Guidance on ALARP for Major Hazard Facilities

Adrian Bunn, Manager, HSE Director, Fluor Ltd, Fluor Centre, 140 Pinehurst Road, Farnborough, GU21 7BF

Successful management of Health, Safety, Security and the Environment (HSSE) involves the assessment of HSSE risks associated with business activities and the implementation of controls that are appropriate to the level of risk. These principles including a risk based approach to the design, construction and operation of facilities are most operating company's group policy. A documented demonstration that HSSE risks are both tolerable and are reduced to a level that is As Low As Reasonably Practicable (ALARP) is a requirement of most company's group HSSE Management System.

Although there is no single correct approach to risk based design or the demonstration of ALARP, there are approaches that are more applicable to a particular situation than others and a decision framework is useful in the selection process.

This paper provides guidance to assist and promote consistent risk related decision making for major hazard facilities and control of major accident hazards. This includes guidance on determination of risk tolerability and justification that risks have been reduced to a level that can be considered to be ALARP.

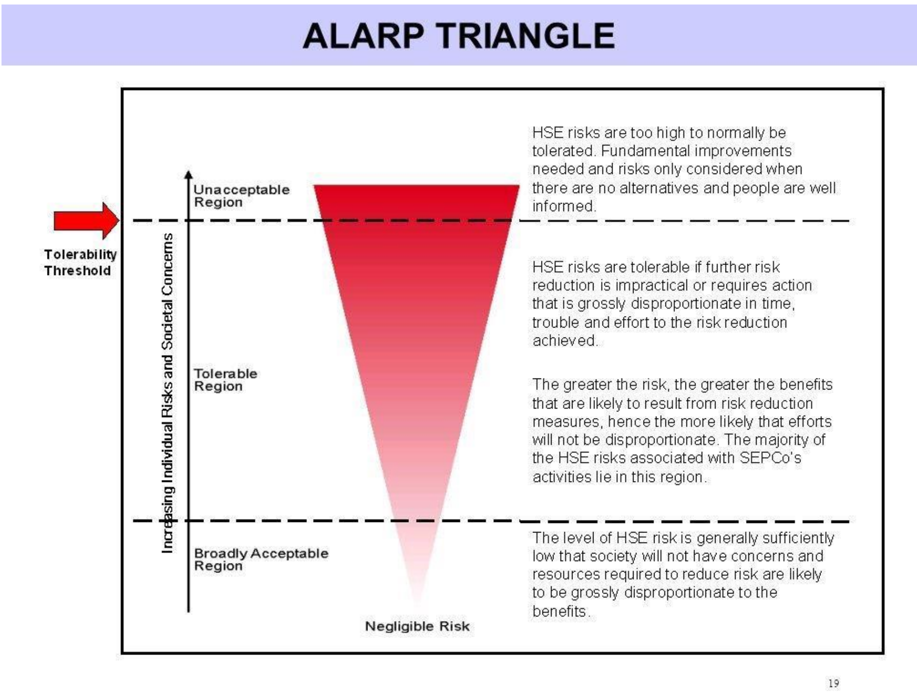
Although the guidance is specifically aimed at major hazard facilities, the general principles are also applicable to health, security, environment and other safety risk based decision making.

Keywords: ALARP, major hazards, risk assessment, risk criteria, risk matrix, impact criteria, risk reduction

Demonstration of ALARP

To reduce a risk to a level which is As Low As Reasonably Practicable (ALARP) involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it. This level represents the point, objectively assessed, at which the time, trouble, difficulty and cost of further reduction measures become unreasonably disproportionate to the additional risk reduction obtained.

Risk tolerability can be defined as three broad risk bands as follows:



ALARP is not just a demonstration that risks of the preferred or selected option are tolerable and/or comparable to other similar developments. Demonstrating ALARP requires consideration of fundamentally different options for further risk reduction over the lifetime of a facility or operation. Demonstrating ALARP requires consideration of all the issues related to a range of options and a judgmental decision at the right level in the organization with the full knowledge of all the options and associated risks and costs.

The process of demonstrating that the risks have been or will be reduced to ALARP typically consists of addressing the following questions:

What is the decision context?	Assess relative importance of codes and standards, good practice, qualitative, quantitative and cost benefit analysis, and company and societal values when making ALARP decisions.

