DETERMINATION OF SAFETY INTEGRITY LEVELS TAKING INTO ACCOUNT ALARP – COST BENEFIT ANALYSIS

Clive Timms
Asset Integrity Management Limited

INTRODUCTION

Safety Instrumented Systems (SIS) are one of the most commonly used methods of reducing the risks associated with major accident hazards in the process sector. They can be found in various systems such as emergency shut down, fire and gas and machinery protection. A single SIS normally provides protection against a single hazard, and this poses a dilemma for designers when they are trying to fulfil the overall requirements for reducing risk to as low as reasonably practicable (ALARP) – *UK HSE – Reducing Risks Protecting People (R2P2), 2001 and the BS IEC 61511, 2003* standard, since the concepts of ALARP are concerned with the total risk from all likely hazards to workers or society. R2P2 provides guidance on ALARP for the purposes of the Statutory Instrument *Control of Major Accident Hazards Regulations 1999 (COMAH)* as the UK implementation of the *European Seveso II Directive, 1996.*

This paper sets out a methodology for setting a tolerable risk level or Safety Target, to the principles as low as reasonably practicable, when undertaking safety integrity level (SIL) determinations for safety instrumented systems protecting against single hazards.

It should be recognised that the primary objectives are to ensure that the correct safety functions have been identified from the risk assessment, and that the functionality of these safety functions is specified and implemented correctly; so, that in normal operation, the safety instrumented system operates as required to prevent a hazardous situation and does not itself operate in any way that could lead to a hazardous situation. The determination of a safety integrity level is secondary to these primary objectives.

The paper discusses the determination of safety integrity levels for safety functions where failure results in injury/fatality of workers and also the societal risk aspects when members of the public could be injured due to failure of the safety function.

ASSESSING RISK

IDENTIFYING THE HAZARDS

Identifying the possible hazards is fundamental to any risk assessment process, as these hazards represent the potential source of harm that could arise from damaging property, the process or the environment. As a direct or indirect consequence of this damage, people could suffer harm through physical injury or damage to their health.

If the hazards are not identified then it will not be possible to assess the risks involved.

The multi disciplinary Hazard and Operability (HAZOP) approach introduced by ICI following Flixborough (Nypro UK) is the most widely used since it is a detailed study and reporting technique that systematically analyses every part of the process by lines and major equipment nodes. Deviations from design intent such as more pressure, less pressure, more flow, less flow etc. are analysed to determine if they could cause a hazardous condition. The frequency or likelihood of these cause/consequence scenarios and the consequences that would result if the condition occurred are recorded.

Thus HAZOP provides the vehicle for identifying the need for improvements in the form of additional safeguarding, and some of this could be Safety Instrumented Functionality (SIF).

AS LOW AS REASONABLY PRACTICABLE (ALARP) CONCEPT

Having identified the hazards, the requirement of the UK Regulator and the *BS IEC 61511, 2003* standard is to demonstrate that risks are reduced to as low as reasonably practicable. Thus residual risk should be tolerable and at a level that falls between two extremes of intolerable and broadly acceptable.

Tolerable is not the same as acceptable, it is a level at which there is a willingness to live with the risk in order to obtain the benefits.

Figure 1 demonstrates the ALARP principle of reducing risks to a level that is at least tolerable and where the time, effort and cost of further measures becomes grossly disproportionate to the additional reduction in risk achieved.

METHODS OF RISK ASSESSMENT

Having identified the hazards then the risks involved need to be established where:

$$\text{Risk} = \text{Harm} \times \text{Probability}$$

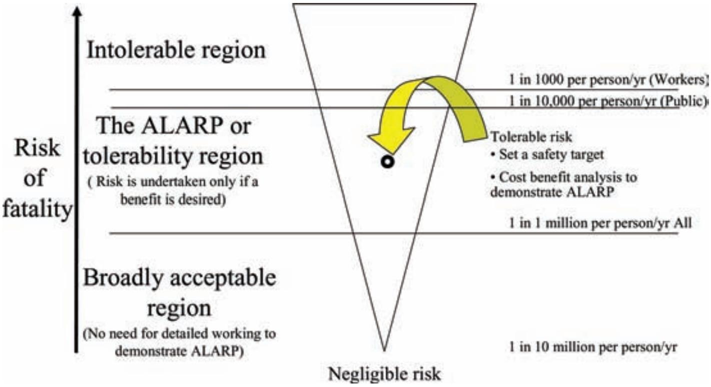

Intolerable region
1 in 1000 per person/yr (Workers)
1 in 10,000 per person/yr (Public)
The ALARP or tolerability region
(Risk is undertaken only if a benefit is desired)
Tolerable risk
• Set a safety target
• Cost benefit analysis to demonstrate ALARP
Risk of fatality
1 in 1 million per person/yr All
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
1 in 10 million per person/yr
Negligible risk

Figure 1. The tolerability of risk framework

And harm could be the consequences with respect to people, property or the environment or a combination.

