

SIL

Process Design and Maintenance in Safety-Related Systems

Last revised 30/05/2008

G.M. International s.r.l

Via San Fiorano, 70
20058 Villasanta (Milano)
ITALY

www.gmintsrl.com

info@gmintsrl.com



Technology for Safety



What is Safety?

“freedom from unacceptable risks”



Figure 40, Example of a vapor cloud explosion (BLEVE)



Risk Reduction

$$RRF = \frac{\text{Frequency of accidents without protection}}{\text{Frequency of tolerable accidents}} = \frac{1}{PFD_{avg}}$$



Figure 66, Basic concept of risk reduction



Risk Reduction Factor

- Nr. of accidents per year without protections: 10
- Nr. of tolerable accidents: 1 per 100 years
- $10 \times 100 / 1 = 1000 = \text{RRF}$
(Risk Reduction Factor)
- $1 / 1000 = 0.001 = \text{PFD}_{\text{avg}}$ per year
(Average Probability of Failure on Demand)



A.L.A.R.P.

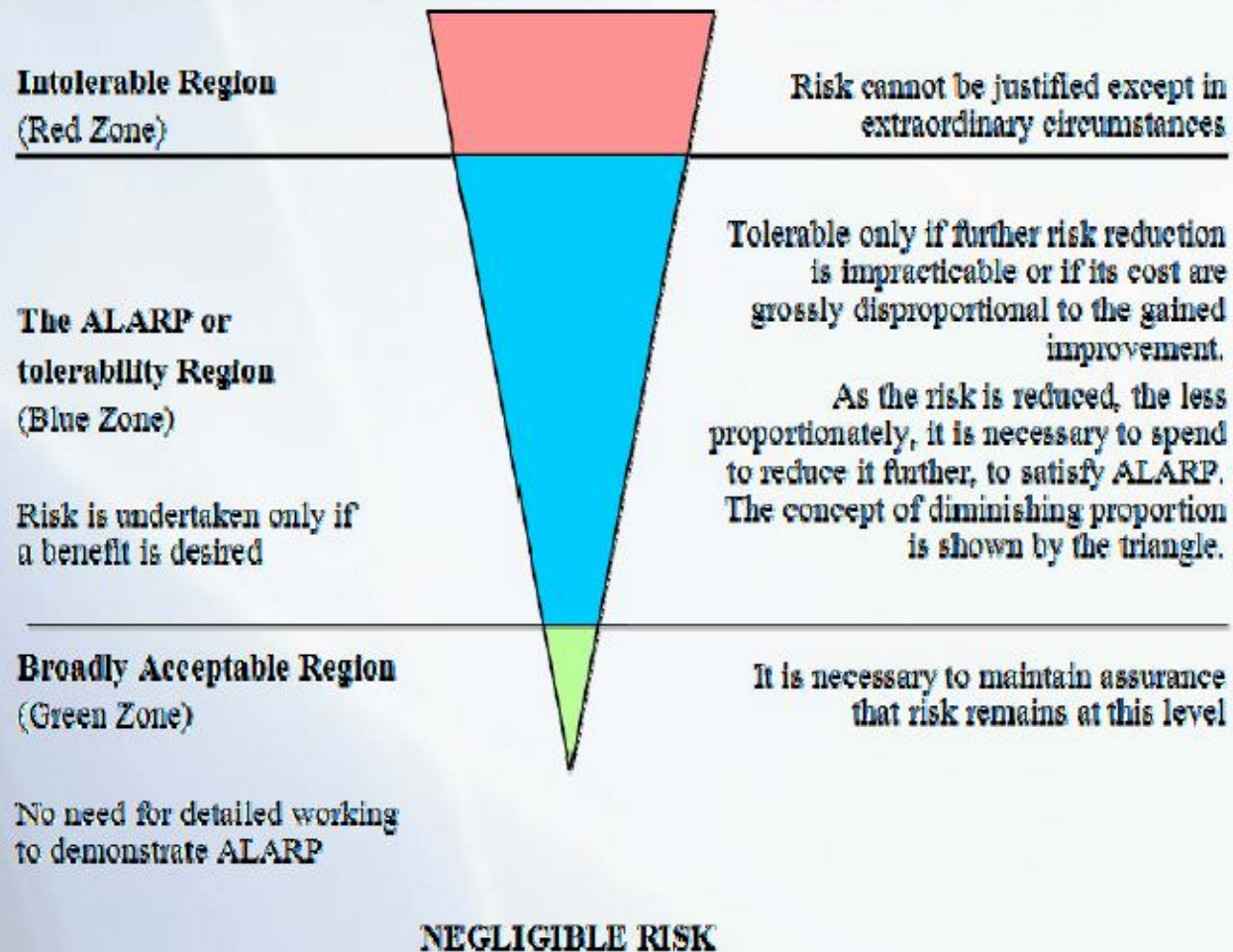


Figure 67, Risk and ALARP zone



Benefits Vs. Costs in the ALARP blue Zone

$$\frac{\text{Benefits}}{\text{Costs}} = \frac{F_{\text{NO-SIS}} \times EV_{\text{NO-SIS}} - F_{\text{SIS}} \times EV_{\text{SIS}}}{\text{COST}_{\text{SIS}} + \text{COST}_{\text{NT}}}$$

Where:

- B-C ratio : The ratio of benefits to costs
- $F_{\text{NO-SIS}}$: Frequency of the unwanted event without a SIS.
- $EV_{\text{NO-SIS}}$: Total expected value of loss of the event without a SIS.
- F_{SIS} : Frequency of the unwanted event with a SIS.
- EV_{SIS} : Total expected value of loss of the event with a SIS.
- COST_{SIS} : Total lifecycle cost of the SIS (annualized).
- COST_{NT} : Cost incurred due to nuisance trip (annualized)

Example:

A SIS is being installed to prevent a fire that will cost the company \$1,000,000.
 The frequency prior to application of SIS has been calculated in one every 10 years.
 After SIS installation the expected frequency is one every 1000 years,
 and its annualized cost is approximately \$66,000.
 Cost for nuisance trip is negligible, being F&G normally de-energized.
 What is the benefit-to-cost ratio for the F&G project?
 The Benefits/Costs relation will be:

$$\text{Benefits} = \left(\frac{1}{10} \times 1000000\right) - \left(\frac{1}{1000} \times 1000000\right) = 99000$$

$$\text{Costs} = (66000 + 0) = 66000$$

$$\frac{\text{Benefits}}{\text{Costs}} = \frac{99000}{66000} = 1.5$$

A benefit-to-cost ratio of 1.5 means that for every \$1 of investment the plant owner can expect \$1.5 in return.



