# ALARP Framework

## Guidance on achievement of ALARP in the Process Industries

# 1 Contents

# 2 Revision History

| Version | Date | Author | Comments |
|---|---|---|---|
| 1 | 05/03/19 | R Martin | First Published issue |

**Foreword**

This paper is challenging. Not because it is long and detailed (which it is), but because it questions what has become normal. As the paper describes, the concept of ALARP is a key part of demonstrating compliance with the laws of the land. But it is typical in hazardous industries to treat ALARP as "tick-box" exercise at the end of the project, by confirming that there are no simple ways of providing further risk reduction to the hazards that remain in the process. This paper argues that ALARP should instead be treated as a philosophy and mindset that should be applied throughout the lifecycle of a project.

The 61508 Association has published guidance for many years, but it has been mostly confirming what the members all knew was the right approach. This paper is different – it challenges and questions the approach that many of us have become comfortable with. I – along with others in the association - find the contents very persuasive and thought provoking. I recommend it to you and hope that you will find it as stimulating as I did.

Dil Wetherill

Chair of The 61508 Association.

## Preface

ALARP as a concept is often associated with afterthought, but it should be so much more. This document is written from an ALARP perspective because in the UK and many other countries, ALARP is what links risk management with the law.

The document is aimed at process risk management / process safety practitioners who wish to ensure that the ALARP concept is embedded in the safety management system.

ALARP is associated with the management of safety and has no particular association to BS EN 61508 (and the daughter standard, BS EN 61511). In this document, references to these standards are kept to a minimum.

Whilst the concept of ALARP is reasonably straight forward, Working Group 10 (the authors of this document) found several challenges in attempting to produce a document which is, as near as possible, a 'once through' read which also serves the need to provide useful reference.

The 61508 Association welcomes constructive comments on all its publications (for directions on how to comment, please refer to http://www.61508.org/contact.htm).

Whilst every effort has been made to ensure the accuracy and applicability, neither the Association nor its members accept any liability for any adverse consequences of use made of the information herein.

# 3 Introduction

In the UK ALARP is principally established in the Health and Safety at Work etc. Act 1974 [1] (HSWA). This is an 'enabling act' which allows parties (in this case the HSE) appointed by parliament to develop regulations and use their powers to ensure such regulations are met: the regulations in effect become secondary law. The HSE is empowered to bring prosecutions on behalf of the crown if the regulations are not followed.

The EU Framework Directive (1989/391/EEC) 1989 [14] establishes general principles for managing health and safety including the responsibility of the employer, the rights/duties of workers, the using of risk assessments to continuously improve company processes and workplace health and safety representation.

The Management of Health and Safety at Work Regulations 1999 [2] implement into UK law the requirements of the EU Framework Directive, together with the five other regulations, collectively referred to as 'the six pack'.

In these regulations some key duties are laid down for employers (duty holders); these include:

- Carrying out a suitable and sufficient risk assessment of all risks to people;
- Reducing risks to people 'so far as is reasonably practicable';
- Having an effective Safety Management System in place.

The UK courts (in case law established by Edwards v NCB 1948) have established the principle of gross disproportion. This has the effect of requiring that costs are grossly disproportionate to benefits before a risk reduction measure is deemed not to be reasonably practicable.

The HSWA requires duty holders to reduce risks 'so far as is reasonably practicable'. The HSE uses the term 'as low as reasonably practicable' (ALARP).and states that the two terms have essentially the same meaning.

In essence, the prime duty of the duty holder is therefore to ensure that risks are managed to be ALARP. The HSE has made an interpretation of what that should entail and sets this out in Reducing Risk and Protecting People (R2P2 [3]).

The HSE addresses all types of work and hence identifies a wide range of risk assessment and ALARP techniques covering the full spectrum of risks ranging from what it describes as 'Broadly Acceptable' through to 'Intolerable'. What the duty holder must do to demonstrate an ALARP case depends considerably on the degree and the complexity of the risk. In the Process Industries, the aggregated residual risk for a worker exposed to process plant risks would be at the riskier end of the spectrum.

## 3.1 Aim of this guidance

This guidance is aimed at the Process Industries and associated process plant risks (as covered by IEC 61511 [7]). In particular this guidance focuses on interpreting what systems must be in place in order to establish ALARP for cases of large projects and for ongoing maintenance (Phases 1 to 7 of the safety lifecycle according to IEC 61511).

In R2P2, the HSE sets out the framework for Tolerability of Risk and demonstration of ALARP. In effect, tolerability of risk and ALARP are defined quantitatively where tolerability sets the boundaries and ALARP is demonstrated by application of relevant good practice, risk assessment and reaching a point where costs of further or alternative risk reduction measures are grossly disproportionate to benefit.

The need to demonstrate, by way of costs and benefits, implies a necessity for a quantitative approach to risk measurement and control. We shall see, however, that where risk is of a 'day-to-day' nature (e.g. driving, crossing the road, slips, trips and falls) or for cases where the risk is very low and non-complex and risk controls are well evidenced, the HSE does not insist on a quantitative demonstration.

This guidance assumes that where an individual works in a Process Industries environment (where daily work involves exposure to process plant risks), a quantitative demonstration of the individual's overall risk of fatality is required.

This guidance also considers the challenges to the concept of ALARP for process plant risks. It discusses many of the issues related to the concept of ALARP and offers a basic framework setting out what is required for ALARP to be managed as a lifecycle concept.

Further guidance is offered on how best to manage specific aspects. The intention is that it is structured in a form where the further guidance offered can be expanded in the future.

## 3.2 Intended readership for this guidance

The intended readership is anyone working in the Process Industries with an engineering or management role associated with the inception, design, installation, commissioning, operation and maintenance of process plant where an understanding of what is meant by ALARP and how to achieve it is required.

## 3.3 Background - ALARP Challenges

From the HSE perspective, the risks must be ALARP and to be ALARP they must also be tolerable. It is therefore assumed in applying any final ALARP justification that risks will already have been demonstrated to be tolerable.

In understanding what needs to be done to establish an ALARP justification for the process plant risks, a number of issues arise which need careful consideration. These include:

- The ALARP case for an existing facility is based on demonstrating that costs of all proposed additional / alternative risk reduction measures are grossly disproportionate to the benefits that they would bring. (see http://www.hse.gov.uk/risk/theory/alarpcba.htm [10]). How should this be demonstrated? Can a qualitative judgement ever be used to justify ALARP and if so under what circumstances would that be reasonable?
- Where does a proposed risk reduction measure come from? Who has to propose it? What if one can't be thought of?
- Given that a proposed risk reduction measure exits, what reasonable steps can be used to avoid spending and inordinate amount of time and expense in searching for a solution. For example, much time may be spent designing alternative risk reduction only to find that once the benefits

are evaluated the costs are found to be grossly disproportionate. What if several proposed measures exist? Is there a better way to approach the problem?

- In the case of a new or substantially modified plant (not yet designed), what do we mean by 'additional / alternative risk reduction measures' when no measures currently exist? Would we leave some risk reduction out of a design to give scope to add 'ALARP' measures at the end? Would such an approach itself be ALARP?
- There is a tendency for engineers to build what has 'worked' in the past. But there is an HSE expectation (see [5]) that newer plants are safer than old because they benefit from new knowledge and technology. If we build what worked in the past, we effectively build a 'legacy' plant where the ALARP considerations are likely to arrive at the same point as an existing legacy plant. How do we ensure our whole approach is ALARP?
- Since the advent of IEC61508 [6], phrases like 'SIL Determination' have arisen which appear to relate to an approach where the process plant is designed with an insufficient degree of safety and then risk assessed retrospectively with a view to 'determining' what additional instrumented safety functions are required in order to make it safe enough. Would such an approach itself be ALARP? Also, does this not lead to the EC&I disciplines being seen as responsible retrospectively for process safety?

When considering the issues above, it helps to first step back and look at a fuller lifecycle picture and how ALARP as a concept fits in. In the Process Industries, the issues associated with ALARP cannot be considered without a full understanding of tolerability of risk, risk assessment and the design process.

The HSE discusses related issues in ALARP "at a glance" [8]. It is not the intention here to replicate that discussion, but it is necessary to distil some key guidance from it.

- The process of ALARP involves adopting all reasonably practicable measures unless they have been ruled out because the cost is grossly disproportionate to the benefit.
- In cases where there is wide experience of a risk, there are usually some established methods of reducing the risk to an acceptable level. These established methods could be in the form of regulations or standards and guidance published by institutions. Such established methods are collectively referred to by the HSE as 'relevant good practice'. There is an HSE expectation that relevant good practice is adopted 'as a baseline'. For high risk hazards, new or complex situations, the expectation is to 'build on good practice'.
- When relevant good practice is recognised as satisfying the law the HSE can endorse it as an Approved Code of Practice.
- There is an expectation by the HSE that duty holders implement relevant good practice as a minimum and (where a duty holder intends to depart from such) there is an expectation that it is first demonstrated to be of satisfaction to the HSE.
- Where good practice has not been established (or the relevance is questionable), where risks are intrinsically high or the risks are complex, there is an expectation that cost benefit analysis is applied to aid decision making.

- For many ALARP decisions, HSE does not expect a detailed Cost Benefit Analysis to be carried out. A simple comparison of cost and benefits (i.e. engineering judgement) can be used to demonstrate gross disproportion where it would be obvious.
- There is a general expectation that the degree of rigour is proportionate to the risk.
- It is emphasised that CBA cannot form the sole argument. There must be a justification for not having considered all available measures.
- Cost and benefit have to be weighed in the same units (money).
- ALARP decisions should be justified and recorded.
- The HSE recognises competence as being highly important when dealing with risks that are not 'day-to-day' risks. To claim competence in a particular area, a person must also understand relevant good practice and how to achieve it.

## 3.4 The approach of this guidance

This guidance first looks at the challenges to the concept of achieving ALARP for the Process Industries and some of the direction given by the HSE.

Following the Introduction, there are three main sections:

- **Risk Assessment, Design and ALARP** - This section looks in detail at the challenges introduced in section 3.3 and discusses how the concepts of Risk Assessment, Design and ALARP must relate to one another. It points at the legal and regulatory framework and makes deductions which are later applied.
- **ALARP Framework** - This section sets out (in terms of requirements) a framework of how to achieve an ALARP approach in project work (covering risk assessment and design). It separately identifies requirements for maintaining an ALARP status. It naturally concludes that the end point of the project phase must also be the start of the maintenance phase.
- **Further Guidance on ALARP Framework** - This section offers detailed examples of how the ALARP Framework requirements may be met. The guidance is not exhaustive and where no further guidance is offered there is a statement to that effect. The intention is that this further guidance may continue to be developed (and further detailed examples added) in the future.

# 4 Definitions and Abbreviations

## 4.1 Terminology

| | |
|---|---|
| EU | European Union |
| Harm Zone | Physical areas of a plant that can be occupied by humans associated with the Hazardous Events |
| Hazardous Event | An event where a Process Hazard can affect the safety of humans |
| Human Exposure | The product of Occupancy and Vulnerability |
| Independent Layer of Protection | A function of people, equipment or system that acts independently to prevent a Hazardous Event. |
| Intrinsic Risk | The risk associated with the unmitigated underlying Process Hazard |
| Occupancy | The statistical probability of being randomly present in a specific Harm Zone |
| Process Hazard | A Hazard associated with the Process |
| Process Hazard Register | A register of Hazardous Events for a defined environment |
| Residual Risk | The risk that remains after all risk control measures have been applied. |
| Safety Function | Any functional measure (whether human or system based) having an effect on the risk to humans the likelihood of failure of which is expressed is as a failure rate or as a probability of failure on demand. |
| Tolerable Risk Criteria | The stated maximum level which an enterprise will tolerate for a given level of harm to an individual or collection of individuals. |
| Vulnerability | Given a Hazardous Event occurs, the statistical probability of fatality for a person in an associated Harm Zone. |

## 4.2 Abbreviations

| | |
|---|---|
| ALARP | As Low as Reasonably Practicable |
| CBA | Cost Benefit Analysis |
| FTA | Fault Tree Analysis |

| | |
|---|---|
| HSE | Health and Safety Executive |
| HSL | Health and Safety Laboratory |
| HSWA | Health and Safety at Work Act |
| IFOF | Individual Frequency of Fatality |
| IPL | Independent Layer of Protection |
| LOPA | Layer of Protection Analysis |
| MHSWR | Management of Health and Safety at Work Regulations (1999). |
| PFD | Probability of Failure on Demand |
| R2P2 | Reducing Risks and Protecting People |
| RA | Risk Assessment |
| RIFOF | Residual Individual Frequency of Fatality |
| QRA | Quantitative Risk Assessment |
| TRC | Tolerable Risk Criteria |

# 5 Risk Assessment, Design and ALARP

It is fundamental to our society that we tolerate risk in order to survive. We understand that life contains 'unavoidable' risks: many of these we have no control over as individuals and little control over as a society. In the UK, the HSE sets out its mission in Reducing Risks and Protecting People (R2P2) [3]. It acknowledges risk as a fact of life.

*The risk of suffering harm is an inescapable aspect of living.*

The HSE recognises that we tolerate additional risks if we see the associated benefits as making the risks worthwhile. This tolerance includes our reliance on industrial processes. There is also a recognition that society changes over time and that the general trend is to become more risk averse and the aim should always be to reduce risk.

*'Tolerable' does not mean 'acceptable'. It refers instead to a willingness by society as a whole to live with a risk so as to secure certain benefits and……in the confidence that the risk is one worth taking and that it is being properly controlled.*

Whilst we tolerate additional risks, the HSE recognises that society demands certain boundaries.

*There are some risks from certain activities, processes or practices which are not tolerable whatever the benefits.*

R2P2 [3] contains a Tolerability of Risk framework for work related risks that reflects those aspects of our society (depicted in the form of the 'carrot' diagram). It makes clear that for certain types of risk (e.g. individual fatality) the duty holder must set out the level of risk that would be tolerated and sets the limit for what is tolerable for individual fatality covering any kind of work but with no definitive boundaries for specific types of work or for outcomes other than fatality.

The Tolerability of Risk framework doesn't focus exclusively on risk of fatality but notes that it is important in any work environment to focus at the right level. In an office environment, for example, skeletal injury, RSI and stress are all health related risks that are far more dominant than the risk of fatality. In a typical office environment (see [12]) the expected fatality rate for an individual is 1e-06 pa. At this level, risk assessments would not need to be quantitative. For people in the Process Industries at risk from the process plant, there are usually several Process Hazard scenarios where it would be expected that the associated risk assessment would be quantitative and the 'currency' of risk would be 'fatalities'.