There are many popular methods for undertaking a risk assessment and the most commonly used are:

Fault Tree Analysis
Risk Graphs
Risk Matrices
Layers of Protection Analysis (LOPA)

The purpose of risk assessment is to consider a hazard in conjunction with all the existing or proposed risk reduction measures in order to establish if the level of residual risk is tolerable.

The risk assessment method may be either qualitative or quantitative and it does not have to be quantified if it can demonstrate that the residual risk is better than, or close to, the broadly acceptable region.

However, for higher levels of risk it is usual to use a quantified or semi quantified approach. Fully quantified methods such a Fault Tree tend to be time consuming and when a whole process plant is to be analysed then it is recommended that a semi quantified approach such as a risk graph or risk matrix is used to undertake the initial risk assessment. These are relatively quick to use and also conservative due to their rigid framework that limits the number of parameters for which risk reduction credit can be claimed. A more detailed analysis of the higher SIL results can then be undertaken by methods such as Fault Tree or LOPA. Risk graphs and LOPA are discussed in more detail in Section 2.6.

Whether quantified or semi quantified analysis is used, they require a numerical value for the tolerable risk or safety target to make them to work.

SETTING A SAFETY TARGET

In order to establish if sufficient risk reduction measures are in place, and demonstrate ALARP, a Safety Target for meeting ‘tolerable risk’ is needed. Although most major process operating organisations will have established corporate values, this is often a new experience for the majority of end users of Safety Instrumented Systems (SIS), and an area which causes considerable problems.

None of the UK regulations offer a ‘typical’ value for a safety target and this is understandable since it will be dependant on the disproportional cost of further risk reduction, and this will never have any ‘typical’ value.

However, experience shows that end users often need to have some guidance on what constitutes a safety target and, even more importantly, they are usually confused by the principles of ALARP.

The HSE document ‘*Reducing Risks, Protecting People, 2001’* (R2P2) (paragraph 128) indicates upper limit boundary between Tolerable and Unacceptable risk, for workers, would be 1 in 1,000 per annum, as shown in Figure 1.

In (Paragraph 130) of R2P2 the boundary between Tolerable and Broadly Acceptable risk, for risks entertaining fatalities, for both workers and public is indicated as 1 in

1,000,000 (1.0E-06) per annum as this corresponds to a very low level of risk, as shown in Figure 1.

The dilemma is to understand and/or calculate where the tolerable risk, or safety target, should sit within the upper and lower boundaries.

Where a major accident hazard could impact on both workers and the public then it is necessary to establish tolerable risk levels for both. It is generally expected that the tolerable risk for the public, often referred to as societal risk, will be at least ten times less, i.e. more restrictive than for workers.

In addition, a SIL determination only makes an assessment of the risk associated with a single hazard whilst ALARP is concerned with the most exposed person to ALL risks per annum. It is practically impossible for the SIS designer to estimate how many simultaneous risks an individual might be exposed to when considering a design to protect against a specific hazard, as 'all risks' embrace a wide spectrum of hazards including slips, trips and falls. It is simply not practicable to try and resolve such a complex problem for all workers and society.

Thus some rationale needs to be established to make allowance for the fact that only single hazards are analysed during SIL determination. It is suggested that a single hazard Safety Target is made factor of ten more sensitive than a corporate all risks per annum tolerable risk target, in order to make allowances for these uncertain multiple risk conditions; e.g. if a corporate all risks per annum was set at of 1 in 1000 (1.0E-03), for the most exposed individual, then the single hazard tolerable risk would need to be at least 1 in 10,000 (1.0E-04). The HSE do not currently provide guidance on the scale of this factor, and opinion ranges between 10 and 100, but there is general agreement in the industry that a factor of at least 10 is sufficient.

Where the consequences of a hazardous event impact upon the public then a Societal Risk assessment is required. Each operating organisation must set their societal risk criteria and this is quite commonly set to be a factor of ten times more sensitive than for on site workers; e.g. If the tolerable risk for workers was set at 1.0E-04 then the tolerable societal risk could be 1.0E-05.