General Risk Reduction concepts

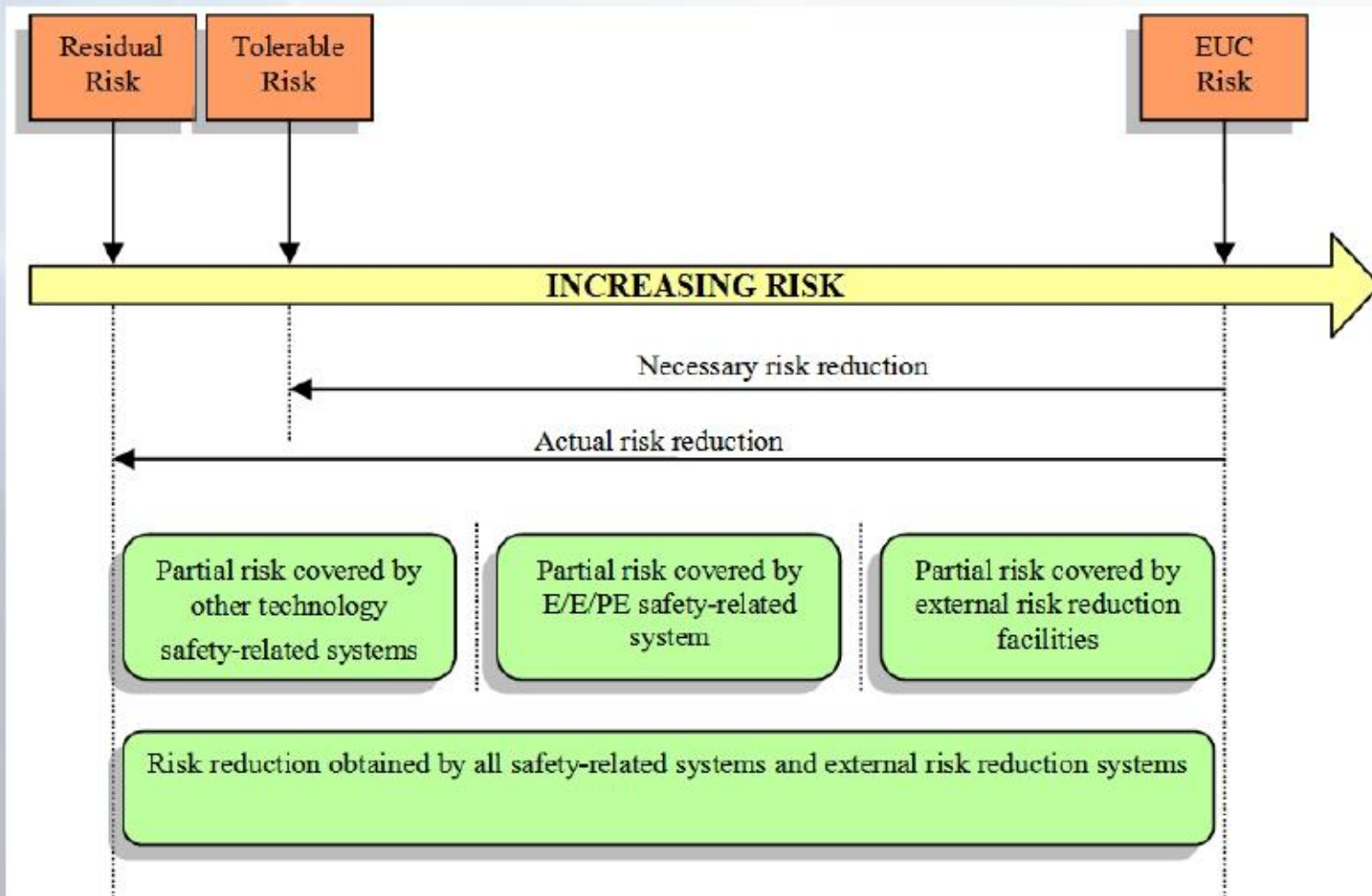


Figure 66, General concepts of risk reduction, according to IEC 61508

Risk Reduction with Protection Layers

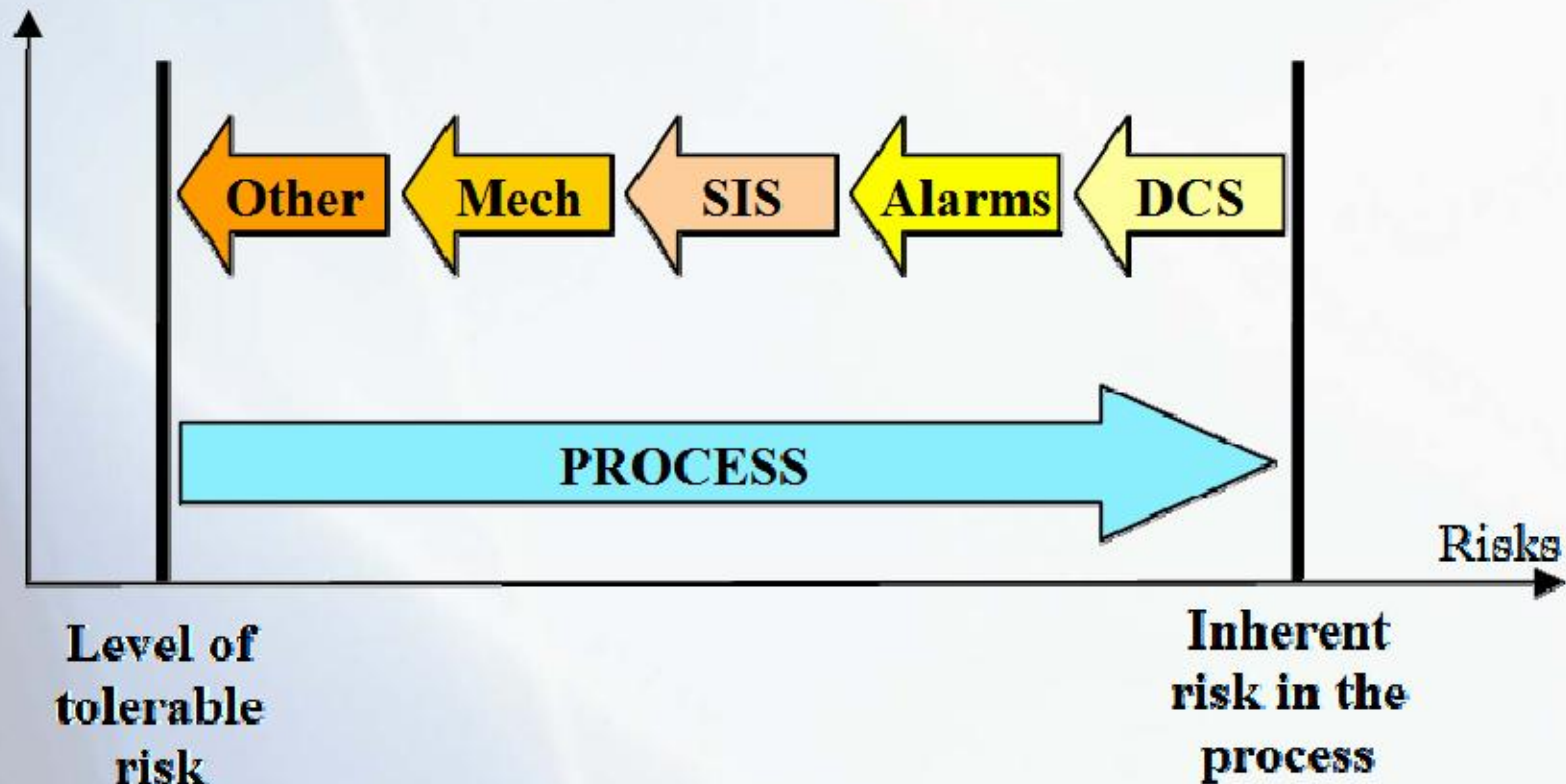


Figure 4, Risk reduction with several prevention layers



Layers of Protection

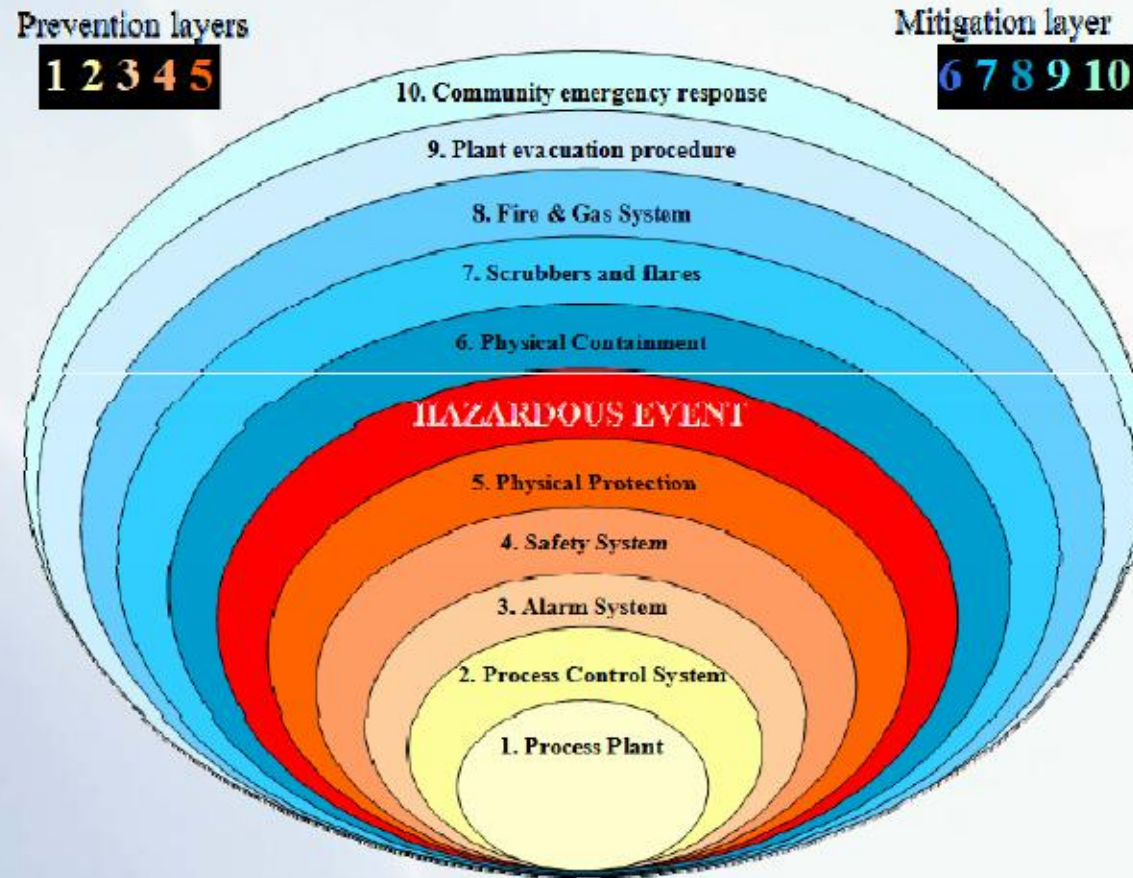


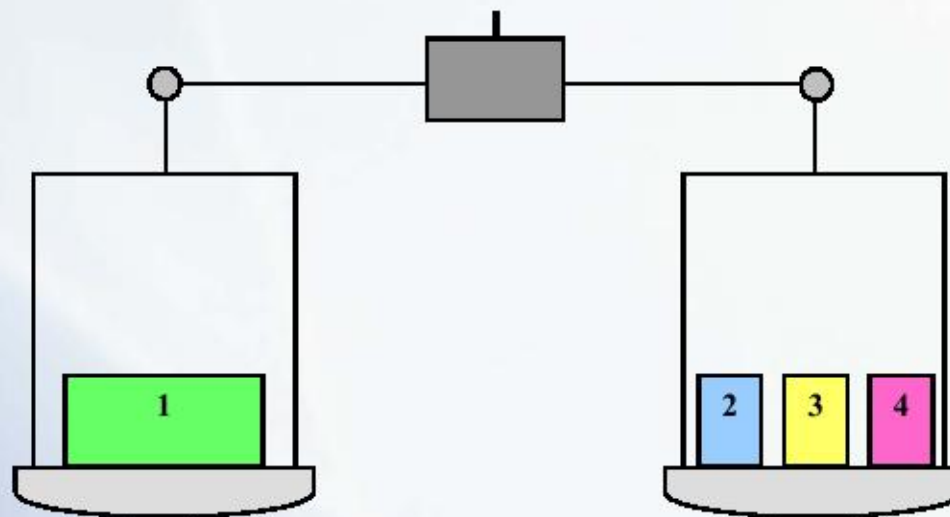
Figure 5. Prevention and mitigation layers of the hazardous event



Risk Protection Balance

The Risk Must be balanced by the Protection Layers

(Optimal Safety Balance)



RISK

1. Plant, Process and Environment

PREVENTION

2. DCS

3. SIS / ESD

4. Physical Protections



Dangerous Event / Accident



Figure 36, Example of Pool fire



Mitigation Layers

- Mitigation layers are implemented to reduce the consequences once the event has already happened.
- They may contain, disperse or neutralize the release of hazardous substances.