## 5.1 Tolerability of Risk

In the UK, the HSE Tolerability of Risk framework (see [3]) refers to numerical Tolerable Risk Criteria (TRC), it states:

*HSE has proposed numerical criteria for informing decisions on the tolerability of risks only for very limited categories of risk, for example, those entailing fatalities either individually or in multiple fatality accidents.*

This reinforces the point that HSE only expects quantitative measures where risks of fatality (other than background risks) are involved. This guidance therefore assumes that for process plant risks of fatality, quantitative TRC and corresponding quantitative measures are essential.

Note: This guidance does not propose values for TRC for adoption by a duty holder but (in order to support examples) it makes use of realistic criteria.

### 5.1.1 Tolerable Risk Criteria

Tolerable Risk Criteria (TRC) are a duty holder's statement of what risks associated with its undertaking it will tolerate to its employees and others. For example, a duty holder might state that the maximum fatality risk it will tolerate to an individual employee equates to an expected frequency of fatality of 3e-05pa. This would then be applied to the aggregation of all potential causes of fatality for each employee.

Note: Although the above risk criterion is described as a 'tolerable' risk, it would be better referred to as the 'maximum tolerated risk' – i.e. it represents the upper limit of the tolerable zone. Clearly, there would be no lower limit.

The above TRC represent the maximum tolerated frequency associated with the consequence of fatality to an individual. There are separate categories of risk for other consequences (e.g. broken bones or injury to / fatality of several individuals in one incident) which implies there should be other criteria. In a process plant, it may also be appropriate to have tolerable risk criteria for various degrees of harm. However, with most Process Hazards, reducing the expected frequency of fatality will also reduce the expected frequency of other harm by a similar degree. If the worst-case consequence of a Process Hazard is fatality, the associated risk assessment should consider fatality quantitatively. However, if fatality is extremely unlikely and the risk outcomes dominated by another kind of harm (for example, a chemical hazard might result in a far greater likelihood of loss of eyesight or disfigurement than that of fatality) it is appropriate to concentrate on those outcomes – i.e. those which over time would be seen as more significant.

In R2P2 [3] HSE's stated upper limit of tolerability for expected Individual Frequency of Fatality (IFOF) is given as 1e-03pa and 1e-04pa for worker and member of the public respectively. There is no lower limit, but it is suggested that 1e-06pa may be seen as 'Broadly Acceptable' for both employee and member of the public. For a particular undertaking it is left to the duty holder to specify and justify the upper boundary of tolerability.

Notes:

- HSE Health and Safety statistics show that office workers (e.g. Managerial, Administrative) have a yearly work related fatality expectance of 0.1 per 100,000 workers (see http://researchbriefings.files.parliament.uk/documents/CBP-7458/CBP-7458.pdf [12]) – this is the same level that the HSE deems to be Broadly Acceptable.
- The criteria (as with all TRC) relate to the aggregation of all risks with that consequence.
- It is assumed in this guidance that a person who is exposed to process plant risks is at an overall residual risk that is considerably greater than that which can be considered Broadly Acceptable.

- With respect to risks with consequences other than fatality, the HSE does not give any indication of acceptable boundaries.
- There is a regulatory expectation that a duty holder's TRC migrate over time to reflect improvements in technology and society's decreasing tolerance to risk.

As risk is the product of consequence and likelihood, it follows that higher frequencies are generally tolerated for consequences resulting in lesser harm.

Some duty holders use a scaling system that means risks of different consequence can be compared. This allows comparisons which help in determining the highest impact consequence. This is usually achieved by converting different measures of harm into monetary units.

Some duty holders treat fatality and a serious life changing injury as equal value. Whilst the public perception may be different, the rationale is:

- A serious life changing injury (e.g. resulting in confinement to a wheelchair) may have an equivalent or even greater impact on a person and their family over time than a fatality.
- Estimating the relative probability of a serious injury as opposed to a fatality as a consequence of a hazardous event is very subjective.

### 5.1.2 Tolerable Risk to Individual Hazard Scenarios

Should TRC also carry a limit on an individual Hazard Scenario?

Whilst it is appropriate to limit what would be tolerated as an outcome of an individual Hazard Scenario (or group of related scenarios) there are several potential pitfalls in attempting to use this approach in isolation.
For example, if a worker is at an aggregated risk where the expected IFOF is 1e-04 pa, the risk may be tolerable but it is 100 times higher than the HSE considers to be 'Broadly Acceptable' and only 10 times lower than what would be considered intolerable under any circumstances.
If TRC intended for use for aggregated risk are used for single scenarios, conclusions are likely to be misleading.

To illustrate the point, consider the case where a worker's fatality risks comprise 100 scenarios each of which in isolation would be considered Broadly Acceptable. Can the worker's risk be said to be Broadly Acceptable?

Whether the worker is considered to be at risk of 10 events each with a frequency of fatality of 1e-05 pa or 100 events each with a frequency of fatality of 1e-06 pa is dependent on the quite arbitrary way the various scenarios are constructed. How would it be possible to consider the latter to be Broadly Acceptable and the former not when the risk is identical?

By the same token, it should be clear that it would be possible to manipulate scenarios to the point where they all appear Broadly Acceptable with no change in reality.

When detailed engineering design is taking place, however, it would not be possible to be considering aggregated risk at all times. There is without doubt a need to define realistic TRC for projects, scenarios or

groups of scenarios as step to managing overall risk. It is important to justify the criteria being used in the specific context and with reference to the overall TRC.

Important conclusions from the above are:

- A worker's risk of fatality in a typical Process Industries environment is very unlikely to be in the region of Broadly Acceptable.
- Whilst individual scenarios in isolation may pose low residual risk, it is inappropriate to use that fact to form any overall projection of degree of risk to an individual without taking account of the full risk profile.
- Realistic TRC should be apportioned for parts of the risk profile (e.g. scenario, logical group of scenarios, project) but these would need to be justified in the context and the overall TRC.
- All 'part' TRC should be applied in addition to overall TRC.
- TRC should be stated in a fashion that concisely describes their scope. The associated risks should be calculated against the same scope such that a meaningful comparison with TRC can be made.

Note: It may prove necessary to separate similar Hazardous Events in certain cases in order to closer model the effect on various human groups but otherwise this guidance recommends that Hazardous Event likelihood is treated as a summation of the likelihoods of all constituent scenarios.

### 5.1.3 Societal Risk

The HSE also expresses a concern for 'societal risk' (where a single Hazardous Event can cause multiple fatalities). They contend that society's aversion to such incidents is greater the higher the fatality count. The associated criteria are related to the frequency / number (F-N) where the boundaries of 'Intolerable' and 'Broadly Acceptable' are represented as F-N curves (curves in the F-N domain) (see http://www.hse.gov.uk/research/rrpdf/rr703.pdf [13]).

The tolerable risk criteria for societal risks are applied to single Hazardous Events without any apparent requirement to aggregate. Even if each event on its own is in the tolerable region, clearly the more events in total, the more dangerous the environment is. This lack of requirement for aggregation of societal risks is disconcerting to some extent but it should be noted that these TRC apply simultaneously with others and therefore all such risks should separately be aggregated for all individuals. It is also reasonable that a larger site would have more processes and staff than a smaller one and therefore a higher overall fatality rate would be statistically tolerable.

Whilst R2P2 gives indications of what the HSE see as F-N boundaries, there is some interpretation required in what constitutes a societal hazard – i.e. what does 'N' need to be before the risk is considered societal. By definition, a multiple fatality incident is one involving 2 or more fatalities but in order to know when to apply societal TRC, it is necessary for a duty holder to decide at what point these criteria are applied. There is no specific guidance offered by the HSE. This guidance recommends that the minimum for N should be no greater than 5 for the risk to be considered 'societal'.

### 5.1.4 Summary Notes

The following notes summarise the learning points on Tolerability of Risk:

- Tolerable risk criteria in respect of fatality aren't optional for a duty holder. HSE [3] expects the duty holder to state the level of risk tolerated.
- HSE [3] does not tell a duty holder what is tolerable but it does say what it considers to be intolerable in any circumstances with respect to the consequence of fatality to the individual / society. HSE expects the duty holder to justify the level of risk tolerated.
- The term 'Tolerable' has no lower boundary in theory but (in practical terms) the HSE's 'Broadly Acceptable' risk is the lowest foreseeable residual risk for any occupation.
- The HSE figures given on their 'carrot diagram' in the Tolerability of Risk framework apply to aggregated risk (i.e. all risks to which an individual is exposed as part of an occupation). In particular, for individual 'risk of fatality' (more mathematically: the 'expected frequency of fatality') the duty holder must show that aggregated risks are tolerable.
- Societal risk is a separate measure with separate criteria applied to a number of fatalities from a single incident. Whilst criteria are applied to each incident, there is no requirement from HSE to aggregate risks from a societal perspective.
- All tolerable risk criteria apply simultaneously.
- TRC must be stated in a way that clarifies the scope and a measure made of the risks to which they apply in order that a meaningful comparison can be made.
- The minimum number of people which constitutes a societal risk is not clear; this guidance recommends it is no greater than 5.

## 5.2 Risk Assessment

In order to manage risk, it is first necessary to ensure that the hazard mechanisms and their controls are understood and documented. The mechanisms should be analysed such that the controls and the expected integrity of those controls are also understood and also documented. The effect of those hazards on individuals should then be analysed such that risks can be demonstrated to be tolerable. The expected performance of the controls should be continually assessed and the risks to humans kept under review such that risks are constantly managed ALARP.

In order to inform design and ongoing monitoring, it is important that process plant risk assessment is structured around the hazard mechanisms and the safety functionality.

Regulations must by definition be adhered to. In the UK, the HSE has also set an expectation that relevant good practice will also be applied.

Many risks which are familiar to society come directly under regulations and/or are incorporated in easily recognised good practice standards and guidance produced by representative bodies. In following regulation, standards and guidance it is likely that most risks will be found to be tolerable and ALARP. However, the emphasis here is on the words 'found to be': residual levels of risk should not normally be assumed. In exceptional cases, where there is a wealth of public experience covering the risk and its controls, a tolerable and ALARP position can be justified by applying HSE approved codes of practice. This principal also applies to most day-to-day (background) risks but, due to the complexity and specific nature, most process plant risks would require additional detailed risk assessment.

In any case, if a hazard is one of many to which an individual is exposed, the residual level of risk from all non-background risk contributions must be understood sufficiently to be able to assert that overall risks are tolerable.

Note: In addition to regulation and good practice, there may be relevant 'learning'. For example, past incidents experience by the duty holder or other similar industries might raise considerations that are not yet established in regulation or good practice.

### 5.2.1 Intrinsic Risk

Intrinsic Risk is a term used here to describe the risk associated with an Intrinsic Hazard. Intrinsic Hazard is a term used by HSL (see [5]) to describe an unprotected Hazard. Intrinsic Risk is therefore best appreciated by considering a risk associated with the worst-case consequences of a Hazardous Event.

The concept of Intrinsic Risk is important because the way in which a risk is measured and managed should depend on the degree of Intrinsic Risk rather than the degree of Residual Risk. Intrinsic risk has a strong bearing on the HSE's expectations with regard to the degree of rigour required (see 5.2.5).

Risks which are intrinsically high quite often have associated regulation and / or good practice. For example, the event of a boiler explosion due to over-pressurisation gives a high probability of fatality to anyone in the vicinity. Consequently, there is both regulation and much good practice which duty holders are obliged to implement. The residual risk is likely to be low but that is as a result of robust risk controls.

A low Residual Risk should not be confused with a low Intrinsic Risk.

### 5.2.2 Day-to-day Risk

Day-to-day Risk is a term used here to describe the risk associated with a Day-to-day Hazard. Day-to-day Hazard is a term used by HSL (see [5]) to describe a Hazard which is potentially intrinsically high but which humans are exposed to on a day-to-day basis.

The concept of day-to-day risk is important because it relates to human familiarity with a risk mechanism and risk controls in managing the risk to a tolerable level. A risk being of a 'day-to-day' nature also has a strong bearing on the HSE's expectations with regard the degree of rigour required for risk assessment.

For instance, driving a car is a day-to-day activity which exposes us to risks which are intrinsically high. Without a suitably maintained vehicle and high degree of caution and skill on the part of all drivers, we could expect many fatalities but statistically this is not the case. The reason the residual risk is tolerably low is because statistically our vehicles and our drivers perform well enough to result in a tolerably low risk. Such a risk is treated as a 'day-to-day' risk where it is quite straight forward to demonstrate through statistical evidence that, with existing risk controls properly applied (even though the barriers involve a lot of human activity), sufficient measures are in place to ensure fatalities are tolerably infrequent. In this example, the pursuit of ALARP is still present but it is mostly achieved through vehicle and road safety measures which are applied through regulation.

Note: On process plants, an example of 'day-to-day risks would be those associated with slips, trips and falls. In contrast, process hazard risks cannot be seen as of a 'day-to-day' nature.

### 5.2.3 Risk Assessment – Reaching Decisions

At many points in a project or lifetime of a process plant, safety related decisions are made which set a future course in the design and /or operation of the facility.

Where decisions are safety related, it is important that they are owned, justified and recorded. In some cases, the 'right choice is apparent to all' – for instance where a decision is made to implement a standard which exceeds that of relevant good practice. In such cases a safety related decision can be recorded without particular need for justification.

In other instances, the 'right choice' is not so obvious and some effort should therefore be made to own, justify and record the justification for the decision. Commercial reasoning is expected to form part of the justification, but the appropriate framework should be applied. Here, it must be satisfactorily demonstrated that risks would be tolerable and that the costs of the rejected alternatives would be grossly disproportionate to the benefit (for further information see 5.4.2).

It may be questioned why a decision to implement relevant good practice should be recorded at all: that would depend on circumstance. What is apparent to a person with appropriate competence is not necessarily apparent to all those who may be involved in current or future stages of design or implementation. For purposes of complete audit trail, recording of all safety related decisions together with the reasoning and justification together with a system which ensures that any such decisions are followed is recommended by this guidance.

In contrast, it may be that company standards and procedures already include appropriate provisions and the company's QA system ensures that those involved in a design would follow these. In cases where company standards and procedures have been diligently produced and a suitable QA system is in place to ensure that relevant regulation and good practice is 'inbuilt', the decision to implement company standards and procedures is all that would be necessary. Note: Implicit in this statement is that the company standards and procedures are maintained up to date to ensure that both the scope and the detail of the relevant risks and risk reduction methods are properly developed and policed by competent people.

### 5.2.4 Aggregated Risk

The argument has already been made that, in a process plant, the IFOF is likely to considerably higher than 'Broadly Acceptable' and thus TRC will need to be stated and applied (see 5.1.1).

As TRC are given in quantitative terms, it follows that the measurement of risk must also be given in quantitative terms and in order to demonstrate that TRC are being met, aggregation must first take place.

Notes:

- Some risk assessments involving risk of fatality may exceptionally be risk assessed using non-quantitative methods. Here, a suitable estimate of the measure of fatality risk will be required (see 5.2.5).
- Not all risk consequences will be on the same scale as fatality so it is not intended to imply that all other risks must be quantified or aggregated.