Thus the suggested factor of ten increased sensitivity for single hazards can be applied to both the tolerable risk for workers and society.

If the risk is being assessed for a multiple proximity plant site then the target for society/public needs to be proportionally further reduced, i.e. if there are ten plants in close proximity then the public risk target needs to be a factor of another ten times lower. This would not be the case for workers as they usually work on one plant and is only at risk from that plant, however consideration needs to be given too any potential for domino escalation between sites.

SAFETY TARGET AND RISK REDUCTION

Risk reduction is generally made up of a number of different layers and some typical examples are shown in Figure 2.

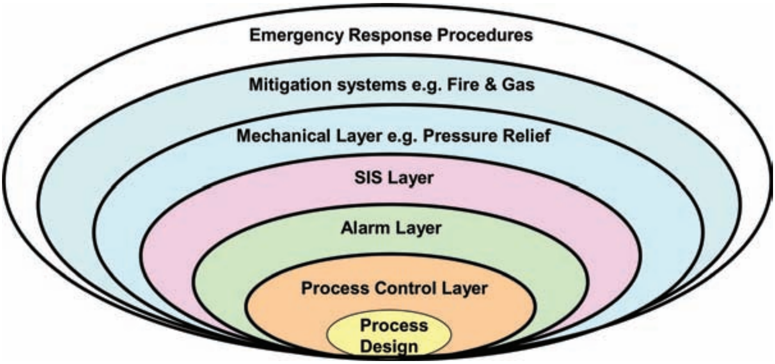

Emergency Response Procedures
Mitigation systems e.g. Fire & Gas
Mechanical Layer e.g. Pressure Relief
SIS Layer
Alarm Layer
Process Control Layer
Process Design

Figure 2. Typical risk reduction layers

Total risk reduction is a product of the individual risk reduction measures and this combination can be demonstrated in Figure 3. Having established a Safety Target or tolerable risk for any single hazard, the objective of the risk assessment is to estimate the risk reduction achieved by existing measures, in numerical terms, and to compare this with the Safety Target such that:

$$\frac{\text{Safety Target}}{\text{Existing Risk Reduction Measures}}$$

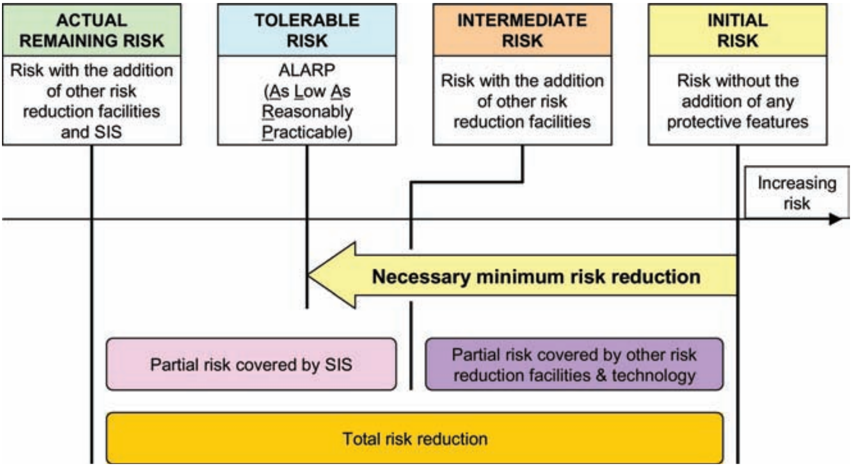

ACTUAL REMAINING RISK
Risk with the addition of other risk reduction facilities and SIS
TOLERABLE RISK
ALARP (As Low As Reasonably Practicable)
INTERMEDIATE RISK
Risk with the addition of other risk reduction facilities
INITIAL RISK
Risk without the addition of any protective features
Increasing risk
Necessary minimum risk reduction
Partial risk covered by SIS
Partial risk covered by other risk reduction facilities & technology
Total risk reduction

Figure 3. Combination of risk reduction measures

Thus will indicate if additional risk reduction measures are needed and the required risk reduction value they must achieve. The relationship between the required risk reduction and the probability of failure on demand (PFD) used in SIS design is:

$$\frac{1}{\text{Risk Reduction}} = \text{PFD}$$

The remainder of this paper will outline the steps for undertaking risk assessments to a safety target of tolerable risk within the principles of ALARP.

ASSESSMENT OF THE RISK

Two of the most popular methods for undertaking risk assessments associated with SIS are Risk Graphs and layers of Protection Analysis (LOPA).

