Assessment of the Safety Integrity of Electrical Protection Systems in the Petrochemical Industry

Author: Colin Easton
ProSalus Limited ~ Independent Safety Consultants

1. Introduction

Within the United Kingdom process industries the functional safety standard IEC 61511 [2] is now recognised by the Health and Safety Executive (HSE) as relevant good practice for the design, installation, operation, maintenance and decommissioning of protection systems in the process industry sector. It is HSE's view that if the requirements of IEC 61511 are met, thereby demonstrating that the risks under the control of protection systems have been reduced to a level that can be considered as low as reasonably practicable, enough will have been done to comply with UK Health and Safety law so far as protection systems are concerned.

The Safety Integrity assessment is a process that reviews and assesses a SIS based on the consequences of previously identified hazardous events. The verification process focuses on the ability of a protection system to meet the recommendations of IEC 61511 and the system design intent. The verification process examines the proposed protection system components and functions for purpose and adequacy and will determine what measures of protection and intervention they perform to minimise the risks of an incident and will establish what, if any remedial works are required to the system.

The IEC 61511 standard is concerned with the functional safety of process plant protection systems. It requires:

- That a hazard and risk assessment is carried out to identify the overall safety requirements, this usually takes the form of a HAZOP study which is then used to develop the site's safety management system and COMAH compliance strategy.
- That an allocation of the safety requirements to the protection system(s) is carried out.
- That a business works within a framework which is applicable to all methods of achieving functional safety.
- Detailed use of certain activities, such as safety management, which may be applicable to all methods of achieving functional safety, this is normally addressed by the site's safety management system.

IEC 61511 covers the whole safety lifecycle from design, installation, operation, maintenance and decommissioning and requires that an evaluation of the protection systems is undertaken and that all components of the protection system are considered as a part of that evaluation.

Electrical supply protection forms apart of the overall protection system and must therefore be considered in the evaluation. Recently published "Guidance on the assessment of electric protection systems" by the Energy Institute (ref [3]) has added to the existing guidance and has now introduced a framework for applying IEC 61511 to electrical supply protection systems

The objective of this paper is to introduce to the electrical engineer to the concepts of functional safety as described in IEC 61511 and to describe were the EI guidance fits within the overall safety lifecycle when applied to an electrical project to provide assurance that the identified protection function is capable of achieving the required contribution to risk reduction.

2. Tolerability of Risk and the Identification of Hazards and Safeguards

The assessment of protection systems commences with the identification of the hazards associated with a business undertaking. One of the most popular hazard identification techniques is the hazard and operability study report, (HAZOP), which is a systematic assessment of the plant to identify causes / consequences of plant deviations from design intent and an assessment of the adequacy of safe guards, intended to protect the plant form these deviations. Fig-1 gives an overview of typical risk reduction methods as identified in IEC 61511.

