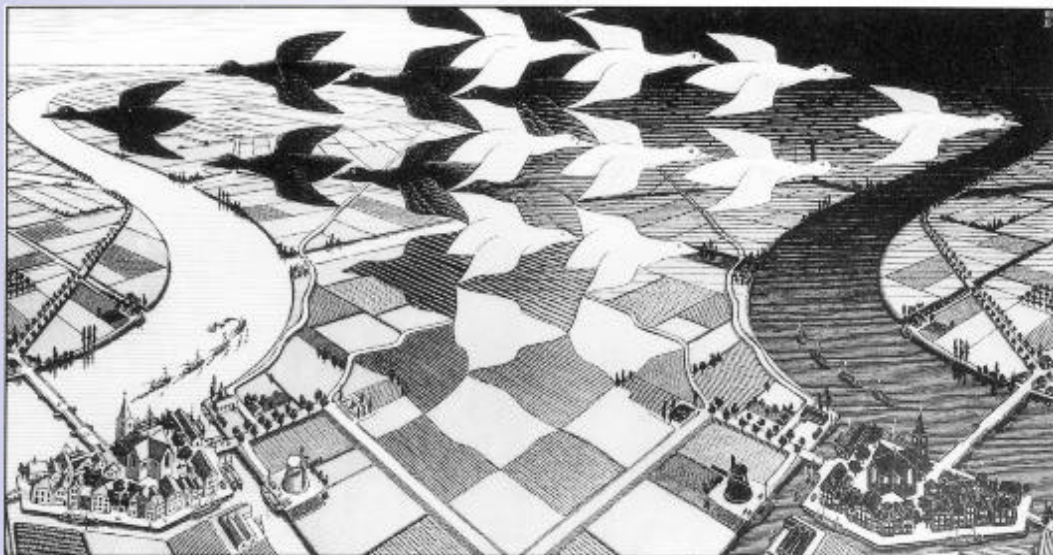© 1938 M.C. Escher/Cordon Art - Baarn - Holland.

ENVIROSIL

GUIDANCE NOTE FOR ENVIRONMENTAL SAFETY INSTRUMENTED SYSTEMS

P & I Design Limited

2 Reed Street, Gladstone Industrial Estate,
Thornaby, TS17 7AF.
Tel: +44 (0) 1642 617444 Fax: +44 (0) 1642 616447
www.pidesign.co.uk
Support: sales@pidesign.co.uk

Contents

References

Gruhn and Cheddie - Safety Shutdown Systems -ISA,1998
IEC 61508 & IEC 61511

1.0 PROTECTION LAYERS

Safety Instrumented Systems (SIS) are designed to monitor the process and control outputs to prevent or mitigate hazardous events.

The design process strives for inherent safety, which is enhanced by applying multiple independent safety layers.

Prevent accidents with prevention layers and minimise the consequences with mitigation layers.

LAYER	DESCRIPTION	KEY ELEMENTS
1	**Process plant design**	HAZID, HAZOP, fault analysis, design procedures, design reviews and design audits
2	**Process control system**	Involve operations in the design process for system structure and graphics hierarchy. This must not be the only safety layer.
3	**Alarm and monitoring systems**	Detect problems at a low hazard level to allow operator intervention to prevent a major hazard. System must be independent of the devices being monitored.
4	**Management and operations**	Testing, operator training and management procedures. Audit control, alarm and monitoring system performance
5	**Safety instrumented systems**	Determine SIL and evaluate SIS. Agree testing frequency. Backstop to failure of safety layer levels 2,3 and 4

2.0 VOTING SCHEMES AND REDUNDANCY

SIS utilise a variety of non redundant and redundant schemes the most common of which are shown in the following table:

SENSORS	PHILOSOPHY
1oo1	Single sensor installed. Used if the system meets the performance requirements
1oo2	Two sensors installed. Only one required to trip. This scheme is more fail-safe than 1oo1 system, but nuisance trip rate is doubled.
2oo3	Three sensors installed. Two required for trip. Used if the frequency of failures have to be minimised.
FINAL ELEMENTS	
1oo1	Single valve installed. Used if the system meets the performance requirements
1oo2	Two valves installed. Only one required to trip. Scheme is susceptible to twice the incidence of nuisance trips than 1oo1 systems.
2oo2	Two valves installed. Both are required to trip. Although 2oo2 voting substantially reduces the probability of nuisance trips, it is twice as susceptible to fail-to-danger of undetected faults.