Risk Graphs

The general arrangement of the *BS IEC 615, 2003* risk graph used for a Personnel Safety is shown in Figure 4. The graph uses the following parameters for making the risk assessment:

C = Consequence severity
F = Occupancy of the hazardous area being considered

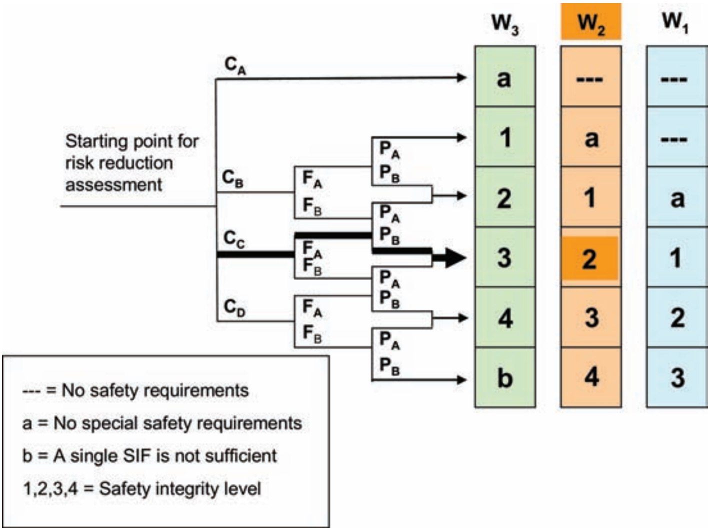

W3
W2
W1
C_A
Starting point for risk reduction assessment
C_B
C_C
C_D
F_A
F_B
P_A
P_B
a --- ---
1 a ---
2 1 a
3 2 1
4 3 2
b 4 3
--- = No safety requirements
a = No special safety requirements
b = A single SIF is not sufficient
1,2,3,4 = Safety integrity level

Figure 4. IEC 61511 personnel safety risk graph (general arrangement)

Table 1. Relationship between SIL, Risk Reduction and PFD

SIL	Risk Reduction	PFD
1	10–100	1.0E-1–1.0E-2
2	100–1000	1.0E-2–1.0E-3
3	1000–10000	1.0E-3–1.0E-4
4	10000–100000	1.0E-4–1.0E-5

P = Alternatives to avoid the hazard
W = Frequency of demand on the SIS or likelihood
1,2,3,4 = Safety integrity level (SIL)

The Safety Integrity Level (SIL) which is delivered by this type of risk graph represents the additional risk reduction that is required to meet the Tolerable Risk or Safety Target.

The Relationship between SIL, risk reduction and PFD is provided in *BS IEC 61511, 2003* and is shown in Table 1.

Risk graphs can be calibrated to deliver a specific safety target or tolerable risk and this can be demonstrated by considering an example which has a calibration shown in Table 2. The outcome of a SIL determination exercise has delivered W2, CC, FA, PB, and SIL 2 as highlighted.

From Table 2 it can be seen that each parameter has a value range with a 'high' end value and a 'low' end value; e.g. for the frequency of demand parameter of W2 this will be 0.03 years or 0.3 years. Obviously the risk is less if the demand is 0.03/year than if it was 0.3/year.

If all the parameters were at their 'low' end this would result in the highest level of achievable risk reduction of 3.0E-08 as shown in Case 1:

Case 1 = (Low CC)*(Low FA)*(PB)*(Low W2)*(Low end SIL 2)
Case 1 = (0.1)*(0.01)*(1.0)*(0.03)*(0.001)
Case 1 = 3.0E-08

If all the parameters were at their 'high' end this would result in the lowest level of achievable risk reduction of 3.0E-04 as shown in Case 2:

Case 2 = (High CC)*(High FA)*(PB)*(High W2)*(High end SIL 2)
Case 2 = (1.0)*(0.1)*(1.0)*(0.3)*(0.01)
Case 2 = 3.0E-04

Thus taking the two extreme cases the average risk reduction can be calculated as follows: The risk reduction afforded by the best case:

Case 1 = 3.0E-08

Table 2. Example risk graph calibration

	Parameter	Low Value	High Value
An example risk graph has been assigned parameters with the values opposite:	W3	0.3	3.0
	W2	0.03	0.3
	W1	0.003	0.03
	CA	0.01	0.01
	CB	0.01	0.1
	CC	0.1	1.0
A 'typical SIL determination has resulted in a risk path with the highlighted parameters.'	CD	>1.0	0.01
	FA	0.01	
	FB	0.1	1.0
	PA	0.1	0.1
	PB	1.0	1.0
	SIL 1	0.01	0.1
Each parameter has a range value with a high end and low end value	SIL 2	0.001	0.01
	SIL 3	0.0001	0.001
	SIL 4	0.00001	0.0001

and

The risk reduction afforded by the worst case:

$$\text{Case } 2 = 3.0\text{E-}04$$

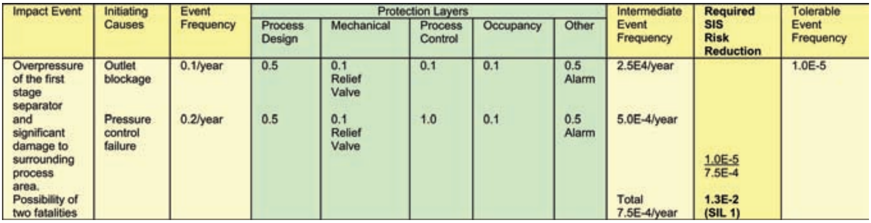
Since the risk graph is based on a logarithmic scaling the average risk figure is the logarithmic average of the Best and Worst risk figures:

$$\text{Ln(Average risk)} = (\text{Ln A} + \text{Ln B})/2$$
$$\text{Ln(Average risk)} = ((\text{Ln}(3.0\text{E-}08) + \text{Ln}(3.0\text{E-}04))/2$$

Average risk for this example = 3.0E-06 for any single hazard
Similar risk graphs with specific tolerable risk targets for societal consequences, asset loss and environmental consequences usually form a complete risk assessment.

Layers of Protection Analysis (LOPA)
LOPA is rapidly becoming a popular method for risk assessment and SIL determination ant it was developed by the American Institute of Chemical Engineers Centre for Chemical Process Safety as *'Layer of Protection Analysis Simplified Process Assessment', 2001.* An example of a LOPA worksheet is shown in Figure 5.

The consequence severity and likelihood of a hazardous event are quantified for every cause/consequence pair in the absence of any protection or mitigation measures. Credit is taken for risk reduction afforded by independent protection layers and also factors which are considered to make a contribution towards mitigating the consequences.



Impact Event	Initiating Causes	Event Frequency	Protection Layers					Intermediate Event Frequency	**Required SIS Risk Reduction**	Tolerable Event Frequency
			Process Design	Mechanical	Process Control	Occupancy	Other			
Overpressure of the first stage separator and significant damage to surrounding process area. Possibility of two fatalities	Outlet blockage	0.1/year	0.5	0.1 Relief Valve	0.1	0.1	0.5 Alarm	2.5E4/year		1.0E-5
	Pressure control failure	0.2/year	0.5	0.1 Relief Valve	1.0	0.1	0.5 Alarm	5.0E-4/year		
								Total 7.5E-4/year	1.0E-5 7.5E-4 **1.3E-2** **(SIL 1)**	

Figure 5. LOPA worksheet example

Conditional modifiers are also used to credit further risk reduction which might only be specific to workers, society, the asset or the environment; e.g. a bund round a tank or closed drains will reduce the environmental impact of a spillage but have no effect on the asset loss. Some typical risk reduction layers are shown in Figure 2 and might include:

- Inherent process design factors;
- Process control systems;
- Alarm systems if independent from the process control;
- Existing safety instrumented functionality;
- Personnel occupancy of the area;
- Mechanical protection such a pressure relief;
- Mitigating measures such as fire and gas systems;
- Safety procedures;
- Emergency response procedures.

The total mitigated risk is compared with the tolerable risk targets set for workers, society, the asset and environment and the difference equates to any additional risk reduction factor to be contributed by the SIS. As with risk graphs LOPA must be calibrated to provide meaningful risk targets.

USE OF COST BENEFIT ANALYSIS

BACKGROUND

When a safety target is set then, by achieving the determined SIL for the SIS, the safety target will be met.

However, there still remains the question about whether sufficient risk reduction has been made for satisfying the 'as low as reasonably practicable' requirement i.e. should additional risk reduction measures be applied?

In Figure 6 this would amount to moving the safety target further down the tolerable risk region if the costs were not disproportionate.

