Applying the latest standard for Functional Safety - IEC 61511

1.1 Authors

A G Foord, W G Gulland, C R Howard, T Kellacher, W H Smith (4-sight Consulting)

1.2 Synopsis

This paper focuses on a technique for risk assessment, Layer of Protection Analysis (LOPA), that is relatively new to Europe and compares it with two established techniques: Quantitative Risk Assessment (QRA) and Risk Graphs. It describes our experience in applying the latest standard for functional safety "BS IEC 61511:2003 Functional Safety - Safety Instrumented Systems (SIS) for the Process Industry Sector" [1]. The main lessons learned are illustrated by real examples, changed to preserve confidentiality but still illustrating relevant issues.

1.3 Acknowledgements

Section 3.5 was first published by Springer [2] and we are grateful to them and the Safety Critical Systems Club for permission to include it. The other definitions in Section 3 and Section 9 are quoted from IEC 61511 [1].

2 Introduction

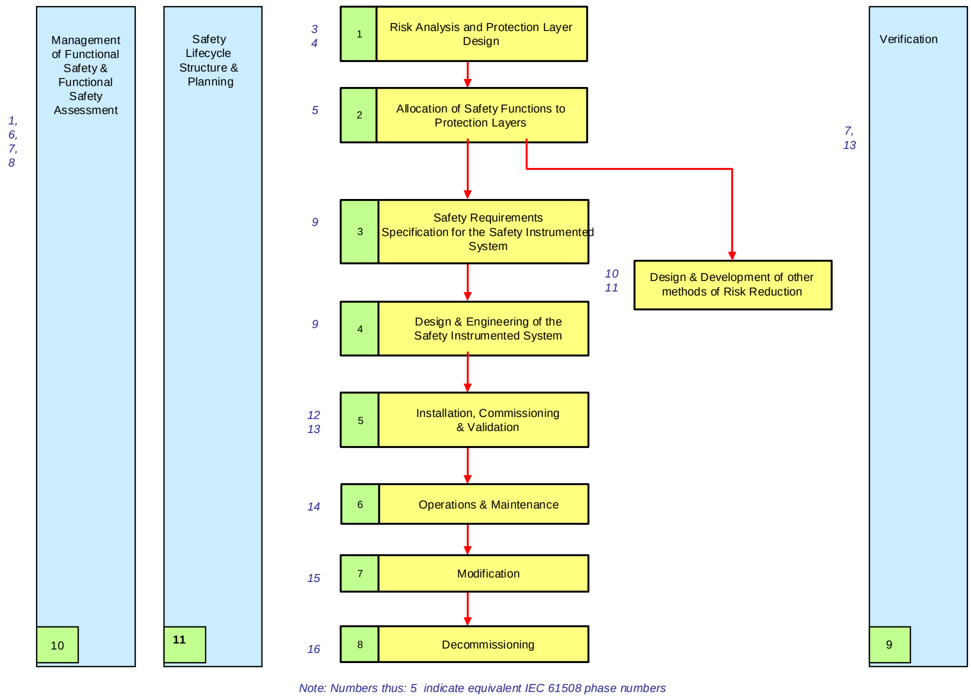

Figure 1 - Lifecycle from IEC 61511

"Functional" and "safety" are words that have been used for centuries and, although using "functional safety" to describe the action of a protection system is a relatively recent innovation, the meaning is clear enough. Other terms used are less obvious and are defined in the standard and repeated below for those not familiar with them. This paper discusses the application of three popular methods of determining Safety Integrity Level (SIL) requirements – Quantitative Risk Assessment (QRA), risk graph methods and Layer Of Protection Analysis (LOPA) – to process industry installations. It identifies some of the advantages and limitations of each method and suggests criteria for identifying which of these methods is appropriate in specific situations.

3 Definitions

IEC 61511 covers the whole lifecycle as shown in Figure 1, but this paper is concerned only with phases 1 through 3, leading to the "Safety Requirements Specification for the Safety Instrumented System".

3.1 Layers of Protection

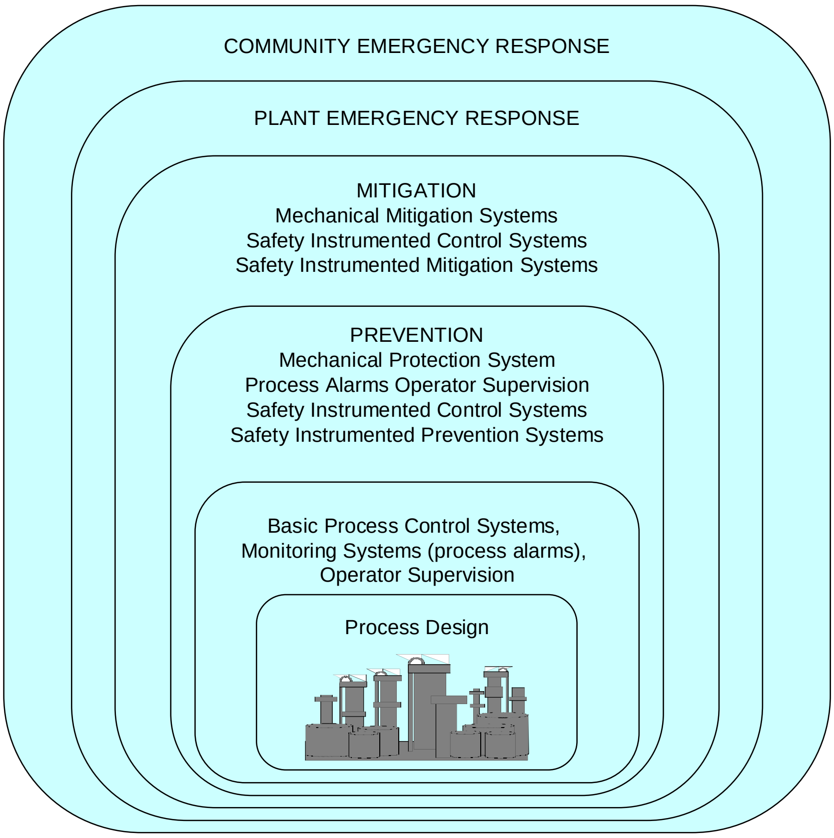

Figure 2 - Typical risk reduction methods found in process plants from IEC 61511-1 Figure 9

The introduction of the layers of protection concept shown in Figure 2 originates from the American approach to Safety Instrumented Systems (SIS) in ANSI ISA-SP 84.01-1996 [3]. This American standard has been the major influence in the differences between IEC 61508 [4] and IEC 61511 and the importance of independence between layers and the implications of common cause issues between layers is emphasised. The allocation of safety functions to specific layers or systems (for example a hazard may be protected by a combination of relief valves, physical barriers and bunds and a SIS); and the contribution required of each element to the overall risk reduction should be specified as part of the transfer of information from the risk analysis to those responsible for the design and engineering.