MTTF

MTTF is an indication of the average successful operating time of a device (system) before a failure in any mode.

- **MTBF**: Mean Time Between Failures
 - $\text{MTBF} = \text{MTTF} + \text{MTTR}$
 - $\text{MTTF} = \text{MTBF} - \text{MTTR}$
 - **MTTR**: Mean Time To Repair
- Since $(\text{MTBF} \gg \text{MTTR})$
 $\text{MTBF} \neq \text{MTTF}$
 (very close in values)

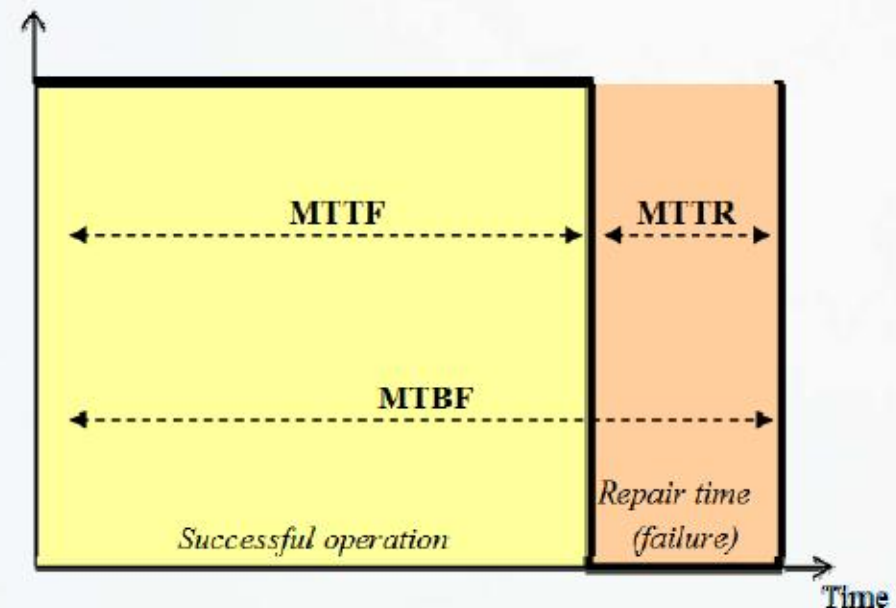
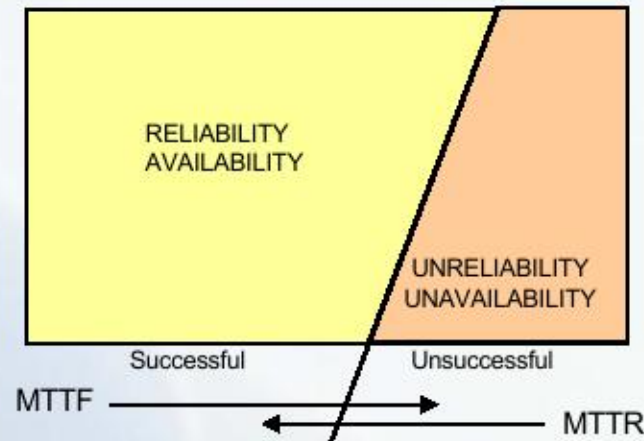


Figure 17. Schematic representation of MTTF, MTTR, MTBF

MTBF and Failure Rate

$$\text{Failure Rate} = \lambda = \frac{\text{Failures per unit time}}{\text{Number of components exposed to functional failure}}$$

$$\text{MTBF} = \frac{1}{\lambda}$$



*Venn Diagram: Reliability-Unreliability;
Availability-Unreliability and relations with MTTF and MTTR*

MTBF and Failure Rate

Relation between MTBF and Failure Rate λ

$$\lambda = \frac{\text{Failure per unit time}}{\text{Quantity Exposed}} = \frac{1}{\text{MTBF}}$$

$$\text{MTBF} = \frac{1}{\lambda} = \frac{\text{Quantity Exposed}}{\text{Failure per unit time}}$$



MTBF - Example

- Instantaneous failure rate is commonly used as measure of reliability.
- Eg. 300 Isolators have been operating for 10 years. 3 failures have occurred. The average failure rate of the isolators is:

$$\lambda = \frac{\text{Failure per unit time}}{\text{Quantity Exposed}} = \frac{3}{300 \cdot 10 \cdot 8760} =$$

= 0.000000038 per hour = 0.001 per year
 = 38 FIT (Failure per billion hours) =
 = 38 probabilities of failure in one billion hours.
 = 0.001 probability of failure per year

- MTBF = $1 / \lambda$ = 1000 years (for constant failure rate)



FIT

Failure In Time is the number of failures per one billion device hours.

$$\begin{aligned} 1 \text{ FIT} &= \\ &= 1 \text{ Failure in } 10^9 \text{ hours} \\ &= 10^{-9} \text{ Failures per hour} \end{aligned}$$



Failure Rate Categories

$$\lambda_{tot} = \lambda_{safe} + \lambda_{dangerous}$$

$$\lambda_s = \lambda_{sd} + \lambda_{su}$$

$$\lambda_d = \lambda_{dd} + \lambda_{du}$$

$$\lambda_{tot} = \lambda_{sd} + \lambda_{su} + \lambda_{dd} + \lambda_{du}$$

Where:

sd = Safe detected

su = Safe undetected

dd = Dangerous detected

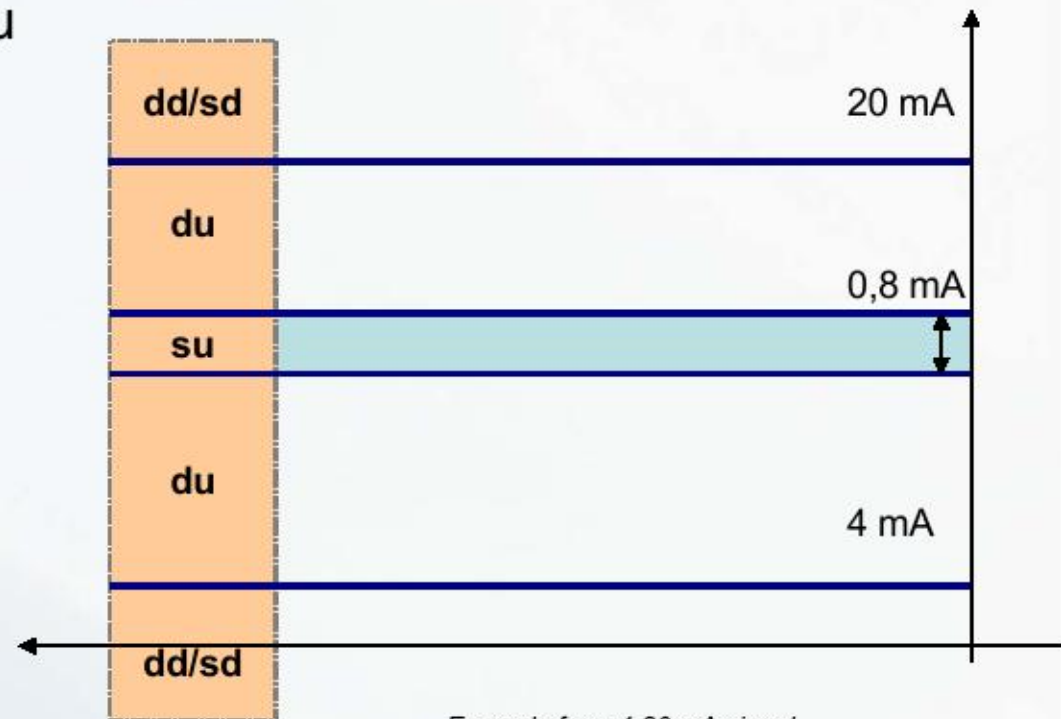
du = Dangerous undetected

$$\lambda_{tot} = \lambda_{safe} + \lambda_{dangerous}$$

(MTBF = MTBF_s + MTBF_d)

λ_{safe} : spurious trip (nuisance trip)

$\lambda_{dangerous}$: safety trip



Example for a 4-20 mA signal



Safe Failure Fraction (SFF)

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

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

SFF	Hardware fault tolerance 0	Hardware fault tolerance 1	Hardware fault tolerance 2
< 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

Table 23, SFF (Safe Failure Fraction) for A type components

- **Type A** components are described as simple devices with well-known failure modes and a solid history of operation.
- **Type B** devices are complex components with potentially unknown failure modes, e.g. microprocessors, ASICs, etc.