When calculating the average probability of failure (PFD_{avg}) for a given loop or combination of loops certain assumptions have to be made concerning the configuration for a dangerous failure.

Consider the following examples:

1) Two shut off valves in series where only one is required to operate to stop the flow is a 1oo2 system. Despite the system calling for both valves to operate on tripping. It is not a 2oo2 system.
2) Two switches in parallel where both are required to operate to trip is a 2oo2 system.
3) Two temperature sensor/trip amplifier combinations where only one is required to operate to trip is a 1oo2 system.
4) Invariably one device will be a 1oo1 system. An arrangement where a number of devices for example "n" relays in a group could be treated in a variety of ways depending on their configuration; the most conservative being to treat as "n" 1oo1 arrangements.

3.0 DETERMINING THE SAFETY INTEGRITY LEVEL (SIL)

Each hazard has its associated level of risk determined by the frequency or probability and severity.

The US military standard MIL-STD 882 presents a method based on categorising frequency and severity into five qualitative levels resulting in a subjective approach. This method is adopted by the Lihou HAZOP procedure marketed and used by P & I Design.
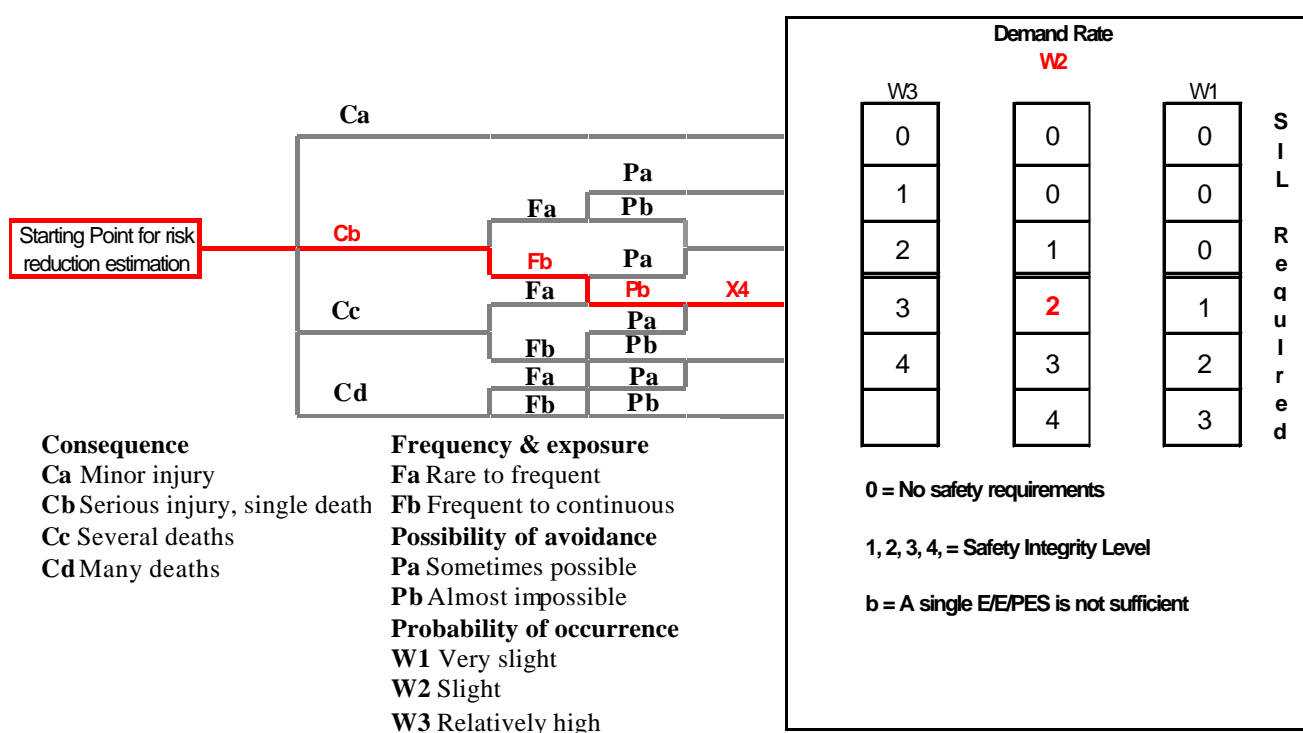
As an initial basis for relating the level of risk to the level of performance of the safety system the following table has been proposed. This table should be monitored against current IEC standards.