### 5.2.5 Degree of Rigour

Whether a quantitative method of risk assessment is required depends on the degree of rigour required which itself depends on other factors. The HSE's expectation is that the degree of rigour of risk assessment (and by inference the degree of rigour in the establishment of ALARP) should be proportionate to the level of intrinsic risk and the complexity (see HSL RR151 [5]). In an environment where risks are intrinsically low and aggregated IFOF is in the Broadly Acceptable region, HSE would expect no more than a qualitative risk assessment and adherence to relevant good practice.

However, there is something of a conundrum in the above because it appears that a QRA is required in order to demonstrate that one is not required. There is clearly a need to understand the general order of magnitude of risk in the first instance.

Some risks of fatality might be associated with intrinsically low risk Hazardous Events or may be well understood and covered in detail by regulation and/or good practice. In such cases, whilst it is essential to understand the risk mechanisms and manage the associated risks, it may not be essential to carry out a quantitative risk assessment. An example of this might be where an employer provides car parking for its employees. In a car park, where people are walking and driving in the same area, there is undoubtedly a risk of fatality and it could be argued that the risk was intrinsically high (i.e. the collision between a car and a human is usually 'high consequence'). However, because these risks are well understood and statistics show that, with application of good practice risk controls, the residual risk is tolerable, the employer's duty is fulfilled by the application of good practice.

Similarly, for an individual exposed to a 'basket' of process plant risks, there may be some which are close to negligible or may otherwise be in the category where meeting regulation and good practice is all that is required to demonstrate ALARP. However, as indicated in 5.2.4, there is a necessity to compare aggregated risk with TRC. It follows that a method is required of linking the output of a qualitative risk assessment to a quantitative measure.

In justifying that a risk is low in the first instance, some quantitative argument has to be made and therefore must exist.

The following approach is therefore recommended by this guidance:

- Use qualitative methods for risks where the hazard mechanisms are simple, good practice is available and there is good evidence that residual risks are low.
- In other cases, use quantitative methods.
- Provide a justification in cases where qualitative methods are used. As part of that justification, provide:

  - an ALARP justification by reference to the relevant good practice which has been applied.
  - an engineering estimate of the risk to humans including (where relevant) the expected frequency of any hazardous event, the associated harm zone and vulnerability thus providing a conservatively bounded residual risk to individuals.
- Aggregate the residuals from all process plant risks (including those where qualitative methods have been used).

Note: There is some debate about what constitutes a qualitative, a semi-quantitative and a quantitative approach. For avoidance of doubt, this guidance assumes:

- a quantitative approach is one that results in a calculation of risk in risk units (e.g. frequency of fatality) using justified engineering estimates or referenced data as a starting point and developing logically reasoned outputs: for example, employing the use of LOPA or FTA.
- a semi-quantitative approach is one that results in a calculation of risk in risk units with engineering estimates or referenced data as a starting point but using a banded process to develop logically reasoned outputs: for example, where protections layers are taken to be independent with risk reduction taken to an order of magnitude.
- a qualitative approach is one that does not involve units: for example, a 5 x 5 risk matrix using qualitative guide words for consequence and frequency.

When selecting a semi-quantitative approach over a quantitative approach, there will be a loss of accuracy and the logical development will be constricted to some preformed structure. There is a concern that if a technique is chosen blindly (without ensuring it is suitable for the application) it may not result in a realistic estimate of risk or clearly identify the risk controls. A further concern is that if wrongly used, it may well obstruct design decision making and the target driven allocation process and thus the ongoing monitoring and reassessment process. This guidance recommends a technique is only used if it has been shown to be capable of supporting these aspects.

### 5.2.6 The Full Picture

TRC are applied to the expected frequency of fatality for an individual but sometimes addressing risks on this basis alone can obscure some of the picture (particularly with respect to ALARP). Understanding both the total scope of claims made against a safety function and all individuals affected by its failure is key for the purposes of ALARP.

For example, the expected human cost of a Hazardous Event depends on how many people it can affect. In the case of reducing the expected frequency of a Hazardous Event, it is necessary to show the total reduction in expected frequency of fatality and this can only be achieved by mapping the effect of the event to all affected individuals.

Another example is where a single safety function has an effect on several hazardous scenarios. For ALARP purposes, a full measure of the consequence of failure of that safety function is required. Consider the ‘safety function’ as simple as the provision of cooling water across the site: if the expected failure rate of that safety function were reduced, the instantaneous expected fatality rate would be required in an ALARP calculation.

It will be shown in 5.4.2 that, in reaching ALARP justified decisions, it is necessary to have a means of assessing the full 'cost' of an undesirable event in terms of human fatalities and other losses.

To support such an ALARP calculation, a risk assessment method is required which:

- gives an understanding of the total expected 'cost' of the realisation of a Hazardous Event.
- gives an understanding of the increase in risk level associated with failure or impairment of a safety function that can affect multiple scenarios.

### 5.2.7 HAZOP and LOPA

Hazard and Operability Study (Hazop) and Layer of Protection Analysis (LOPA) are mentioned here because they are familiar tools which are often used to facilitate risk assessment. Carefully constructed Hazop and LOPA may generate the information required to support demonstration of both a tolerable and an ALARP position but, used in isolation or without sufficient care, there is a concern that they can create a misleading picture. Careful consideration should be given to the nature and complexity of the risks and when choosing the most effective tools and methods. Care should also be taken in ensuring that safety related decisions made during the course of design lead to an ALARP position and that the tools used help support this.

Hazop is a risk study process whose use is aimed at a completed design: as such, it has lost much of the power to 'inform' design. It is a technique for viewing risks from a bottom upward perspective where it may reveal mechanisms that had not been apparent to the design team from the inherent top downward approach. It's contribution to safety and operability comes from asking guideword led 'what-if' questions of a team who has suitable awareness of all aspects of the design.

However, Hazop has potential pitfalls which include:

- If used in isolation or at the wrong stage in a process it is likely to give a difficult to interpret and incomplete picture of risk.
- Hazop, because of its perspective, can often succeed in revealing Hazard Scenarios that had not been understood from the top downward approach. However, by the same token, it can also fail in finding those that were understood in top downward design and thus should be used to enhance top down risk assessment and not in isolation.
- The choice of 'nodes' can be too small where 'what-if' questions can appear too trivial; or they can be too large where 'what-if' questions can appear too complex.
- If the choice of 'nodes' does not properly reflect the control system architecture, the answers to 'what-if' questions can be too complex to be fully comprehended.
- Sometimes a Hazop rule is imposed where the team attempts to consider only Hazardous Events associated with the node currently under consideration. If so, how is any node cross boundary risk understood or captured for consideration elsewhere?
- Sometimes a Hazop rule is imposed where the team attempts to consider Hazardous Events that can occur in any node. That would require members of the team to have access to and be familiar with the whole plant design.
- Hazop is 'guideword' led but guidewords are often introduced in an order which doesn't consider the most appropriate 'deviations' first: this can easily lead to fragmented scenario capture.

- Hazop, like many others, is a lifecycle activity and therefore its outputs should themselves be maintained throughout the lifecycle. It is sometimes mistakenly seen as a one-off exercise whose output 'report' is fixed throughout time thus obstructing intelligent revision at a later date.

Therefore, this guidance recommends:

- Use of Hazop as a complementary process on a design which has been declared complete to an appropriate degree.
- Use of Hazop to contribute to the expansion of (and not supersede) the Risk Assessment.
- Choosing nodes carefully to be of the optimum size and (importantly) to reflect the architecture of the control system so that the plant is seen as 'equipment under control' in a 'process under control'.
- Including the control system 'what-if' questions in the Hazop.
- Setting the rules clearly so that the node cross-boundary hazard mechanisms are managed in a systematic fashion.
- Choosing guidewords which reflect the process and order their use to best reflect the type of process to help produce a well consolidated output.
- Regarding Hazop as a lifecycle activity and not a single 'report' fixed in time. Ensure that if Hazop was used on an incomplete design, it is revisited and revised for the completed design.

LOPA is a tool that may be used to assess the residual frequency of an event after applying several independent layers of protection to the 'unmitigated' frequency of the initiating event. Its appeal is in its simplicity and ease of use. It usually appears as a spreadsheet where it is used to multiply the independent probabilities and give a result that can be readily compared with TRC.

However, it has potential pitfalls which include:

- LOPA is sometimes applied directly to the output of a risk assessment (e.g. Hazop) where the scenarios have not been consolidated. Attempting to apply TRC to fragmented scenarios can lead to confusion amongst the team and to meaningless measurements of risk.
- LOPA's simplicity can be a drawback when attempting to deal with complex scenarios (i.e. those where the mechanism is not easily represented by a series of independent layers of protection).
- Where two or more 'events' need to have occurred for a scenario to manifest itself then LOPA would treat this as an initiating event with one or more enabling event(s) but, depending on what order events occur in, events can be initiating events or enabling events in the same hazard mechanism. A simple example of this is the fire/explosion 'triangle' of fuel, oxygen and ignition source. In the general case, each of the 3 events can be enabling or initiating events and thus would require 3 separate lines of LOPA to cover. Ensuring that that the full picture of a mechanism appears in such cases can be challenging and leads to a lot of repetition when LOPA is selected.
- LOPA is often used to include the mapping of the exposure of the 'most exposed' hypothetical individual in order to demonstrate that the residual frequency of fatality associated with a scenario is tolerable. If the residual frequency is found to be particularly low, the scenario is not

flagged for ALARP consideration. However, ALARP considerations must consider the effect on the whole human population and also the non-human costs associated with the event. Care would need to be taken in adapting LOPA to generate the relevant information.

- Observing the significance of a single event (such as failure of motive power, cooling water or process steam) is a very important ALARP step. To be able to test the sensitivity of such events requires being able to study the combined effect on a number of scenarios simultaneously on the whole of the population. Care would need to be taken in adapting LOPA to generate the relevant information.

Therefore this guidance recommends:

- Ensuring that Hazard Scenarios are properly consolidated and that the risk assessment is structured around the hazard mechanisms and the safety functionality.
- Ensuring that there is a suitable method for applying human fatality TRC to 'rolled up' scenarios.
- Using LOPA only where the scenarios are suitably simple.
- Ensuring that the expected frequency of the Hazardous Event is derived as part of the process and that there is a mechanism for mapping on all Human Exposure (not just the most exposed individual).
- Ensuring that there is a suitable complementary method in place to reveal the consequences of a single event that affects many Hazard Scenarios.

### 5.2.8 SIL Determination

An approach which is sometimes followed involves a retrospective risk assessment process after the majority of the design process is complete (often referred to as SIL Determination). Retrospective consideration of process risks is necessary, but care should be taken not to encourage the situation where a process plant could be designed without regard to safety functionality during the design process. Relevant regulation, good practice and prior learning (where such exist) are likely to help but for most process hazards there is also a necessity for a specific risk assessment. Allocations of safety functionality should take place before detailed design so that design is suitably informed.

In essence, SIL Determination is a process which identifies 'risk gaps' which are then (by inference) allocated to instrumented safety functions. However, if a risk informed design had been carried out, it should be of concern if any 'risk gaps' remain and consideration would then need to be given to whether the approach had truly been ALARP. In particular:

- How did the design process to this point lead to unsupportable levels of residual risk?
- Is there a practicable instrumented function that can achieve this risk reduction?
- Should the required risk reduction be allocated to an instrumented function or are there other practical ways of reducing risk higher up the hierarchy of controls (see 5.4.3)?
- According to regulations and good practice, has any order of preference for allocation of risk reduction been taken into account?

In summary, SIL Determination appears to be a method best suited to 'legacy' process plants rather than new plants or projects. Its name implies that there is a presumption that the allocation of any gap will be to an instrumented function.

Therefore, this guidance recommends that: SIL Determination should not be used for new plant or projects; if used on legacy plants, if 'risk gaps' are found, there should be no automatic allocation to instrumented functions.

### 5.2.9 Engineering Judgement and Justification

As described, risk assessment analyses the hazard mechanisms and the deployed controls. The problem for engineers is in estimation of the residual frequencies of Hazardous Events when those frequencies are very low. Rarely does suitable detailed data exist and a common pitfall is to arrive at estimated frequency of a Hazardous Event which cannot be justified by experience or reference data.

It is often assumed that without studying a mechanism in detail, a team of people might qualitatively judge the frequency of a very rare event. There are several associated concerns:

- There is an implicit assumption that, because the judgement belongs to several people, it leads to a higher degree of accuracy. If the event (which itself is a complex derivative of other events) is so rare that it is outside of the experience of anyone present, the judgement is no safer than if one person made it.
- Also, the more people involved, the less direct ownership of the judgement there is.
- It is impossible to keep 'under review' or to establish leading indicators. When the next risk assessment is periodically reviewed, if the event has not taken place there would be no new information to help refine the assessment so the risk assessment could not be improved with experience.

There are other examples of poor practice:

- The team has made a qualitative judgement that a Hazardous Event is 'very rare' and has used that in a risk graph that has been calibrated on the basis that a 'very rare' event occurs at a frequency of 1e-05pa.
- There have been several hazardous events of this kind around the world but none so far in the UK. The team have therefore judged that an event likelihood is vanishingly small because this plant is in the UK.
- The safety information for a project carried out by a supplier has arrived so it is given to the C&I engineer to review.

The above are all examples of where engineering judgement is being used or requested inappropriately. An important principle is to use the study of the mechanisms by an appropriately selected multi-disciplined team together with use of engineering estimates made by appropriate disciplines. The mechanisms are logical so should not be subjective but if broken down into suitable elements, the likelihood of failure of elements becomes within the scope of engineering judgements. A justifiable judgement could be based on statistics (e.g. a failure rate database), relevant plant experience or (perhaps better) a mixture of both. The emphasis is on 'justifiable': all engineering judgements should be justified, recorded and kept under review.

By logically combining knowledge of mechanisms with justified engineering judgements, it is possible to produce a realistic (and justified) engineering assessment of the frequency of a Hazardous Event.

Engineering judgements should also be capable of and be 'kept under' review and should be the subject of allocated performance targets (allocations).