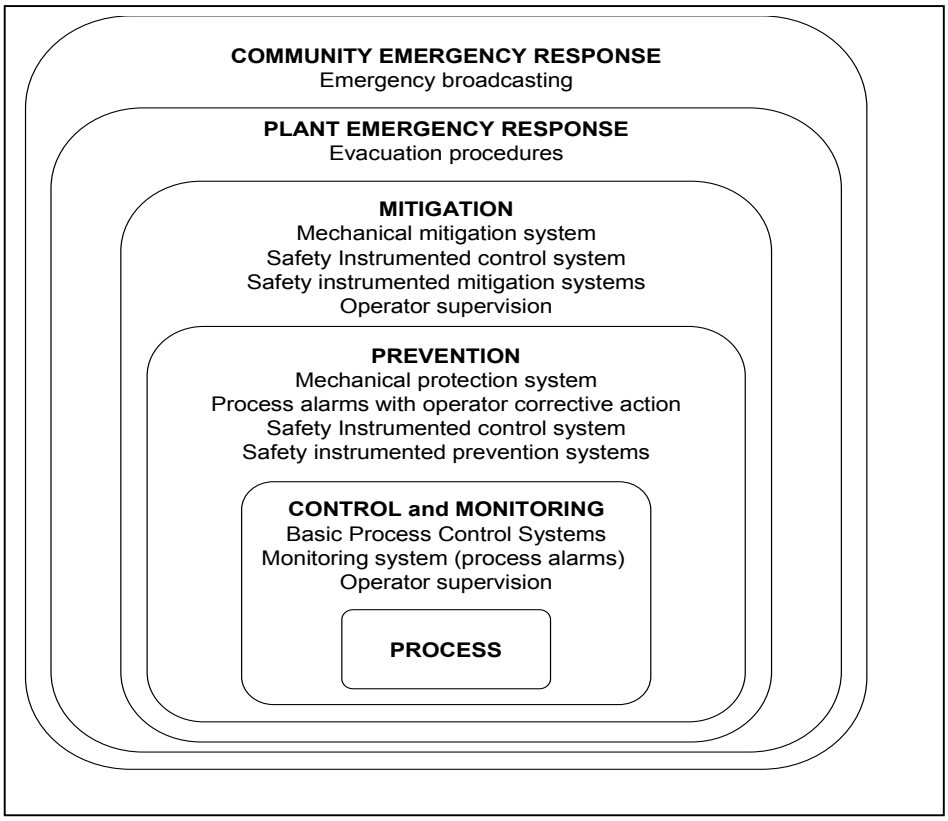


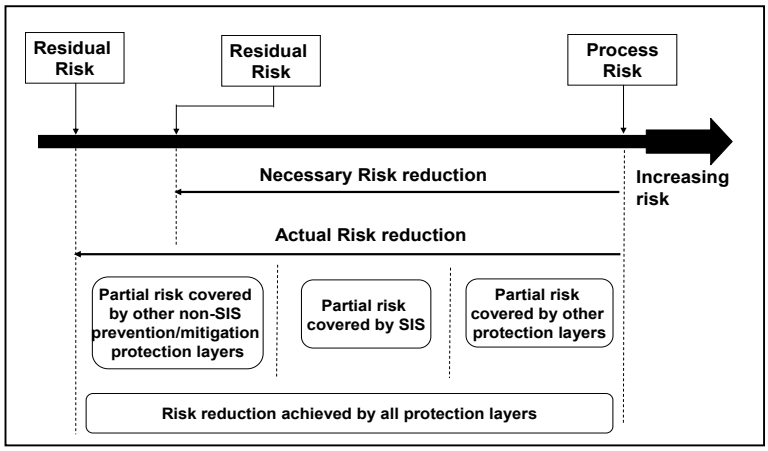
Fig - 1: From IEC-61511; typical plant safeguards found in process plants

The HSE require that the risks from hazards identified in the HAZOP are reduced to a level that can be considered as low as reasonably practicable, thereby demonstrating that the business has the risks under the control, this is commonly termed the ALARP argument.

The ALARP argument essentially means weighing a risk against the trouble, time and money needed to control it. The decision making process requires the company to exercise 'judgement', apply 'good practice' and for high risk situations use formal techniques including cost benefit analysis to form a judgement. IEC 61511 is recognised by the Health and Safety Executive (HSE) as relevant good practice and as such is acceptable as a part of the ALARP argument (Ref 4, 5, 6 & 7)

The necessary risk reduction may be achieved by either one or a combination of protection layers, such as electrical protection in the form of stopping an electric pump or fan by disconnecting the supply to it.

The figure below, taken from IEC 61511, illustrates the general concepts of risk reduction.The various risks indicated are as follows:

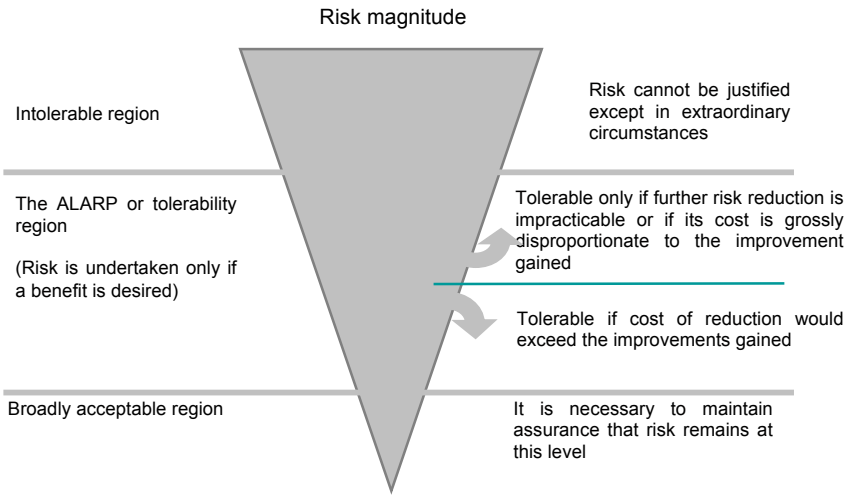


Process risk:

The hazards and risks for a specific plant as identified in the HAZOP, these are generally cause by equipment failures, control system failures or human error. Safeguards are not considered when evaluating the process risk although the protection provided by the control system is, but, it's contribution to risk reduction is limited to one order of magnitude.