Correlation between Overall Risk Level and Required Safety System Performance

Risk Level	Safety Integrity Level SIL	Required Safety Availability	Probability of Failure on Demand PFD	Risk Reduction Factor
	4	>99.99%	<0.0001	>10000
High	3	99.9-99.99%	0.001-0.0001	1000-10000
Medium	2	99-99.9%	0.01-0.001	100-1000
Low	1	90-99%	0.1-0.01	10-100

3.1 Safety Case SIL Risk Graph

The IEC standard 61511-3 in Figure D1 has adopted a procedure for ranking the risk to personnel as shown in the flowchart detailed below which is still subject to "calibration"

Consequence
Ca Minor injury
Cb Serious injury, single death
Cc Several deaths
Cd Many deaths

Frequency & exposure
Fa Rare to frequent
Fb Frequent to continuous
Possibility of avoidance
Pa Sometimes possible
Pb Almost impossible
Probability of occurrence
W1 Very slight
W2 Slight
W3 Relatively high

0 = No safety requirements

1, 2, 3, 4, = Safety Integrity Level
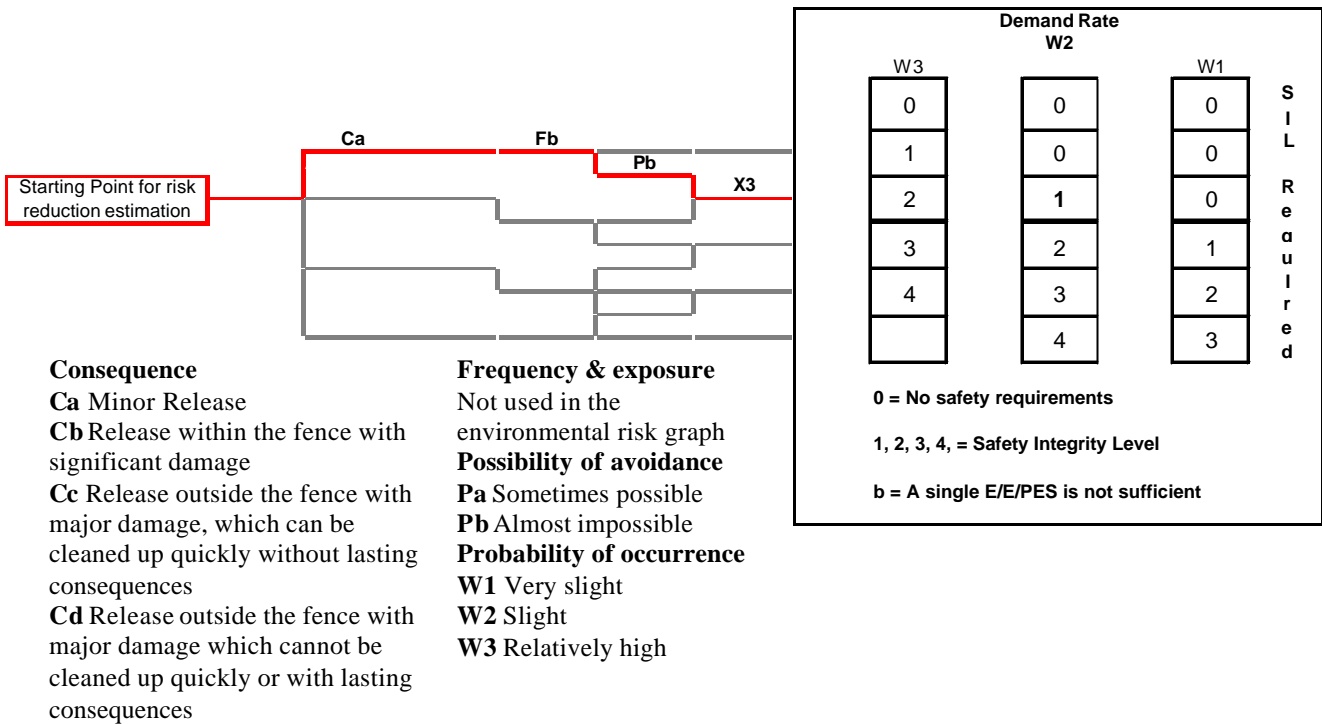
b = A single E/E/PES is not sufficient

P&I Design have developed a software toolkit XLSILSAF which enables a rapid evaluation of the SIL using the above IEC approach.

