HSE
Health & Safety Executive

Marine risk assessment

Prepared by **Det Norske Veritas**
for the Health and Safety Executive

OFFSHORE TECHNOLOGY REPORT
2001/063

Marine risk assessment

Det Norske Veritas
London Technical Consultancy
Palace House
3 Cathedral Street
London SE1 9DE
United Kingdom

HSE BOOKS

First published 2002

ISBN 0 7176 2231 2

Summary

Risk assessment provides a structured basis for offshore operators to identify hazards and to ensure risks have been to reduced to appropriate levels in a cost-effective manner. The regulations applying to offshore operations in the UK require operators to undertake risk assessment in order to identify appropriate measures to protect people against accidents, so far as is reasonably practicable. However, few marine operations have been reviewed using risk assessment methods. It may well be that the use of Quantitative Risk Assessment (QRA) for Temporary Refuges has given the impression that risk assessment is synonymous with QRA.

The safety of offshore installations against marine hazards has traditionally relied on International Maritime Organization (IMO) legislation and classification society rules. These rules have been developed by expert judgement, responding to previous accident experience, and in general prescribe specific design solutions. They are only rarely based on risk assessment, and do not by themselves satisfy the requirement to perform a risk assessment.

It is the purpose of this Guidance to encourage greater use of risk assessment methods for marine operations – especially those methods towards the simpler end of risk assessment: the qualitative and semi-quantitative techniques. It explains risk assessment technology as it might apply to marine operations, emphasising techniques appropriate to marine hazards. While QRA has a role in some marine applications, this Guidance demonstrates how the wider range of techniques can help operators perform a suitable and sufficient risk assessment, and demonstrate that risks are As Low As Reasonably Practicable (ALARP).

Section 1 of the guide outlines the regulatory system for safety of marine operations, and discusses the role of risk assessment in meeting this framework. In particular, it reviews some recent HSE and industry views on risk assessment; and considers the overlap with Classification Society Rules and newer risk-based rules.

Section 2 gives details on the various approaches to risk assessment, including qualitative, semi-quantitative and quantitative techniques. It considers their strengths and weaknesses for marine applications, and gives references to source material with further information.

Section 3 describes the way risk assessment results can be used to provide input to a decision-making process. This includes the use of risk criteria and cost-benefit analysis within an ALARP framework.

Appendix I gives a glossary of terms and abbreviations used in the guide.

Appendix II gives some worked examples of how to choose an approach to marine risk assessment that will be suitable and sufficient.

This guide primarily covers mobile offshore installations, which include semi-submersibles, jack-ups and heavy lift vessels. It also covers floating production systems (FPS), which are often based on semi-submersible or ship hulls. Some of the hazards and hence the guidance may also be relevant for fixed steel and concrete installations and tension leg platforms. The guide does not cover shuttle tankers, supply vessels, stand-by vessels and other offshore industry vessels not required to submit a safety case.

Contents

Appendices

1. INTRODUCTION

1.1 Background

The use of risk assessment techniques in major hazard industries has grown significantly in recent years. This is particularly true in the offshore industry in the UK where many aspects are subject to full risk assessment, notably the Temporary Refuge assessment which is mandated to be analysed using Quantitative Risk Assessment (QRA). Other aspects of offshore facilities, such as related marine operations have tended to rely on meeting regulatory requirements, industry codes of practice, or Classification Society Rules.

Risk assessment is now a proven technology for operators to address larger hazards in a structured manner, and to ensure risks have been to reduced to appropriate levels cost effectively. This applies as well to marine operations as to topsides safety. However, the Offshore Safety Division (OSD) has noted few marine operations have been reviewed using risk assessment methods. It may well be that the use of QRA for Temporary Refuges have confused people in the maritime industry into thinking that risk assessment was synonymous with QRA.

At the QRA: Alchemy to Acceptability Conference in London in 1993, a set of quotes was presented reflecting the industry view of risk assessment and how this perception had changed over a 15 year period. Whilst this was specifically the oil industry view, it is likely that other industries introducing these techniques will also pass through these stages, albeit in less time if they learn from other industry's lessons.

Changing attitudes to Risk Assessment

Bleak: (1980: Major Oil Company Representative)

"QRA is equivalent to counting the number of angels that can stand on the head of a pin. It can be concluded that risk analysis is likely to be a waste of time if applied to chemical processes."

Bland: (1985: International Study Group on Risk Analysis)

"The whole analytical exercise might be considered to be objective. However, it must be realised that because of the large body of assumptions, estimates, judgements and opinions involved, much of the input information is often subjective."