3.2 BPCS

The Basic Process Control System (BPCS) is a key layer of protection "which responds to input signals from the process, its associated equipment, other programmable systems and/or operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL≥1". Note that in IEC 61508 the BPCS is part of the definition of Equipment Under Control (EUC).

3.3 SIF

A Safety Instrumented Function (SIF) is a safety function with a specified SIL which is necessary to achieve functional safety. IEC 61511 also includes a note to explain that this normally refers to protection systems and that if it is applied to control systems then "further detailed analysis may be required to demonstrate that the system is capable of achieving the safety requirements".

3.4 SIS

A Safety Instrumented System (SIS) is used to implement one or more SIFs. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).

3.5 SIL

The two standards (IEC 61508 and IEC 61511) define Safety Integrity as "probability" of success and then define the Safety Integrity Level (SIL) as four discrete levels (1 to 4) such that "level 4 has the highest safety integrity". Although the standards concentrate on "Safety" and "SIL", the principles that they address can also be applied to protection against environmental and financial risks; "EIL" and "FIL" can be applied analogously with "SIL", and Integrity Level (IL) used as a term applying to all three protection functions.

The definition of SIL is clear for those SIFs that are only called upon at a low frequency / have a low demand rate Elsewhere the same two standards recognise that safety functions can be required to operate in quite different ways (for example, continuously) and SIL is defined as a failure rate (in units of failures/hour). These two different uses of the same SIL terminology have caused considerable confusion. This section of this paper was first presented at the Safety-Critical Systems Symposium in February 2004 (SSS04) [2] and attempts to clarify the definition of SIL. Consider a car; examples of low demand functions are:

- Anti-lock braking (ABS). (It depends on the driver, of course!).
- Secondary restraint system (air bags).

On the other hand there are functions that are in frequent or continuous use; examples of such functions are:

- Normal braking
- Steering

The fundamental question is how frequently will failures of either type of function lead to accidents. The answer is different for the 2 types:

- For functions with a low demand rate, the accident rate is a combination of 2 parameters – i) the frequency of demands, and ii) the Probability the function Fails on Demand (PFD). In this case, therefore, the appropriate measure of performance of the function is PFD, or its reciprocal, Risk Reduction Factor (RRF).

- For functions that have a high demand rate or operate continuously, the accident rate is the failure rate, λ, which is the appropriate measure of performance. An alternative measure is Mean Time To Failure (MTTF) of the function. Provided failures are exponentially distributed, MTTF is the reciprocal of λ.

These performance measures are, of course, related. At its simplest, provided the function can be proof-tested at a frequency that is greater than the demand rate, the relationship can be expressed as:

$$PFD = \lambda T/2 \quad \text{or} \quad = T/(2 \times MTTF), \text{ or}$$
$$RRF = 2/(\lambda T) \quad \text{or} \quad = (2 \times MTTF)/T$$

where T is the proof-test interval. (Note that to significantly reduce the accident rate below the failure rate of the function, the test frequency, 1/T, should be at least 2 and preferably ≥ 5 times the demand frequency.) They are, however, different quantities. PFD is a probability – dimensionless; λ is a rate – dimension t^{-1}. The standards, however, use the same term – SIL – for both these measures, with the following definitions:

In low demand mode, SIL is a proxy for PFD; in high demand / continuous mode, SIL is a proxy for failure rate. (The boundary between low demand mode and high demand /continuous mode is in essence set in the standards at one demand per year. This is consistent with proof-test intervals of 3 to 6 months, which in many cases will be the shortest feasible interval.)

Now consider a function which protects against 2 different hazards, one of which occurs at a rate of 1 every 2 weeks, or 25 times per year, i.e. a high demand rate, and the other at a rate of 1 in 10 years, i.e. a low demand rate. If the MTTF of the function is 50 years, it would qualify as achieving SIL1 for the high demand rate hazard. The high demands effectively proof-test the function against the low demand rate hazard. All else being equal, the effective achieved SIL for the second hazard is given by:

$$\text{PFD} = 0.04/(2 \times 50) = 4 \times 10^{-4} \equiv \text{SIL3}$$

So what is the SIL achieved by the function? Clearly it is not unique, but depends on the hazard and in particular whether the demand rate for the hazard implies low or high demand mode.

In the first case, the achievable SIL is intrinsic to the equipment; in the second case, although the intrinsic quality of the equipment is important, the achievable SIL is also affected by the testing regime. This is important in the process industry sector, where achievable SILs are liable to be dominated by the reliability of field equipment – process measurement instruments and, particularly, final elements such as shutdown valves – which need to be regularly tested to achieve required SILs.

The difference between these two definitions of SIL often leads to mis-understandings.

4 Concepts of Residual Risk, Risk Reduction and Required SIL

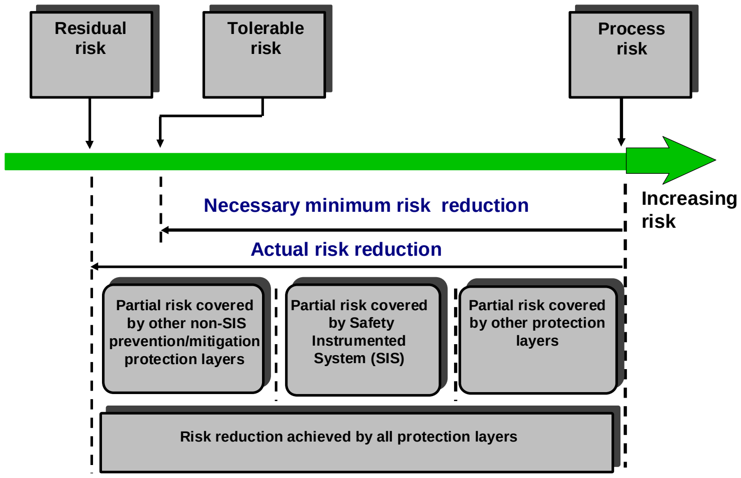

Figure 3 - Risk Reduction Model from IEC 61511

Both IEC 61508 & 61511 imply that the only action of a SIS is to reduce the frequency or likelihood of a hazard. Thus the model of risk (reproduced in Figure 3) is one-dimensional. All the methods of determining SIL are based on similar principles:

Step 1 Identify the “process risk” from the process and the BPCS

Step 2 Identify the “tolerable risk” for the particular process

Step 3 If the process risk exceeds the tolerable risk, then calculate the necessary risk reduction and whether the protection layers will operate in continuous or demand mode

Step 4 Identify the risk reduction factors achieved by other protection layers

Step 5 Calculate the remaining risk reduction factor (RRF) or the failure rate that should be achieved by the SIS and thus from Table 1 or 2 the required SIL

SIL	Range of Average PFD	Range of RRF[1]
4	$10^{-5} \leq PFD < 10^{-4}$	$100{,}000 \geq RRF > 10{,}000$
3	$10^{-4} \leq PFD < 10^{-3}$	$10{,}000 \geq RRF > 1{,}000$
2	$10^{-3} \leq PFD < 10^{-2}$	$1{,}000 \geq RRF > 100$
1	$10^{-2} \leq PFD < 10^{-1}$	$100 \geq RRF > 10$

Table 1 - Definitions of SILs for Demand Mode of Operation from IEC 61511-1 (Table 3)

SIL	Range of λ (failures per hour)	~ Range of MTTF (years)[2]
4	$10^{-9} \leq \lambda < 10^{-8}$	$100{,}000 \geq MTTF > 10{,}000$
3	$10^{-8} \leq \lambda < 10^{-7}$	$10{,}000 \geq MTTF > 1{,}000$
2	$10^{-7} \leq \lambda < 10^{-6}$	$1{,}000 \geq MTTF > 100$
1	$10^{-6} \leq \lambda < 10^{-5}$	$100 \geq MTTF > 10$

Table 2 - Definitions of SILs for Continuous Mode of Operation from IEC 61511-1 (Table 4)

The residual risk is the process risk reduced by all the risk reduction factors and will normally be less than the tolerable risk. Identifying the tolerable risk is a major issue that is discussed in Reducing Risks, Protecting People (R2P2) [5] and is beyond the scope of this paper. Identifying the frequencies of all initiating causes (or the demand rates used in Steps 1 & 3 above) is also difficult unless excellent records of all incidents are available.

5 Some Methods of Determining SIL Requirements

5.1 IEC 61508 offers 3 methods of determining SIL requirements:

- Quantitative method.
- Risk graph, described in the standard as a qualitative method.
- Hazardous event severity matrix, also described as a qualitative method.

5.2 IEC 61511 offers:

- Semi-quantitative method (incorporating the use of fault and event trees).
- Safety layer matrix method, described as a semi-qualitative method.
- Calibrated risk graph, described in the standard as a semi-qualitative method, but by some practitioners as a semi-quantitative method.
- Risk graph, described as a qualitative method.
- Layer of protection analysis (LOPA). (Although the standard does not assign this method a position on the qualitative / quantitative scale, it is weighted toward the quantitative end.)

These are developments and extensions of the methods originally outlined in IEC 61508-5. They have all been used by various organisations in the determination of SILs, but with varying degrees of success and acceptability; and do not provide an exhaustive list of all the possible methods of risk assessment. All of these methods require some degree of tailoring to meet the requirements of an individual company, together with training of the personnel who will apply them, before they can be used successfully. QRA, risk graphs and LOPA are established methods for determining SIL requirements, particularly in the process industry sector, but LOPA is less well known in the UK and is the focus of this paper.

[1] This column is not part of the standards, but RRF is often a more tractable parameter than PFD.
[2] This column is not part of the standards, but the authors have found these approximate MTTF values to be useful in the process industry sector, where time tends to be measured in years rather than hours.

5.3 Typical Results

SIL	Number of Functions	% of Total
4	0	0%
3	0	0%
2	1	0.3%
1	18	6.0%
None	281	93.7%
Total	300	100%

Table 3 - Typical Results of SIL Assessment

As one would expect, there is wide variation from installation to installation in the numbers of functions that are assessed as requiring SIL ratings, but the numbers in Table 3 were assessed for a reasonably typical offshore gas platform. Typically in the process sector there might be a single SIL3 requirement in an application of this size, while identification of SIL4 requirements is very rare. If a SIL3 or SIL4 requirement is identified it is reasonable to investigate the use made of the basic process design and other protection layers in risk reduction and whether undue reliance is being placed on the SIS; and indicates a serious need for redesign.

6 After-the-Event Protection

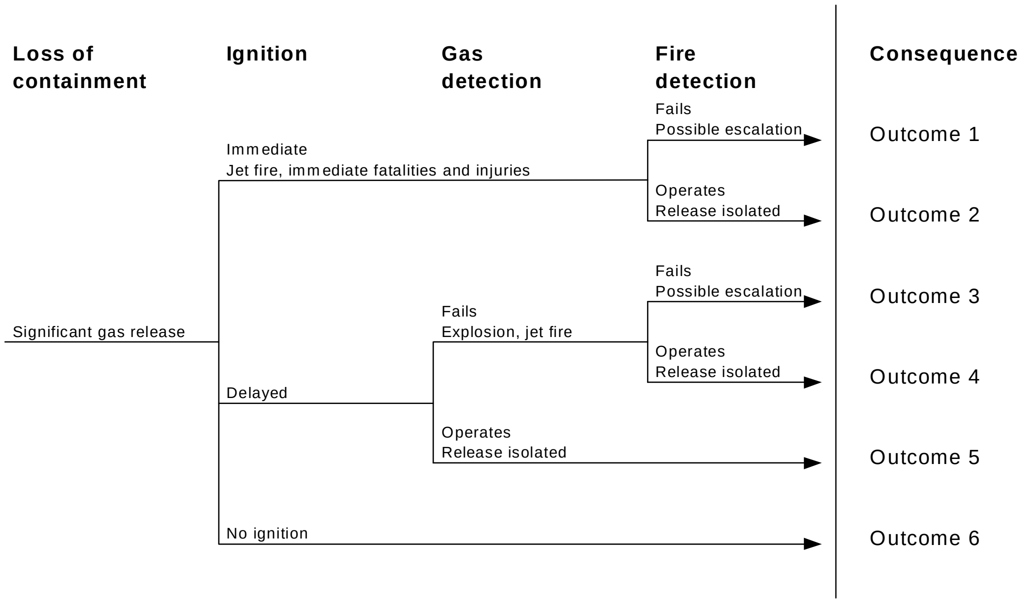

Figure 4 - Event Tree for After the Event Protection

Some functions on process plants are invoked "after-the-event", i.e. after a loss of containment, after a fire has started or an explosion has occurred. Fire and gas detection and emergency shutdown are the principal examples of such functions. Assessment of the required SILs of such functions presents specific problems:

- Because they operate after the event, there may already have been consequences that they can do nothing to prevent or mitigate. The initial consequences must be separated from the later consequences.

- The event may develop and escalate to a number of different eventual outcomes with a range of consequence severity, depending on a number of intermediate events. Analysis of the likelihood of each outcome is a specialist task, often based on event trees (Figure 4).

7 QRA

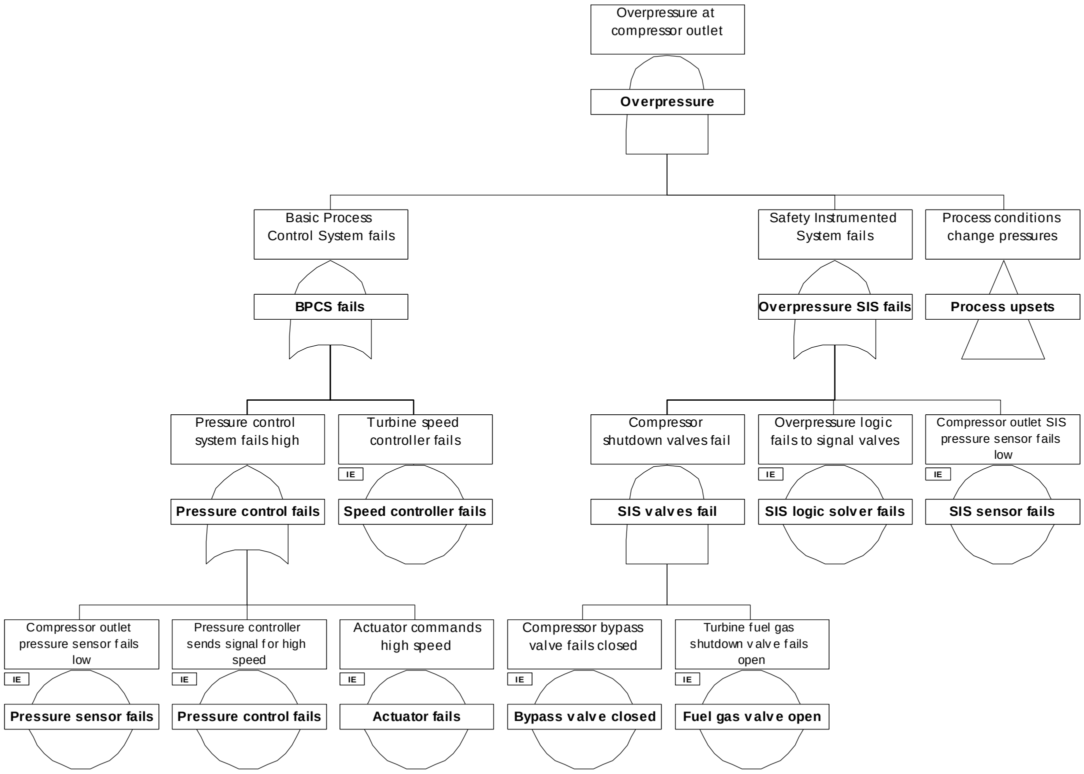

Figure 5 - Fault Tree for Overpressure at Compressor Outlet

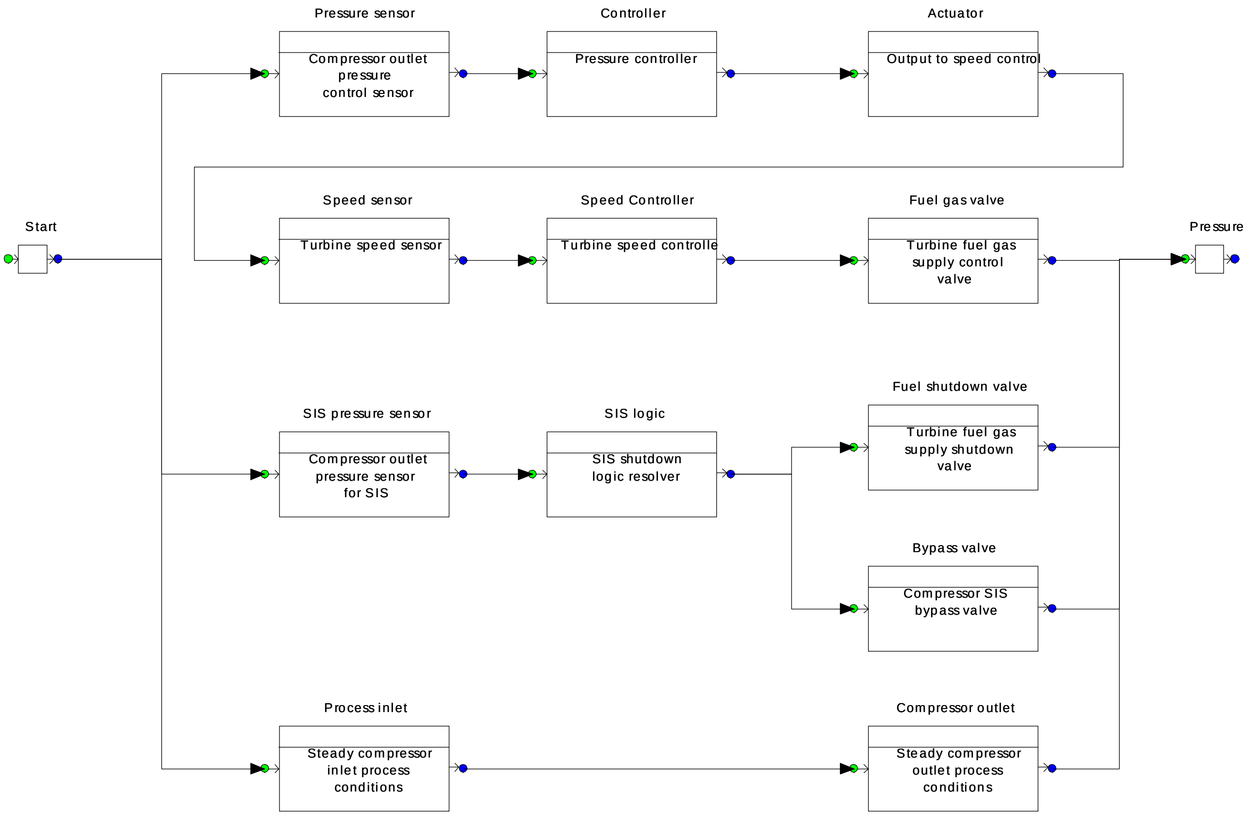

Figure 6 - Reliability Bock Diagram of Compressor Outlet Pressure

Quantitative Risk Assessment is usually done with Fault Trees and Event Trees or Reliability Block Diagrams (RBDs). Some people refer to a combination of Fault and Event Tree as a Cause-Consequence Diagram. Figure 4 shows an example of an Event Tree and Figures 5 and 6 show a Fault Tree and a RBD. Normally the "Top Event" will be a particular hazard and provided that:

- appropriate failure models are chosen for each basic event or block;
- accurate data is available for the particular environment for each of the failure modes, repairs and tests; and
- all the relationships are correctly modelled; then

the frequency at which the hazard occurs, and hence the risk can be calculated (see textbooks, for example [6]). The successful outcome of a QRA is highly dependent on the assumptions that are made, the detail of the model developed to represent the hazardous event and the data that is used. However well a QRA has been done it does not provide an absolute indication of the residual risk. A sensitivity analysis of the data and assumptions is a fundamental element of any QRA.

8 Risk Graph Methods

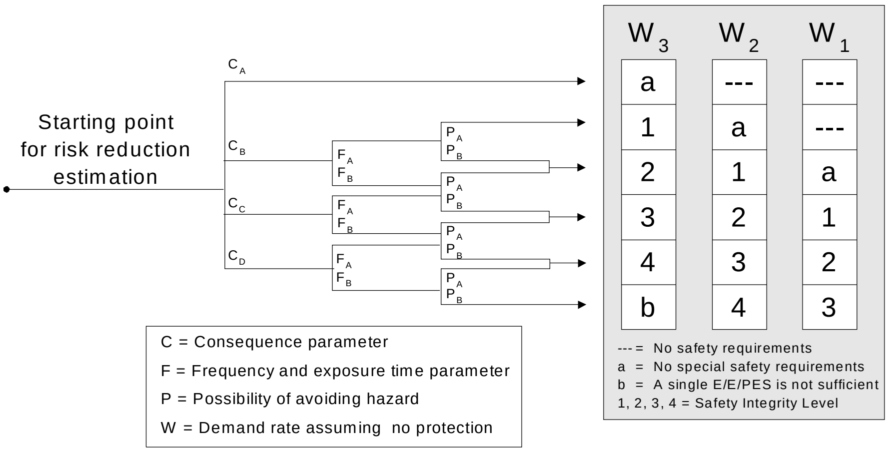

Figure 7 - Typical Risk Graph

Figure 7 shows a typical risk graph. The risk graph method is described in both IEC 61508 & 61511 and is an excellent means of quickly assessing and screening a large number of safety functions so as to allow effort to be focused on the small percentage of critical functions. The advantages and disadvantages and range of applicability of risk graphs are the main topic of a previous paper by W G Gulland at SSS04 [2]. The results of that paper are given in the conclusions below. In use the risk graph needs calibration to align with a company's corporate risk criteria.