The following is an example of good use of engineering judgements:

- A safety related engineering judgement has been made that a motor driven pump will fail to pump cooling water for a number of reasons (e.g. control failure, motor failure, pump mechanical failure).
- The summated failure frequency for all failure modes has been judged to be 0.1pa.
- The estimated failure rate used in a constructed risk assessment is 0.1 pa but because of redundancy in the system, this results in the overall failure to provide sufficient cooling water having a derived frequency of 3.0 e-4 pa (a figure that is outside the experience of anyone but is derivable from logical reasoning and events which are within experience).
- The allocation of a safety function to the cooling water system is then made to provide sufficient cooling water with a failure frequency of no worse than 3.0e-4 pa. Data is collected on cooling water system failure but (given this frequency) there is very unlikely to be any in the life time of the plant.
- The allocation of a safety function to each cooling water pump is also made to provide its share of cooling water with a failure frequency of no worse than 0.1 pa. Data is collected on cooling water pump failure but (because there are 5 cooling water pumps) the expected total failure frequency is 0.5 pa.
- After 2 years of running there have been 3 failures of cooling water pumps. A review of the risk assessment shows that this is a 50% higher than expected failure rate. That data was fed into the same system calculation which meant that the cooling water safety function failure frequency was revised to 4.5 e-4 pa.
- Risk scenarios affected by loss of cooling water were examined and recalculated. Resulting risks were shown to be tolerable and still with a comfortable margin.
- A low-level investigation was launched to see if the 3 failures which had occurred shared anything in common or whether there was any practicable improvements in operation and maintenance that could be implemented.

This guidance recommends that all safety related engineering judgements:

- must be within experience.
- attributed to appropriately competent individuals.
- justified and recorded.
- allocated.
- kept under review together with related risk assessment.

### 5.2.10 Risk Graphs

There is belief in many places in the benefits of using Risk Graphs. Risk graphs work by grouping risks and risk controls into one of several categories and then using a simple graphical means to identify risk gaps.

When used for process plant risks of fatality, there are a number of potential pitfalls:

- Typically, a risk graph takes into account the expected frequency of a Hazardous Event and maps on the human exposure (likelihood of consequence, number of people affected, and chance of

escape). In this form they cannot be used to build a picture of the hazard mechanism and thus usually lead to unjustifiable estimates of the frequency of a Hazardous Event (see 5.2.9)

- Risk graphs cannot be easily adapted to produce other information (e.g. risk to an individual; or a sensitivity test of failure of a safety function; the summation of risk for comparison to overall TRC) which are requirements of the overall safety management system.
- Risk graphs must be calibrated to specific TRC and, because of the inherent coarseness, the calibration must be conservative.
- Risk graphs can only identify overall risk gaps, they cannot help to inform design decisions. They are often used simply as 'SIL Determination' tools.

In summary, risk graphs appear to be an elaborate method of providing a simple calculation and in doing so lead the user towards many of the pitfalls identified in this section. As such this guidance does not recommend their use.

### 5.2.11 Insignificant Risks

Is there a point at which a risk of fatality is so low that it can be treated as insignificant or tolerated without treating further? Certainly, this seems to be the case for day-to-day risks but is it ever the correct approach for process plant risks?

Issues that give rise to concern include:

- The risk from an intrinsically high Hazardous Event may be managed low so it follows that the risk and its barriers need to be understood and continually accounted for to keep the risk low. It is necessary to be able to measure the effect of removed or impaired barriers (even on a temporary basis). It is not therefore appropriate to discount the risk from a hazard scenario when the risk is intrinsically high.
- If a risk of fatality from a scenario is considered insignificant and therefore discounted, it may be that there are a multitude of scenarios which lead to the realisation of the same Hazardous Event which (when aggregated) may result in a level of risk which requires further assessment and potentially further mitigations.
- If a risk of fatality from a scenario is considered insignificant and therefore discounted, it may be that there are many seemingly insignificant risks which (when aggregated) amount to a significant risk.
- There is not definition of a single scenario. If the level of risk to a particular scenario appears intolerable, it is always possible to divide a scenario into several scenarios until a point is reached where the residual risk from each scenario appears to be tolerable.

In summary, care needs to be taken with process plant risk to ensure that the full picture of each hazardous event emerges; that risks which are managed low rather than intrinsically low are fully examined and fully accounted for; and that the aggregation of discounted risk is insignificant.

### 5.2.12 Temporary Exposure to Hazards

Risk Assessments are generally constructed for daily running of a process plant. This should include risk associated with all foreseeable tasks such as planned testing and general maintenance. However, plant is

often designed with redundancy such that major maintenance or refit can be carried while the plant is still operating in some capacity – i.e. with many of the process hazards still present. Risk Assessments around major maintenance are usually dealt with as 'construction' type issues but, if a large construction workforce is present whilst process plant risks exist, surely that gives rise to the need for a process plant risk assessment.

It would not be expected to foresee every major maintenance case during the risk assessments performed during the development of a design, so it becomes essential that a means is at hand to extend the current risk assessment process to model risk to people who are temporarily deployed to carry out some unforeseen task.

A temporary 'construction' worker is likely to experience a much higher occupancy of particular Harm Zones than would be experienced by normal operational staff. Care should therefore be taken that if those are high risk Harm Zones, the risk is managed to a tolerable level.

The fact that the work is 'temporary' may at first sight imply that the overall risk can be seen as low. For example, if construction workers were to spend a full working day in a high-risk Harm Zone for a period of 2 weeks, that may be seen as a small fraction of a year and therefore tolerable if risks are 'annualised'. However, the risk on a day by day basis should be managed to a tolerable level which means any required additional risk barriers should be looking at the appropriate continual level of risk. It would also be inappropriate to make any assumptions about the level of risk to a worker for times when a temporary worker is not acting under the direction of the duty holder.

In addition, there may be many more occupants of a high-risk Harm Zone than in daily running. Care should therefore be taken to ensure that any relevant societal risk concerns are examined and demonstrated to be tolerable and ALARP.

In summary:

- Occupancy of particular Harm Zones is likely to be much higher for temporary work than daily running occupancy.
- The expected number of fatalities for particular Hazardous Events can be much higher than daily running so societal TRC should be applied in addition to that for the individual.
- Temporary risk levels for construction workers should not be seen as 'averaged' over a wider time frame.
- In calculating the required strength of additional temporary barriers, it is the current level of risk that is the important measure.

### 5.2.13 Lifecycle and Audit Trail

As with all activities associated with process safety, it is important to relate them and the documentation produced to the lifecycle of the plant.

The form of the lifecycle documentation needs to be understood and planned early on and then all activities planned so as to contribute to the development and maintenance of those documents. It also

follows that lifecycle documents must be capable of being evolved with the necessary mechanism to support change and revision.

Equally important is to ensure that the audit trail covering the development, revision and maintenance of those documents is also recorded. A mechanism to record relevant meetings, relevant expert advice and relevant decisions must also be in place.

Note: Having the necessary systems in place leads also to the issues of roles and responsibilities and competency management. These issues are not within the scope of this document.

### 5.2.14 Ongoing Risk Assessment

It is important to recognise that Risk Assessment is a lifecycle process and should be used to inform design as well as assess design (this is further discussed in 5.3.1). It should be demonstrable for a design that all reasonably practicable steps have been taken to minimise risk as design has progressed.

In a project context, it is therefore necessary for risk assessment to increase in detail as a project progresses through design. Risk Assessment must also be 'ongoing' (where it is periodically reviewed in the light of relevant new information). It follows that at the point of completion of a project, the Risk Assessment needs to adopt a 'retrospective' form where it may be used to demonstrate risks are both tolerable and ALARP and thus form the basis for 'Ongoing Risk Assessment'.

The retrospective form must also provide measures of risk (further discussed in 6.2 and illustrated in 7.2) in order that it can be demonstrated that risks to all individuals are tolerable and also to facilitate demonstration of ALARP (further discussed in 5.4.2). This entails providing an expected frequency of all Hazardous Events and mapping the human exposure of all individuals to those events.

Note: The form of Ongoing Risk Assessment should also be readily adaptable for modelling temporary situations (see 5.2.12).

### 5.2.15 Summary Notes

The following notes attempt to summarise the learning points on Risk Assessment:

- Relevant regulation must always be applied to risk management. In the UK and many other countries relevant good practice and learning must also be applied.
- For fatality to the individual, the terms Broadly Acceptable and Tolerable if ALARP apply to aggregated risk.
- Intrinsic risk relates to the magnitude of a hazard related risk without risk controls being taken into account. The measure of intrinsic risk should be used amongst other factors to guide the level of rigour in the assessment.
- Day-to-day risk is a term which relates to a risk which is well understood and managed by humans in general where the residual risk is evidentially low. Note: it does not necessarily mean that the intrinsic risk is low but implies that the residuals are demonstrably managed low using universally understood measures.

- The degree of rigour (e.g. qualitative, semi-quantitative, quantitative) applied to a risk assessment must be commensurate with the risk. Hazards with low consequence and low intrinsic risk and /or hazards that are common and well understood may be managed by adherence to regulation and good practice and qualitative risk assessment.
- Quantitative methods must be used where consequences are high and/or the risk is complex.
- Quantitative measures must be used for all significant risks of fatality (even if a qualitative method is used in risk assessment).
- All significant risks of fatality must be aggregated before applying individual TRC.
- It is appropriate to use TRC for portions of overall risk of fatality but these should be applied separately and in addition to the overall company TRC.
- Scenario based TRC, if used, should be managed carefully because it is possible to repeatedly slice scenarios until the risks appear tolerable (see 5.2.11).
- A 'full picture' measure of the consequences of a Hazardous Event is required (i.e. a measure of the summative effect on people at risk to the event as well as the commercial cost of the event).
- A 'full picture' measure of the effect of common events (event common to many hazard scenarios) is required.
- Hazop is a complementary risk assessment technique aimed at use on a completed design. Care should be taken with the process, in particular to: systematically managing cross boundary safety related events; providing challenge to the control system; ensure relevant outputs enhance rather than supersede other risk assessment outputs.
- LOPA is a tool that (other than in simple cases) lacks the versatility required to effectively present the necessary full picture.
- SIL Determination has the connotation of an 'after thought'. If there are 'SIL sized' risk gaps at the end of the design phase, design and associated risk assessment and allocation should be revisited.
- The use of Risk Graphs should be avoided for process plant risks of fatality.
- Estimates of the frequency of Hazardous Events must be justified on the basis of logical understanding of the hazard mechanism and likelihood of failure of elements to which justifiable engineering judgements can be made.
- All safety related decisions should be owned, justified and recorded.
- Both Lifecycle (living documentation) and Audit Trail (historical records) are essential for all safety related issues.
- At the end of a project, risk assessment needs to take on a 'retrospective' form which supports periodic review in light of emerging information.
- Retrospective risk assessment must provide a measure in order that tolerability may be demonstrated and also to facilitate ALARP.
- As with all risks, indicators should be monitored in order to provide ongoing demonstration that the risk assessments remain valid and that risks remain tolerable and ALARP.
- Lifecycle and Audit trail documentation is required to cover all safety related processes and decisions.

## 5.3 Design

### 5.3.1 Design, Risk Assessment, Allocation and ALARP

Risk Assessment aids decision making during design and results in the allocation of safety function requirements. But it's not always easy to see how works in practice.

Safety in design depends heavily on Hazard and Risk Assessment. Risk assessment must be used to 'inform design' (so it occurs before design) but also to determine 'residual risk' (so it occurs after design). In practice, design is a multi-level process and risk assessment must come before and after each level. Viewed more generally, risk assessment is a process that accompanies design where the level of detail in the risk assessment increases with the level of detail in the design.

As design develops into more detail, strategies for managing risk develop. In risk assessment, engineering judgements and assessments become 'assumptions' relating to performance of safety functions. As design and risk assessment progresses, assumptions are realised as safety targets which are then 'allocated' as safety functions with associated integrity. It should be noted that allocated safety functionality and integrity requirements refers to all functions of the safety envelope (not just E/E/PE) and such allocations should be formally specified.

As an example, if it has been assumed during engineering design and risk assessment that a relief valve has a probability of failure on demand (PFD) of 0.005 then there should be an associated safety function specification which states in all terms necessary the limits of acceptable performance of that allocated function together with the required integrity.

It may seem a straight forward process but many of the aspects of the allocation of safety functionality require a forward- looking approach and may well involve negotiation and mutual acceptance between several disciplines who together take overall responsibility for the safety of the design. In the detailed design stage, all allocations should be owned by the relevant parties and thereafter managed.

As the detail of design closes to a finish, the corresponding risk assessment and allocation of safety functionality take on the retrospective form (see 5.2.13). At this stage, the risk assessment should show no 'required risk reductions' but it should assume that all allocated functions and their respective integrity targets will be met. The risk assessment should then show 'residual risks' which should be demonstrably tolerable, but they should also be demonstrated to be ALARP (if necessary, by CBA) before progressing.

It therefore follows that Design, Risk Assessment, Allocation and ALARP Assessment are all parallel activities in a joint process which is ongoing and iterative: they are all interdependent and coterminous.

Once a design is implemented and commissioned the above process is revisited at times of change; at times of unexpected process hazard incidents; and (in any case) periodically. At these times, it should be confirmed that relevant process and operation data continues to support the case for safety.

### 5.3.2 Tolerable Risk Criteria

Implicit in a design project is that TRC must be set specifically for the project unless the project scope involves the whole facility. The project TRC will therefore depend on the scope of the project and the TRC (see 5.1.1) for the facility where a realistic proportion of the overall risk is allocated to the project.

Note: The allocation of risk to the project should be justified and recorded.

### 5.3.3 Adoption of Good Practice / Best Practice

In the UK and many other countries adoption of relevant good practice is a regulatory expectation (see 5.2). Defining all relevant good practice depends to a large extent on the understanding of the process plant hazards and their mechanisms. Any relevant prior learning should also be considered.

Note: The regulatory requirement is to adopt relevant 'good practice' and not 'best practice' but when building new or substantially modifying plant, making the right choice is important because 'current best practice' if reasonably practicable is likely to become the expectation of 'good practice' over a relatively short time.

### 5.3.4 Testability

An important consideration during design is that of ongoing testing of safety functionality.

The risk of failure of a control measure is part of risk assessment and minimising that risk is an important part of design.

If a safety function is of a 'control' type, failure of that function is likely to be detected (usually it can't escape attention) – the critical measure is 'frequency of failure'. If the safety function is of a 'protection' type, failure of the function generally goes un-noticed until there is a demand placed up on it or it is tested – hence the critical measure is 'probability of failure on demand' (PFD). Any safety functionality that can be subject to 'undiagnosed' dangerous failures should be subject to proof test. The scope and the periodicity of the testing would depend on the integrity requirements and the failure modes and inherent integrity of the components which carry out the safety function.

There are some principles which should be considered:

- Where practicable, a safety function should make use of 'auto test'. In non-continuous plants where 'actions' are taking place relatively frequently, it is usually relatively easy to use feedback to show that the safety function failures mechanisms (or a high degree of them) are in a functioning condition. In a continuous plant, sometimes similar can be achieved by designing redundant paths and specific auto-test routines.
- Important is the consideration of what happens in the case of a discovered failure of a protection type function. The strategy may be shut-down and lock out but if failure of the function would not affect the operation of the process it may be to alarm and repair in due course. The latter would entail operating a plant with reduced protection for short periods which itself should be justified ALARP.