XLSILSAF provides multiple selection of the parameter combinations and a dynamic flowchart indicating the SIL selected.

3.2 Environmental Case SIL Risk Graph

The IEC standard 61511-3 in Figure D2 has adopted a procedure for ranking the risk to the environment as shown in the flowchart detailed below which is still subject to "calibration"

Consequence
Ca Minor Release
Cb Release within the fence with significant damage
Cc Release outside the fence with major damage, which can be cleaned up quickly without lasting consequences
Cd Release outside the fence with major damage which cannot be cleaned up quickly or with lasting consequences

Frequency & exposure
Not used in the environmental risk graph
Possibility of avoidance
Pa Sometimes possible
Pb Almost impossible
Probability of occurrence
W1 Very slight
W2 Slight
W3 Relatively high

P&I Design have developed a software toolkit XLSILENV which enables a rapid evaluation of the SIL using the above IEC approach.

XLSILENV provides multiple selection of the parameter combinations and a dynamic flowchart indicating the SIL selected.

4.0   SAFETY INSTRUMENTED SYSTEM (SIS) EVALUATION

An SIS can fail in one of two ways:-

A **safe failure** resulting in the system functioning when not required to resulting in a nuisance trip or initiating failure which shuts the plant down when nothing was wrong.

A **dangerous failure** resulting in the system not functioning or inhibited from responding when required to which results in the plant not shutting down when something was wrong. Only testing will find this failure.

Mean time between failures (MTBF) in years or mean time to failure (MTTF) are used for evaluation. It should be appreciated that a device can have an MTBF of 3000 years but not have a useful life of 3000 years because what we are saying is that out of 3000 items we can expect one failure per year.

The failure rate (failures/year)
$$\lambda = \frac{1}{MTBF} = \lambda_s + \lambda_d$$

λ_s safe(initiating) failure rate
λ_d dangerous (inhibiting) failure rate
x_s safe failure split fraction
x_d danger failure split fraction
n   number of components or sets(groups) under consideration

Where
$$\lambda_s = \lambda\, x_s \qquad\qquad \lambda_d = \lambda\, x_d \qquad\qquad x_s + x_d = 1$$

Mean time between failures based on safe split
$$MTBF_{sp} = \frac{1}{\lambda_s}$$

The formulae for safe failures (nuisance trip) are as follows where **MTTR** mean time to repair in years where $1/MTTR \gg \lambda$ and that safe failures are revealed in all systems including 2oo2 and 2oo3.

1oo1
$$MTBF_{sp} = \frac{1}{n\,\lambda_s}$$

1oo2
$$MTBF_{sp} = \frac{0.5}{n\,\lambda_s}$$

2oo2
$$MTBF_{sp} = \frac{0.5}{n\,\lambda_s^2\,MTTR}$$

2oo3
$$MTBF_{sp} = \frac{0.1667}{n\,\lambda_s^2\,MTTR}$$

The formulae for dangerous failures (inhibiting), the average probability of failure on demand **PFD$_{avg}$** for undetected failures are as follows where **TI** is the manual test interval

1oo1
$$PFD_{avg} = 0.5\ n\ \lambda_d\,TI$$

1oo2
$$PFD_{avg} = 0.333\ n\ \lambda_d^2\,TI^2$$

2oo2
$$PFD_{avg} = n\ \lambda_d\,TI$$

2oo3
$$PFD_{avg} = n\ \lambda_d^2\,TI^2$$

P & I Design have developed a software toolkit XLPFD which enables a rapid evaluation of the PFD$_{avg}$ using the above formulae for a wide variety of loop and system configurations.