Tolerable risk:

The figure opposite shows the general concepts of the "ALARP" principle and in order to apply this principle a tolerable criterion must be set by the business to determine what levels of risk are considered tolerable and which are considered intolerable. Intolerable risks can not be justified on any grounds and therefore any risks within this region must be reduced to a level considered tolerable.



The tolerable risk criteria identified in "Guidance on the assessment of electric protection systems" by the Energy Institute (ref [3]) is a probability value for serious injury or fatality to an individual worker of no more than 1.0E-5/yr. The UK tolerability of risk framework used in HSE guidance (ref [4], [5], [6] & [7] indicates an upper limit of a risk of death to any individual worker at a frequency of one in one thousand per annum therefore the EI guidance criteria is two orders of magnitude less than that which is considered as a reasonable maximum and is only one order of magnitude above what is considered to be a broadly acceptable risk to any individual worker 1.0E-6/yr.

This means that any assessment undertaken using the EI risk criteria for electrical plant failure will be at least 100 times more conservative than a general risk assessment using the HSE criteria for a individual worker and would usually be considered as the criteria for multiple fatalities.

Residual risk:

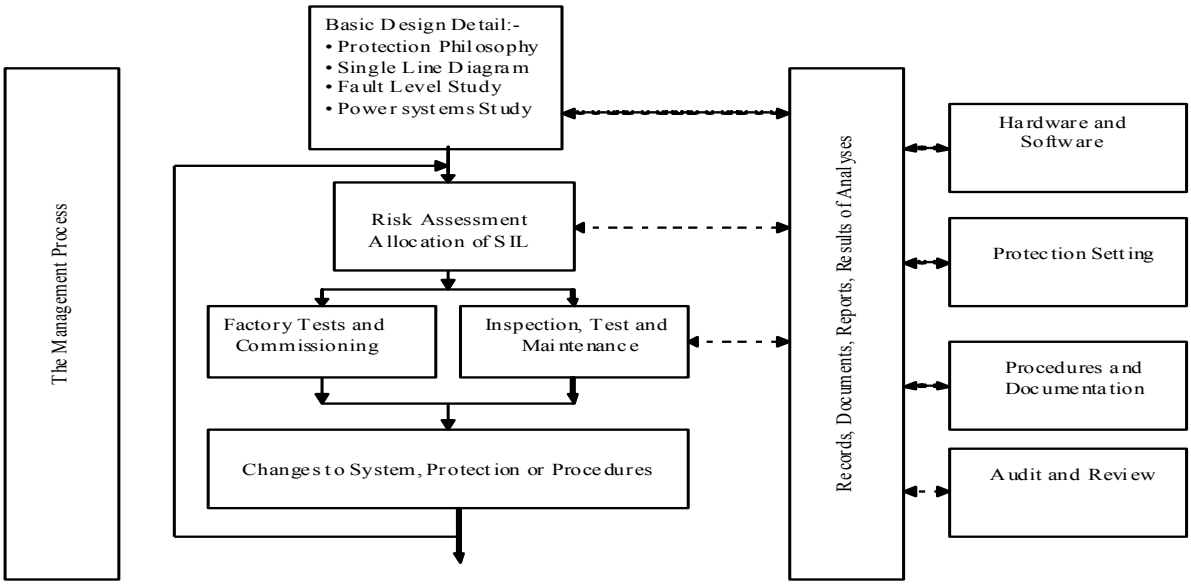
The residual risk is the risk of a hazardous event occurring after the addition of all protection systems and is sometimes designated as the background risk, for example slips trips and falls.