- Where auto testing is impracticable, periodic testing needs to be applied. Importantly, the design must include the facility to test a function or device. It is not appropriate to assume an operator would know how to test a function or device periodically and, moreover, the test itself has to be reasonably practicable.

### 5.3.5 Leading Indicators

During risk assessment, engineering judgements are turned into assumptions which are in turn turned into targets (see 5.3.1). During plant operation it is important that these targets are met or exceeded. The understanding of hazard mechanisms built during the design risk assessment activity leads to the ability to focus on strategic data which has the potential to indicate and alert operators to an under performance. Determining these 'leading indicators' is an ongoing responsibility but should first be done in the design phase.

Important note: Risk graphs particularly and even LOPA are risk assessment tools that are difficult to use to drive out the best range of leading indicators. Structured methods (such as Fault Tree Analysis) lend themselves much more readily to identifying suitable data to monitor.

### 5.3.6 Summary Notes

The following notes attempt to summarise the learning points on Design:

- Risk Assessment, Design, Allocation and ALARP are parallel, interdependent and co-terminus activities.
- At the point of completion of a project, Risk Assessment, Allocation and ALARP should adopt the 'retrospective' form.
- Lifecycle and audit trail documentation for safety related aspects must be produced and maintained.
- Adoption of relevant regulation, good practice and prior learning must be applied to design.
- Good practice and not best is required but caution should be exercised because best practice tends to become good practice over time.
- Testing strategy, testability and testing methods are part of design.
- Identifying leading indicators is part of design.

## 5.4 ALARP

### 5.4.1 Tolerable If ALARP

Risks are said to be 'tolerable' (see 5.1) if they fall below the Maximum Tolerable Risk and they are said to be 'Broadly Acceptable' by the HSE if they fall below a suggested figure. The region sometimes referred to as 'Tolerable if ALARP' is that which lies between the Broadly Acceptable risk level and Maximum Tolerable Risk.

Stated simply, risks are said to be 'ALARP' if they are:

- tolerable; and
- it is demonstrated that cost of implementation of any further or alternative risk control measure is grossly disproportionate to the suitably weighted risk avoidance benefit.

Note: There is an implicit assumption that all relevant regulation, good practice and prior learning has been implemented and that ALARP assessments are made in support of decisions throughout the lifecycle.

Because the 'Tolerable' region explicitly relates to aggregated risk then, by implication, the 'Tolerable if ALARP' region must also apply to aggregated risk. It follows therefore that the degree of rigour required for justification of ALARP position must in general depend on the level of aggregated risk. However, it would be impracticable to carry out an ALARP assessment to a degree of rigour that exceeds that of the associated risk assessment.

In making any ALARP justification (see also 5.4.2), it is important to apply the right scope. For example, if the integrity of an evacuation alarm were being assessed, it would not be meaningful to assess it with a single scenario in mind where, in reality, it affected many. For the scope to be appropriate, the justification would need to be based on all the scenarios to which the site evacuation alarm is relevant and for all the people that would be affected. If risk assessments involving site evacuation were carried out qualitatively, there might be no available measure of risk benefit. In such an instance, the qualitative methods would need to be supplemented with reasoned quantitative measure to allow the appropriate judgement to be made.

Therefore, in justifying an ALARP position, this guidance recommends:

- in general, that the assessment is commensurate with the degree of rigour used in risk assessment (see 5.2.5).
- where the assessment relates to the integrity of a safety function that has been qualitatively assessed and which affects a multitude of scenarios, that conservatively bounded quantitative measures (see 5.2.5) are justified and adopted.

### 5.4.2 Cost Benefit Analysis

If risks are significantly above the Broadly Acceptable threshold the HSE expectation is that ALARP will be demonstrated by showing that the cost of all practicable risk reduction measures is grossly disproportional to the benefits that would be achieved including those of averted fatalities.

It is assumed here (see also 3.1 and 5.1.1) that process plant risks result in an overall level of risk considerably greater than that of Broadly Acceptable and thus generally require a quantitative risk assessment (QRA). For an ALARP assessment to be commensurate with the QRA, the HSE (see [10]) indicates that Cost Benefit Analysis (CBA) is required.

In order to form a CBA based judgement, there needs to be a means of establishing the costs and the benefits of additional or alternative means of risk reduction. At any point in the lifecycle, in general, to compare the benefits of proposed alternatives the following must first be established (see [9]):

- The value of a human life.
- A suitable factor for assessment of gross disproportion (to be applied to the human part of the cost).
- The additional cost saving (if any) to the business of avoidance of an incident.

- The expected frequency of associated Hazardous Events for various alternative measures.
- The full susceptibility of humans to each of the associated Hazardous Events.

The HSE has not formulated an algorithm which can be used to determine a factor of gross disproportion. However, it suggests that the factor should range between 2 and 10 depending on the level of risk – the higher the risk, the higher the factor to be adopted.

The HSE does address the value of avoiding harm to humans in their Cost Benefit Analysis Checklist [9]. The value of an averted fatality is given as £1,336,800 (as at Q3 2003).

This guidance recommends as at 2019 a value for averted fatality of £2.2M is adopted together with 5 as a factor of gross disproportion.

Cost benefit analysis is an objective way of determining whether a proposed change to risk reduction measures is worth implementing but calculating the cost of implementation of every potential additional or alternative risk reduction measure could be a daunting task.

However, given that QRA has been applied (and therefore for each Hazardous Event the aggregated IFOF calculation is in place) calculating the benefits of a change in expected frequency of the event is a straight forward exercise. The following method shows how to calculate the benefit based on a notional additional risk reduction measure.

Note: When using CBA, the reference to Hazardous Events (plural) is important. Where safety functionality has an effect on multiple Hazardous Events (see also 5.4.1), the full picture of a change to this functionality is the effect on overall risk. In order that the value of averted fatalities of a proposed change can readily be found, this guidance recommends that fatality risk is modelled in a way that provides and overall expected frequency of fatality (FOF) which aggregates the risk to all individuals.

### *Calculating the Benefit of avoided fatalities*

Before considering the benefit of avoiding a fatality, it is necessary first to understand the cost of a fatality. In order to compare like for like, the HSE requires that the cost of avoided fatalities is converted to a monetary measurement (see [9]).

The basic formula for the cost [pa] for a group of individuals exposed to a Hazardous Event is given by:

Expected Individual Frequency of Fatality (IFOF) x Number of People (N) x Value of life (V).

This assumes that there is only one group of people exposed to the hazard where individuals in a group by definition have equal exposure factor. In the general case, there is more than one group. For additional groups a summation is required (see formula below).

There are a number of different groups (k) each with different exposure to the Hazardous Event and therefore a different IFOF.

$$Cost\_of\_lives = V \times \sum_{i=1}^{k} IFOF_i \times N_i$$

Where:

$N_i$ is the number of individuals in group i

$IFOF_i$ is the individual frequency of fatality of individual in group i

### *Value of Lives Saved for a Specific Additional Risk Reduction Measure*

The 'Value of Lives Saved' by an additional risk reduction measure is the difference between the Cost of Lives before the measure and the Cost of Lives after the measure.

To work out the value of lives saved: take the cost of lives for the original case without the addition risk reduction measure (referred to below as case 0); subtract the cost of lives for the modified case with the additional risk reduction measure (referred to below as case 1)

Note: All figures below are on a per annum basis

$$Cost\_of\_lives\_(0) = V \times \sum_{i=1}^{k} IFOF_{i_0} \times N_i$$

$$Cost\_of\_lives\_(1) = V \times \sum_{i=1}^{k} IFOF_{i_1} \times N_i$$

$$Value\_of\_lives\_saved = V \times \sum_{i=1}^{k} (IFOF_{i_0} - IFOF_{i_1}) N_i$$

However, in order to give a threshold value for comparison purposes, it is directed by the HSE to weight the value (in favour of preservation of life) by the gross disproportion factor (Gd). The value of lives saved for cost comparison purposes is therefore give as:

$$Value\_of\_lives\_saved = V \times Gd \times \sum_{i=1}^{k} (IFOF_{i_0} - IFOF_{i_1}) N_i$$

### *Treating Additional Risk Reduction Measure as an Independent Layer of Protection*

Where the additional risk reduction measure is independent and has a probability of failure on demand (PFD) then:

$$IFOF_{i_1} = PFD \times IFOF_{i_0}$$

Therefore value of lives saved as a benefit is given by:

$$Value\_of\_lives\_saved = V \times Gd \times (1 - PFD) \times \sum_{i=1}^{k} IFOF_{i_0} N_i$$

The HSE also direct the duty holder to include any additional benefits. i.e. very often if an incident is such that there is a chance of fatality, there is also mechanical damage, investigation, forced outage and loss of income. There could also be follow up action, reputation damage and increased insurance costs. If there is an actual fatality, the follow up actions may increase significantly. Here, these are referred to in total as 'Other Cost Avoidance'.

It is assumed here that a cost (C) had been arrived at that represent these costs.

Let $F_0$ be the expected frequency of event before the added risk reduction measure and $F_1$ be the frequency after the added risk reduction measure. The 'Other Cost Avoidance' is then given by:

$$Other\_\cos t\_avoidance = C \times (F_0 - F_1)$$

But

$$F_1 = PFD \times F_0$$

So therefore other cost avoidance as a benefit is given by:

$$Other\_\cos t\_avoidance = C \times (1 - PFD) F_0$$

By summation of Value of Lives Saved and Other Cost Avoidance, it is possible to see the Benefit part of the cost benefit analysis as a function of the PFD of a further independent risk reduction measure.

*Cost of Additional Risk Reduction Measure*

Note: the Benefit measure will be given in a per annum figure (i.e. the Value of Lives Saved [pa]). For comparison purposes, it will be necessary to analyse costs on a pa basis.

The Cost [pa] measure is a summation of:

- the cost of work carried out for the modification divided by the design life [years] of the measure.
- the cost of maintenance and testing [pa]
- the cost of any associated production loss [pa]
- the cost of upkeep (i.e. keeping under review in safety management system)

### 5.4.3 Hierarchy of Controls

As previously described, before applying CBA at any stage in a design it is important to ensure that relevant regulation, good practice and prior learning has first been applied. However, the HSE advises that to be ALARP also requires decisions follow the appropriate hierarchy of risk controls (see [11]):

- Eliminate;
- Substitute;
- Engineering Controls;
- Administrative Controls;
- PPE.

Note that within the Engineering Controls layer, there is also a hierarchy:

- Containment – plant is built to withstand an event;
- Mechanical protection – e.g. diversion of hazard to a safe (or safer) place;
- Civil protection – e.g. blast wall, sheltered traffic routes;
- Instrumented protection;
- Alarms.

When in justifying decisions to be ALARP it's important the HSE hierarchy of controls are followed.

### 5.4.4 ALARP – Reaching Decisions

If a new or substantially modified plant is not (from a safety perspective) to be a copy of a legacy plant, the arrival at the point in a project where retrospective ALARP is carried out also requires an ALARP route has been followed prior to this stage. It follows that all safety related decision making during the course of a project should be ALARP justified.

Implicit in the assessment of ALARP and the application of CBA is that a relevant risk assessment exists, that risks are tolerable and that all relevant regulation, good practice and prior learning is being (or has been) applied (see 5.3.3) and the HSE hierarchy of controls has been followed (see 5.4.3)

Although CBA of a proposed additional or alternative risk reduction measure is important, it is generally seen as the final (retrospective) step of a design phase in establishing an ALARP position. Whether this retrospective step is on an existing plant or a new design, historic decisions that can have significant effects on risks have by that time been made. It follows that CBA should be carried out as a final step but, if it is the appropriate test of a decision, it follows that it should also be applied to all such decisions at whatever point in the lifecycle they are made.

In calculating the elements for CBA, it might not seem possible to measure risk accurately before a design is complete but it should be recognised that risk analysis at any point is based on assumptions (which are justified rather than proven) and that assumptions become allocated targets.

Therefore, where risk levels demand CBA, this guidance recommends that (although at earlier stages in design it may be necessary to make use of broader assumptions and broader allocated targets) associated decisions should still be justified ALARP using CBA.

### 5.4.5 Lifecycle and Audit Trail

As with Risk Assessment (see 5.2.12), ALARP is a documented lifecycle process.

The form of the lifecycle documentation needs to be planned and understood early on and then all activities planned so as to contribute to the development and maintenance of those documents. It follows that the form of lifecycle documents must be developed to be evolved with the necessary mechanism to support change and revision.

Equally important is to ensure that the audit trail covering the development, revision and maintenance of those documents is also recorded. A mechanism to record relevant meetings, relevant expert advice and relevant decisions must also be in place.

### 5.4.6 Ongoing ALARP Assessment

It is important to recognise that ALARP assessment is a lifecycle process and should be used to inform design as well as assess design (this is further discussed in 5.3.1). It should be demonstrable for a design that all reasonably practicable steps have been taken to minimise risk as the design has progressed.

In a project context, it is therefore necessary for ALARP assessment to increase in granularity as a project progresses through design. ALARP assessment must also be 'ongoing' (where it is periodically reviewed and updated in the light of relevant new information). It follows that at the point of completion of a project, the ALARP justification needs to adopt a 'retrospective' form where it may be used as a basis for 'Ongoing ALARP Assessment'.

The retrospective form must also provide measures of change of risk in order to demonstrate the benefits of additional or alternative risk reduction measures (see also 5.4.2).

When considering the integrity to be applied to a proposed risk reduction measure, it is often difficult to choose an appropriate target. Referring to 5.4.2, it should be apparent that if an independent layer of protection (IPL) were added to an existing design, then 90% of the potential benefit would be realised with a PFD of 0.1, 99% for a PFD of 0.01 etc. The incremental benefit of an increase in level of integrity may not be cost justifiable. If a high level of integrity is proposed, it may 'pass' the CBA challenge where a lower level may not. It is therefore important to choose the right level for the circumstances.

Therefore, this guidance recommends a process which determines the maximum possible benefit – i.e. the total benefit per year (in human and commercial terms) of reducing the frequency of the Hazardous Event to 0. This figure gives a very important indication of where the optimum gains lie and where there is little point in reducing risk further (see also 6.3 and illustration in 7.3).

Note: If an additional protection measure acts across several scenarios, for CBA purposes it is important to calculate the full effect of its addition. In such a case, the above would have to be adapted to measure the effect across multiple scenarios.

### 5.4.7 Summary Notes

The following notes attempt to summarise the learning points on ALARP:

- Risk assessment, Design, Allocation and ALARP are parallel, interdependent and co-terminus, but, at the point of completion of a project, it should adopt the 'retrospective' form.
- As the term 'Tolerable' is associated with aggregated risk then 'Tolerable if ALARP' must also be so. If aggregated risks are not in the region of Broadly Acceptable then CBA should be applied to all significant contributions to risk reduction.
- Safety related design decisions should follow HSE hierarchy of risk controls and be justified ALARP at whatever point in the design they occur.
- Lifecycle and audit trail documentation for safety related aspects must be produced and maintained.
- Adoption of relevant regulation, good practice and prior learning must be applied to design.
- ALARP has no lower boundary in theory, but (in practical terms) the 'Broadly Acceptable' risk is the lowest foreseeable residual risk of any occupation and, at this level of risk, adoption of good practice is generally sufficient to justify ALARP.