What could go wrong?	Identification of the major hazards from normal and abnormal operation
How serious could it be?	Severity, consequence or impact analysis
How likely is it to happen?	Frequency or probability analysis
What control measures are implemented?	Identification of control measures to eliminate or, if it is not practicable to eliminate, reduce the risks.
What more can be done to further reduce the risks?	Identification of practicable options or alternatives for further risk reduction
Why have risk reduction measures not been implemented?	Evaluation of the reasonable practicability of identified measures
How will ALARP be assured?	Monitoring, audit and review of actions and controls to achieve ALARP

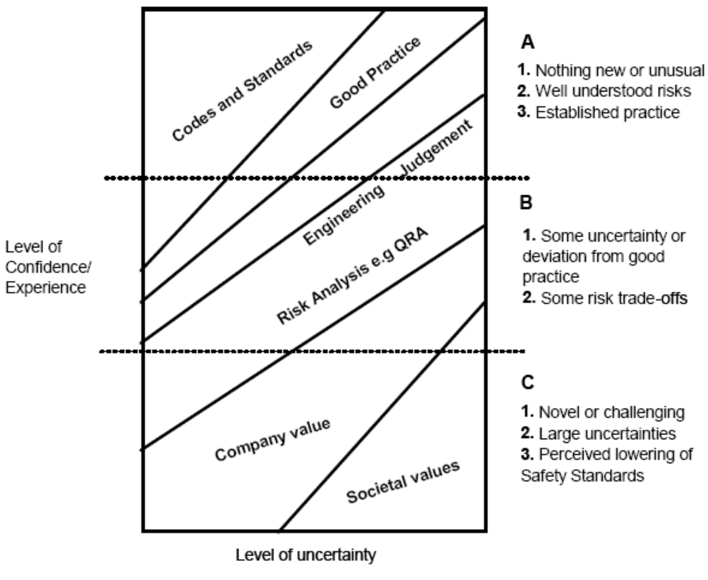
Decision Basis

UKOOA Framework for Risk Related Decision Support

Understanding and defining the decision(s) that must be made is critical. This includes definition of the decision to be made (e.g. to do or not to do something, how best to improve a facility or operation etc.), who needs to be involved/consulted (e.g. key stakeholders), options available, factors and issues that influence the decision(s) and decision context (e.g. novelty vs. well understood situation or practice, risk trade-offs, uncertainties, risk perceptions, business and economic implications) and factors that influence stakeholders (internal and external).

UKOOA (Oil and Gas UK) has developed a framework to promote transparent decision making and assist decision-makers choose an appropriate basis for their decisions and demonstration of ALARP (reference 7). The framework helps decision makers assess the relative importance of codes and standards, good practice, engineering judgement, risk analysis, cost benefit analysis and company and societal boundaries.

Figure 1: Risk Related Decision Support Framework



The framework takes the form of a spectrum of decision bases, ranging from those decisions dominated by purely engineering concerns (technology based decisions) to those where company and societal values are the most relevant factors (value based decisions). Typical characteristics which indicate the decision context are given on the right hand side of the framework. Once the decision context type has been identified, reading horizontally across the framework shows the suggested balance of decision bases to be taken into account (see Table 1). The relative proportions of the horizontal band in the various zones of the framework indicate the relative importance that should be attached to each of the decision bases (e.g. codes & standards, good practice, use of QRA/CBA, or consideration of company or societal values). Some means of calibrating or checking the decision basis are shown on the left hand side of the framework (Figure 2)