A serious limitation of the risk graph method is that it does not lend itself at all well to assessing "after the event" outcomes:

- Demand rates would be expected to be very low, e.g. 1 in 1,000 to 10,000 years. This is off the scale of most of the risk graphs used.
- The range of outcomes from function to function may be very large, from a single injured person to major loss of life. The outcomes are also potentially random depending on a wide range of circumstances. Where large-scale consequences are possible, use of such a coarse tool such as the risk graph method can hardly be considered "suitable" and "sufficient".

The QRA and the LOPA methods do not have these limitations, particularly if the LOPA method is applied quantitatively and, as such, are more suited to analysing "after the event" outcomes.

9 Layer of Protection Analysis (LOPA)

The LOPA method was developed by the American Institute of Chemical Engineers as a method of assessing the SIL requirements of SIFs (see textbooks, for example [7]).

The method starts with a list of all the process hazards on an installation as identified by Hazard And Operability Studies (HAZOPs) or other hazard identification techniques. The hazards are analysed in terms of:

- Consequence description ("Impact Event Description")
- Estimate of consequence severity ("Severity Level")
- Description of all causes which could lead to the Impact Event ("Initiating Causes")
- Estimate of frequency of all Initiating Causes ("Initiation Likelihood")

The Severity Level may be expressed in semi-quantitative terms, linked to target Mitigated Event Likelihoods expressed as target frequency ranges (analogous to tolerable risk levels), as shown in Table 4; or it may be expressed as a specific quantitative estimate of harm, which can be referenced to F-N curves.

Severity Level	Consequence	Target Mitigated Event Likelihood
Minor	Serious injury at worst	No specific requirement
Serious	Serious permanent injury or up to 3 fatalities	< 3E-6 per year, or 1 in > 330,000 years
Extensive	4 or 5 fatalities	< 2E-6 per year, or 1 in > 500,000 years
Catastrophic	> 5 fatalities	Use F-N curve

Table 4 - Example Definitions of Severity Levels and Mitigated Event Target Frequencies

Similarly, the Initiation Likelihood may be expressed semi-quantitatively, as shown in Table 5; or it may be expressed as a specific quantitative estimate.