- Safety functions and associated performance criteria (targets) are specified (allocated) at every stage and systematically followed down through the design.
- The Ongoing Risk Assessment and ALARP Assessment are revisited periodically and additionally at times of change or significant event.

Note: Because of the interdependence between Risk assessment, Design, Allocation and ALARP, many of the summary notes are shared with 5.2 and 5.3.

# 6 ALARP Framework

Cost benefit analysis and the test of gross disproportion is a familiar concept when applied to ALARP assessing a completed design.

However, for risks to be truly ALARP the concept needs to be applied at all stages of the lifecycle. The concept of being ALARP also includes other principles such as the hierarchy of control measures (see 5.4.3).

This section provides a suggested ALARP route for Project Work (from inception of a project through to a completed design) followed by an ongoing approach to maintain ALARP status by applying Ongoing Risk Assessment and Ongoing ALARP Assessment.

## 6.1 Project Work

Safety in design is part of good engineering practice and is an underlying expectation of the HSE but on large projects where many disciplines work together to achieve an overall process safety goal, the method for identifying, assessing and managing hazards and their associated mechanisms needs to be formalised.

The IChemE Hazard Study process is perhaps the best-known formalised method in the process industries. Like all methods, if it is applied incorrectly or incompletely, or if it is not complemented by good design practice, it can lead to a false sense of safety which later can be difficult to resolve.

In particular, the use of Hazop only or its use at the wrong place in the process is a common misuse of the overall process (see 5.2.7 for further discussion).

Note: Projects are often broken down into several parts (physical sections) and / or several phases. It would be impossible to produce guidance in detail suitable for any project but the following is given as general guidance for outlining the approach on a project where philosophies should be preserved.

### 6.1.1 Concept and Hazard Study 1 (HS1)

HS1 is a concept stage hazard and risk assessment where the basic hazards of the materials and process to humans and the environment are identified and considered. Hierarchical considerations such as elimination and substitution are considered at this stage. All safety design decisions and their justifications should be documented.

In many projects, the 'process' itself is already defined – i.e. the considerations of elimination and substitution have already taken place and/or the process is already well established and generally accepted. However, this guidance recommends that all safety design decisions and their justifications are documented.

This should also be the point at which the safety planning for the remainder of the lifecycle takes place. Tolerable Risk Criteria, relevant regulation, relevant good practice and prior learning should be identified.

Note: With respect to TRC, depending on the scope of the project it may be that the associated Process Hazards represent a subset of the Process Hazards that could be experienced. This guidance therefore recommends that a specific set of criteria are agreed and justified for each project.

### 6.1.2 Project Plan and Safety Plan

Safety planning has two aspects:

- There is the safety lifecycle where the concepts and the general approach are defined. The safety lifecycle covers the general process for managing the safety aspects of anything new or revised. It provides useful reference when planning or assessing the impact of any change.
- There is the activity plan which details on a time line basis what activities are required in order to fulfil the foreseen requirements of the safety lifecycle.

Note: The safety lifecycle remains as a reference, but the activity plan must be integrated with the more general project plan and maintained up to date so that those working on the project can see the whole activity picture in time line view.

The lifecycle element should include development of a management system for the Process Safety issues covering the project and into the foreseeable future.

### 6.1.3 Preliminary Hazard and Risk Assessment – Hazard Study 2 (HS2)

HS 2 (often referred to as HAZID) is a preliminary process hazard and risk assessment where a formalised hazard identification process takes place. The purpose of the study is to identify Hazardous Events and their mechanisms together with the effects on potential occupants of the plant such that the high-level requirements for risk controls are understood and specified at an early stage in the design.

Note: Requirement for risk controls include both a statement of functionality together with associated target reliability. For example, if a plant's process safety relies heavily on the cooling water system, a safety function at this level of design is the provision of sufficient cooling water with sufficient reliability. The provision of such a system is likely to involve redundant mechanical parts as well as instrumented safety functions at a more detailed level of design. If this important safety functionality were overlooked at this early stage, it would be difficult and potentially costly to recover later on in the design process. Specifying additional instrumented safety functions at a later stage or looking for other means of risk reduction in order to compensate for an unreliable cooling water system cannot be seen as ALARP.

It should be ensured that the design of the plant to be delivered or modified is managed in terms of organisational systems and all systems are managed with responsible roles and associated role holders clearly defined.

Activities should include the following:

- Carrying out hazard and risk assessment, producing lifecycle documentation (describing risk mechanisms and how they are to be managed) and documenting the audit trail (recording all aspects of how the lifecycle documentation was established and developed and how decisions were made).
- Using appropriate degree of rigour (see 5.2.5) to determine the expected frequency of each Hazardous Event in each relevant Harm Zone.
- Identifying separately any hazardous activity where the pattern of risk is not dependent on random occupancy of a Harm Zone (e.g. a task associated with plant start up).
- Identifying separately any hazardous events that lead to societal risk (see 5.1.3).
- Developing functional and integrity requirements for risk control measures in order to ensure TRC are met;
- Negotiating and allocating safety functionality across disciplines to people, equipment and systems.
- Ensuring that all safety related assumptions made during risk assessment are translated into allocated safety functions (see 5.3.1).
- Producing ALARP justifications based on relevant regulation, good practice and (where appropriate) CBA) to demonstrate decisions are ALARP.

Note: the list above is the start of the formal process that should be continued throughout the project.

Process Safety Information (including the following) should be documented for a new plant (or information updated for an existing plant):

- Tolerable Risk Criteria for the project – identifying tolerated frequency of fatality for an individual to all Hazardous Events and (where relevant) for collections of individuals to individual Hazardous Events.
- Relevant regulations and good practice – identify all regulatory/ non-regulatory national / international / company standards, guides and procedures that are aimed at protecting humans from the identified Hazardous Events.
- Process Hazard Register - identifying all Hazardous Events and their expected frequencies.
- Human Group – identifying groups of humans (plant operator, mechanical technician, cleaner etc).
- Harm Zone and Vulnerability definitions – identifying the Harm Zones of the Hazardous Events and the associated Vulnerability with sufficient granularity to allow mapping of risk to different Human Groups.
- Occupancy Register – identifying the random occupancy of Harm Zones by members of Human Groups.

- Separate risk assessment of any activity-based risks using appropriate degree of rigour (see 5.2.5).
- Separate quantitative assessments of any societal risks.
- Quantitative ALARP assessments to demonstrate key decisions are ALARP.
- Safety Functions Requirement Specification – identify all functional safety requirements (covering all types of equipment, systems and human actions)
- Safety Plan – to be updated (Lifecycle Form).

Note: The Process Safety Information needs to be in a form and under a management system such that it can be developed throughout the project and into the foreseeable future.

### 6.1.4 Basic (Risk Informed) Design

At this stage the design should be developed and documented for a new plant (or information updated for an existing plant) so as to inform detailed design.

It should include the following:

- Site Plans, Plant Layouts and General Arrangements Drawings.
- Process Flow Diagrams.
- Staffing philosophies
- General philosophies – identifying approaches and conventions to be followed in the detailed design stage including:
    - Operation and Control philosophies
    - Alarm philosophy
    - HMI Philosophy
    - Electrical philosophy
    - Control and Electrical interface philosophy
- Design responsibilities – who / what discipline is responsible for what systems and devices and the boundary points between them.
- Project Plan - (with integrated safety activities)
- Process Safety Information - to be updated

Process Safety aspects of the project continue throughout design and will resulting in increasing level of detail (and possibly modification) to the Process Safety Information.
In particular, it is important to:

- Plan and facilitate meetings ensuring a suitable variety of people with appropriate competencies are present.
- Ensure relevant information is available and circulated suitably in advance of meetings.
- Record relevant content of meetings and ensure that individuals are seen and recorded as taking responsibility for information and decisions in their areas of competence.
- Continue to develop and refine Process Safety Information including meeting outcomes.
- Use relevant techniques (see 5.2.5) to determine the expected frequency of each Hazardous Event in each relevant Harm Zone.

- Develop safety function requirements for robust risk controls and ensure that TRC are to be met or bettered.
- Negotiate (where necessary) safety functions across various disciplines such that the resulting allocation is seen collectively as feasible and balanced.
- Ensure that all Process Safety related assumptions are mapped onto Allocated Safety Functionality.
- Allocate safety functionality to various disciplines (via the lead in the disciplines) such that all safety claims are 'owned' and managed.
- Create detailed Safety Requirement Specifications for all allocated safety functions and break this down into relevant disciplines / systems.
- Support disciplines in assessments of safety functionality within their scope.

### 6.1.5 Detailed Design

This phase involves the detailed engineering design where engineering disciplines translate the requirements and philosophies set out in the Basic Design and produce a Detailed Design which includes implementation of relevant regulatory requirements and good practice.

In particular the Detailed Design must also include analysis of the design such that it confirms conformance to safety functionality requirements and associated performance targets set out in the Process Safety Information.

Basic Design documentation is reviewed and updated.

Detailed Project design documentation is produced.

Process Safety Information is updated to reflect design development and enhanced to include the above assessments.

Notes:

- This is the phase where much of the design effort takes place and therefore changing key decisions (whether related to safety or other aspects) will henceforth become far more costly. A design review by all disciplines covering safety and all aspects should therefore take place before commencing detailed design.
- It will be necessary to apportion overall tolerable risk criteria to parts of the risk profile (e.g. scenario, logical group of scenarios, project) (see 5.1.2).
- It will be necessary to carry out 'engineering risk assessments' to give expected probability and/or frequency of failure for engineered safety functions.

### 6.1.6 Detailed Hazard and Operability Study – Hazard Study 3 (HS3)

Hazop (Hazard and Operability Study) is a systematic study of the detailed design. It is a process which usually starts from the detail of the physical plant and takes a bottom upward perspective of the way in which hazards may be generated. The purpose is to challenge the design by:

- Trying to identify hazard mechanisms that may have been overlooked in top downward design.

- Assessing how failures of equipment or people may promote hazard mechanisms.
- Assessing whether the design is over susceptible to failures of equipment and people.
- Assessing whether the design provides ease of through life operation and maintenance.

At this stage Actions can be set for the design team to address – either to provide assurances of certain aspects or to revisit certain areas of design that are considered to be inadequate.

Notes:

- Hazop is a review of the design and not a part of the design process. It must therefore be an independent activity and independently led.
- Hazop is carried out by a team consisting of the relevant disciplines. Independence from the design team is not essential but sufficient independence is required to enable it to act independently.
- Hazop considers all detailed design documentation as well as Process Safety Information (see 6.1.3).
- Hazop is part of the Safety Lifecycle – i.e. it must be applied and once applied must continue to be applied.
- Hazop and its documentation must therefore exist in up-to-date 'Life Cycle' form as well as have a full audit trail.

### 6.1.7 Manufacture

This is part of the project where equipment that has been designed is built and tested.

ALARP considerations here are generally concerned with systematic design and testing, following good quality assurance procedures which result in manufacture which is as free as possible from systematic (inbuilt) failings.

### 6.1.8 Construction

This is part of the project where the buildings are erected and manufactured equipment is assembled, installed and tested on site.

It also includes pre-commissioning where the mechanical, electrical and control equipment is demonstrated to perform its functions properly and safely. It can also include dry or wet runs containing safe fluids in order to verify its capability.

As with manufacture, ALARP considerations are concerned with a systematic assembly and testing, following good quality assurance procedures which result in integrated systems which are as free as possible from systematic errors.

### 6.1.9 Hazard Study 4 (HS4)

HS4 is performed at the end of the construction stage. Its purpose is to verify that evidence exists that:

- the plant hardware (and software) performs as it is required to when integrated;
- all documentation is complete and in place;

- no significant adverse issues have arisen;
- the plant is properly staffed and all necessary training has taken place;
- all actions from previous stages have been reviewed to ensure that any relevant to starting up the plant has been successfully completed and any findings appropriately acted upon;
- all relevant legislative requirements and company procedures have been complied with.

This is also the stage at which a Pre-Start-up Safety Review (USA legislation term) is carried out.

### 6.1.10 Commissioning

In this stage the plant is brought on line with process fluids in a controlled manner ensuring that each stage of the process is set up so that it performs its design operational and safety functions.

### 6.1.11 Hazard Study 5 (HS5)

HS5 is performed following start up to ensure the plant and process is operating as the design intended. This is also the stage where any unexpected / unforeseen circumstances are reviewed for operational safety.

## 6.2 Ongoing Risk Assessment Process

It is important to recognise that Risk Assessment is a lifecycle process rather than a process which is applied at the end of a design. It should be demonstrable for a design that all reasonably practicable steps have been taken to minimise risk. However, following completion of a project, it is necessary to have a risk assessment process which continues to assess risk. It follows that at some point, the risk assessment process must adopt the form that continues to address risk. Once the point of a completed design is arrived at, an 'Ongoing Risk Assessment' process should be applied which is first used to scrutinise the completed design and used iteratively thereafter.

In section 5 there are many qualitative aspects to the approach to Hazard and Risk Assessment which are discussed. However, there is an underlying requirement for a quantitative methodology which satisfies the need to derive the aggregated risk to an individual (see 5.2.4) and provide the full picture (see 5.2.6)

The required attributes of the risk assessment methodology are:

- In order to derive the expected frequency for each Hazardous Event, it is able to construct that frequency from a logical breakdown of the mechanism and sound engineering estimates of the failure statistics of all related elements.
- In order to derive the expected frequency of fatality to each individual, it is able to map the Human Exposure of each individual onto the Hazardous Event frequency.
- In order to compare with relevant TRC, it is capable of deriving the aggregated frequency of fatality to any individual.
- In order to derive the total effect of a Hazardous Event, the risk assessment methodology must be capable of mapping all Human Exposure on to each Hazardous Event.
- In order to derive the total effect of a proposed modification to safety functionality, the risk assessment methodology must be capable of mapping safety functionality onto all related Hazardous Events.

Notes:

- A proposed risk reduction measure (safety function) could affect the expected frequency of the Hazardous Event (e.g. by adding instrumented functions); limit the size of a Harm Zone (e.g. by use of blast wall); reduce Occupancy (e.g. by managing activities which in such a way as to minimise presence in Harm Zones at times when the risk is present).
- There are some cases where the likelihood of occurrence of a Hazardous Event is not random during plant operation. If the human occupancy is also not random then care should be taken to ensure that, where significant, the joint probability is accounted for.