Table 1: Decision Bases

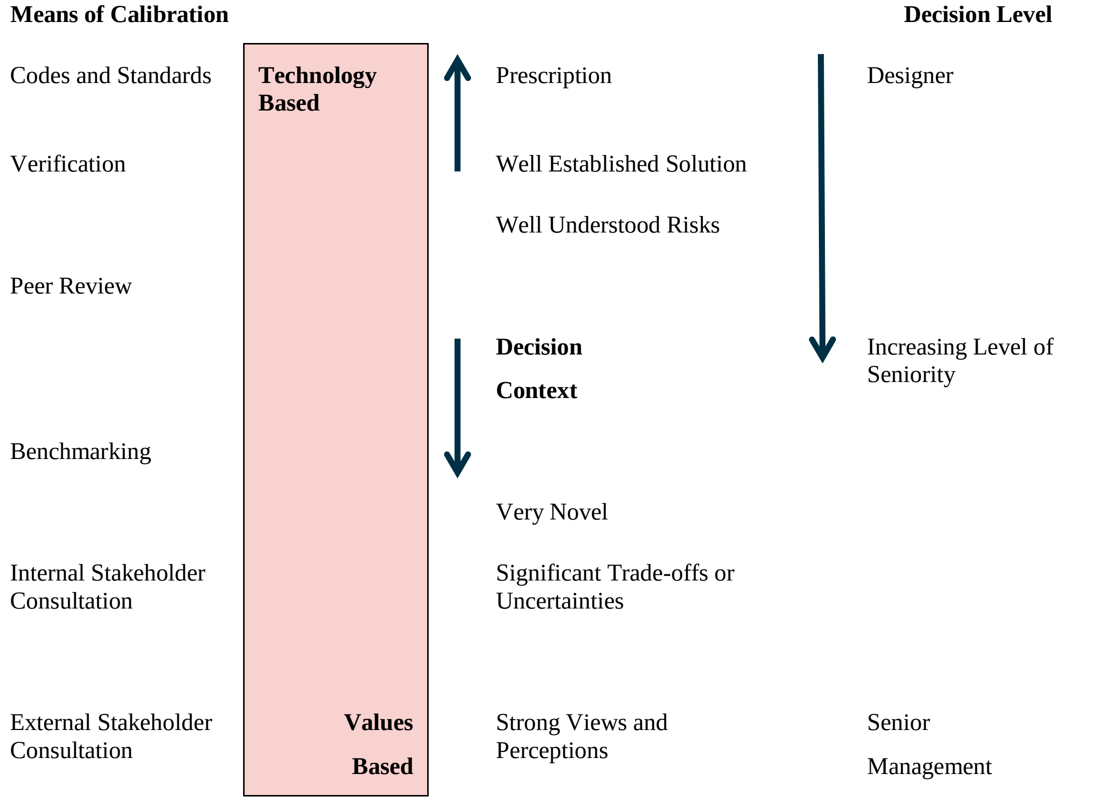
Codes and Standards Decision basis is to follow the requirements of the relevant codes and standards. Codes and standards embody the lessons learnt over past years, and for well understood hazards and situations often provide an appropriate solution.
Good Practice Decision basis is to follow what is generally accepted as current standard or good/best practice. Good practice embodies both the requirements of codes etc. and other good engineering, analysis and management practices for common situations. Good practice may include solutions that have not yet found their way into codes and standards. What is good practice may differ from situation to situations. Care should be taken to benchmark against the relevant good practice or emerging practice.
Engineering Judgement Decision basis is to follow what sound engineering judgement indicates as the best solution. This would be expected to include recognition of what is good/best/emerging practice, and an understanding and application of sound engineering and scientific principles and methods. It could include: engineering analysis, consequence modelling, deterministic cases for hazard management as well as competent judgement and interpretation of these and other information.
Risk Based Analysis (QRA, CBA etc.) Decision basis is to make use of the results of probabilistic analysis such as QRA, reliability analysis and CBA to support the decision making process. The assessment could be qualitative or quantitative. Uncertainties and the resolution of the analysis vs. the needs of the decision will be key issues to address.
Company Values Decision basis should take account of the views, concerns and perceptions of the stakeholders directly affected by the decision/option and the values of the company in terms of its safety commitment, image etc.
Societal Values Decision basis should take account of the views, concerns and perceptions of all the relevant stakeholders, including society at large etc.

Table 2: Means of Calibrating the Decision Bases

Codes and Standards Refer to the latest codes and standards, regulations, approved code of practice, guidance and classification rules.
Verification Use verification process to demonstrate compliance with codes and standards, established performance standards or good practice. Make reference to 'verified' arrangements and designs to demonstrate meeting 'good' practice.
Peer Review Use internal peer/expert review or consultation with external industry experts to confirm the validity and robustness of any judgements or analyses made.
Benchmarking Benchmarking practices against others in the industry or other industries where appropriate to show relevance and robustness of the approach and any principles this is based on e.g. via technical committees /forums, industry contacts and experts. Benchmark the scope, method and detail of the analysis and any assessment of uncertainty against practices in other companies/similar situations to show the robustness of the approach.
Internal Stakeholder Consultation

Consult with, or otherwise elicit the views and perceptions of the stakeholders (such as the workforce) directly affected by the decision/options e.g. by surveys, direct consultation with safety representatives. Benchmark these against the views of similar stakeholders in other companies or business units. Make attempts to identify and record the values of the company/project/unit or other culture in which the decision is to be taken and the values of those which might be affected by the decisions (e.g. downstream business/units/partners etc.)
External Stakeholder Consultation Consult with or otherwise elicit the views and perceptions of the stakeholders directly and indirectly affected by the decisions/options e.g. by surveys, direct consultation. Consider local, National, European or international societal and industry views and perceptions.

Figure 2: Risk Related Decision Levels



Technology based decisions which only require reference to codes and standards or established practice can generally be taken by the designer. As the risk or economic implications increase, the decision should be elevated within the organization. Values based decisions which could have a major impact on the business as a whole or company reputation should be referred to senior management.

Although primarily aimed at the offshore oil and gas industry the framework could be used to provide a more transparent decision making process across other sectors. For example, development of a remote onshore LNG facility or a gas transmission pipeline would typically fall into a 'Type A' context whereas developments in or near urban areas or where uncertainties exist would more likely be 'Type B'. In some circumstances, especially where these involve sensitive areas such as the environment or public risk, or where there are large risk implications or uncertainties, internal and external stakeholder views or expectations may need to be addressed i.e. 'Type C'.

Codes and Standards

In many common engineering situations or for well understood hazards and effects, what is reasonably practicable may be determined simply by compliance with accepted international, national or industry codes and standards, recommended or best practice guidelines or national guidelines. The majority of ALARP decision making will usually fall into this category. However, care needs to be taken to ensure that the limits of applicability are in accordance with the intended use. On occasion this can be complicated by the fact that the code or standard may not fully define its range of application or why particular measures are specified. For new or non-standard designs and large or complex facilities, it is unlikely that all possible scenarios can be identified using codes and standards alone.