SFF	Hardware fault tolerance 0	Hardware fault tolerance 1	Hardware fault tolerance 2
< 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

Table 24, SFF (Safe Failure Fraction) for B type components



Example of FMEDA Analysis

ID	Component type	λ (FIT)	% of failure rate	Simulated failure type	Effect on output signal	λ_{con} (FIT)	λ_{scr} (FIT)	λ_{err} (FIT)	λ_{unc} (FIT)
C1A	Cond. MC 10 nF 50V 10 % \pm 7R 0805 SMD	21.8	80 20	Open Short	SD SU	25.4	6.26		
C2A	Cond. MC 10 nF 50V 10 % \pm 7R 0805 SMD	21.8	80 20	Open Short	DU SC		6.26		15.4
C12A	Cond. MC 10 nF 50V 10 % \pm 7R 0805 SMD	21.8	80 20	Open Short	DD SU		3.72	22.8	
R48A	Res. TF792KK 1/8 W 1% 100 ppm 0805 SMD	9.6	20 40 15 25	Open Short 0.5 \times R 2 \times R	SU SD SD SD	3.88 1.46 2.43	1.94		
R52A	Res. TF792KK 1/8 W 1% 100 ppm 0805 SMD	9.6	80 80	Open Short	DU DD SU		1.46 2.43	3.88	1.94
T1A	Ind. EP16 1p/1s 40-95s Vds 90V Ids 200 mA 2.612.6 mH		80 80	Open Short	SD DD	8.9		8.9	
TR5A	Trans. 2N7002 Nmos Vds 60V Ids 200 mA Rds 9.1R 90T23 SMD	25	80 80	Open Short	SD SU	12.5	12.5		
TR7A	Trans. 2N7002 Nmos Vds 60V Ids 200 mA Rds 9.1R 90T23 SMD	25	80 80	Open Short	DU DD			12.5	7.3
IC3A	Integ. TLC772 Ampl. Operat. SOS SMD	27	40 40 20	Open Short Unstable	SD SU DU		1.08 1.08		19.4 0.054
IC4A	Integ. TLC772 Ampl. Operat. SOS SMD	27	40 40 20	Open Short Unstable	SU SD DU	1.08	1.08		0.054
Total Failure Rates						55.65	40.01	48.16	24.95

Table 31. Example of FMEDA analysis

Failure
Modes
Effects
Diagnostic
Analysis



PFDavg 1001 Calculation

Equation for 1001 loop

$$\text{PFDavg (T1)} = \lambda_{dd} * RT + \lambda_{du} * T1/2$$

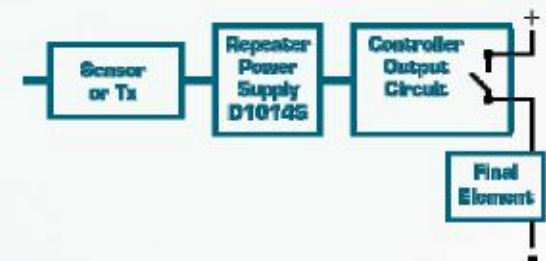
Where:

RT = repair time in hours (conventionally 8 hours)

T1 = T proof test, time between circuit functional tests (1-5-10 years)

λ_{dd} = failure rate for detected dangerous failures

λ_{du} = failure rate for undetected dangerous failures



Loop PFD_{avg} calculation

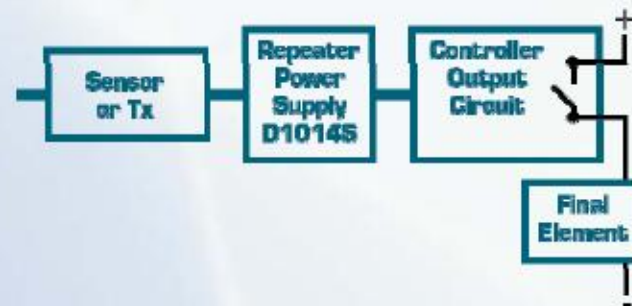
$$\text{PFD}_{\text{avg}} (T1) = \lambda_{\text{dd}} * RT + \lambda_{\text{du}} * T1/2$$

If T1 = 1 year then

$$\text{PFD}_{\text{avg}} = \lambda_{\text{dd}} * 8 + \lambda_{\text{du}} * 4380$$

but being $\lambda_{\text{dd}} * 8$ far smaller than $\lambda_{\text{du}} * 4380$

$$\text{PFD}_{\text{avg}} = \lambda_{\text{du}} * T1/2$$



PFDavg simplified equations

Architecture	PFDavg TI = 1 year	PFDavg TI = 3 years	PFDavg TI = 5 years	PFDavg TI = 10 years
1oo1	$\frac{\lambda_{DU}}{2}$	$3 \times \frac{\lambda_{DU}}{2}$	$5 \times \frac{\lambda_{DU}}{2}$	$10 \times \frac{\lambda_{DU}}{2}$
1oo2	$\frac{\lambda_{DU}^2}{3}$	$9 \times \frac{\lambda_{DU}^2}{3}$	$25 \times \frac{\lambda_{DU}^2}{3}$	$100 \times \frac{\lambda_{DU}^2}{3}$
2oo2	λ_{DU}	$3 \times \lambda_{DU}$	$5 \times \lambda_{DU}$	$10 \times \lambda_{DU}$
2oo3	λ_{DU}^2	$9 \times \lambda_{DU}^2$	$25 \times \lambda_{DU}^2$	$100 \times \lambda_{DU}^2$
1oo3	$\frac{\lambda_{DU}^3}{4}$	$27 \times \frac{\lambda_{DU}^3}{4}$	$125 \times \frac{\lambda_{DU}^3}{4}$	$1000 \times \frac{\lambda_{DU}^3}{4}$
2oo4	λ_{DU}^3	$27 \times \lambda_{DU}^3$	$125 \times \lambda_{DU}^3$	$1000 \times \lambda_{DU}^3$

Table 2. Simplified equations for PFDavg calculation



Common fault / Beta Factor

Architecture	Simplified equation	Simplified equation with β factor
1oo2	$\frac{1}{3} \times (\lambda_{DU} \times TI)^2$	$\frac{1}{3} \times [(1 - \beta) \times (\lambda_{DU} \times TI)]^2 + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI)$
1oo2D	$\frac{1}{3} \times (\lambda_{DU} \times TI)^2$	$\frac{1}{3} \times [(1 - \beta) \times (\lambda_{DU} \times TI)]^2 + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI)$
2oo2	$\lambda_{DU} \times TI$	$[(1 - \beta) \times (\lambda_{DU} \times TI)] + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI)$
2oo3	$(\lambda_{DU} \times TI)^2$	$[(1 - \beta) \times (\lambda_{DU} \times TI)]^2 + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI)$
1oo3	$\frac{1}{4} \times (\lambda_{DU} \times TI)^3$	$\frac{1}{4} \times [(1 - \beta) \times (\lambda_{DU} \times TI)]^3 + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI)$

For redundant subsystems using electronic components, the value of β ranges from 1% to 5%.

The second term of the equations is the PFDavg value contribution due to the **β factor**, derived from the 1oo1 architecture.

Example:

$\lambda_{du} = 0.01 / \text{yr}$; $TI = 1 \text{ yr}$; $\beta = 0.05$

For 1oo2 the equation is:

$$\begin{aligned}
 & \frac{1}{3} \times [(1 - \beta) \times (\lambda_{DU} \times TI)]^2 + \frac{1}{2} \times (\beta \times \lambda_{DU} \times TI) = \\
 & = \frac{1}{3} \times [0.95 \times 0.01]^2 + \frac{1}{2} \times (0.05 \times 0.01 \times 1) = \\
 & = 0.00003 + 0.00025 = 0.00028 / \text{yr}
 \end{aligned}$$



Considerations

Comparisons using different values of β factor:

[PFDavg] 1oo1 = 0.005 / yr	[RRF] 1oo1 = 200
[PFDavg] 1oo2 = 0.00003 / yr (no β factor)	[RRF] 1oo2 = 33.333 = 200 x 166.6
[PFDavg] 1oo2 = 0.000082 / yr (with 1% β factor)	[RRF] 1oo2 = 12.195 = 200 x 61
[PFDavg] 1oo2 = 0.00028 / yr (with 5% β factor)	[RRF] 1oo2 = 3571 = 200 x 17.8
[PFDavg] 1oo2 = 0.000527 / yr (with 10% β factor)	[RRF] 1oo2 = 1897 = 200 x 9.48

Considerations:

- The value 0.00003 is 166.6 times lower than 0.005.
- The value 0.000082 is 61 times lower than 0.005.
- The value 0.00028 is 17.8 times lower than 0.005.
- The value 0.000527 is 9.48 times lower than 0.005.
- Without β factor the PFDavg, of 1oo2 architecture, is 166.6 times better than PFDavg value of 1oo1 architecture.
- With 1% β factor the PFDavg, of 1oo2 architecture, is 61 times better than PFDavg value of 1oo1 architecture.
- With 5% β factor the PFDavg, of 1oo2 architecture, is 17.8 times better than PFDavg value of 1oo1 architecture.
- With 10% β factor the PFDavg, of 1oo2 architecture, is 9.48 time better than PFDavg value of 1oo1 architecture.



System architectures

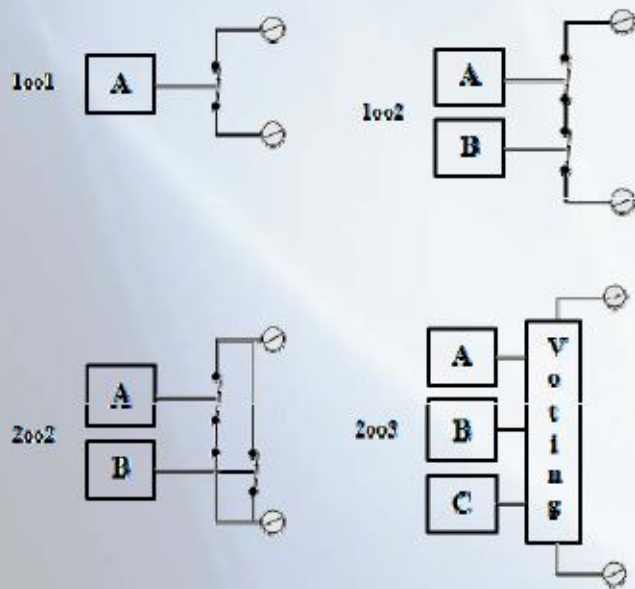


Figure 43: Schematic diagrams of some system architectures

Architecture	Probability of safe failure per year	MTTF _S (yrs)	Probability of dangerous failure per year	MTTF _D (yrs)
1oo1	0,0400	25	0,0200	50
1oo2	0,0800	12,5	0,0004	2500
2oo2	0,0016	625	0,0400	25
2oo3	0,0048	208	0,0012	833