The degree of rigour applied to the risk assessment of Hazardous Events is dependent on whether the risk is simple and intrinsically low and / or other factors such as regulation extensive good practice. For more detail, refer to 5.2.4. The various degrees of rigour mean that different methods (qualitative and quantitative) can be applied depending on the specific Hazardous Event. However, there is an overall requirement to provide a quantitative measure for comparing to relevant TRC.

This guidance therefore recommends the following pragmatic approach:

- The degree of rigour that should be applied to assessing a worker's overall risk of fatality depends on the relative position of the total risk within the Intolerable to Broadly Acceptable band. If the overall risk is not in the Broadly Acceptable region, the degree of rigour required for the overall risk requires aggregation and therefore quantitative measures of constituent parts of the risk.
- Should there be any question of whether risks are in the Broadly Acceptable region, an initial rough numerical estimate of aggregated risk should be carried out.
- The degree of rigour applied to scenarios with low intrinsic risk and low complexity or where strong evidence exists that the specific risk mechanisms and controls are capable of managing the risk low, qualitative methods are permitted but, in such cases, a conservative engineering estimate of the residual risk is provided as a constituent in the aggregation process.
- Risks which are intrinsically high but managed low should be managed quantitatively however low the residual risk.

### 6.3 Ongoing ALARP Process

It is clear (especially with project work) that ALARP is a thread that runs through the approach to defining risk control measures. However, in finally establishing that risks are ALARP in an environment where risks are complex and do not result in a Broadly Acceptable risk, there is the need to calculate and compare the cost and benefits of further or alternative risk reduction measures (see 5.4.2).

Note: In order to assess the full benefit of a proposed change in risk reduction measures it is necessary for the risk assessment process to have a full picture of the benefit – the benefit of all the avoided human harm and any other savings that would result (see 5.4.2 and 5.2.6)

## 7 Further Guidance on ALARP Framework

### 7.1 Ongoing Risk Assessment Process

In this section, the methods apply to risk to humans from Hazardous Events which are taken as random – i.e. there is no significant correlation between the likelihood of the occurrence of the event and the

occupancy. For cases where there is significant correlation, similar techniques can be used where the expected frequency of the event and the occupancy are combined in a single column reflecting the joint probability. However, in the interests of simplicity, this guidance does not include techniques for dealing with such correlation.

Risk is defined as a combined measure of likelihood (frequency) and consequence of an unwanted event. In this case, as the consequence (fatality) is already stated, the measure of the associated risk is given in frequency (pa) as are the guidelines given by the HSE. The appropriate term (used here) is therefore the Individual Frequency of Fatality (IFOF).

The risk profile of an individual is determined by the tasks they perform that results in Human Exposure by taking them into the Harm Zones associated with Hazardous Events.

In the Process Industries typically there are a number of different groups of workers (operators, mechanical technician, electrical technicians, instrumentation technicians, cleaners etc.). Individuals within groups have statistically identical risk profiles but groups have differing risk profiles because of the different tasks they perform.

In a safety management system, it is important to achieve the right level of granularity to be able to adequately reflect the risk profile of all the groups.

The purpose here is to propose a method of viewing the risk profile of groups of workers based on their Occupancy profile of Harm Zones.

Note: Determining the expected frequency of Hazardous Events is treated as a separate issue and one to which there is no universal solution. This section addresses mapping of harm to all humans to all Hazardous Events based on assumed information.

The proposed tool is spreadsheet based and an extract example is given.

The following information is assumed to be available:

- A Process Hazard Register with a list of all Hazardous Events.
- The expected frequencies of all Hazardous Events.
- Details of Harm Zones associated with each Hazardous Event and the Vulnerability within each Harm Zone.
- Human occupancy mapping (a mapping of random occupancy of all Harm Zones for each group of workers).

Notes:

- It is sometimes advantageous to split Hazardous Events into sub-events if there are several different cases. For example an overpressure event in pipework might be such that any one of several relief devices could prevent rupture of the pipework or the event could be such that it could overcome all available relief devices – i.e. the probability of failure of protection measures varies depending on the case and thus the residual event for each case will vary significantly in frequency. It is therefore not appropriate to treat them as the same Hazardous Event.

- The Vulnerability to a single Hazardous Event might be quite different depending on the activity or task that puts a worker in danger from that event. It is sometimes necessary to describe several Harm Zones in relation to one Hazardous Event in order to obtain the necessary granularity for risk profiling. For example, if a shell boiler were to explode, there would be an immediate zone where Vulnerability would be considered to be 1 but (as distance from the explosion increases) the Vulnerability decreases towards 0. It is unlikely that one nominated Harm Zone would give the necessary granularity.
- Where the level of risk is highly dependent on a task because the task takes a worker into a Harm Zone with high Vulnerability, it is often useful to nominate a specific Harm Zone for that task because the ongoing risk management will be highly dependent on managing occupancy of the high-risk Harm Zone rather than the more general low risk Harm Zone.

The following two pages show a spreadsheet-based risk assessment process.

The first page is an example Process Hazard Register which includes:

- Descriptions of Hazardous Events and their various mechanisms.
- Descriptions of Harm Zones associated with different Hazardous Mechanisms.
- Statement of Vulnerability for the Hazardous Event / Harm Zone combination.
- Statement of Expected Hazardous Event Frequency.

The second page is an Individual Frequency of Fatality Assessment which includes:

- Classification of workers into Groups and a statement of how many in each.
- Mapping of occupancy for all Groups to the Harm Zones associated with Hazardous Events.
- Aggregation of workers' IFOF in groups to all Hazardous Events to which they are exposed.
- Aggregation of all workers to all Hazardous Events (the bottom right hand cell is the current expected fatality rate).

# PROCESS HAZARD REGISTER

| Risk ID | Event Description & Consequences [description] | Initiating Event & Hazard Mechanism [description] | Harm Zone [description] | Link to file with supporting information | Vuln'ty | Expected Event Frequency [pa] |
|---|---|---|---|---|---|---|
| 01-01 | *Event 1 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 1 Harm Zone 1* | *insert hyperlink* | 1.00E-01 | 1.00E-02 |
| 01-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 1 Harm Zone 2* | *insert hyperlink* | 1.00E-01 | 5.00E-03 |
| 01-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 1 Harm Zone 3* | *insert hyperlink* | 1.00E-01 | 1.00E-03 |
| 01-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 1 Harm Zone 4* | *insert hyperlink* | 1.00E-01 | 1.00E-03 |
| 01-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 1 Harm Zone 5* | *insert hyperlink* | 1.00E-01 | 1.00E-03 |
| 01-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 1 Harm Zone 6* | *insert hyperlink* | 1.00E-01 | 1.00E-03 |
| 01-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 1 Harm Zone 7* | *insert hyperlink* | 1.00E-01 | 1.00E-03 |
| 01-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 1 Harm Zone 8* | *insert hyperlink* | 5.00E-01 | 1.00E-03 |
| 02-01 | *Event 2 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 2 Harm Zone 1* | *insert hyperlink* | 1.00E+00 | 1.00E-03 |
| 02-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 2 Harm Zone 2* | *insert hyperlink* | 1.00E+00 | 1.00E-03 |
| 02-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 2 Harm Zone 3* | *insert hyperlink* | 2.00E-01 | 1.00E-03 |
| 02-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 2 Harm Zone 4* | *insert hyperlink* | 2.00E-01 | 1.00E-03 |
| 02-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 2 Harm Zone 5* | *insert hyperlink* | 5.00E-01 | 1.00E-04 |
| 02-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 2 Harm Zone 6* | *insert hyperlink* | 1.00E-01 | 1.00E-04 |
| 02-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 2 Harm Zone 7* | *insert hyperlink* | 1.00E-01 | 1.00E-04 |
| 02-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 2 Harm Zone 8* | *insert hyperlink* | 1.00E-01 | 1.00E-04 |
| 03-01 | *Event 3 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 3 Harm Zone 1* | *insert hyperlink* | 5.00E-01 | 1.00E-04 |
| 03-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 3 Harm Zone 2* | *insert hyperlink* | 1.00E-01 | 1.00E-04 |
| 03-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 3 Harm Zone 3* | *insert hyperlink* | 1.00E-01 | 1.00E-04 |
| 03-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 3 Harm Zone 4* | *insert hyperlink* | N/A | N/A |
| 03-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 3 Harm Zone 5* | *insert hyperlink* | N/A | N/A |
| 03-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 3 Harm Zone 6* | *insert hyperlink* | N/A | N/A |
| 03-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 3 Harm Zone 7* | *insert hyperlink* | N/A | N/A |
| 03-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 3 Harm Zone 8* | *insert hyperlink* | N/A | N/A |

# INDIVIDUAL FREQUENCY OF FATALITY ASSESSMENT

| | | | | | | | *Exposed Group 1* | | | | *Exposed Group 2* | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Risk ID** | **Hazardous Event/consequence** | **Initiating Event** | **Harm Zone [descript]** | **Link to file with info** | **Vuln'ty Factor [no units]** | **Expected Event Freq'cy [pa]** | **Occupancy Factor [no units]** | **Vuln'ty Factor [no units]** | **Human Exposure Factor [no units]** | **RIFOF [pa]** | **Occupancy Factor [no units]** | **Vuln'ty Factor [no units]** | **Human Exposure Factor [no units]** | **RIFOF [pa]** | **MAX RIFOF [pa]** | **Totals RFOF [pa]** |
| 01-01 | *Event 1 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 1 Harm Zone 1* | *insert hyperlink* | 1.00E-01 | 1.00E-02 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-06 | 7.00E-02 | 1.00E-01 | 7.00E-03 | 7.00E-05 | 7.00E-05 | |
| 01-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 1 Harm Zone 2* | *insert hyperlink* | 1.00E-01 | 5.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 2.50E-06 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 2.50E-06 | 2.50E-06 | |
| 01-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 1 Harm Zone 3* | *insert hyperlink* | 1.00E-01 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | |
| 01-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 1 Harm Zone 4* | *insert hyperlink* | 1.00E-01 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | |
| 01-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 1 Harm Zone 5* | *insert hyperlink* | 1.00E-01 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | |
| 01-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 1 Harm Zone 6* | *insert hyperlink* | 1.00E-01 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | |
| 01-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 1 Harm Zone 7* | *insert hyperlink* | 1.00E-01 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | |
| 01-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 1 Harm Zone 8* | *insert hyperlink* | 5.00E-01 | 1.00E-03 | 1.00E-02 | 5.00E-01 | 5.00E-03 | 5.00E-06 | 1.00E-02 | 5.00E-01 | 5.00E-03 | 5.00E-06 | 5.00E-06 | |
| | | **Total** | | | | **2.10E-02** | | | | **1.50E-05** | | | | **8.00E-05** | **8.00E-05** | |
| | | | | | | | | | | **7.50E-05** | | | | **6.40E-04** | | **7.15E-04** |
| 02-01 | *Event 2 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 2 Harm Zone 1* | *insert hyperlink* | 1.00E+00 | 1.00E-03 | 3.50E-03 | 1.00E+00 | 3.50E-03 | 3.50E-06 | 3.50E-03 | 1.00E+00 | 3.50E-03 | 3.50E-06 | 3.50E-06 | |
| 02-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 2 Harm Zone 2* | *insert hyperlink* | 1.00E+00 | 1.00E-03 | 1.25E-01 | 1.00E+00 | 1.25E-01 | 1.25E-04 | 1.25E-01 | 1.00E+00 | 1.25E-01 | 1.25E-04 | 1.25E-04 | |
| 02-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 2 Harm Zone 3* | *insert hyperlink* | 2.00E-01 | 1.00E-03 | 1.30E-03 | 2.00E-01 | 2.60E-04 | 2.60E-07 | N/A | N/A | N/A | 0.00E+00 | 2.60E-07 | |
| 02-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 2 Harm Zone 4* | *insert hyperlink* | 2.00E-01 | 1.00E-03 | 3.13E-01 | 2.00E-01 | 6.26E-02 | 6.26E-05 | N/A | N/A | N/A | 0.00E+00 | 6.26E-05 | |
| 02-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 2 Harm Zone 5* | *insert hyperlink* | 5.00E-01 | 1.00E-04 | 1.25E-01 | 5.00E-01 | 6.25E-02 | 6.25E-06 | N/A | N/A | N/A | 0.00E+00 | 6.25E-06 | |
| 02-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 2 Harm Zone 6* | *insert hyperlink* | 1.00E-01 | 1.00E-04 | 1.30E-03 | 1.00E-01 | 1.30E-04 | 1.30E-08 | N/A | N/A | N/A | 0.00E+00 | 1.30E-08 | |
| 02-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 2 Harm Zone 7* | *insert hyperlink* | 1.00E-01 | 1.00E-04 | 3.13E-01 | 1.00E-01 | 3.13E-02 | 3.13E-06 | N/A | N/A | N/A | 0.00E+00 | 3.13E-06 | |
| 02-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 2 Harm Zone 8* | *insert hyperlink* | 1.00E-01 | 1.00E-04 | 5.90E-03 | 1.00E-01 | 5.90E-04 | 5.90E-08 | N/A | N/A | N/A | 0.00E+00 | 5.90E-08 | |
| | | **Total** | | | | **4.40E-03** | | | | **2.01E-04** | | | | **1.29E-04** | **2.01E-04** | |
| | | | | | | | | | | **1.00E-03** | | | | **1.03E-03** | | **2.03E-03** |
| 03-01 | *Event 3 Description & Consequences* | *Initiating Event & Hazard Mechanism 1* | *Event 3 Harm Zone 1* | *insert hyperlink* | 5.00E-01 | 1.00E-04 | 3.50E-03 | 5.00E-01 | 1.75E-03 | 1.75E-07 | N/A | N/A | N/A | 0.00E+00 | 1.75E-07 | |
| 03-02 | | *Initiating Event & Hazard Mechanism 2* | *Event 3 Harm Zone 2* | *insert hyperlink* | 1.00E-01 | 1.00E-04 | 3.50E-03 | 1.00E-01 | 3.50E-04 | 3.50E-08 | N/A | N/A | N/A | 0.00E+00 | 3.50E-08 | |
| 03-03 | | *Initiating Event & Hazard Mechanism 3* | *Event 3 Harm Zone 3* | *insert hyperlink* | 1.00E-01 | 1.00E-04 | 3.50E-03 | 1.00E-01 | 3.50E-04 | 3.50E-08 | N/A | N/A | N/A | 0.00E+00 | 3.50E-08 | |
| 03-04 | | *Initiating Event & Hazard Mechanism 4* | *Event 3 Harm Zone 4* | *insert hyperlink* | N/A | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0.00E+00 | 0.00E+00 | |
| 03-05 | | *Initiating Event & Hazard Mechanism 5* | *Event 3 Harm Zone 5* | *insert hyperlink* | N/A | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0.00E+00 | 0.00E+00 | |
| 03-06 | | *Initiating Event & Hazard Mechanism 6* | *Event 3 Harm Zone 6* | *insert hyperlink* | N/A | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0.00E+00 | 0.00E+00 | |
| 03-07 | | *Initiating Event & Hazard Mechanism 7* | *Event 3 Harm Zone 7* | *insert hyperlink* | N/A | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0.00E+00 | 0.00E+00 | |
| 03-08 | | *Initiating Event & Hazard Mechanism 8* | *Event 3 Harm Zone 8* | *insert hyperlink* | N/A | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0.00E+00 | 0.00E+00 | |
| | | **Total** | | | | **3.00E-04** | | | | **2.45E-07** | | | | **0.00E+00** | **2.45E-07** | |
| | | | | | | | | | | **1.23E-06** | | | | **0.00E+00** | | **1.23E-06** |
| | | **Total IFOF in group** | | | | | | | | **2.16E-04** | | | | **2.09E-04** | | |
| | | **No of Employees in group** | | | | | | | | **5** | | | | **8** | **13** | |
| | | **Total FOF for group** | | | | | | | | **1.08E-03** | | | | **1.67E-03** | **2.75E-03** | **2.75E-03** |

## 7.2 Project Work

*No further guidance offered*

## 7.3 The Ongoing ALARP Process

The Ongoing ALARP process is concerned with weighing up the relative cost and benefits of further or alternative risk reduction measures where a risk reduction measure could either reduce the expected frequency of the Hazardous Event or reduce the Human Exposure.