The adopted codes and standards, and the control measures that they specify, should all be shown to be suitable and appropriate to the specific major hazard facility, taking account of its type, scale, activities, location etc. In addition, compliance with the adopted codes and standards or achievement of an equivalent level of safety by other means should be clearly demonstrated. This could include reference to certification, independent verification and/or detailed statements against each clause within the adopted code or standard.

In some cases there are over-arching codes and standards that apply to many aspects of the design and operation of a facility, for example, LNG facilities (references 1 and 2) or high pressure gas transmission pipelines (references 3 and 4). For simple facilities of this type it may be possible to base a demonstration of ALARP largely on compliance with such codes and standards. However, for large or complex facilities of these types or facilities in sensitive locations, it will most likely be necessary to go beyond compliance to demonstrate ALARP.

For other facilities, for example offshore installations, onshore oil or gas terminals, power generation, there are often no single over-arching codes and standards for all aspects of the facility design and operation. Instead, codes and standards exist for specific areas of design (pressure vessels, area classification, fire protection etc.) and safety management (management systems, permit to work, isolation etc.). A suite of standards is thus adopted for a particular facility and considerable effort may be necessary to demonstrate that the overall suite is suitable and appropriate, as well as individual parts.

Compliance with codes and standards provides a sound design basis for many cases but does not replace risk assessment altogether. The greater the potential exposure to total loss or multiple fatalities, the less desirable it is to use only conventional rule-based approaches for decision making (e.g. codes and standards). Many of the new generation of codes and standards have moved away from a prescriptive approach, to one of goal-setting objectives recognizing the fact that there may be several means of providing adequate control and the value of risk assessment.

Risk Assessment

Risk assessment can provide a better understanding of the consequences and likelihood of a hazardous event allowing the most appropriate (cost effective) means of prevention or mitigation to be selected. Risk assessment can be particularly useful in situations where, for example, there is high complexity, high costs, conflicting risks, risk trade-offs and uncertainty.

There are various approaches and many specific methods for risk assessment. Whilst there is no single approach for a specific facility, there are approaches that are more suitable than others. Key factors in the selection of a suitable risk assessment approach include; Lifecycle stage, Major hazard potential, Risk decision context.

Lifecycle stage implies greater or lesser flexibility to change design elements, knowledge of specific design and operational details, availability of historical records. Lesser design or operational knowledge will limit the approach to coarser methods.

The depth of the assessment should be proportionate to the scale and nature of the major hazards presented by the facilities and activities on them and the risks posed to the workforce and neighbouring populations. The depth of analysis thus ranges from qualitative at the lowest risk level through semi-quantitative up to quantitative and Cost Benefit Analysis (CBA) at the highest level. It is not necessary to use QRA or CBA to demonstrate whether risks are ALARP for all major hazard facilities or activities, but these are likely to have some degree of input to many decisions. QRA is particularly important for decisions involving risk trade-offs, novel systems, deviations from standard practice or significant economic implications. The key is choosing the right approach to provide the required information for robust decision making without overworking the problem.

Risk assessment may be considered to consist of structured engineering judgement and risk base analysis within the UKOOA decision support framework. The framework indicates that risk assessment has a major input to Type B decisions. For Type A and C decisions, risk assessment is still relevant but is likely to be much less influential in reaching the final ALARP decision. Higher elements of novelty, uncertainty or stakeholder concern will demand more thorough risk assessment.

Further guidance on the various assessment approaches and methods including applicability to the lifecycle stage is given in ISO 17776 (reference 5).

Risk assessment involves the systematic evaluation of the risks (combination of likelihood and consequence of potential hazardous events) together with a rational evaluation of their significance, risk tolerability and ALARP.

Values

Risk assessment and good practice analyses cannot always address all the relevant factors. There may also be the need to take into account the views and concerns of those affected by the decision. Stakeholder perceptions of the risk and benefits may be different from that analysed affecting their view on what is reasonably practicable. Company values may also affect the decision in these circumstances. Where new or potentially controversial activities are proposed, where there are large risk implications or uncertainties, or where these involve sensitive areas such as the environment or public risk it may be appropriate to consider more carefully the views, perceptions and expectations of all stakeholders. In some cases it may be worthwhile initiating a period of consultation to help clarify these factors and involve stakeholders in the decision making process.

Overall Decision Framework

An overall framework taking account of all the decision factors and options outlined above us is presented in Figure 3 based on reference 6. In general, options towards the upper rows are less detailed and options lower down are more detailed. It is not simply a matter of taking a horizontal slice through the diagram. Some parts of the analysis can be more detailed than others, and the concept here is appropriateness – not over complexity. An example is provided at the end of this paper to illustrate and clarify these points.