Initiation Likelihood	Frequency Range
Low	< 1 in 10,000 years
Medium	1 in > 100 to 10,000 years
High	1 in ≤ 100 years

Table 5 - Example Definitions of Initiation Likelihood

The strength of the method is that it recognises that in the process industries there are usually several layers of protection against an Initiating Cause leading to an Impact Event. Specifically, it identifies:

- <u>General Process Design.</u> There may, for example, be aspects of the design that reduce the probability of loss of containment, or of ignition if containment is lost, so reducing the probability of a fire or explosion event.

- <u>Basic Process Control System (BPCS).</u> Failure of a process control loop is likely to be one of the main Initiating Causes. However, there may be another independent control loop that could prevent the Impact Event, and so reduce the frequency of that event.

- <u>Alarms.</u> Provided there is an alarm that is independent of the BPCS, sufficient time for an operator to respond, and an effective action to take (a "handle" to "pull"), credit can be taken for alarms to reduce the probability of the Impact Event up to a RRF of 10.

- <u>Additional Mitigation, Restricted Access.</u> Even if the Impact Event occurs, there may be limits on the occupation of the hazardous area (equivalent to the F parameter in the risk graph method), or effective means of escape from the hazardous area (equivalent to the P parameter in the risk graph method), which reduce the Severity Level of the event.

- <u>Independent Protection Layers (IPLs).</u> A number of criteria must be satisfied by an IPL to be assured that it is genuinely independent of other protective layers and achieves RRF ≥ 10. Relief valves and bursting disks usually qualify for RRF ≥ 100.

Based on the Initiating Likelihood (frequency) and the PFDs of all the protection layers listed above, an Intermediate Event Likelihood (frequency) for the Impact Event and the Initiating Event can be calculated. The process must be completed for all Initiating Events, to determine a total Intermediate Event Likelihood for all Initiating Events. This can then be compared with the target Mitigated Event Likelihood (frequency). So far no credit has been taken for any SIF. The ratio:

(Intermediate Event Likelihood) / (Mitigated Event Likelihood)

gives the required RRF (or 1/PFD) of the SIF, and can be converted to a required SIL using Table 1. Alternatively the inverse ratio

(Mitigated Event Likelihood) / (Intermediate Event Likelihood)

gives the required PFD of the SIF that can be converted to a required SIL using Table 1.

10 Examples of LOPA

10.1 Compressor

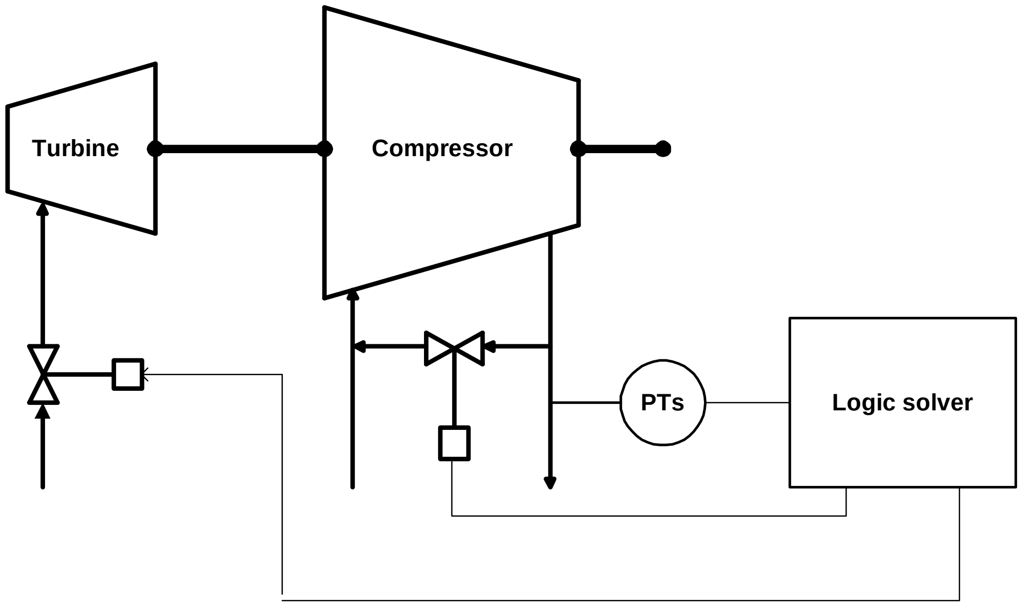

Figure 8 - Example of overpressure protection for a compressor driven by a gas turbine

10.1.1 Key Assumptions for LOPA of overpressure protection for a compressor driven by a gas turbine

Overpressure of the piping downstream of compression could result in the release of significant quantities of flammable gas within or outside the compressor building.

The study team focused only on the explosion hazard as this had the more significant consequences. Three cases were considered for high pressure:

- Case A: a sudden increase in pressure from the source of gas.
- Case B: closing a control, shutdown or isolation valve in the piping, or equipment downstream of the compressor.
- Case C: a failure of the BPCS.

The study team used the values for Individual Risk Per Annum (IRPA) (see R2P2) [5] defined in the Control of Major Accident Hazards (COMAH) safety report for the most exposed person. The As Low As Reasonably Practicable (ALARP) region (see R2P2) [5] was defined as IRPA in the range 10^{-3} to 10^{-6}.

There are no occupied buildings on the neighbouring sites within 100m of the compressor building. Staff are required not to stay within the compressor building for longer than 15 minutes at a time and for 20 minutes in one day (unless it is shutdown). There may be one or two staff exposed for 10 – 20 minutes each day in the compressor building (giving a severity of Serious). The compressor building is classified as a hazardous area, with explosion proof equipment and no exposed hot surfaces.

10.1.2 Results of LOPA Study

The study team assumed an IRPA Mitigated event target likelihood of 10^{-7}. The worst case Intermediate event likelihood was 10^{-2} and thus a Safety Instrument Function (SIF) Probability of Failure on Demand (PFD) of 10^{-5} is required. The details of the other figures are shown in Table 6. Severity levels are specified as C = Catastrophic, E = Extensive, S = Serious, M = Minor; and likelihood values are events per year. Other numerical values are probabilities of failure on demand average.

10.1.3 Layer of protection analysis (LOPA)

Some of the results of the LOPA are shown in Table 6.

10.2 Pipeline

The Pipeline studied contained a liquid that would evaporate if released and had Passive Fire Protection (PFP). Two of the impact events considered were Jet Fires and a Boiling Liquid Expanding Vapour Explosion (BLEVE). Some of the results of the LOPA are shown in Table 7.