The Hazardous Installations Directorate (HID) approaches 'as low as reasonably practicable' (ALARP) in the same way as the guidance provided in the *HSE R2P2 document, 2001.*

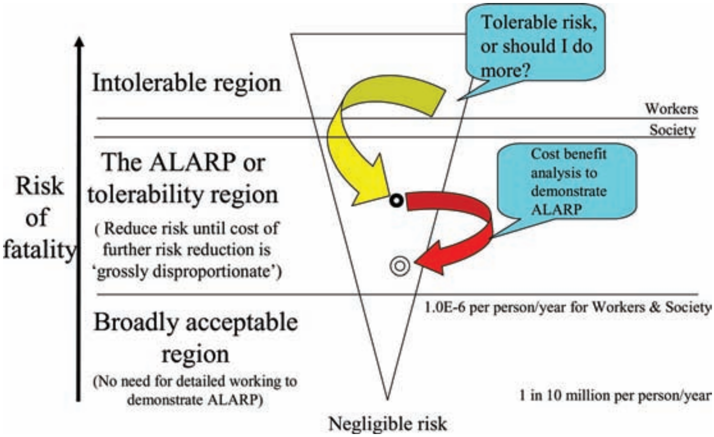

Tolerable risk, or should I do more?
Intolerable region
Workers
Society
The ALARP or tolerability region
(Reduce risk until cost of further risk reduction is 'grossly disproportionate')
Cost benefit analysis to demonstrate ALARP
Risk of fatality
1.0E-6 per person/year for Workers & Society
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
1 in 10 million per person/year
Negligible risk

Figure 6. Requirement for additional risk reduction measures

The cost benefit analysis (CBA) is based on an estimate of the costs of a risk reduction measure and the number of casualties saved by implementation.

This takes:

$$\text{The cost of preventing a fatality (CPF)} = \frac{\text{Total cost of the risk reduction measure}}{\text{Total fatalities prevented}}$$

Then by comparing this with the value of preventing a fatality (VPF)* an estimate can be made of the proportion factor:

$$\text{Proportion Factor} = \frac{\text{CPF}}{\text{VPF}}$$

When the Proportion Factor is 1 or less (or even 2 or less) then R2P2 advises that additional measures should be implemented.

**R2P2 Appendix 3 Para graph 13: 'VPF is often misunderstood to mean that a value is being placed on a life. This is not the case. It is simply another way of saying what people are prepared to pay to secure an average risk reduction. A VPF of £1,000,000 corresponds to a risk reduction of 1 in 100,000 being worth £10 to an average individual. VPF is therefore not to be confused with what society, or the courts, might put on the life of a real person or the compensation appropriate to its loss.' 'VPF will vary depending on the particular hazardous situation.'*

This is fine for assessing the benefit where no risk reduction has been previously specified. The CBA is a little more complex when an operator already has specified certain risk reduction measures, but needs to demonstrate whether further risk reduction would be cost effective. This is often the situation when designing SIS. In many cases the cost of existing measures is not known, particularly on legacy or brown field installations.

Thus the difference between the current risk reduction measures and the additional risk reduction, achieved by implementation of further measures, has to be analysed. This involves the additional costs of implementation, the difference in risk reduction achieved and the value for all fatalities prevented over the predicted life time operation of the facility.

In this case:

$$\text{Proportion Factor} = \text{CPF/VPF}$$

Or

$$P_f = \text{CPF/VPF}$$

Then:

$$\text{CPF} = P_f{}^{*}\,\text{VPF} \tag{1}$$

And since

$$\text{CPF} = \frac{\text{Total cost of the risk reduction measures}}{\text{Total fatalities prevented}}$$

Then

$$P_f^{*}\ \text{Total fatalities prevented} = \text{Total cost of risk reduction measures} \tag{2}$$

Substituting (1) for CPF:

$$(\text{Pf}^{*}\,\text{VPF})^{*}\,\text{Total fatalities prevented} = \text{Total cost of risk reduction measures} \tag{3}$$

And since the total fatalities prevented is represented by a product of the frequency of demand (F) on the SIS, the probability of failure on a demand (PFD), the operating life of the plant and the number of fatalities (N) resulting from the hazardous event:

$$\text{Total fatalities prevented} = \text{F} \times \text{PFD} \times \text{PL} \times \text{N} \tag{4}$$

Then substituting for (4 in 3):

$$(\text{Pf}^{*}\,\text{VPF})^{*}\,(\text{F}^{*}\,\text{PFD}^{*}\,\text{PL}^{*}\,\text{N}) = \text{Total cost of risk reduction measures} \tag{5}$$

where:

$$\begin{aligned}\text{Pf} &= \text{Proportion factor}\\ \text{VPF} &= \text{Value of preventing a fatality}\\ \text{F} &= \text{Frequency of demand on the SIF (for a range use high frequency value)}\\ \text{PFD} &= \text{Probability of failure of the SIF}\\ \text{PL} &= \text{Plant operating life}\\ \text{N} &= \text{Number of fatalities per hazardous event}\end{aligned}$$

Where an existing risk reduction proposal has been made through a risk assessment (such as by use of a risk graph or LOPA), then the comparison between the existing solution and further achievable risk reduction will be the difference in the PFD of the existing proposal and the PFD of the additional risk reduction measures.