Safeguards:

As discussed above several layers of protection will be employed to reduce the risk to an acceptable level and electrical protection systems can form a part of those layers of protection. The problem with any protection layer is that the design, installation, operation, maintenance and decommissioning must be considered; this is addressed by applying a whole safety lifecycle approach to each protection system

3. IEC 61511 Safety Lifecycle Approach and the EI Guidance

The safety lifecycle for electrical protection systems is detailed below:



By permission of the Energy Institute

3.1. Identification of relevant documentation for protection system assessment

The first step in the life cycle is to identify information for the protection system under review, these drawings should include:

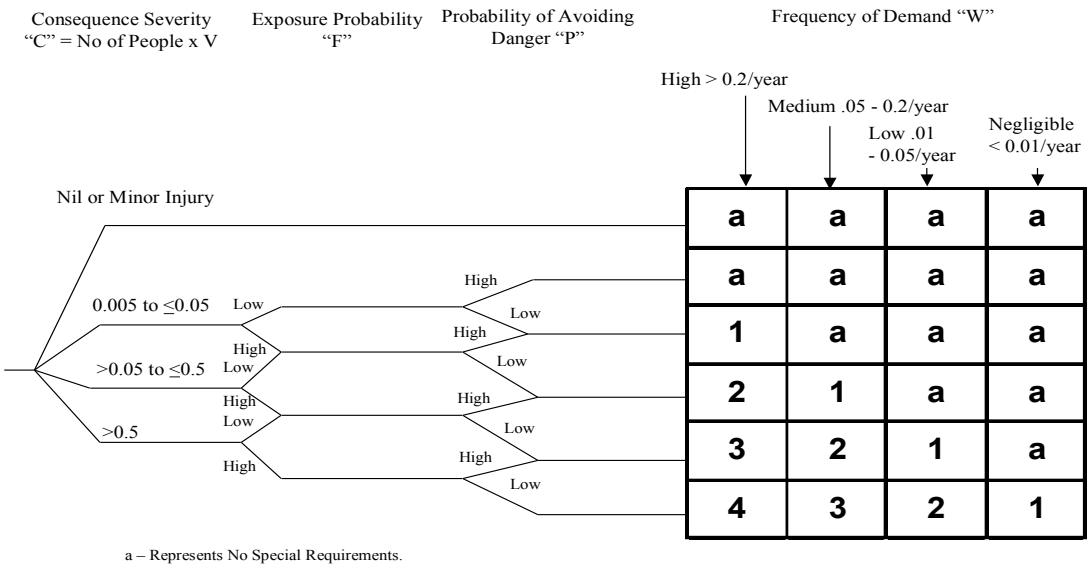
1. Plant Hazard and Operability Study (HAZOP)
2. Plant Process and Instrument diagrams (P&ID)
3. System Block Diagrams
4. Single Line Diagrams (SLD)
5. Circuit Diagrams
6. Plant layout drawings
7. Plant Operating Procedures
8. Control and Electrical protection philosophy.
9. Power System study
10. Operating and Maintenance Manuals for equipment
11. Site Safety Health and Environmental (SHE) Management System
12. Site maintenance and test records
13. Site Maintenance training records

The assessment process comprises two main stages. The first stage is an evaluation of the risk reduction contribution required from the protection system ((target safety integrity level (SIL)) and the second stage is a numerical evaluation of the system to verify that the required risk reduction contribution can be achieved (Achieved safety integrity level). For this stage historical or estimated failure data and information about the quality systems / control, current status, remaining life and serviceability of equipment needs to be obtained. Where possible, original equipment manufacturers data sheets should be

used annex b of the EI guidance provides reliability data for the most common elements of electrical protection systems.

3.2. Safety Integrity Level Determination using the Risk Graph method

The second step, the SIL Determination methodology should be based on that described in IEC 61511 (ref [2]), and requires a team of experienced people. The risk graph calibration parameters contained in the EI guidance annex A (ref [3]); provide typical examples for use in process industry applications. A typical example is shown below



a	a	a	a
a	a	a	a
1	a	a	a
2	1	a	a
3	2	1	a
4	3	2	1

Figure 1 SIL Graph for safety risk assessment (Copyright Energy Institute)

In this methodology, the hazards due to each electrical protection failure are assessed. The aspects of Consequence, Exposure probability, Possibility of Avoidance of danger and Frequency of demand are scored using the calibrated Risk graph for the hazard resulting in a qualitative risk assessment for each protection system based on the probability value for serious injury or fatality to an individual worker of no more than 1.0E-5/yr which defines the target SIL required. Using this method a worksheet is produced for each protection system which describes the critical performance aspects for the protection system in protecting safety, environment and commercial

The methodology for conducting the SIL Determination was as follows:

- Identify the potential hazard.
- Consider the hazardous event.
- Assess the Consequences of the hazardous event should the protection function fail.
- Assess the Exposure probability.
- Assess the Possibility of avoiding danger.
- Assess the frequency of demand.
- Repeat until all hazards have been analysed.

