IEC 61508

UNDERSTANDING SAFETY INTEGRITY LEVELS

IEC 61511

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)

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

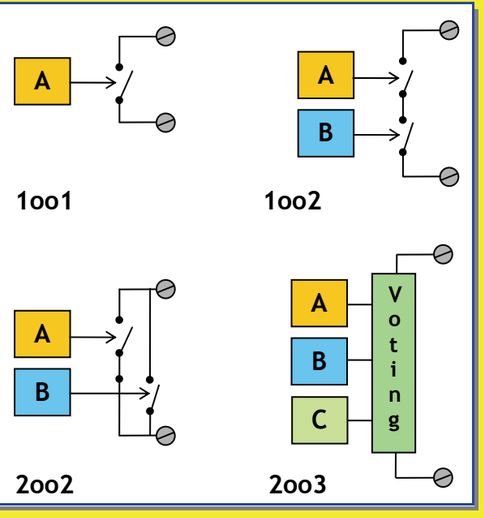
Simplified equations

	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 ($E_t \neq 100\%$)	$\lambda_{DU}\left[\left(Et\times\frac{TI}{2}\right) + (1-Et)\frac{SL}{2}\right]$	TI: Proof Test time interval Et: Test Effectiveness λ_{DU}: dangerous undetected failures

Mean Time To Failure Spurious

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

System Architectures



Safe Failure Fraction (SFF) and SIL Levels

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

	Hardware fault tolerance 0	Hardware fault tolerance 1	Hardware fault tolerance 2
TYPE A Components			
< 60%	SIL 1	SIL 2	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			
< 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 rates categories: λ_{DD}: dangerous detected; λ_{DU}: dangerous undetected
λ_{SD}: safe detected; λ_{SU}: safe undetected

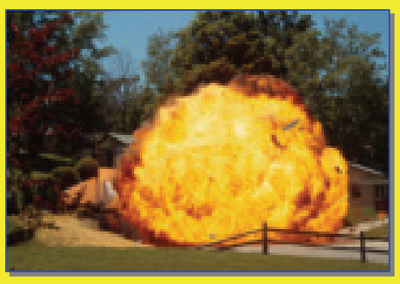
SAFETY: FREEDOM FROM UNACCEPTABLE RISK

Boiling Liquid Expanding Vapor Explosion (BLEVE)

