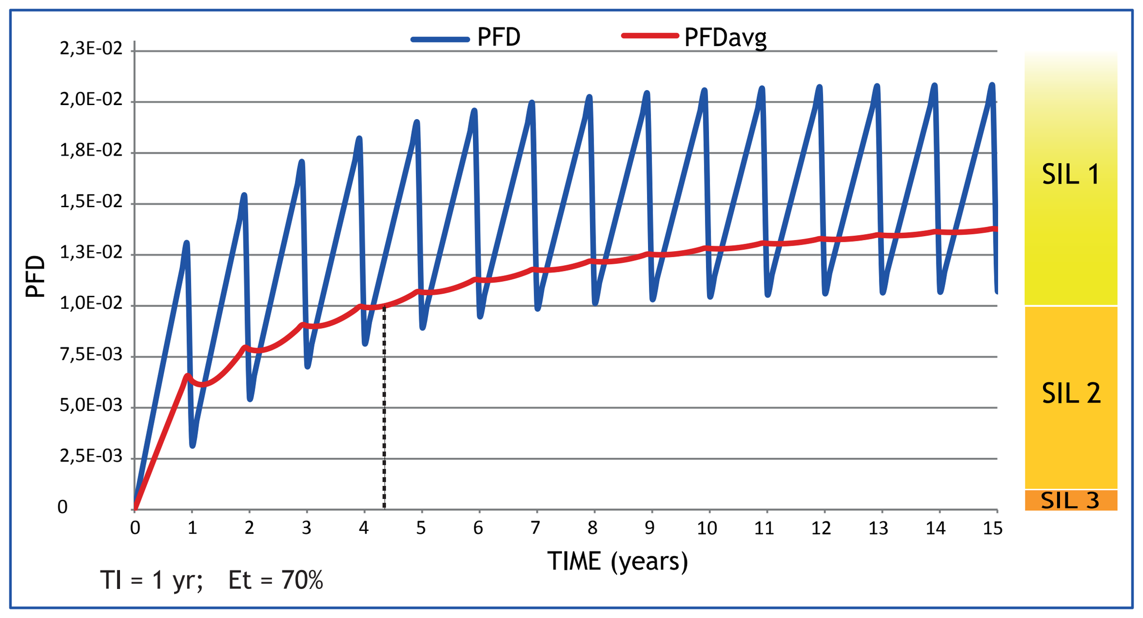
where:

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:

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

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.



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.

INTERNATIONAL
TECHNOLOGY FOR SAFETY

ITALY
G.M. International SRL
Via San Fiorano, 70
I-20852 Villasanta (MB)
Tel: +39 039 2325038
Fax: +39 039 2325107
info@gmintsrl.com
www.gmintsrl.com

UNITED ARAB EMIRATES
GM International JLT
1201, Fortune Executive Tower, JLT
PB 111365, Dubai
Tel: +971 4 422 5844
Fax: +971 4 422 5843
info@gminternational.ae
www.gminternational.ae

UNITED STATES OF AMERICA
GM International Safety Inc.
17453 Village Green Drive
77040 Houston, TX
Tel: +1 713 896 0777
Fax: +1 713 896 0782
info@gmisafety.com
www.gmisafety.com