In order to provide a practical methodology for Ongoing ALARP Assessment, this guidance recommends calculating the benefit per annum of risk reduction prior to proposing risk reduction measures (see 5.4.2). By calculating the 'weighted benefit' (which includes the factor of gross disproportion applied to fatalities) it becomes possible to make a ready comparison with the cost of implementing risk reduction measures.

If the benefit returned by the calculation is small (e.g. £250 pa) then, clearly, it would need only a rough qualitative assessment to demonstrate that little could be achieved for that cost. If there is a measure that could be done for that yearly amount, it is likely to have come under the scope of relevant good practice and is therefore an expectation in any case. There is also the issue of choosing the right target which is described below. For example, in this case it might be possible to implement a control system function for this amount pa which may be able to return 90% of the Available Benefit.

In the majority of cases an engineering judgement can (and should) record that all relevant good practice has been applied and when no practicable further risk reduction measures are available.

For the remaining cases, where the amount is significant, a more robust case may be required but only to a point if it becomes clear that costs will exceed the weighted benefits.

The following example 'proposes' a target for risk reduction associated with the Maximum Residual Individual Frequency of Fatality (MAX RIFOF). The steps are as follows:

- Identify the worst-case aggregated RIFOF (i.e. that applying to the individuals with the highest expected fatality rate).
- Calculate the PFD for the notional additional risk reduction measure (based on the above worst-case) that would be required to reduce the aggregated risk to that of Broadly Acceptable.
- Using that notional PFD, for each risk, calculate the notional 'weighted benefit' value (using the method in 5.4.2).

Once the weighted benefit for each risk is established::

- Consider available risk reduction measures and make rough estimation of the costs of a risk reduction measure that would give the target PFD.
- Proceed with further investigation only if the costs appear to be less, otherwise record a brief justification.
- Consider whether a similar lower integrity function might be available for the available money. Estimate the PFD available and then replace the above target PFD with this one. Repeat the calculation using the method in 5.4.2.

- Proceed with implementation only if the costs appear to be less, otherwise record a brief justification.

See the realistic example below followed by ‘choosing the right target’ for a more detailed explanation.

# ALARP ANALYSIS

| Risk ID | Expected Event Freq'y [pa] | *Exposed Group 1* | | | | *Exposed Group 2* | | | | MAX RIFOF [pa] | Totals RFOF [pa] | *Proposed Added Risk Reduction Calculation* | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Occ'y Factor [no units] | Vuln'ty Factor [no units] | Human Exposure Factor [no units] | RIFOF [pa] | Occ'y Factor [no units] | Vuln'ty Factor [no units] | Human Exposure Factor [no units] | RIFOF [pa] | | | Proposed ALARP RIFOF Target | PFD of proposed added risk reduction [no units] | Equiv't SIL | Value of fatalities averted pa [£/y] | Value of other savings per incident | Value of other savings pa [£/y] | Value of fatalities and other savings pa [£/y] |
| 01-01 | 1.00E-02 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-06 | 7.00E-02 | 1.00E-01 | 7.00E-03 | 7.00E-05 | 7.00E-05 | | 1.00E-07 | 1.43E-03 | 2 | 5,842 | 1.00E+05 | 999 | 6,840 |
| 01-02 | 5.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 2.50E-06 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 2.50E-06 | 2.50E-06 | | 1.00E-07 | 4.00E-02 | 1 | 312 | 1.00E+05 | 480 | 792 |
| 01-03 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | | 1.00E-07 | 2.00E-01 | 0 | 52 | 1.00E+04 | 8 | 60 |
| 01-04 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | | 1.00E-07 | 2.00E-01 | 0 | 52 | 1.00E+04 | 8 | 60 |
| 01-05 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | | 1.00E-07 | 2.00E-01 | 0 | 52 | 1.00E+04 | 8 | 60 |
| 01-06 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | | 1.00E-07 | 2.00E-01 | 0 | 52 | 1.00E+04 | 8 | 60 |
| 01-07 | 1.00E-03 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-03 | 1.00E-01 | 5.00E-04 | 5.00E-07 | 5.00E-07 | | 1.00E-07 | 2.00E-01 | 0 | 52 | 1.00E+04 | 8 | 60 |
| 01-08 | 1.00E-03 | 1.00E-02 | 5.00E-01 | 5.00E-03 | 5.00E-06 | 1.00E-02 | 5.00E-01 | 5.00E-03 | 5.00E-06 | 5.00E-06 | | 1.00E-07 | 2.00E-02 | 1 | 637 | 1.00E+04 | 10 | 647 |
| | 2.10E-02 | | | | 1.50E-05 | | | | 8.00E-05 | 8.00E-05 | | | | | 7,051 | | 1,528 | 8,579 |
| | | | | | 7.50E-05 | | | | 6.40E-04 | | 7.15E-04 | | | | | | | |
| 02-01 | 1.00E-03 | 3.50E-03 | 1.00E+00 | 3.50E-03 | 3.50E-06 | 3.50E-03 | 1.00E+00 | 3.50E-03 | 3.50E-06 | 3.50E-06 | | 1.00E-07 | 2.86E-02 | 1 | 442 | 1.00E+06 | 971 | 1,413 |
| 02-02 | 1.00E-03 | 1.25E-01 | 1.00E+00 | 1.25E-01 | 1.25E-04 | 1.25E-01 | 1.00E+00 | 1.25E-01 | 1.25E-04 | 1.25E-04 | | 1.00E-07 | 8.00E-04 | 3 | 16,237 | 1.00E+06 | 999 | 17,236 |
| 02-03 | 1.00E-03 | 1.30E-03 | 2.00E-01 | 2.60E-04 | 2.60E-07 | N/A | N/A | N/A | 0 | 2.60E-07 | | 1.00E-07 | 3.85E-01 | 0 | 8 | 1.00E+05 | 62 | 70 |
| 02-04 | 1.00E-03 | 3.13E-01 | 2.00E-01 | 6.26E-02 | 6.26E-05 | N/A | N/A | N/A | 0 | 6.26E-05 | | 1.00E-07 | 1.60E-03 | 2 | 3,125 | 1.00E+05 | 100 | 3,225 |
| 02-05 | 1.00E-04 | 1.25E-01 | 5.00E-01 | 6.25E-02 | 6.25E-06 | N/A | N/A | N/A | 0 | 6.25E-06 | | 1.00E-07 | 1.60E-02 | 1 | 308 | 1.00E+05 | 10 | 317 |
| 02-06 | 1.00E-04 | 1.30E-03 | 1.00E-01 | 1.30E-04 | 1.30E-08 | N/A | N/A | N/A | 0 | 1.30E-08 | | 1.00E-07 | N/A | N/A | N/A | 1.00E+05 | 0 | 0 |
| 02-07 | 1.00E-04 | 3.13E-01 | 1.00E-01 | 3.13E-02 | 3.13E-06 | N/A | N/A | N/A | 0 | 3.13E-06 | | 1.00E-07 | 3.19E-02 | 1 | 152 | 1.00E+04 | 1 | 152 |
| 02-08 | 1.00E-04 | 5.90E-03 | 1.00E-01 | 5.90E-04 | 5.90E-08 | N/A | N/A | N/A | 0 | 5.90E-08 | | 1.00E-07 | N/A | N/A | N/A | 1.00E+04 | 0 | 0 |
| | 4.40E-03 | | | | 2.01E-04 | | | | 1.29E-04 | 2.01E-04 | | | | | 20,271 | | 2,143 | 22,414 |
| | | | | | 1.00E-03 | | | | 1.03E-03 | | 2.03E-03 | | | | | | | |
| 03-01 | 1.00E-04 | 3.50E-03 | 5.00E-01 | 1.75E-03 | 1.75E-07 | N/A | N/A | N/A | 0 | 1.75E-07 | | 1.00E-07 | 5.71E-01 | 0 | 4 | 1.00E+05 | 4 | 8 |
| 03-02 | 1.00E-04 | 3.50E-03 | 1.00E-01 | 3.50E-04 | 3.50E-08 | N/A | N/A | N/A | 0 | 3.50E-08 | | 1.00E-07 | N/A | N/A | N/A | 1.00E+05 | 0 | 0 |
| 03-03 | 1.00E-04 | 3.50E-03 | 1.00E-01 | 3.50E-04 | 3.50E-08 | N/A | N/A | N/A | 0 | 3.50E-08 | | 1.00E-07 | N/A | N/A | N/A | 1.00E+05 | 0 | 0 |
| 03-04 | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0 | 0 | | 1.00E-07 | N/A | N/A | N/A | 0.00E+00 | 0 | 0 |
| 03-05 | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0 | 0 | | 1.00E-07 | N/A | N/A | N/A | 0.00E+00 | 0 | 0 |
| 03-06 | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0 | 0 | | 1.00E-07 | N/A | N/A | N/A | 0.00E+00 | 0 | 0 |
| 03-07 | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0 | 0 | | 1.00E-07 | N/A | N/A | N/A | 0.00E+00 | 0 | 0 |
| 03-08 | N/A | N/A | N/A | N/A | 0.00E+00 | N/A | N/A | N/A | 0 | 0 | | 1.00E-07 | N/A | N/A | N/A | 0.00E+00 | 0 | 0 |
| | 3.00E-04 | | | | 2.45E-07 | | | | 0 | 2.45E-07 | | | | | 4 | | 4 | 8 |
| | | | | | 1.23E-06 | | | | 0 | | 1.23E-06 | | | | | | | |
| | | | | | 2.16E-04 | | | | 2.09E-04 | 2.16E-04 | | | | | | | | |
| | | | | | 5 | | | | 8 | 13 | | | | | | | | |
| | | | | | 1.08E-03 | | | | 1.67E-03 | 2.75E-03 | 2.75E-03 | | | | | | | |

*Choosing the Right Target*

In the above example, a seemingly arbitrary target of 1e-07pa has been used and the reasoning should be explained.

- This uses a heuristic approach. If the Maximum aggregated RIFOF was in the region of 1e-06pa, the risks by definition would be Broadly Acceptable. This is the lower limit of the region that is often referred to as 'Tolerable if ALARP' – the implication being that at this point further risk reduction measure need not be considered. If there were 10 equally weighted Hazardous Events on the page, it would make sense to target each at 1e-07pa because (in the unlikely event that the same group was most exposed to all Hazardous Events) that would still attempt to hit the Broadly Acceptable target. In reality, it is likely that there will be several hazards for which no suitably practicable risk reduction measure could be found.
- However, it would be possible to use the above to show a function of the Weighted Value versus the PFD of a theoretic IPL. It is readily noticeable that by adding a further 10-fold risk reduction, the Weighted Value only increments slightly. For example, if the target in scenario 01-01 was modified from 1e-07 to 1e-08, the Weighted Value (final column) changes from £6840 to £6849pa but the required risk reduction moves from SIL2 to SIL3. If a target of 1e-06pa is set, the Weighted Value only falls to £6752. This demonstrates that in realistic cases, the higher the residual risk target we choose, the more likely we are to find something worth implementing. This presents something of a conundrum in choosing of targets – we like to think we are aiming at the best targets but this is often failing to find the ALARP position.
  **Importantly, this guidance considers that the demonstration of ALARP is not complete without considering lower integrity theoretical solutions.**

Therefore, this guidance recommends that a residual risk target of 0 is chosen initially to get a picture of the total Available Benefit. The required PFD of the additional IPL should then be treated as the subject of negotiation given the knowledge that in cases as simple as this, a RRF of 10 will give 90% of the Available Benefit; a RRF of 100 will give 99% etc.
The selected RRF should be that which is highest achievable within the limits of gross disproportion.

Notes:

- This guidance recognises that in many complex cases, it is not as simple as adding an IPL, in which case engineering reasoning will play an important part in decision, but this guidance strongly recommends the concept of determining the Available Benefit as part of the reasoning.
- It is possible depending on how scenarios have been broken down that an additional layer of protection would apply to more than one scenario or even to more than one Hazardous Event. In any such cases, it would be necessary to aggregate the benefit from all affected scenarios.

# 8 References

## 8.1 References used in this guidance

[0] T6A - Legacy Systems: Basic Principles for Safety

[1] Health and Safety at Work, etc. Act (1974)

[2] Management of Health and Safety at Work Regulations (1999)

[3] HSE – Reducing Risks and Protecting People (2001)

[4] HSE - ALARP Suite – see HSE website

[5] HSL – RR151 Good practice and pitfalls in risk assessment (2003)

[6] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety related systems

[7] IEC 61511 Functional safety - Safety instrumented systems for the process industry sector

[8] HSE – ALARP "at a glance" – http://www.hse.gov.uk/risk/theory/alarpglance.htm

[9] HSE - Cost Benefit Analysis (CBA) checklist - http://www.hse.gov.uk/risk/theory/alarpcheck.htm

[10] HSE - principles for Cost Benefit Analysis (CBA) in support of ALARP decisions. http://www.hse.gov.uk/risk/theory/alarpcba.htm

[11] HSE – risk – frequently asked questions http://www.hse.gov.uk/risk/faq.htm

[12] House of Commons Library Briefing Paper 7458 – Health and Safety Statistics http://researchbriefings.files.parliament.uk/documents/CBP-7458/CBP-7458.pdf

[13] HSE –Societal Risk: Initial briefing to Societal Risk Technical Advisory Group http://www.hse.gov.uk/research/rrpdf/rr703.pdf

[14] EU Framework Directive (1989/391/EEC) (1989)