Table 7: The Impact of redundancy

Safety Integrity Levels (SIL)

- SIL levels (Safety Integrity Level)
- RRF (Risk Reduction Factor)
- PFD avg (Average Probability of Failure on Demand)

SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand)	(1-PFDavg) Safety availability	RRF Risk Reduction Factor	PFDavg Average probability of failure on demand per hour (high demand)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	99.99 to 99.999 %	100000 to 10000	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	99.9 to 99.99 %	10000 to 1000	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	99 to 99.9 %	1000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	90 to 99 %	100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

Table 26, Risk reduction factor, as function of SIL levels and Availability



PFDavg calculation

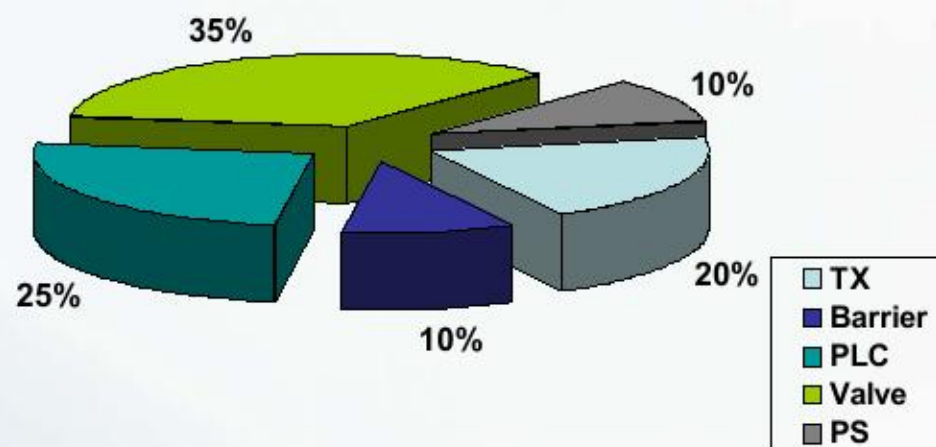
Each subsystem's PFDavg has a percentage value in relation to the total.

Component manufacturers list, in their functional safety manual, the value of PFDavg obtained by authorized certification bodies like TUV, EXIDA, FM, etc.

These bodies apply a conventional "weighing" of the PFDavg of the component in consequence of the importance that it has in the entire loop, as reported in the following Table:

Subsystem	PFDavg 1oo1 (%)
Transmitter	20 %
Barrier	10 %
PLC	25 %
Valve	35 %
Power Supply	10%
Total (SIF)	100 %

Table 5, PFDavg "weighing" for 1oo1 system architecture



Introduction to SIS

- It is a common thought that a safety function or a device which are rated SIL (1-2-3) will be so forever.
- We know that this is false:
SIL integrity level depends on the PFD_{avg} value, therefore, the SIL level lasts for a certain predetermined period of time: T-proof Time Interval.



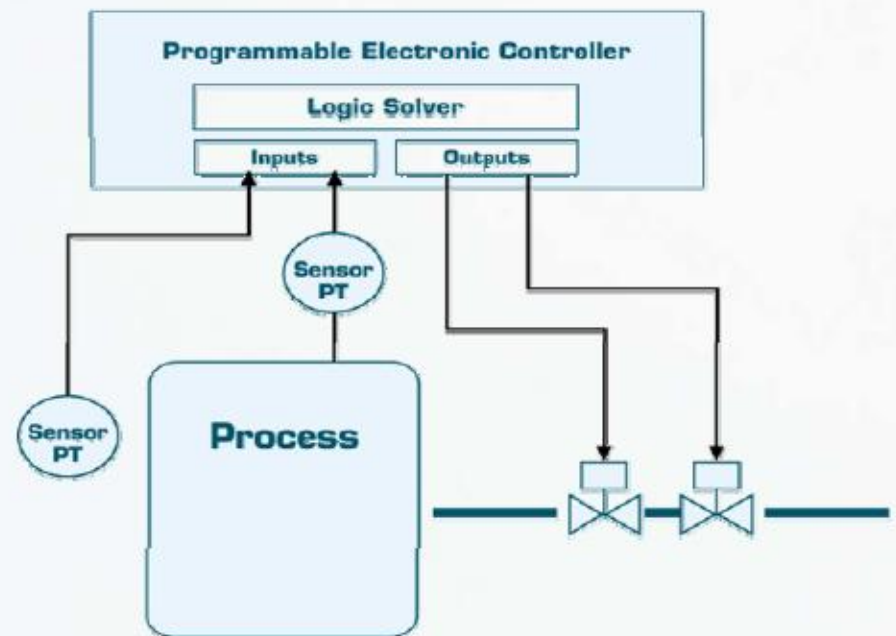
Introduction to SIS

- A SIL level which is maintained for 1 year is very different from one that remains so for 10 years; Although, both are used on the same safety function.
- T-proof time interval then is the time for which the conditions for maintaining a certain SIL level are met.



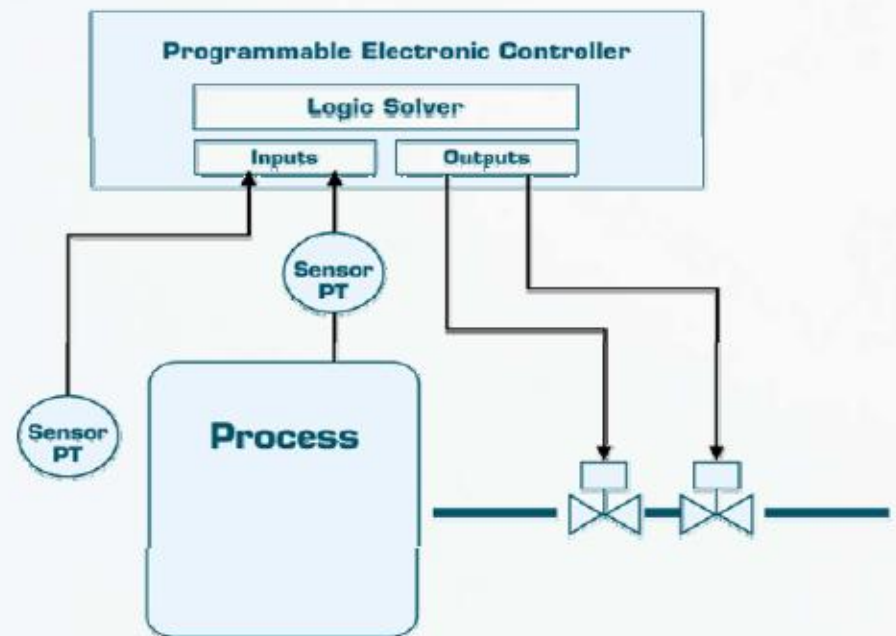
Safety Instrumented Systems (SIS)

- A simple SIS, with one logic solver, is a safety function as shown in the picture.
- A SIS is made up of multiple SIFs: one for each potentially dangerous condition.



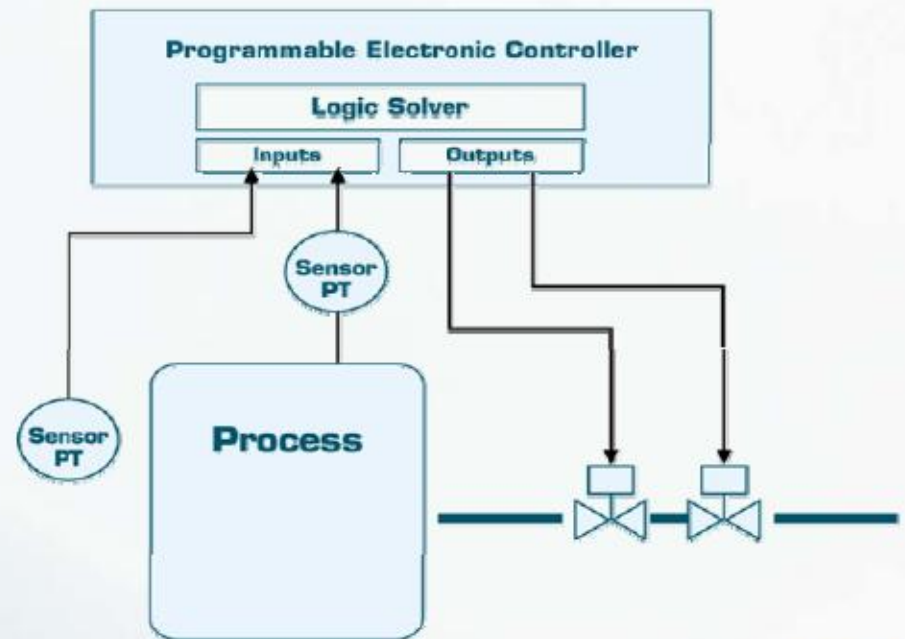
Safety Instrumented Systems (SIS)

- Its objective is to collect and analyzes data information from sensors to determine if a dangerous condition occurs, and consequently to start a shutdown sequence to bring the process to a safe state.
- A potentially dangerous condition is called "demand".



Safety Instrumented Systems (SIS)

- The majority of SIS are based on the concept of de-energizing to trip. In normal working conditions input and output are energized (F&G systems are the opposite)
- For each SIF, the required Risk Reduction Factor (RRF) is determined.
- IEC 61508 and IEC 61511, recognized Standards, cover in detail these safety aspects.