The study team should be composed of a combination of personnel consisting of an:

Experienced facilitator

Electrical engineer

Instrument Engineer

Process engineer

Maintenance

Operations

Safety

The results of the study are normally recorded live during the meeting in the meeting using an appropriate software tool projected onto a screen for all team members to view.

3.3. Safety Integrity of Safety Instrumented Functions

The performance criteria for the protection system, the target safety integrity level, also identifies the target hardware integrity probability of failure on demand (PFDavg) and this numerical value is shown in IEC61511-1 Table - 3: Safety Integrity Levels (Low Demand Mode).

SIL Level	Average probability of failure to perform its design function on demand
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 $< 10^{-1}$

Key aspects of the verification are dependant upon the system-operating mode, which is defined as either Low Demand or High Demand (or continuous) Mode. Based on plant historical data a Low Demand Mode of operation is considered when a demand will not placed on the protection system more than once per year or twice the proof test interval.

4. SIL Verification

The lifecycle approach now advances to check the validity of the claim of the SIL capability for the protection function. The SIL Verification must be carried out using the techniques referenced in IEC 61508 (ref [1]) and the EI guidance annex D (ref [3]).

For each component in the protection system, its "SIL capability" is evaluated, that is the maximum SIL for which it can be used within a system while meeting the requirements of BS EN 61508. This is achieved in one of three ways.

1. Component certification, or evaluation, which deems it suitable for use up to a given SIL
2. Demonstrate "prior use" according to BS EN 61511 (Ref [2]) in which case a simplified set of requirements, as defined by BS EN 61511 are applied to evaluate SIL capability
3. If "Prior Use" cannot be demonstrated, the requirements of BS EN 61508-1, BS EN 61508-2, BS EN 61508-3 and BS EN 61508-6 are used to identify SIL capability.

4.1. Architectural Constraints on Hardware Safety Integrity (61508-2 Sect 7.4)

The evaluation procedure should include analysis of hardware fault tolerance for each protection system. The required hardware fault tolerance is assessed in respect to the tables below to identify if any concession can be claimed for the protection system based on the achieved Safe failure Fraction, the ratio of the undetected dangerous failure rate to the total failure rate of the protection system, as stated in vendor data, independent body report or estimated from vendor supplied data and failure data.

The protection systems are classified as either 'Type A' or 'Type B' in respect to architectural constraints depending on the known vendor data, programmable electronic features and failure characteristics of the devices (BS EN 61508-2 (Ref [1]).

An example of the failure characteristics of a 'Type A' system are:

a. The failure mode of all constituent components is well defined;

b. The behaviour of the subsystem under fault conditions can be completely determined;

c. There is sufficient dependable failure data from field experience to show the claimed rates of failure for detected and undetected dangerous failures are met (BS EN 61508-1 7.4.7.3 and 4).

The 'Type A' system architectural constraints are described in table 1 below.

Table 1 - Type "A" Component Hardware Tolerance

Safe Failure Fraction	Hardware fault tolerance (see note 1)		
	0 (note 2)	1	2
< 60%	SIL1	SIL2	SIL3
60% - < 90%	SIL2	SIL3	SIL4
90% - 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

NOTE 1 Hardware fault tolerance is the maximum number of faults in a subsystem, arising from random hardware failures that can occur without leading to a dangerous failure of the SIS.
NOTE 2 A hardware fault tolerance of zero means a single fault could cause a dangerous failure (see note 3).
NOTE 3 A dangerous failure is a failure, which has the potential to put the SIS into a hazardous or fail to function state.

An example of the failure characteristics of a 'Type B' system are:

a. The failure mode of at least one constituent component is not well defined;

b. The behaviour of the subsystem under fault conditions cannot be completely determined;

c. There is sufficient dependable failure data from field experience to show the claimed rates of failure for detected and undetected dangerous failures are met (BS EN 61508-1 7.4.7.3 and 4).

The 'Type B' system architectural constraints are described in table 2 below.

Table 2 - Type "B" Component Hardware Tolerance

Diagnostic coverage	Hardware fault tolerance (see note 1)		
	0 (see note 2)	1	2
None (0%)	Not allowed	SIL1	SIL2
Low (60%)	SIL1	SIL2	SIL3
Medium (90%)	SIL2	SIL3	SIL4
High (99%)	SIL3	SIL4	SIL4

NOTE 1 Hardware fault tolerance is the maximum number of faults in a subsystem, arising from random hardware failures that can occur without leading to a dangerous failure of the SIS.
NOTE 2 A hardware fault tolerance of zero means a single fault could cause a dangerous failure (see note 3).
NOTE 3 A dangerous failure is a failure, which has the potential to put the SIS into a hazardous or fail to function state.