Figure 3: Overall Decision Framework

Key Drivers		
Lifecycle Stage	**Major Hazard Potential**	**Decision Context**
Concept Design Operations Abandonment	Potential Catastrophic Loss Significant Number of People Significant Environmental Potential	Type A Nothing new or unusual Well understood risks Established practice No major stakeholder implications Type B Lifecycle implications Some risk trade-offs/ transfers Some uncertainty or deviation from standard or best practice Significant economic implications Type C Very novel or challenging Strong stakeholder views and perceptions Significant risk trade-offs or risk transfer Large uncertainties Perceived lowering of safety standards

Risk Assessment Approach Selection			
Hazard Identification Technique	**Risk Approach**	**Technique and ALARP Demonstration**	**Decision Making**
Judgement Checklists FMECA Structured HAZID HAZOP	Codes and Standards Engineering Judgement Risk Analysis a) Qualitative b) Semi-Quantitative c) Quantitative Value Systems	Simple Tabulation Risk Matrix 'Bowtie' Analysis Consequence Analysis Quantitative Risk Analysis Stakeholder Consultations	Team Judgement Minimum Number of Controls Cost Benefit Analysis Senior Management Judgement

Risk Criteria

Tolerability and Acceptability

'Tolerability' does not mean 'acceptability'. It refers to a willingness to live with a risk so as to secure certain benefits and in the confidence that it is being properly controlled. To tolerate a risk implies that it is not regarded as negligible or something that is to be ignored but rather as something that needs to be kept under review and reduced still further if and when possible. For a risk to be 'acceptable' means that for the purposes of life or work it is to be taken pretty well as it is.

Expressions such as 'acceptably safe' or 'an acceptable risk' are to be avoided. Risks are never acceptable when the benefits of an activity are not perceived to be larger than the risks. Also, a risk is never considered acceptable while there are effective alternates to lower the risk. If there are no further effective (cost or practical) alternatives it may be necessary 'to tolerate' the risk.

Qualitative Risk Matrix and Criteria

Risk matrices provide a traceable framework for consideration of the frequency and consequences of hazards. The matrices can be used to rank the risk in order of significance, screen out insignificant risks, or evaluate the need for risk reduction. Each hazard identified using a structured hazard identification technique is categorized, based upon the judgement of the assessment team, according to the magnitude of the likelihood and consequence of occurrence. The matrix then gives some form of evaluation or ranking of the risk for the particular hazard. Figure 4 shows the general risk matrix with associated tolerability criteria than can be used as a screening tool. Further definition of the consequence severity is given in Table 3 based on potential incident categories.

Figure 4: General Risk Matrix

Consequence					Increasing Probability				
Severity Rating	**People**	**Assets**	**Environment**	**Reputation**	**A**	**B**	**C**	**D**	**E**
					Never heard of in industry	**Has occurred in industry**	**Incident has occurred in Company**	**Incident occurs several times per year in Company**	**Incident happens several times per year at location**
0	Zero injury	Zero damage	Zero effect	Zero impact	Low	risk			
1	Slight injury	Slight damage	Slight effect	Slight impact	Manage continuous	for improvement			
2	Minor injury	Minor damage	Minor effect	Limited impact				Medium	risk
3	Major injury	Local damage	Local effect	Considerable impact			Incorporate reduction	Risk measures	
4	Single fatality	Major damage	Major effect	Major national impact		Demonstrate	ALARP	High	Risk
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact					Intolerable

The above matrix is useful for initial screening purposes but only has limited value for major hazards. These invariably fall into Severity Rating 4 or 5 and using history to indicate the likelihood of very infrequent events such as major accidents is not always valid. However, the matrix is useful for identifying the major hazards and for initial screening of risk reduction options. An alternative matrix for further assessment of major hazards is given in Figure 5.

Where risk matrices are used:

- Judgements made on consequence and likelihood should be properly recorded else the basis for the risk decisions will be lost
- Consensus among different team members should be strived for
- For multiple consequences (e.g. a fall at grade could lead to a consequence ranging from nothing to a broken neck) a reasonably foreseeable but more pessimistic outcome (e.g. broken leg) should be used rather than the very rare worst case or most likely trivial outcome
- Risk decisions should be based on the totality of all risks and thus some view on this needs to be developed, risk matrices only consider hazards one at a time.