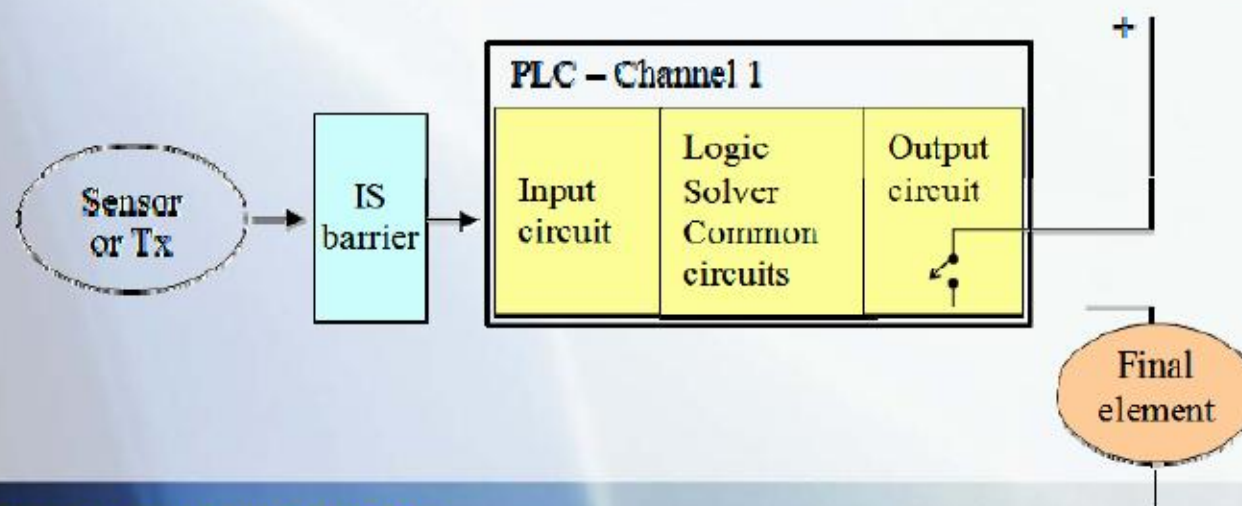


SIF Example

**Calculate values of MTBF, PFDavg, RRF
for a possible SIL level of the following SIF.**

These values are given by the manufacturers:

Tx:	MTBF = 102 yrs;	$\lambda_{DU} = 0,00080$ / yr;	$\lambda_{DD} = 0,0010$ / yr;	$\lambda_S = 0,00800$ / yr
Barrier:	MTBF = 314 yrs;	$\lambda_{DU} = 0,00019$ / yr;	$\lambda_{DD} = 0,0014$ / yr;	$\lambda_S = 0,00159$ / yr
PLC:	MTBF = 685 yrs;	$\lambda_{DU} = 0,00001$ / yr;	$\lambda_{DD} = 0,0001$ / yr;	$\lambda_S = 0,00135$ / yr
Supply:	MTBF = 167 yrs;	$\lambda_{DU} = 0,00070$ / yr;	$\lambda_{DD} = 0,0000$ / yr;	$\lambda_S = 0,00530$ / yr
Valve:	MTBF = 12 yrs;	$\lambda_{DU} = 0,02100$ / yr;	$\lambda_{DD} = 0,0200$ / yr;	$\lambda_S = 0,00400$ / yr



D1014 SIL 3 Analysis

D1014 module
Isolated Hart compatible
Repeater power supply



Table 12: Failure rates

Failure category	Failure rates in FIT
Total FAIL Dangerous Detected	147
Fail Dangerous Detected (internal diagnostics or indirectly)	0
Fail High (detected by the logic solver)	42
Fail Low (detected by the logic solver)	105
Fail Dangerous Undetected	22
No Effect	182
No Part	19
MTBF = MTTF + MTTR	312 years
MTTF _S = 1/λ _S	627 years
MTTF _D = 1/λ _{du}	5189 years

Table 13: Failure rates according to IEC 61508

Failure rate category	λ _{sd}	λ _{su}	λ _{dd}	λ _{du}	SFF	DCs	DCd
Rates	0 FIT	182 FIT	147 FIT	22 FIT	95.86%	0%	87%

Table 14: PFDavg values

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years
PFDavg = 9.43 E-05	PFDavg = 4.71 E-04	PFDavg = 9.43 E-04
Valid for SIL 3	Valid for SIL 2	Valid for SIL 2
See Note 4 Section 6	See Note 3 Section 6	See Note 3 Section 6



Technology for Safety



Summary table for SIL 1

Sub-system	MTBF (yr)	$\lambda / \text{yr} = 1/\text{MTBF}$	$\text{MTBF}_s = 1/\lambda_s$ (yr)	λ_s / yr	λ_{DD} / yr	λ_{DU} / yr	$\text{PFD}_{\text{avg}} 1001 = \lambda_{DU}/2$	% of total PFD_{avg}	$\text{RRF} = 1/\text{PFD}_{\text{avg}}$	SFF	SIL Level
Tx	102	0.00980	125	0.00800	0.0010	0.00080	0.000400	3.52 %	2500	91.8 %	SIL 2
Barrier D1014S	314	0.00318	629	0.00159	0.0014	0.00019	0.000095	0.84 %	10526	94.0 %	SIL 3
PLC	685	0.00146	741	0.00135	0.0001	0.00001	0.000005	0.04 %	200000	99.3 %	SIL 3
Valve	12	0.08100	25	0.00400	0.0200	0.02100	0.010250	92.51 %	95	74.1 %	SIL 1
Power Supply	167	0.00600	189	0.00530	0.0000	0.00070	0.000350	3.08 %	2857	88.3 %	SIL 3
Total (SIF)	10	0.10144	18	0.05624	0.0225	0.02270	0.011350	100 %	88	-	SIL 1

Table 3, 1001 system architecture and TI of 1 year



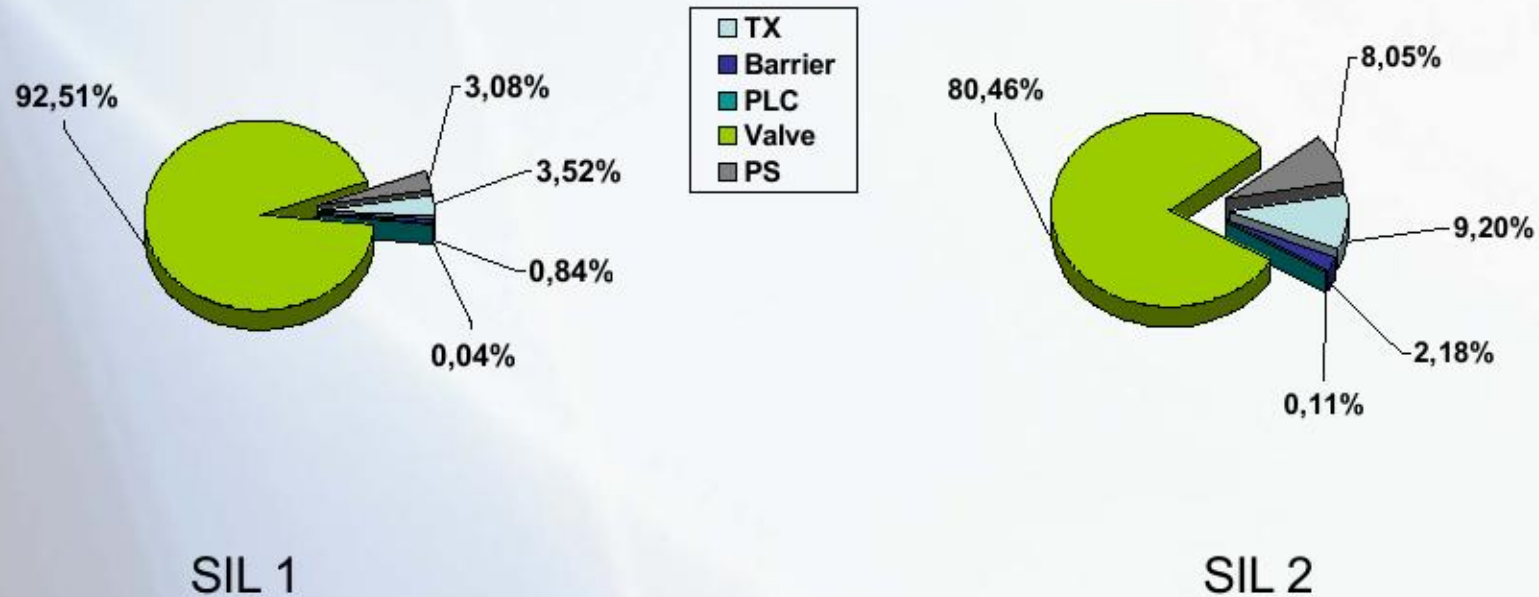
Summary table for SIL 2

Sub-system	MTBF (yr)	$\lambda = 1/\text{MTBF}$ per yr	$\text{MTBF}_S = 1/\lambda_S$ (yr)	λ_S / yr	λ_{DD} / yr	λ_{DU} / yr	$\text{PFD}_{avg} 1001 = \lambda_{DU}/2$	% of total PFD_{avg}	$\text{RRF} = 1/\text{PFD}_{avg}$	SFF	SIL Level
Tx	102	0.00980	125	0.00800	0.0010	0.00080	0.000400	9.20 %	2500	91.8 %	SIL 2
Barrier D1014S	314	0.00318	629	0.00159	0.0014	0.00019	0.000095	2.18 %	10526	94.0 %	SIL 3
PLC	685	0.00146	741	0.00135	0.0001	0.00001	0.000005	0.11 %	200000	99.3 %	SIL 3
Valve	37	0.02700	75	0.01333 / 4 months	0.0066 / 4 months	0.00700 / 4 months	0.003500 / 4 months	80.46 %	286	74.1 %	SIL 2
Power Supply	167	0.00600	189	0.00530	0.0000	0.00070	0.000350	8.05 %	2857	88.3 %	SIL 3
Total (SIF)	21	0.04744	34	0.02957	0.00917	0.00870	0.004350	100 %	230	-	SIL 2