If

$$\begin{aligned}\text{pfd}_1 &= \text{PFD of existing proposal from risk assessment}\\ \text{pfd}_2 &= \text{PFD of additional risk reduction measures}\end{aligned}$$

$$\text{Total ADDITIONAL fatalities prevented} = \text{F}^*(\text{pfd}_1 - \text{pfd}_2)^*\text{PL}^*\text{N} \tag{6}$$

then

$$\text{P}_\text{f}^*\,\text{VPF}^*\,\text{Total fatalities prevented} = \text{Total cost of risk reduction measures}$$

Becomes

$$\text{P}_\text{f}^*\,\text{VPF}^*(\text{F}^*(\text{pfd}_1 - \text{pfd}_2)^*\text{PL}^*\text{N}) = \text{Total cost of FURTHER risk reduction measures}\ldots \tag{7}$$

But at what value should the objective pfd$_2$ be set?

This paper suggests that the ALARP threshold of ‘broadly acceptable’ is the ultimate objective i.e. 1.0E-06 for both workers and public for **all** risks.

Thus using the factor of ten times more sensitive for any single hazard this would be a pfd$_2$ of 1.0E-07.

Note.

R2P2 indicates the Proportion Factor ‘P$_\text{f}$’ should be:

10 when working close to tolerable/unacceptable boundary;
1–2 when working close to the broadly acceptable boundary.

A value of 1 will be used for P$_\text{f}$ as pdf$_2$ is at the ‘broadly acceptable’ level of risk.
This is best demonstrated by way of an example:

CALCULATED EXAMPLE
Where:

- The tolerable risk will be based on the example risk graph calibration described in Section 2.6.1 i.e. 3.0E-06;
- Value of preventing a fatality (VPF) = £2,000,000 for voluntary (workers);
- The boundary between Tolerable and Broadly Acceptable = 1 in 1,000,000 for both workers and public – *HSE R2P2.*
- The number of **onsite** fatalities estimated due to a major toxic release (N) = 10.
- The frequency of demand (F) = 0.1 (1 in ten years).
- The operational plant life expectancy (PL) = 30 years.

The PFD of current proposal (pfd_1) = 3.0E-06 (Tolerable risk calibration of the risk graph).

The PFD of additional measures (pfd_2) = 1.0E-07 (The 'broadly acceptable' value of 1.0E-06 for public and workers increased by a factor of ten for the single hazard analysis).
Then:

Using equation (7) total cost of risk reduction measures (C_t) = P_f*VPF*(F * (pfd_1 - pfd_2) * PL * N)

$$C_t = 1.0 * 2{,}000{,}000 * (0.1 * (3.0E\text{-}6 - 1.0E\text{-}7) * 30 * 10)$$
$$C_t = 174$$