Bullish: (1993: Extract Major Oil Company Risk Engineering Standard)

"QRA is a tool which helps translate hindsight (accidents) into foresight (planning) ... showing ways and means (improved engineering, procedures and supervision) to prevent the calculated accidents from happening."

The HSE commissioned a survey as to the effectiveness of the current offshore regulations and of the satisfaction of key stakeholders. An interim report in 1995 was broadly positive with both senior managers and workers reporting tangible safety benefits from the introduction of risk assessment and the safety case regime. This was updated in 1999 to account for new offshore regulations and for fuller review of the 200 safety case reports submitted (AUPEC 1999). This fuller review made several relevant findings:

- The key objectives of the Cullen Inquiry recommendations had been implemented with no perceived gaps.

- The UK regulatory regime was seen as amongst the best in the world.

- The use of formalised risk assessment had assisted in focusing attention on the more important risks and had improved understanding of these.

- Safety cases were initially too detailed and complex, and successful efforts had been made to simplify and slim them down.

- The specific tool of QRA (Quantitative Risk Assessment) was the subject of criticism, partly because the technique was too mathematical, and partly because there was insufficient agreement within the industry and the HSE on how to use the results of QRA.

- There is a move to more traditional forms of risk assessment and management.

It is the purpose of this Guidance to encourage greater use of risk assessment methods for marine operations – especially those methods towards the simpler end of risk assessment: the qualitative and semi-quantitative techniques. It will explain risk assessment technology as it might apply to marine operations and to demonstrate that there are a wide range of analysis types – all of which constitute risk analysis – but which cover Qualitative, Semi-Quantitative and Quantitative approaches. QRA has a role in some marine applications, but this Guidance will demonstrate the wider range of techniques and show how these can help operators meet suitable and sufficient requirements for demonstration of ALARP – As Low As Reasonably Practicable risks.

In the following introductory sections, the Guidance addresses the regulatory system for safety of marine operations and the role of risk assessment in meeting this framework; it reviews some current HSE and industry views on risk assessment; and finally it considers the overlap with Classification Society Rules and newer risk-based rules.

1.2 Application

This guide addresses marine hazards on offshore installations. Marine hazards are diverse in nature, and can be defined as any potential accident on an offshore installation connected with its interface with the marine environment. They include:

- Loss of position keeping (e.g. mooring, dynamic positioning, rig move)
- Loss of structural integrity (e.g. hull, ballast tank, support structure failure)
- Loss of stability (e.g. ballast system failure, cargo loads)
- Loss of marine/utility systems (e.g. propulsion, power generation, hydraulics)
- Collision (e.g. shuttle tanker, support vessel, passing vessel)

Marine hazards exclude accidents connected with drilling, hydrocarbon releases, other fires, dropped objects, helicopter transportation, diving or other personal hazards.

This guide primarily covers mobile offshore installations, which include semi-submersibles, jack-ups and heavy lift vessels. It also covers floating production systems (FPS), which are often based on semi-submersible or ship hulls. Some of the hazards and hence the guidance

may also be relevant for fixed steel and concrete installations and tension leg platforms. The guide does not cover shuttle tankers, supply vessels, stand-by vessels and other offshore industry vessels not required to submit a safety case.

1.3 Regulatory Context

1.3.1 General Safety Legislation

The Health & Safety at Work etc Act 1974 (HSWA) provides the foundation of offshore safety regulations on the UK Continental Shelf (UKCS). It imposes on an employer a duty "*to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees*" and "*to conduct his undertaking in such a way as to ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not exposed to risks to their health and safety*" (Sections 2 and 3). It also established the health and Safety Executive (HSE) as the body generally responsible for the enforcement of health and safety legislation.

The Management of Health and Safety at Work Regulations 1992 (MHSWR) support the general duties under HSWA by requiring employers to undertake risk assessment for the purpose of identifying the measures that need to be put in place to prevent accidents and protect people against accidents.

1.3.2 Safety Case Regulations

The Offshore Installations (Safety Case) Regulations 1992 (SCR) require the duty holder (i.e. the owner or operator) for each fixed and mobile installation to prepare a safety case, which must be accepted by the HSE before the installation can be operated on the UKCS. The duty holder must "*include in the safety case sufficient particulars to demonstrate that -*

(a) *his management system is adequate to ensure that the relevant statutory provisions will (in respect of matters within his control) be complied with in relation to the installation and any activity on or in connection with it;*

(b) *he has established adequate arrangements for audit and for the making of reports thereof;*

(c) *all hazards with the potential to cause a major accident have been identified; and*

(d) *risks have been evaluated and measures have been, or will be, taken to reduce the risks to persons affected by those hazards to the lowest level that is reasonably practicable.*" (Reg 8).

