

SIL LEVELS ACCORDING IEC 61508 / IEC 61511

IL 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	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10	$\geq 10^{-6}$ to $< 10^{-5}$

**SAFETY:
FREEDOM FROM
UNACCEPTABLE
RISK**



Vapor cloud explosion (BLEVE)



Flash Fire



Jet Fire

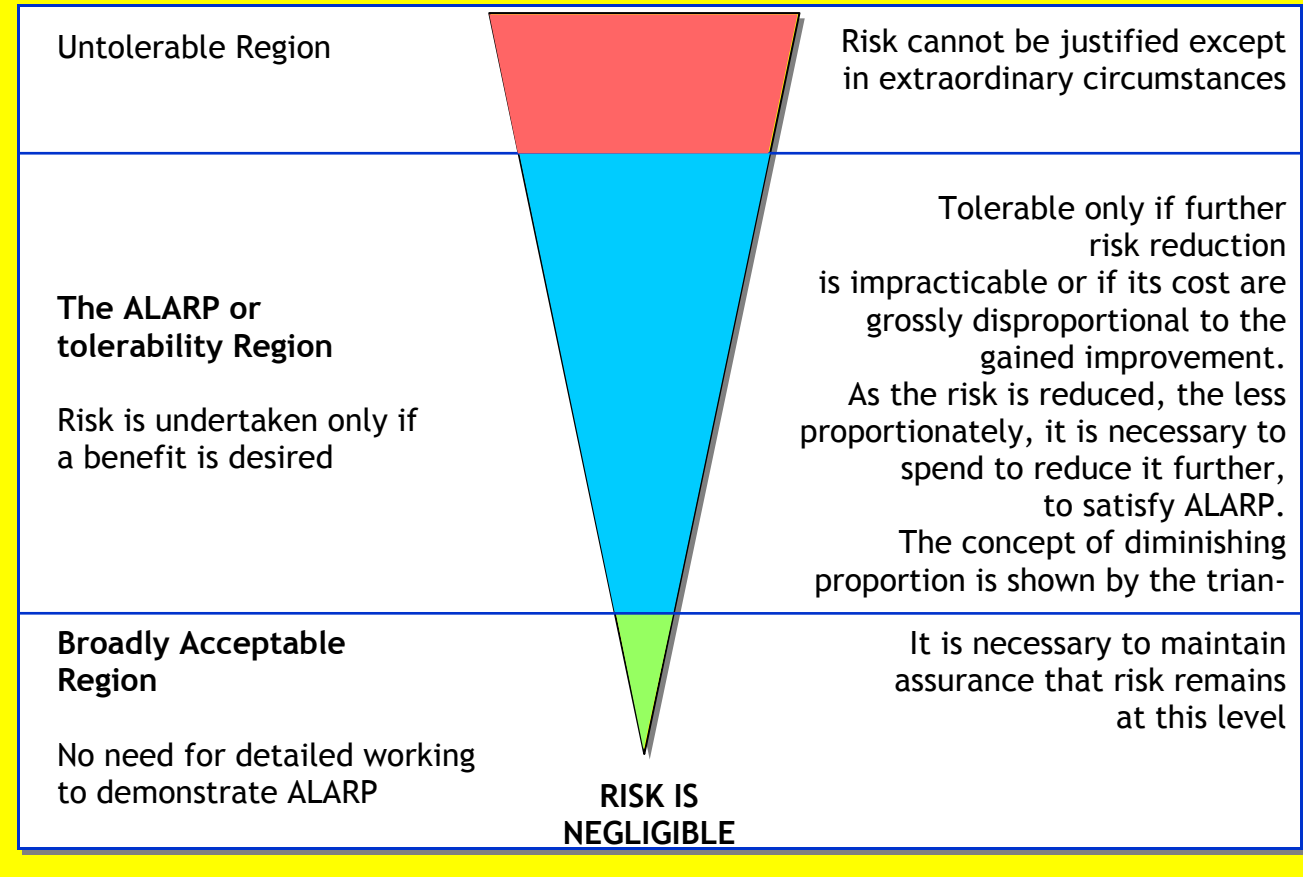


Pool Fire



Fireball

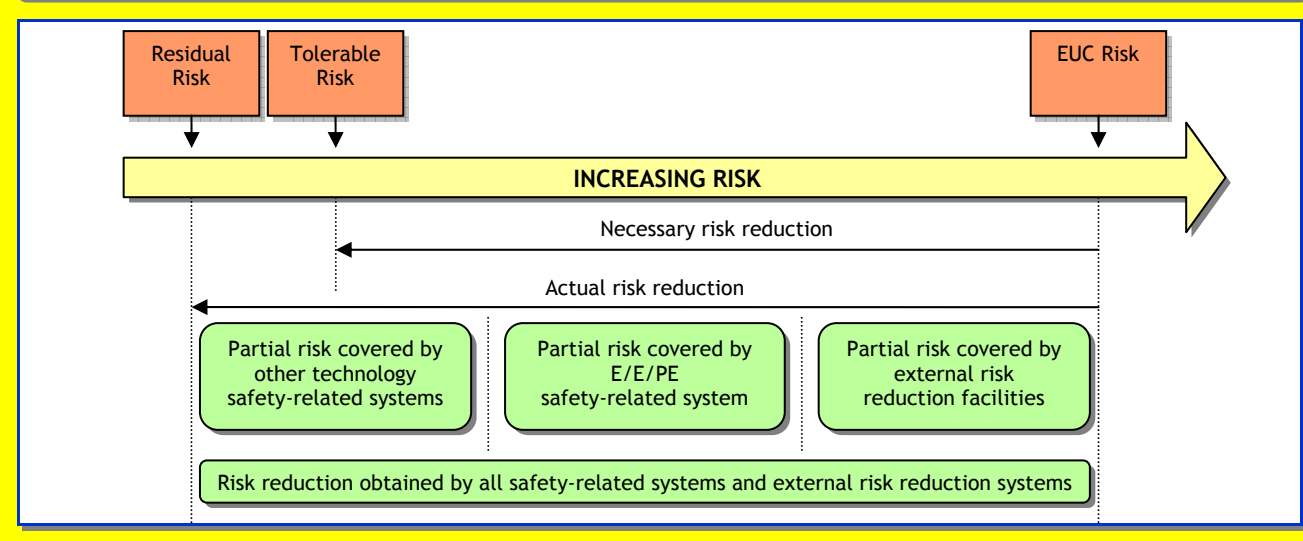
TOLERABLE RISKS AND ALARP (ANNEX 'B')



AVERAGE PROBABILITY OF FAILURE ON DEMAND (PFDavg)

PFDavg	Tolerable accident frequency = $\frac{1}{\text{RRF}}$	
	Without common causes	With common causes (Beta factor)
1oo1	$\lambda_{DU} \times \frac{TI}{2}$	-
1oo2 1oo2D	$\lambda_{DU1} \times \lambda_{DU2} \times \frac{TI^2}{3}$	$\frac{[(1-B) \times (\lambda_{DU} \times TI)]^2}{3} + \frac{(B \times \lambda_{DU} \times TI)}{2}$
1oo3	$\lambda_{DU1} \times \lambda_{DU2} \times \lambda_{DU3} \times \frac{TI^3}{4}$	$\frac{[(1-B) \times (\lambda_{DU} \times TI)]^3}{4} + \frac{(B \times \lambda_{DU} \times TI)}{2}$
2oo2	$(\lambda_{DU1} + \lambda_{DU2}) \times \frac{TI}{2}$	$[(1-B) \times (\lambda_{DU} \times TI)] + \frac{(B \times \lambda_{DU} \times TI)}{2}$
2oo3	$\left[\frac{(\lambda_{DU1} \times \lambda_{DU2}) + (\lambda_{DU1} \times \lambda_{DU3}) + (\lambda_{DU2} \times \lambda_{DU3})}{3} \right] \times \frac{TI^2}{3}$	$[(1-B) \times (\lambda_{DU} \times TI)]^2 + \frac{(B \times \lambda_{DU} \times TI)}{2}$
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