					Protection layers								
#	**Impact event description**	**Severity level (C, E, S or M)**	**Initiating cause**	**Initiation likelihood (events per year)**	**General process design (probability)**	**BPCS (probability)**	**Alarms, etc. (probability)**	**Additional mitigation, restricted access (probability)**	**IPL additional mitigation, dikes, pressure relief (probability)**	**Intermediate Event Likelihood (events per year)**	**SIF PFD (probability)**	**Mitigated Event Likelihood (events per year)**	**Notes**
A	Explosion in compressor building (two deaths)	S	High pressure surge from platform	0.01 as no event in over 30 years and no upstream compression	Source of ignition required. Classified hazardous area, with explosion proof equipment. 0.1	Control system should respond 0.1	Not time for operator action	20 mins per day implies 1 / 72	N/A	1.4 x E-6		1 x E-7	
B	Explosion in compressor building (two deaths)	S	Closure of downstream valve	1 to 0.1 as downstream equipment includes many valves	Source of ignition required. Classified hazardous area, with explosion proof equipment. 0.1	Control system should respond 0.1	Not time for operator action	20 mins per day implies 1 / 72	N/A	1.4 x E-4 to 1.4 x E-5		1 x E-7	
C	Explosion in compressor building (two deaths)	S	Failure of BPCS	0.1	Source of ignition required. Classified hazardous area, with explosion proof equipment. 0.1	No protection as BPCS failed	Not time for operator action	20 mins per day implies 1 / 72	N/A	1.4 x E-4		1 x E-7	This is the dominant source of intermediate event likelihood
	Totals									281 x E-6	Approx 0.0003	1 x E-7	SIL3 to protect against A, B & C

Table 6 - LOPA for compressor

					Protection layers								
#	**Impact event description**	**Severity level (C, E, S or M)**	**Initiating cause**	**Initiation likelihood (events per year)**	**General process design (probability)**	**BPCS (probability)**	**Alarms, etc. (probability)**	**Additional mitigation, restricted access (probability)**	**IPL additional mitigation, dikes, pressure relief (probability)**	**Intermediate Event Likelihood (events per year)**	**SIF PFD (probability)**	**Mitigated Event Likelihood (events per year)**	**Notes**
1	An escalated jet fire from the pipeline fed by inventory of pipeline if not isolated. Could impact persons leaving the site, and cause multiple fatalities (onsite and offsite).	C	Ignited loss of containment as a consequence of component failure.	The frequency of large scale escalation without facility to isolate pipeline is estimated as 2.33E-03 (1 in 430 years).	Source of ignition required. Classified hazardous area, with explosion proof equipment. PFD 1 in 10.	N/A	Operator can initiate manual isolation of pipeline by motor operated HCV. Probability of failure = 1 in 10. No credit taken in "Intermediate event likelihood". See Notes.	Directional probability of jet fire taken as 1/6 = 0.167.	N/A	1 in 26 E+03 years.	RRF required from SIF to isolate the pipeline (automatically or manually) = 385, Pfd required = 1/385 = 0.0026 = SIL2.	There could be up to 50 fatalities. Limit for a 50 public fatalities event is 1 in 100,000 years; target is 1 in 10 million years.	The RRF of the SIF to isolate the pipeline is 385, equivalent SIL2, which could not be achieved with one valve alone. However, having a separate manual valve available as a backup and would make SIL2 achievable.
2	Jet spray fire from Slug Catcher finger following PFP failure >20 minutes after initial event, if no blowdown. Potentially multiple fatalities outside fence.	C	Ignited loss of containment as a consequence of component failure.	From the COMAH report, the frequency of escalation if blowdown fails (or without PFP) is estimated to be less than 1.9E-03 per year (1 in 520 years).	Source of ignition required. Classified hazardous area, with explosion proof equipment. PFD 1 in 10	N/A	Operator can initiate blowdown manually. Probability he misses alarm / fails to respond = 1 in 10, but partial functionality of blowdown SIF still required, so no credit taken.	Estimated exposure ~5 minutes per day, probability ~1 in 300.	N/A	1 multiple fatality event in 1.6 million years.	RRF required from blowdown SIF = 16, PFD required = 1/16 = 0.06 = SIL1.	There could be up to 50 fatalities. Limit for a 50 public fatalities event is 1 in 100,000 years; target is 1 in 10 million years.	Endurance of PFP on Slug Catcher fingers specified for 20 minutes, based on achieving blowdown

					Protection layers								
#	**Impact event description**	**Severity level (C, E, S or M)**	**Initiating cause**	**Initiation likelihood (events per year)**	**General process design (probability)**	**BPCS (probability)**	**Alarms, etc. (probability)**	**Additional mitigation, restricted access (probability)**	**IPL additional mitigation, dikes, pressure relief (probability)**	**Intermediate Event Likelihood (events per year)**	**SIF PFD (probability)**	**Mitigated Event Likelihood (events per year)**	**Notes**
3	BLEVE following PFP failure at liquid header >120 minutes after initial event, if no blowdown. Multiple fatalities of personnel at muster point.	E	Ignited loss of containment as a consequence of component failure.	From the COMAH report, the frequency BLEVEs if blowdown fails (or without PFP) is estimated as 1.9E-03 per year (1 in 520 years).	Source of ignition required. Classified hazardous area, with explosion proof equipment. PFD 1 in 10.	N/A	Operator can initiate blowdown manually. Probability he misses alarm / fails to respond = 1 in 10, but partial functionality of blowdown SIF still required, so no credit taken.	None	N/A	1 in 5,200 years.	RRF required from blowdown SIF = 20, Pfd required = 1/20 = 0.05 = SIL1.	There could be up to 10 employee fatalities. Limit is 1 such event in 1,000 years; target is 1 in 100,000 years.	Endurance of PFP on liquid header specified for 120 minutes, based on achieving blowdown.

Table 7 - LOPA for Pipeline

11 Discussion of all three methods

11.1 QRA

Page 31 of R2P2 [5] states that "The use of numerical estimates of risk by themselves can, for several reasons..., be misleading and lead to decisions which do not meet adequate levels of safety. In general, qualitative learning and numerical estimates from QRA should be combined with other information from engineering and operational analyses in making an overall decision."