4.2. Average PFD/dangerous failure rate

When applying the EI guidance to hardware SIL verification evaluations the calculation of the probability of failure on demand (PFDavg) is based on the per unit time that the protection system is unavailable.

If the protection system is based on a simplex hardware configuration i.e. zero fault tolerance then the probability of failure on demand (PFDavg) is equal to the failure rate per annum of the protection system multiplied by the functional test interval.

$$\mathbf{PFDavg = r \times u/2}$$

Where

r = the failure rate, per year of the protection system

u = No of years to detect protection failure. This is effectively the functional test interval.

To account for back up or other protection system arrangements a more complex reliability analysis is necessary. However the EI guidance offers a more simplified approach to take account of typical arrangements and terminology for electrical power system protection.

For the purposes of rapid assessment the PFD may be approximated by: -

$$\mathbf{PFDavg = r \times u/2 \times s \times t \times v}$$

Where: -

s = A factor accounting for other independent protection on the same circuit

t = A factor accounting for other independent protection that trips upstream circuits.

v = A factor to account for any trip circuit supervision

.

4.3. Systematic safety integrity

BS EN 61508 includes a number of qualitative requirements, which must be met in order for a given SIL capability to be claimed for a protection system. These requirements help to ensure that systematic safety integrity is assured during the system build, installation and commissioning, and is preserved during operation, maintenance and subsequent modification.

The SIS firmware will be built in accordance with BS EN 61508-3 (ref [1]). This includes application software development tools.

The application software must be developed in accordance with either BS EN 61508-3 (ref [1]) or BS EN 61511-1, section 12 (ref [2]) to assure that the application software for each programmable device will meet the target SIL for the protection system. To provide assurance that the application software has been developed in accordance with the standards a functional safety plan should be developed documenting the specifications and reports prepared that validate that the safety requirements as defined by the risk assessment have been met. These project documents prepared should at least include:

a. Functional Safety Management Plan
b. Component and sub-system selection schedule
c. SIS Validation Plan
d. Design Specification (Incorporating Hardware and Software Design)
e. Test Specification (Incorporating Hardware and Software Tests)
f. Safety Manual (incorporating O&M)

4.4. Confirmation of achieved SIL for Protection System

The achieved SIL will be confirmed as the lowest of the achieved SIL ratings identified for:

- Each component of the protection system;
- The protection system as a whole as governed by its average PFD;
- The system as a whole as constrained by the systematic requirements.

Where the achieved SIL is clearly capped by a single component, that single element should be reviewed again to reconfirm that it is absolutely a constraint. This is done to give additional confidence that a higher level of overall system integrity cannot be claimed.

5. References

1. IEC 61508 Functional safety of E/E/PES systems, Parts 0-7
2. IEC 61511 Safety Instrumented systems for the process industry sector, Parts 1-3
3. Guidance on assessing the safety integrity of electrical supply protection – ISBN 9780 852934688 (2006)
4. Reducing Risks, Protecting People, HSE decision making process (R2P2) ISBN 0 7176 2151 0
5. HSE - Principles and guidelines to assist HSE in its judgement that duty-holders have reduced risk as low as reasonably practicable.
6. HSE – Assessing compliance with the law in individual cases and the use of good practice
7. HSE – Policy and Guidance on reducing risks as low as reasonably practicable in design
8. Managing Competence for Safety-related Systems, HSE 2007
9. Safety, Competency and Commitment – Competency Guidelines for Safety-Related Systems Practitioners 1999: The Institution of Electrical Engineers

6. Abbreviations

Term	Description
BPCS	Basic Process Control System
β	Beta Factor - the proportion of failures attributable to a common cause
E/E/PE	Electrical / Electronic / Programmable Electronic
FSA	Functional Safety Assessment
FSCA	Functional Safety Capability Assessment
IPL	Independent Protection Layer
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
MTTR	Mean Time to Repair
PFDavg	Average Probability of Failure on Demand
RRF	Risk Reduction Factor
SFF	Safe Failure Fraction - Ratio of the Undetected Dangerous Failure rate to the Total Failure Rate of the system or Subsystem. (SFF does not include any faults detected by proof tests.)
SIF	Safety Instrumented Function
SIL	Safety Integrity Level