RISK REDUCTION



AVAILABILITY AND RELIABILITY

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

1 FIT = 1×10^{-9} Failures per hour

MTBF = MTF + MTTR

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

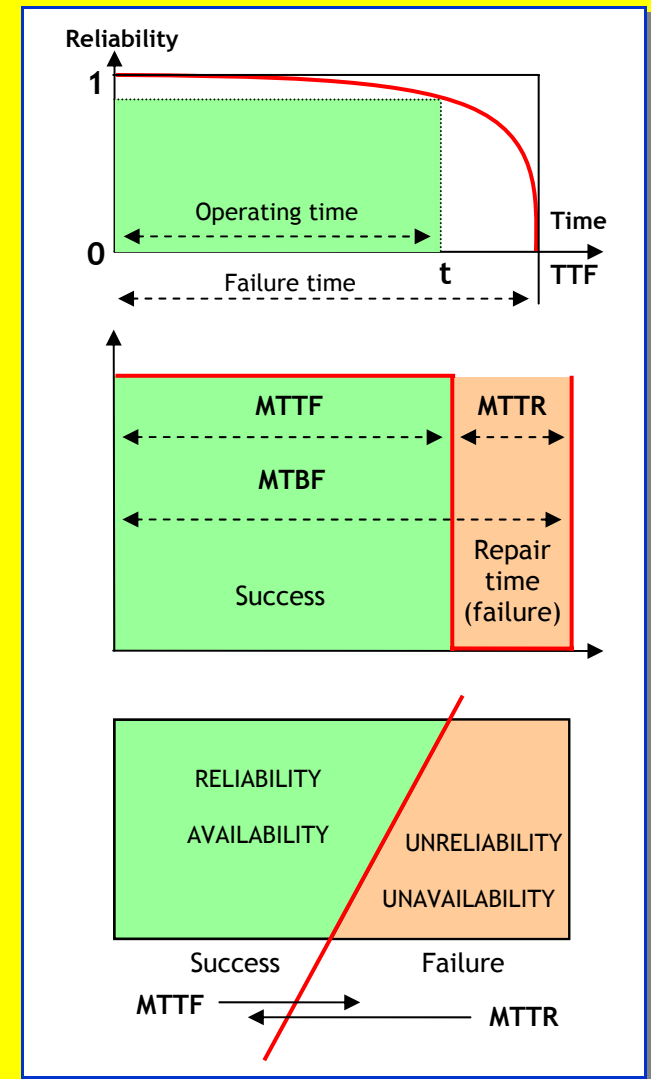
Availability = $\frac{\text{Operating Time}}{\text{Operating Time} + \text{Repair Time}}$

$= \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} = \frac{\text{MTTF}}{\text{MTBF}} = \frac{\mu}{\mu + \lambda}$

$= \frac{\text{MTBM}}{\text{MTBM} + \text{MSD}}$

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

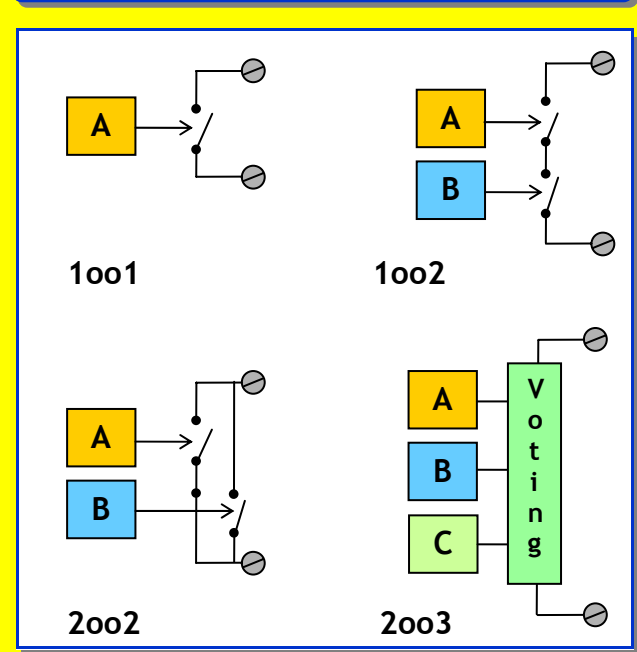
Acronyms:
MTBF: Mean Time Between Failures
MTTF: Mean Time To Failure
MTTR: Mean Time To Repair
MTBM: Mean Time Between Maintenance
MSD: Expected Mean System Downtime



MEAN TIME TO FAILURE SPURIOUS

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

SYSTEM ARCHITECTURES



SAFE FAILURE FRACTION (SFF) AND SIL LEVELS

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			
< 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			
< 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

SAFETY INTEGRITY LEVEL CALCULATION