Fault Trees, Event Trees and RBDs are very valuable in showing relationships between different parts of the process, the BPCS and the protection systems. However, there are difficulties in obtaining good data for all the relevant failure modes as many business sector reliability databases have not been maintained. Therefore numerical estimates of risk will take the form of a range and judgement will be required to assess a realistic figure.

The problems with the data also apply if LOPA is used for quantitative assessments.

11.2 Risk Graphs

The implications of the issues highlighted by W G Gulland at SSS04 [2] are:

- Risk graphs are very useful but imprecise tools for assessing SIL requirements. (It is inevitable that a method with 5 parameters – C, F, P, W and SIL – each with a range of an order of magnitude, will produce a result with a range of 5 orders of magnitude.)

- They must be calibrated on a conservative basis to avoid the danger that they under-estimate the unprotected risk and the amount of risk reduction / protection required.

- Their use is most appropriate when a number of functions protect against different hazards, which are themselves only a small proportion of the overall total hazards, so that it is very likely that under-estimates and over-estimates of residual risk will average out when they are aggregated. Only in these circumstances can the method be realistically described as providing a "suitable" and "sufficient", and therefore legal, risk assessment.

- Higher SIL requirements (SIL2+) incur significant capital costs (for redundancy and rigorous engineering requirements) and operating costs (for applying rigorous maintenance procedures to more equipment, and for proof-testing more equipment at higher frequencies, and to rigorously gather and analyse performance data). They should therefore be re-assessed using a more refined method.

11.3 LOPA

The LOPA method has the following advantages:

- It can be used semi-quantitatively or quantitatively.
  - ♣ Used semi-quantitatively it has many of the same advantages as risk graph methods.
  - ♣ Used quantitatively the logic of the analysis can still be developed as a team exercise, with the detail developed "off-line" by specialists.
- It explicitly accounts for risk mitigating factors, such as alarms and relief valves, which have to be incorporated as adjustments into risk graph methods (e.g. by reducing the W value to take credit for alarms, by reducing the SIL to take credit for relief valves).
- A semi-quantitative analysis of a high SIL function can be promoted to a quantitative analysis without changing the format.
- It can assist in all the team members obtaining and sharing a full appreciation of the issues and uncertainties associated with the hazardous event(s).

12 Conclusions

<table>
<tr><th>QRA</th><th>Risk Graph</th><th>LOPA</th></tr>
<tr>
<td><u>Advantages</u>:

1. Can be applied to complex systems and many different models of failures.

2. Can be performed by an individual.

3. The FTA and RBD diagrams show the relationships between sub-systems and dependencies within the overall system.

4. Gives a numerical result.

5. Tools are available for both FTA and RBDs.

6. Can be used to assess the requirements of after-the-event functions.</td>
<td><u>Advantages</u>:

1. Can be applied relatively rapidly to a large number of functions to eliminate those with little or no safety role, and highlight those with larger safety roles.

2. Can be performed as a team exercise involving a range of disciplines and expertise.</td>
<td><u>Advantages</u>:

1. Can be used both as a filtering tool and for more precise analysis.

2. Can be performed as a team exercise, at least for a semi-quantitative assessment.

3. Facilitates the identification of all relevant risk mitigation measures, and taking credit for them in the assessment.

4. When used quantitatively, uncertainty about residual risk levels can be reduced, so that the assessment does not need to be so conservative.

5. Can be used to assess the requirements of after-the-event functions.</td>
</tr>
<tr>
<td><u>Disadvantages</u>:

1. The precision may be an illusion, particularly in the assessment of human factors.

2. The assessment has to be reviewed by those who understand FTA and RBD.

3. The method is very time-consuming.</td>
<td><u>Disadvantages</u>:

1. An imprecise method, which is only appropriate to functions where the residual risk is very low compared to the target total risk.

2. The assessment has to be adjusted in various ways to take account of other risk mitigation measures such as alarms and mechanical protection devices.

3. Does not lend itself to the assessment of after-the-event functions.</td>
<td><u>Disadvantages</u>:

1. Relatively slow compared to risk graph methods, even when used semi-quantitatively.

2. Not so easy to perform as a team exercise, makes heavier demands on team members’ time, and not so visual.</td>
</tr>
</table>

Table 8 – Advantages and disadvantages of QRA, Risk Graph and LOPA Methods

To summarise, the relative advantages and disadvantages of these methods are shown in Table 8, and as can be seen from Table 8 there is no ideal candidate to cover all requirements - an assessment has to be made as to the most appropriate method for a specific requirement. Should the total number of functions requiring assessment be small (< 10) and acceptable reliability data available then our experience would be to apply LOPA in a semi-quantitative manner. However on new installations the number of functions identified in the HAZOP as requiring a SIF can be very large requiring the involvement of critical people in a team activity over a considerable period of time. Sufficient time for this is a rare commodity these days and, in such a situation, we would recommend the use of risk graphs initially for all required functions (approx. 25 functions assessed per day on average) and then repeat the assessment using LOPA for those functions assessed as $\geq$ IL2 (approx. 5 functions assessed per day on average).

Whatever process of analysis is applied they all require a corporate risk policy defining what risk level is deemed acceptable from both individual and societal perspectives – a politically sensitive decision has to be agreed within any business organisation, with an acute awareness of the perception of risk held by the general public.

Whilst the standards IEC 61508/61511 only relate to Safety of people there is little doubt that the Environmental agencies will require businesses focus to improve the environment whilst stake-holders will require similar attention to commercial performance.

13 References

1. 2003, BS IEC 61511 *Functional safety - Safety instrumented systems for the process industry sector*.

2. Gulland, W. G., 2004, Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons, *Proceedings of the Safety-Critical Systems Symposium - February 2004.*

3. 1996, *Application of Safety Instrumented Systems for the Process Industries*, Instrument Society of America Standards and Practices, ANSI / ISA-SP 84.01-1996.

4. 1998 - 2000, BS IEC 61508, *Functional safety of electrical / electronic / programmable electronic safety-related systems*

5. 2001, *Reducing risks, protecting people – HSE's decision making process*, (R2P2), HSE Books, ISBN 0-7176-2151-0

6. Smith, D. J., 2001, *Reliability, Maintainability and Risk*, 6th Edition, ISBN 0-7506-5168-7

7. 2001, *Layer of Protection Analysis – Simplified Process Risk Assessment*, American Institute of Chemical Engineers, ISBN 9-780816-908110