Table 4, 1001 system architecture and TI of 1 year except for valve



SIF PFDavg confrontation



Summary table for SIL 2 SIF

Since the SIF has a safety integrity level SIL 2 the periodic proof tests can be performed according to the following table:

Subsystem	T-proof test time interval
Transmitter	1 yrs
Barrier	10 yrs
PLC	20 yrs
Valve	4 months

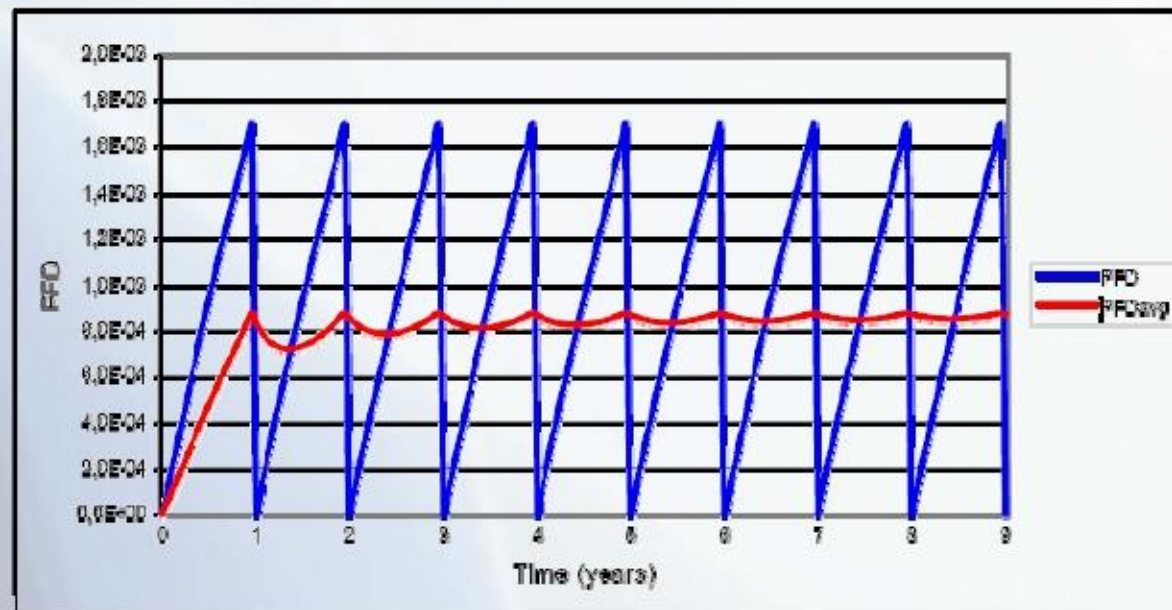
Table 6, 1001 system architecture and T-proof test interval optimization



PFD Versus T- proof time interval (TI)

PFD degrades in time.

The probability of failure of any equipment (therefore the PFD of a SIF) increases with time (linearly for constant failure rate).



Role of PFDavg & Considerations on SIL

- Knowing that two different safety-related equipments have the same SIL level is not enough for a complete evaluation.
The values of PFDavg can be from 1 to 10 times different.
- A lower value of PFDavg is always preferable for its lower contribution to the total SIL level of the SIF, and because, frequently, it allows for longer T-proof time intervals.

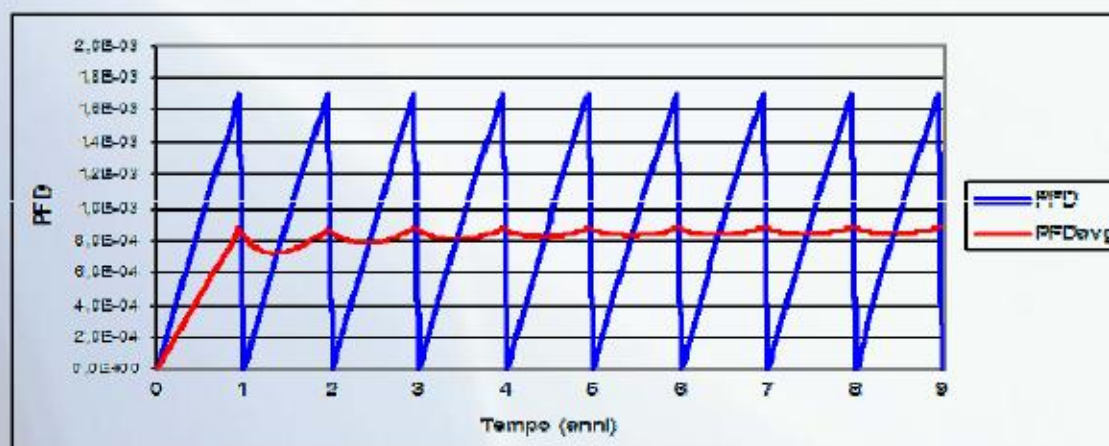
SIL Safety Integrity Level	PFDavg Average probability of failure on demand per year (low demand)	(1-PFDavg) Safety availability	RRF Risk Reduction Factor	PFDavg Average probability of failure on demand per hour (high demand)
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	99.99 to 99.999 %	100000 to 10000	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$> 10^{-4}$ to $< 10^{-3}$	99.9 to 99.99 %	10000 to 1000	$> 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	99 to 99.9 %	1000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	90 to 99 %	100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

Table 26. Risk reduction factor, as function of SIL levels and Availability



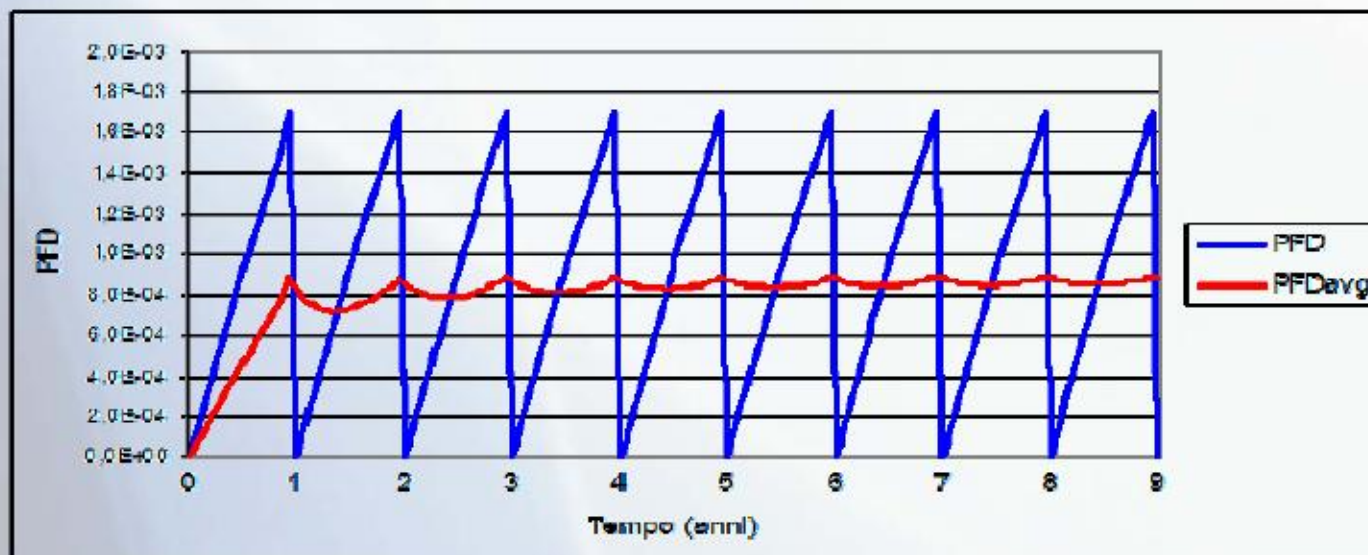
How PFD changes in time

- Since PFD increases with time, its value can be kept under control by actuating maintenance proof tests at certain time intervals.
- A periodic test at T-proof interval (as specified by the manufacturer), is capable of identifying any non directly detectable failure mechanisms in the equipment (dangerous undetected failures);
Note: The grade of the test effectiveness affects the value to which the PFDavg is set afterwards.



How PFD changes in time

- The grade of the test effectiveness affects the value to which the PFDavg is set afterwards.
- If the effectiveness is (99-100%) the equipment can be considered “as new”, from a probability of failure point of view, if it is lower then 100% (70-80-90%), then the SIL level could expire and not reach the required SIL level.