Table 3: Incident Categories

Rating	**People** (Fatalities, Injuries, Occupational Health)		**Assets[1], Equipment**	
	Potential Impact	**Definition**	**Potential Impact**	**Definition**
0	No injury	No injury or damage to health	No damage	No damage to equipment
1	Slight injury/illness	Not detrimental to individual employability or the performance of present work. Agents which are not hazardous to health.	Slight damage	No disruption to the process, minimum cost of repair (below £10,000)
2	Minor injury/illness	Detrimental to the performance of present work, such as curtailment of activities or some day’s absence to recover fully, maximum 1 week. Agents which have limited health effects which are reversible, e.g. irritants, many food poisoning bacteria.	Minor damage	Possible brief disruption of the process; isolation of equipment for repair (estimated cost below £100,000)
3	Major injury/illness	Leading to permanent partial disablement or unfitness for work or detrimental to performance of work over extended period, such as long term absence. Agents that are capable of irreversible damage without serious disability, e.g. noise, poorly design manual handling tasks.	Local damage	Plant partly down; process can (possibly) be restarted. (Estimated cost of repair below £1,000,000)
4	Single fatality/permanent total disability or unfitness for work (small exposed population)	Also includes the possibility of multiple fatalities (maximum 3) in close succession due to incident e.g. explosion. Agents which are capable of irreversible damage with serious disability or death, e.g. corrosives, known human carcinogens	Major damage	Partial loss of plant; plant shutdown (for at most 2 weeks and/or estimated repair costs below £10,000,000)
5	Multiple fatalities	May include 4 fatalities in close succession due to the incident, or multiple fatalities (4 or more) each at different points and/or with different activities. Agents with the potential to cause multiple fatalities, e.g. chemicals with acute toxic effects (e.g. hydrogen sulphide, known human carcinogens).	Extensive damage	Total loss of the plant; extensive damage (estimated cost of repair exceeds £10,000,000)

1. Assets are understood as referring to: the oil and gas reservoirs, production facilities, pipelines, money, capital and other company, contractor and third party property.

Table 3 (continued): Incident Categories

Rating	Environment[2]				Assets[1], Equipment	
	Potential Impact	Definition	Contamination (litres)		Potential Impact	Definition
			Sensitive Areas	Offshore		
0	No effect	No financial consequence No environmental risk			No impact	No public awareness
1	Slight effect	Negligible financial consequences; local environment risk within the fence and within systems	<10	0-100	Slight impact	Public awareness of the incident may exist; there is no public concern
2	Minor effect	Contamination; damage sufficiently large to attack the environment; single exceedance of statutory or prescribed criteria; single complaint; no permanent effect on the environment.	<100	100-1000	Limited impact	Some local public concern; slight local media and/or local political attention with potentially negative aspects for operations.
3	Local effect	Limited loss of discharges of known toxicity; repeated exceedance of statutory or prescribed limit and beyond fence/neighbourhood.	100-1000	1000-10000	Considerable impact	Regional public concern. Extensive attention in local media; slight national media and/or local/regional political attention with possibly negative stance of local government and/or action groups.
4	Major effect	Severe environmental damage; the operator is required to take extensive measures to restore the contaminated environment to its original state. Extended exceedance of statutory or prescribed limit.	1000–10000	10000-100000	Major national impact	National public concern. Extensive negative attention in national media and/or regional national policies with potentially restrictive measures and/or impact on grant of licences, mobilization of action groups.
5	Massive effect	Persistent severe environmental damage or severe nuisance extending over a large area. In terms of commercial or recreational use or nature conservancy, a major economic loss for the operator. Constant high exceedance of statutory or prescribed limit.	>10000	>100000	Major international impact	International public attention. Extensive negative attention in international media and national/international policies with potentially severe impact on access to new areas, grants of licences and/or tax legislation.

2. Incidents relating to air, noise, light and soil vibrations should be addressed on the basis of expert judgement.

Figure 5: Risk Matrix (Major Hazards)

Number of Potential Fatalities	Likelihood (per year)			
	Remote ($10^{-8} – 10^{-6}$)	Very Unlikely ($10^{-6} – 10^{-4}$)	Unlikely ($10^{-4} – 10^{-2}$)	Likely $>10^{-2}$
1	Manage for			
2 – 10	Continuous improvement	Incorporate	risk reduction measures	
11 – 50				
50 – 100	Demonstrate	ALARP		Intolerable
100+				

Where risks fall within the intolerable or tolerable regions of the risk matrix (i.e. high and medium risk) risk reduction measures should be identified and assessed, and implemented where reasonably practicable.

The required number and quality of controls required depends on the magnitude of the risk. The number of controls based on qualitative assessment is a matter of experience and judgement. Although there is no clear rationale to determine the exact required number of controls for a given situation or risk, the general principle should apply that the higher the risks the more, and more stringent, controls are required. The following controls acceptance criteria is provided as guidance and should be modified as appropriate to meet the specific circumstances.