Flash Fire

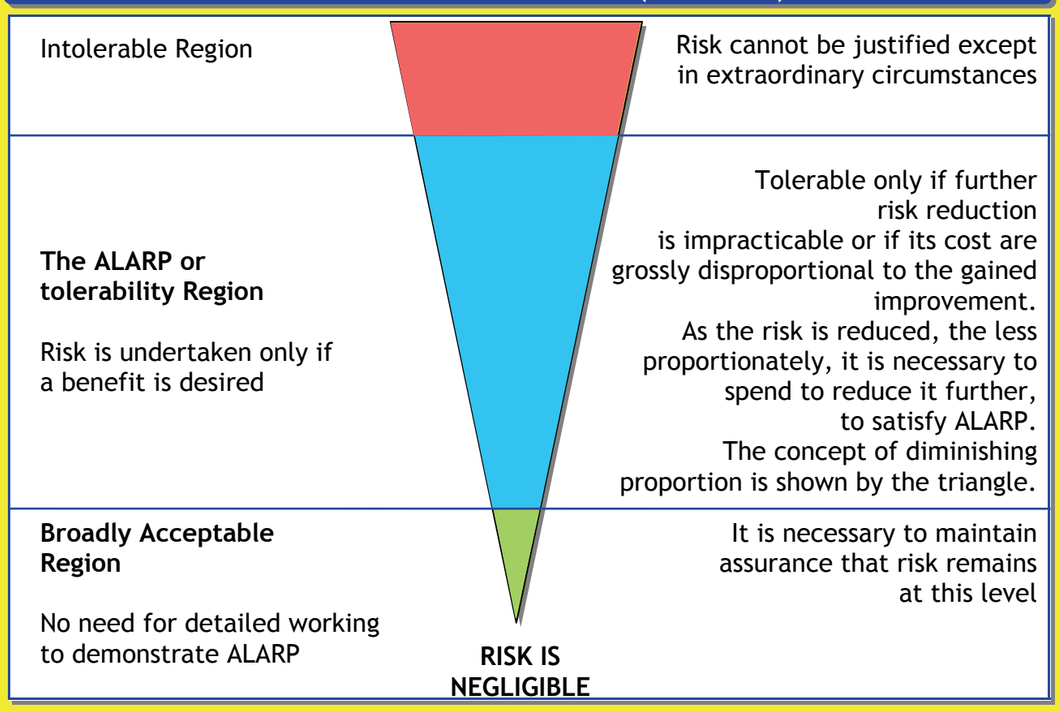
Jet Fire

Pool Fire

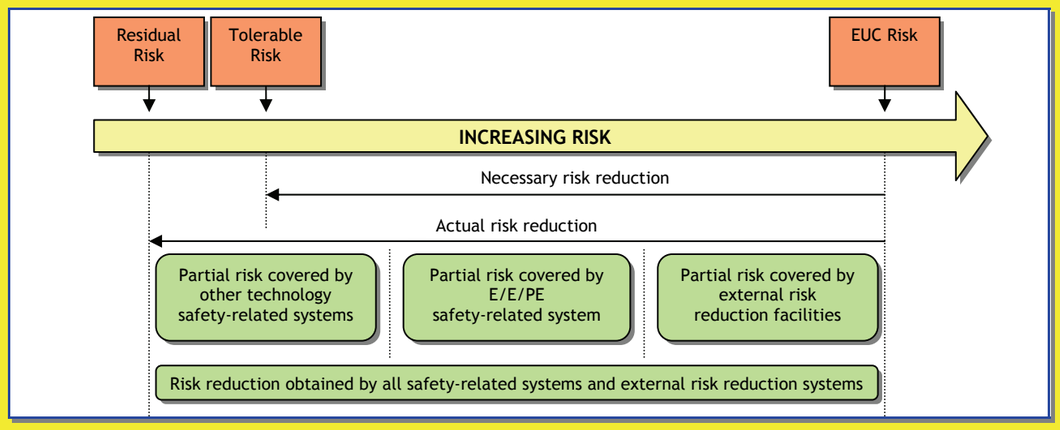


Fireball

Tolerable risks and ALARP (Annex 'B')



Risk Reduction



Availability and Reliability

Basic Concepts:

Failure Rate :

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

1 FIT = 1×10^{-9} Failures per hour

MTBF = MTTF + MTTR

$\mu = \dfrac{1}{MTTR}$

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

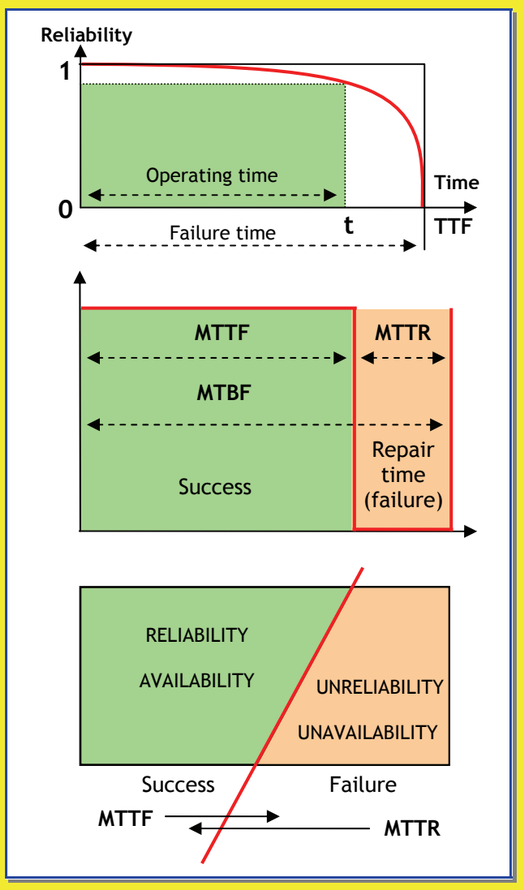
$\lambda = \dfrac{1}{MTTF}$

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

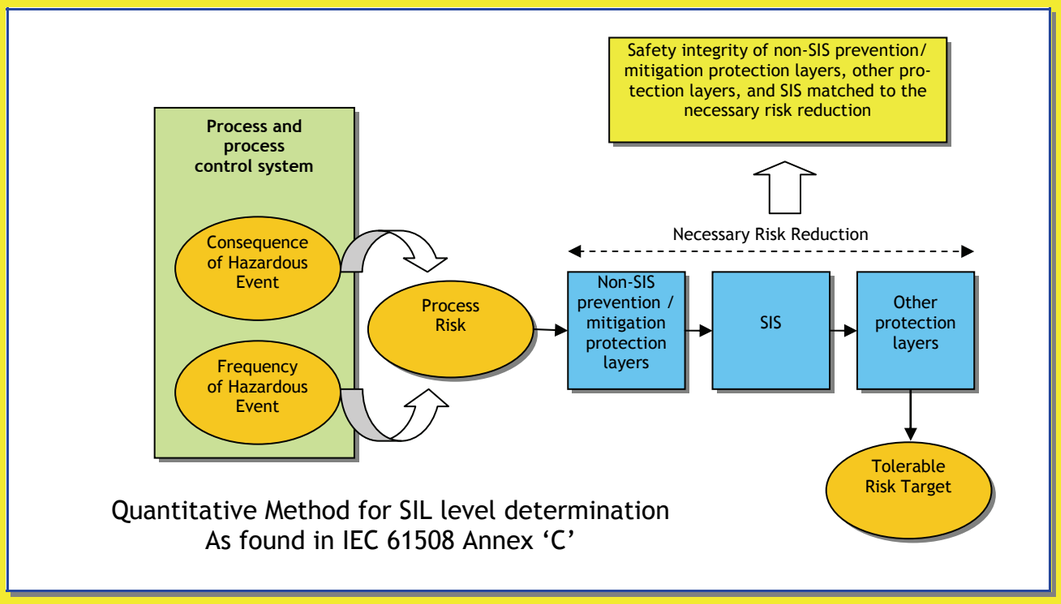
Unavailability = 1- Availability = $\dfrac{\lambda}{\mu}$

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



Safety Integrity Level Calculation



Quantitative Method for SIL level determination
As found in IEC 61508 Annex 'C'

GM INTERNATIONAL
TECHNOLOGY FOR SAFETY

ITALY

G.M. INTERNATIONAL S.R.L
Via San Fiorano, 70
20058 Villasanta (MI)
Tel: +39 039 2325038
Fax: +39 039 2325107

info@gmintsrl.com
www.gmintsrl.com

UNITED STATES OF AMERICA

GM International Safety Inc.
17453 Village Green Drive
Houston, TX 77040
Tel: +1 713 896 0777
Fax: +1 713 896 0782

info@gmisafety.com
www.gmisafety.com