PFDavg: Equations and examples

For each component of the SIF, when the effectiveness of periodic proof test to reveal dangerous failures, is 100%, the PFDavg simplified equation, is:

$$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2}$$

when the effectiveness is not 100%, the PFDavg simplified equation is:

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

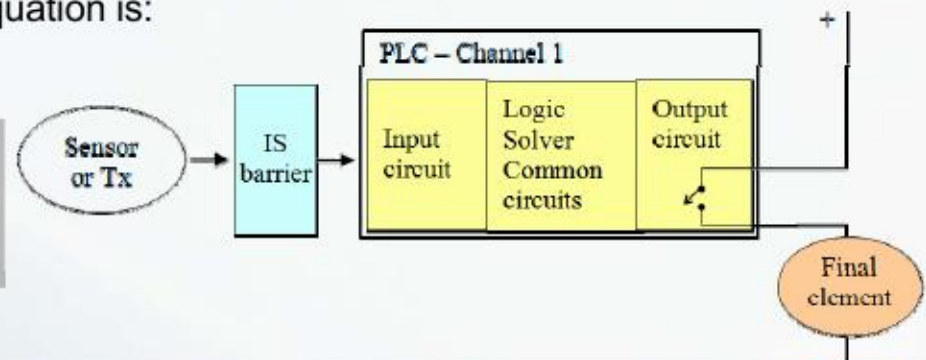
where:

Et: periodic testing effectiveness to reveal dangerous failures (e.g. 90%)

SL: system, or component, test proof interval with 99-100% effectiveness, or between two complete replacement of the device, or the lifetime of the system, or device, if it will never fully tested or replaced.

for TI = 1 yr and SL = 12 years, the PFDavg simplified equation is:

$$PFD_{avg}|_{TI=1,SL=12} = (Et \times \frac{\lambda_{DU}}{2}) + \left[(1 - Et) \times \lambda_{DU} \times \frac{12}{2} \right]$$



PFDavg: Equations and examples

$$PFD_{avg}|_{TI=1,SL=12} = (Et \times \frac{\lambda_{DU}}{2}) + \left[(1 - Et) \times \lambda_{DU} \times \frac{12}{2} \right]$$

Example a:

$$\lambda_{du} = 0,01 / \text{yr}$$

$$TI = 1 \text{ yr}$$

$$Et = 90\% = 0,9$$

$$SL = 12 \text{ yr}$$

At installation:

$$PFD_{avg} = 0,01 / 2 = 0,005$$

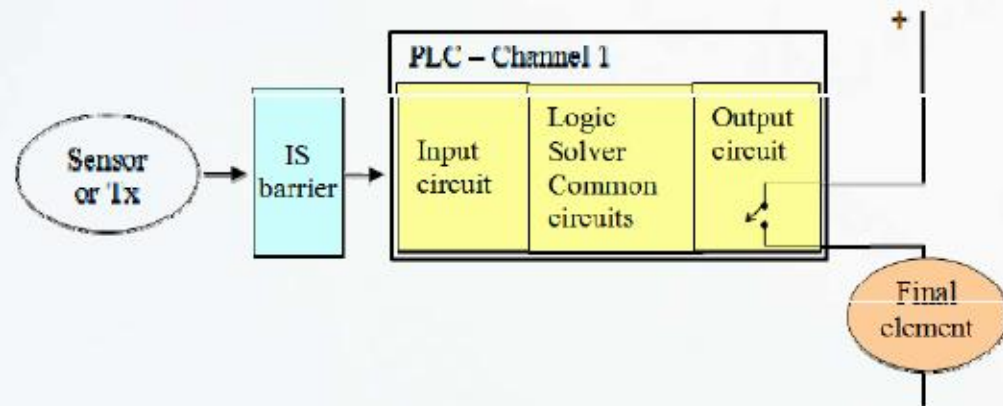
$$RRF = 1 / PFD_{avg} = 1 / 0,005 = \mathbf{200}$$

After one year:

$$PFD_{avg} = (0,9 \times 0,01 / 2) + (0,1 \times 0,01 \times 6) = 0,0105$$

$$RRF = 1 / PFD_{avg} = 1 / 0,0105 = \mathbf{95}$$

Note: **after one year (or after each periodic test) SIL 2 level has become SIL 1.**

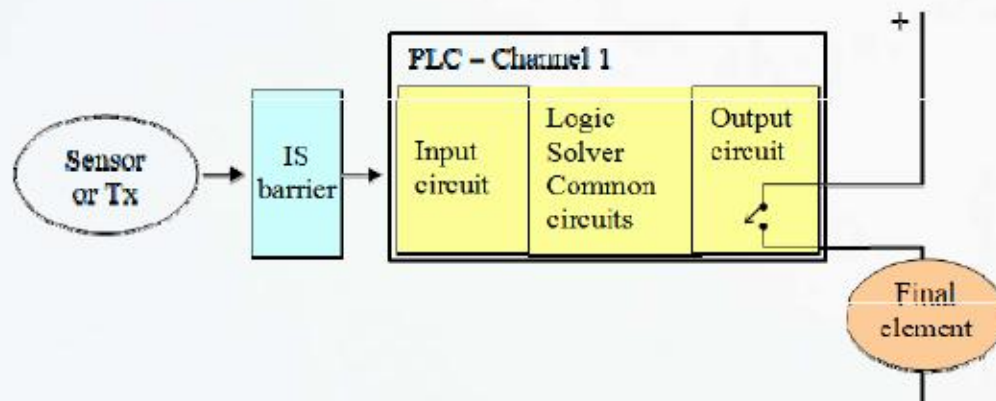


PFDavg: Equations and examples

$$\text{PFDavg}|_{\text{TI}=1, \text{SL}=12} = \left(\text{Et} \times \frac{\lambda_{\text{DU}}}{2} \right) + \left[(1 - \text{Et}) \times \lambda_{\text{DU}} \times \frac{12}{2} \right]$$

Example b:

$\lambda_{\text{DU}} = 0,01 / \text{yr}$
 $\text{TI} = 1 \text{ yr}$
 $\text{Et} = 99\% = 0,99$
 $\text{SL} = 12 \text{ yrs}$



After one year:

$\text{PFDavg} = (0,99 \times 0,01 / 2) + (0,01 \times 0,01 \times 6) = 0,0056$
 $\text{RRF} = 1 / \text{PFDavg} = 1 / 0,006 = 178$

Note: **after one year (or after each periodic test interval)**
SIL2 level is still maintained.



Test interval duration influence on PFDavg

- To test a safety system online (e.g. while the process is still running), a portion of the safety system must be placed in bypass in order to prevent nuisance trips. The length of the manual proof test duration can have a significant impact on the overall performance of a safety system.
- During the test, a simplex 1oo1 system must be taken offline. Its availability during the test is therefore zero. Redundant systems, however, do not have to be completely placed in bypass for testing. One leg, or slice, or a dual redundant system can be placed in bypass at a time.
- Indeed a dual system is reduced to simplex during a test, and a triplicate system is reduced to dual.

$$PFD_{avg} = \lambda_{DU} \times \frac{TI}{2}$$

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



Test interval duration influence on PFDavg

Example c:

$$\lambda_{du} = 0,002 / \text{yr}$$

$$TI = 1 \text{ yr}$$

TD = 8 hrs (time interval)

$$PFD_{avg} = 0,001 + 0,0009 = 0,0019;$$

$$\mathbf{RRF} = 1 / 0,0019 = \mathbf{526}$$

(useful for **SIL 2** level)

Example d:

$$\lambda_{du} = 0,002 / \text{yr}$$

$$TI = 1 \text{ yr}$$

TD = 96 hrs

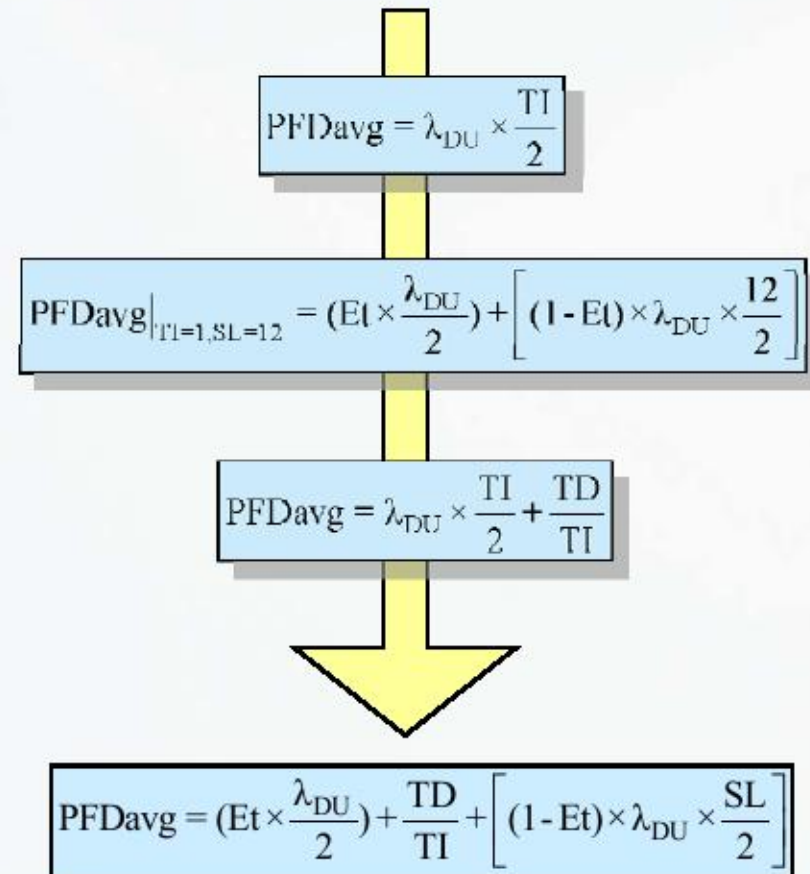
$$PFD_{avg} = 0,001 + 0,01 = 0,011;$$

$$\mathbf{RRF} = 1 / 0,011 = \mathbf{90}$$

(useful for **SIL 1** level)

Note:

The combination of both, effectiveness and test duration, brings to the following PFDavg equation for a 1oo1 architecture.



Strategies for maintaining safety in a SIS

Considerations:

- The SIL level of an equipment alone gives a partial, and incomplete, picture of the prospecting solution for a given SIF application.
- Information concerning:
 - Safe and Dangerous Failure Rates,
 - PFDavg Values for 1-3-5-10 years continuous operation,
 - T-proof Time Intervals,
 - Test proof Procedures & their percentage of effectiveness to reveal the dangerous undetected failures, shall be provided in the Safety Manual of the equipment.



Strategies for maintaining safety in a SIS

- A scheduled maintenance plan of the system is mandatory for each component of a SIF chain to restore the initial level of PFD and therefore its SIL rating.
- Maintenance, in the form of periodic tests at T-proof time interval, normally requires a bypass for the equipment under test, and often implies some critical operations, therefore the time interval should be the longest possible and the proof procedure should be safe, effective, and as quick as possible.