Table 4: Controls Acceptance Criteria

Controls	Intolerable Risk Hazards	Tolerable if ALARP Zone Hazards	Low Risk Hazards
Prevention Measures	Minimum of 3 independent effective prevention measures to be in place for each hazard cause	Minimum of 2 independent effective prevention measures to be in place for each identified hazard cause	Minimum of 1 independent effective measure to be in place for each identified hazard cause
Mitigation/Recovery Measures	Minimum of 3 independent effective mitigation/recovery measures for each identified consequence (including one to detect automatically occurrence of top event and one other to prevent automatically further escalation)	Minimum of 2 independent effective mitigation/recovery measures required for each identified consequence (one to detect occurrence of top event and other to prevent further escalation)	Minimum of 1 independent effective mitigation/recovery measure required for each identified consequence
Escalation Factor Controls	Minimum of 2 independent effective controls for each identified escalation factor	Minimum of 1 independent effective control for each identified escalation factor	Minimum of 1 procedure of each identified escalation factor

Impact Criteria

Impact criteria such as toxicity, thermal radiation or blast overpressure, together with consequence modelling can be used to determine whether the potential impact on people within the boundary of the facility or potential impact at the facility's fence or property line exceeds a tolerable threshold. These are usually defined within codes and standards. For example, BSEN 1473(6) for LNG facilities defines allowable thermal radiation flux inside the boundary for key equipment and buildings (including control room) and outside the boundary for different locations (remote, urban etc.).

Generic impairment criteria can also be applied to determine the adequacy of particular evacuation and escape provisions and the subsequent implication on the risk to personnel. Some examples are given below.

Escape Routes

- Loss of structural integrity
- Thermal radiation in excess of 6.3kW/m^2
- Smoke concentrations in excess of 15% by volume

Muster/Embarkation Areas

- Loss of structural support
- Thermal radiation in excess of 2kW/m^2
- Smoke concentration in excess of 2% by volume

Temporary Refuge

- Loss of structural support
- Collapse of supporting structure (jacket, module support frame)
- Deformation of supporting structure
- Breach of boundaries (walls/floor/roof) by fire or blast overpressure
- Inside temperature of boundaries >200˚C
- Loss of life support
- Ingress or presence of smoke, gas or toxic fumes

-	Smoke	>	2%
-	Carbon Dioxide	>	15000ppm
-	Hydrogen Cyanide	>	300ppm
-	Hydrogen Sulphide	>	10ppm
-	Sulphur Dioxide	>	50ppm
-	Lack of Oxygen	>	16% by vol

- High air temperature
- Loss of command support
- Loss of communications
- Emergency power failure
- Control systems failure

Quantitative Risk Criteria

Individual Risk

Individual risk usually refers to the risk of a fatality, measured on an annual basis (Individual Risk Per Annum (IRPA)), for an individual worker from all the hazards relating to any company activity. Individual risk should be specific to an individual worker or group of workers carrying out similar tasks with similar work patterns. All risk contributors should be included including transport, when provided by the company such as helicopter transport to an offshore installation, and occupational risk, as well as major accident hazards. Assessments should take account of people exposed to exceptional risks, i.e. critical groups exposed to risks significantly higher than average for the facility or activity when evaluating the tolerability of risks.

Individual risk tolerability criteria are defined by the major oil companies, but may typically be:

"The following criteria shall apply when judging the tolerability of risk to persons for XX Group facilities, sites, combined operations or activities.

(a) Individual risk to any worker above 10^{-3} per annum is intolerable and fundamental risk reduction improvements are required

(b) Individual risk below 10^{-3} but above 10^{-6} per annum for any worker is considered tolerable if it can be demonstrated that the risks are ALARP

(c) Individual risk below 10^{-6} per annum for any worker is considered as broadly acceptable and no further improvements are considered necessary provided documented control measures are in place and maintained."

With respect to risk to the general public, the design and operation of major hazard facilities should be such that no accidental release or other event will result in public fatalities or serious injuries. Individual risk to any member of the general public should be calculated on the basis of location specific risk. Location specific risk is typically presented in the form of risk contours. These are useful in guiding public developments close to the facility. A similar approach is applied by the UK Health and Safety Executive for land use planning (references 8 and 9).

Risk Reduction Measures

The key to the demonstration of ALARP whether qualitative or quantitative is the identification and evaluation of risk reduction measures. Risk control measures include both those to prevent incidents (reducing the probability or likelihood of occurrence) and those to mitigate chronic and acute effects (reducing the consequences).

Wherever possible or practicable, precedence must be given to elimination and prevention rather than cure through Inherently Safe Design, and selection of risk control measures should follow the preferred hierarchy:

- Elimination or minimization of hazard
- Engineering design (passive followed by active)
- Suitable systems of working
- Personal protective equipment

Inherent safety is concerned with the removal or reduction of a hazard at source. Examples of inherently safe techniques include; substitution of a less hazardous process, use of corrosion resistant materials of construction, reduction or elimination of hazardous inventory, design for maximum foreseeable operating conditions, fail safe design principles and appropriate plant layout etc.

Passive engineering design measures offer a typically high level of reliability by operating without any devices that sense and/or actively respond to a process variable, e.g. corrosion allowance, double containment, passive fire protection.

Active engineering design measures typically monitor process variables and activate to mitigate a hazardous situation, e.g. leak detection, emergency shutdown, firefighting systems/deluge, relief valves but can be used to actively prevent hazard occurrence e.g. corrosion inhibitor. Active measures are often less reliable than inherently safer or passive measures as they required more maintenance and more operating procedures.