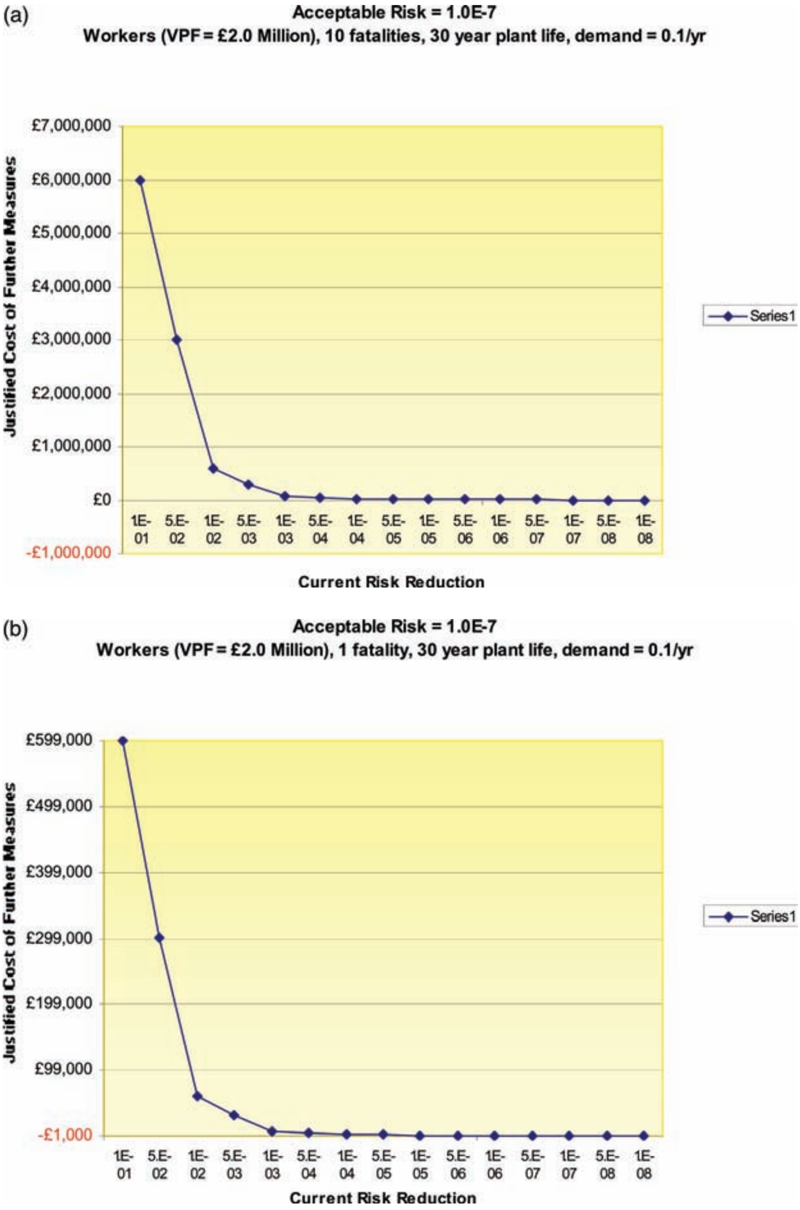
The total discounted cost of further risk reduction measures would need to be below £174. Thus, in this example, additional measures would be implemented if the total cumulative discounted cost over the plant/project life of 30 years was below £174. This also demonstrates that the calibration of the safety target, for the risk graph used in this example, is very close to ALARP.

If a range of pfd_1 values is plotted for 10 fatalities against a 'broadly acceptable' risk for pdf_2 of 1.0E-07 then Figure 7 indicates that further risk reduction measures of many millions of pounds would be justified if the current risk reduction measures achieved less than 1.0E-2. It also indicates that there is a distinct flattening of the curve at around 1.0E-04 indicating that any safety target achieving greater risk reduction than this value is likely to achieve ALARP.

If the curve is plotted for a single fatality over the same range as in Figure 7b the scale of the justified cost of further risk reduction measures decreases, as would be expected but the knee of the curve is identical.

CONCLUSIONS

There is a considerable gap between the current guidance on ALARP which is concerned with total annual risk from all hazards and the situation facing designers of functions within safety instrumented systems protecting against single hazards.



(a) Acceptable Risk = 1.0E-7
Workers (VPF = £2.0 Million), 10 fatalities, 30 year plant life, demand = 0.1/yr

(b) Acceptable Risk = 1.0E-7
Workers (VPF = £2.0 Million), 1 fatality, 30 year plant life, demand = 0.1/yr

Figure 7. 1 Fatality – justified cost of further measures/current risk reduction

Thus designers are currently forced to develop their own rationale for implementing SIS to meet ALARP requirements. This paper has made suggestions for setting tolerable risk targets, or safety targets, for single hazards, and it has also indicated how these can then be developed to demonstrate ALARP through cost benefit analysis.

The purpose of this paper is to stimulate discussion and promote the need for further guidance on ALARP from a Safety Instrumented Systems perspective.

REFERENCES

1. American Institute of Chemical Engineers Centre for Chemical Process Safety, Layer of Protection Analysis Simplified Process Assessment, 2001.
2. BS IEC 61511-3: 2003. Functional safety – Safety Instrumented Systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels.
3. European Seveso Directive, 1982 (Council Directive 81/501/EEC) reviewed 1996 and adopted as Seveso II Directive.
4. HSE document: Reducing Risks, Protecting People (R2P2), 2001 – ISBN: 07176 21 51 0.
5. HMSO Statutory Instruments 1999 No. 743, The Control of Major Accident Hazards Regulations 1999 (COMAH), ISBN 0 11 082192 0.