SIL Assessment – Quick Reference

BS EN (/IEC) 61508 Parts 1-7 "Functional safety of electrical/electronic/programmable electronic safety-related systems" – applies to new **SIL (Safety Integrity level)** rated instruments, controllers & valves. Generic safety standard stating 'lifecycle' requirements and guidelines.

BS EN (/IEC) 61511 Parts 1-3 "Functional safety – **Safety instrumented systems (SIS)** for the process industry sector". All Buncefield-type sites should have had overfill prevention systems assessed & comply with this standard, to the HSE's satisfaction, by the end of 2007.

IEC 61511 is for the process industry, IEC 61513 is for the nuclear industry & IEC 62061 is for the machinery sector. **SRS** in IEC 61508 means **Safety Related System**; SRS in IEC 61511 means **Software Requirement Specification**.

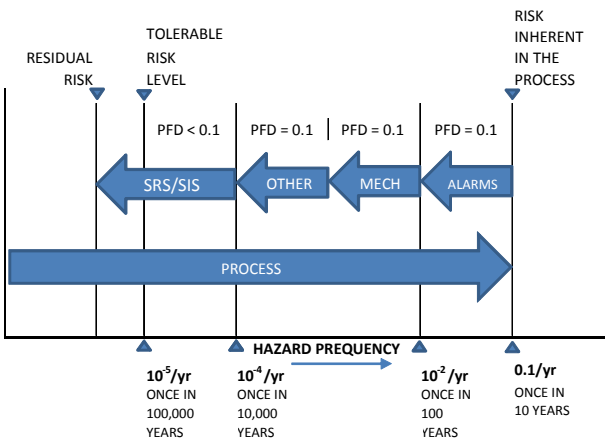
EUC = Equipment Under Control

£1M typical VPF (Value of Preventative Fatality)

Maximum tolerable risk levels:

INDIVIDUAL RISK per annum			
Consequence	Minor/ Serious	Serious/ Fatal	Multi-fatal
Employee	10^{-3}	10^{-4}	10^{-5}
Public	10^{-4}	10^{-5}	10^{-6}

BROADLY ACCEPTABLE RISK (Negligible)			
Consequence	Minor/ Serious	Serious/ Fatal	Multi-fatal
Employee and Public	10^{-5}	10^{-6}	10^{-6}



PFD = Probability of Failure on Demand

LOPA = Layer of Protection Analysis
IPL = Independent Protection Layers
RRF = Risk Reduction Factor

SRS required PFD = Max tolerable risk [pa] / Event likelihood $_{(without\ SRS)}$ [pa]

Event likelihood $_{(without\ SRS)}$ [pa] = Initiating likelihood [pa] x PFD $_{(control\ system)}$ x PFD $_{(alarms)}$ x PFD $_{(mechanical\ protection)}$

SIL Table – **LOW DEMAND** mode of operation

SIL	PFD (probability, unitless)
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

SIL Table – **HIGH DEMAND or CONTINUOUS** mode of operation

SIL	λ_D per hour	~λ_D per year
4	$\geq 10^{-9}$ to $<10^{-8}$	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-8}$ to $<10^{-7}$	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-7}$ to $<10^{-6}$	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-6}$ to $<10^{-5}$	$\geq 10^{-2}$ to $<10^{-1}$

λ_S = failure rate, safe
λ_{DD} = failure rate, dangerous detected
λ_{DU} = failure rate, dangerous undetected

SFF = Safe Failure Fraction
SFF = $(\lambda_S + \lambda_{DD}) / (\lambda_S + \lambda_{DD} + \lambda_{DU})$

Type A Sub System – e.g. valve or simple instrument: Failure modes are well defined, failure behaviour is determined, and there is dependable failure data. Type B Sub System – e.g. programmable controller or instrument.

Type A Fault Tolerance table

SFF	0 (single)	1 (1oo2)	2 (1oo3 or 3oo4)
< 60%	SIL1	SIL2	SIL3
60% - < 90%	SIL2	SIL3	SIL4
90% - <99%	SIL3	SIL4	SIL4
≥99%	SIL3	SIL4	SIL4

Type B Fault Tolerance table

SFF	0 (single)	1 (1oo2)	2 (1oo3 or 3oo4)
< 60%	Not allowed	SIL1	SIL2
60% - < 90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

CCF = Common Cause Failure (typically 5 – 8%)
RBD = Reliability Block Diagram
MTTR = Mean Time To Repair
MDT = Mean Down Time
Tp = Proof Test Interval

Detected failures in simplex (1oo1) systems:
$PFD_{DD} = \lambda_{DD}.MDT = \lambda_{DD}.MTTR$

Undetected failures in simplex systems:
$PFD_{DU} = \lambda_{DU}.Tp/2$

Simplex SIS/SRS: PFD = $\sum PFD_{DD} + \sum PFD_{DU}$

Failure rate per hour x downtime in hours = dimensionless PFD

Failure rate per hour x 8760 hours/year = failure rate/year (useful for LOPA initiating likelihood)