Suitable systems of working such as procedural or management controls; e.g. permit to work, operating procedures, competence assurance, maintenance, emergency response, usually require a person to take action. Human factors may therefore have to be accounted for in the evaluation of control effectiveness. In general, these types of control measure are less reliable than other design solutions.

Factors that should be considered in selecting or rejecting risk measures include:

- Are there controls clearly linked to each hazard, or are there hazards having no (or insufficient) control measures? Does the number of controls reflect the severity of the hazards?
- What is the survivability of the control measure in an incident? Is the control measure able to function as intended during the types of incidents it is intended to reduce or mitigate?

- Is the reliability of individual control measures, and of all control measures in combination, appropriate to the level of risk presented by the associated hazards. Is function testing sufficiently frequent to detect failures, and will failures once detected be rectified sufficiently promptly?
- Has the hierarchy of control measures been considered, with measures to eliminate the hazard adopted first if practicable, followed by measures to prevent, reduce and mitigate.
- Is there a balance of different types of control measure for each hazard, i.e. is there a diversity of control measures? Are the control measures associated with individual hazards independent of each other, or can they all be disabled by the same mechanism?
- Are new control measures compatible with the facility, and any other control measures already in use?
- Can the control measures be implemented at the facility considering their availability and cost?

Conclusions

It has been shown that ALARP demonstration requires consideration of all the issues related to a range of options together with a judgmental decision. To this end the decision support framework can be used as an aid to transparent decision making. Various forms of decision bases together with a means of calibration have been presented. It has also been shown that risk assessment (together with CBA) can provide a better understanding of the consequences and likelihood of a hazardous event. An overall framework taking account of all decision factors and options has been outlined. Typical risk criteria indicating the tolerability of risk have been provided. Finally, measures to reduce risk together with factors to consider in selecting or rejecting such measures are listed.

An illustrative example is provided below.

References

1. Installation and Equipment for Liquefied Natural Gas – Design of Onshore Installations, European Standard EN 1473
2. Standard for the production, Storage and Handling of Liquefied Natural Gas (LNG), National Fire Protection Association NFPA 59A
3. Steel Pipelines for High Pressure Gas Transmission , Institute of Gas Engineers IGE/TD/1
4. Gas Transmission and Distribution Piping System, American Society of Mechanical Engineers ASME B31.8
5. Petroleum and Natural Gas Industries – Offshore Production Installations – Guidelines on tools and techniques for hazard identification and risk assessment, International Standards Organisation ISO 17776
6. Marine Risk Assessment, Health and Safety Executive, Offshore Technology Report 2001/063
7. Industry Guidelines on a Framework for Risk Related Decision Support, UKOOA, May 1999.
8. Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards, Health and Safety Executive, 1989.
9. Reducing Risks, Protecting People, Health and Safety Executive, 2001.

Overall Decision Framework Example

The example presented covers a major hazard facility which might be encountered at the design stage of the life cycle. The example shows which might be the best approach and gives reasons. The example is purely illustrative of the approach and should not be taken as definitive. In practice each specific case must be evaluated for the specific circumstances and issues.

Design: Offshore Production Installation

A hypothetical manned offshore gas production installation is being developed in an area with adverse weather conditions (cold temperatures, high winds, high waves etc.), persons on board 50. Concept selection has determined that the installation will be a single integrated platform with wells, gas processing and gas export to a nearby platform to shore in a common pipeline.

Lifecycle Stage	Design
	Key factors may include layout options, selection of risk control measures, well engineering, process design, structural design, evacuation, escape and rescue options, future development/expansion
Major Hazard Potential	Catastrophic loss possible
Decision Context	Type B (lifecycle implications, risk tradeoffs e.g. fire vs explosion, unique design, some uncertainties)
Hazard ID Technique	Structured HAZID techniques should be used to ensure that all potential major hazards are identified. HAZOP analysis should be used to identify process hazard situations that may arise in normal operation or due to mal-operation. Failure mode, effects and criticality analysis may be used to support HAZOP studies and identification of preventative control measures. Hazard registers produced during concept selection should be updated. Hazards associated with construction, installation and subsequent decommissioning and disposal should be re-evaluated against design developments.
Risk Approach	The risk approach could be quantitative following initial screening using qualitative or semi-quantitative techniques to identify the major hazards requiring further detailed qualitative analysis. Where hazards are eliminated from further study, justification should be given for elimination and the adequacy of control measures for these hazards. Codes and standards, good practice and engineering judgement will also provide useful input.
Technique	Quantitative risk assessment should be used to evaluate different design and risk control options as well as to determine overall risk levels on the installation and vulnerability of safety critical elements. Consequence analysis will be required to support the QRA. Bowtie analysis may be useful in linking safety critical elements with activities and tasks required to assure that their performance standards are achieved during operations.
Decision Making	The decisions are largely technical and would normally be taken by the design team using the QRA results as input to a cost benefit analysis. Referral to the senior management for approval should be considered as a catastrophic incident is possible.