SCR gives a definition of the term "major accident" consisting of 5 particular types of accident. The only ones covered as marine hazards in this guide are:

"(b) *any event involving major damage to the structure of the installation or plant affixed thereto or any loss of stability in the installation;*

(e) any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity in connection with it" (Reg 2)

In other words, marine hazards that may give risk to major accidents (e.g. structural failure, collision, capsize) must be covered in the safety case, which must show that their risks have been made as low as reasonably practicable (ALARP). The other marine hazards (e.g. loss of position keeping, loss of utility systems) might be covered in the safety case as possible initiators of the major accidents, or in response to the more general duty imposed by the HSWA.

The Guidance on SCR (HSE 1998a) gives a brief indication of the type of risk assessment expected:

> "*The evaluation of risk should involve both a qualitative and quantitative approach. Where relevant good or best practice is clear, the balance should be in favour of qualitative arguments to show that the risks have been properly controlled. Where relevant good or best practice is less clear, appropriate support from quantitative arguments will be necessary.*" (para 105).

The Schedules of the SCR, which list the information to be included in safety cases for each type of installation also require "*a demonstration, by reference to the results of suitable and sufficient quantitative risk assessment*" that the temporary refuge (TR) and means of evacuation will make risks ALARP. This requirement only refers to "*protecting persons on the installation from hazards of explosions, fire, heat, smoke, toxic gas or fumes during any period while they may need to remain on the installation following an incident which is beyond immediate control*". In other words, the specific requirement for QRA in SCR does not apply to marine hazards. Duty holders are still free to use QRA for marine hazards, if they consider it suitable, but other approaches are acceptable.

1.3.3 Other UK Offshore Safety Regulations

The Safety Case Regulations are complemented by other regulations dealing with specific features of offshore safety:

- The Offshore Installations and Pipeline Works (Management and Administration) Regulations 1995 (MAR). This includes provisions covering such matters as the appointment of installation managers, the use of permit-to-work schemes, communication arrangements, records of persons on board and the collection of meteorological and oceanographic information. MAR has a high-level impact on marine hazards, but does not directly affect the requirement for risk assessment.

- The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations 1995 (PFEER). This promotes an integrated risk-based approach to managing fire and explosion hazards and emergency response. While the emergency response is relevant for marine hazards, the assessment of risks required by PFEER is outside the scope of this guide.

- The Offshore Installations and Wells (Design and Construction, etc) Regulations 1996 (DCR). This includes requirements for safeguarding the integrity of the installation throughout the its life. This applies specifically to marine hazards affecting the structural

strength, stability and buoyancy of an installation. DCR includes no specific requirement for risk assessment, but the risk assessments required under MHSWR, SCR and PFEER will help meet DCR's requirement to ensure integrity "so far as is reasonably practicable".

The DCR and SCR also require the duty holder to establish a "verification scheme", using "independent and competent persons" to ensure that "safety-critical elements" on the installation are suitable and remain in good condition. The "safety-critical elements" are parts of the installation that might contribute to or prevent or mitigate the effects of a major accident. Identification of these should be an outcome of the risk assessment.

The verification of safety-critical elements is particularly important for marine hazards, because these have traditionally been addressed through classification rules. The requirement for a independent verification is an adaptation of the previous regime, in which certifying authorities (primarily classification societies) inspected the installations to ensure "fitness for purpose".

1.4 Marine Regulations

1.4.1 General Approach of Marine Regulations

The safety of offshore installations against marine hazards has traditionally been managed in the same way as the safety of ships. Marine safety legislation still forms the basis for safety management of mobile offshore installations. This can be justified to the extent that they face common hazards and use similar design solutions.

The shipping safety regime consists primarily of international safety codes and regulations issued by the International Maritime Organization, and rules for the construction of ships issued by independent classification societies. National maritime administrations set relatively few additional requirements, reflecting the international nature of the shipping industry, and its need for uniform regulations applying in all ports. To a limited extent, the same considerations apply to mobile offshore installations.

Classification societies and national administrations have important roles in verifying compliance with the applicable regulations through Port State Control and classification surveys. This is equivalent to the independent verification required for offshore installations.

Marine safety regulations have grown in a mainly reactive way, with accident experience providing the prime motivation for improved regulation. This approach was successful for large fleets of similar ships, in which past experience formed a good basis for safety management. However, it has been less effective for unusual and rapidly changing designs, such as many offshore installations and several important types of ships. In response, the shipping industry is developing formal safety assessment as a more proactive approach to regulation (Section 1.5.4).

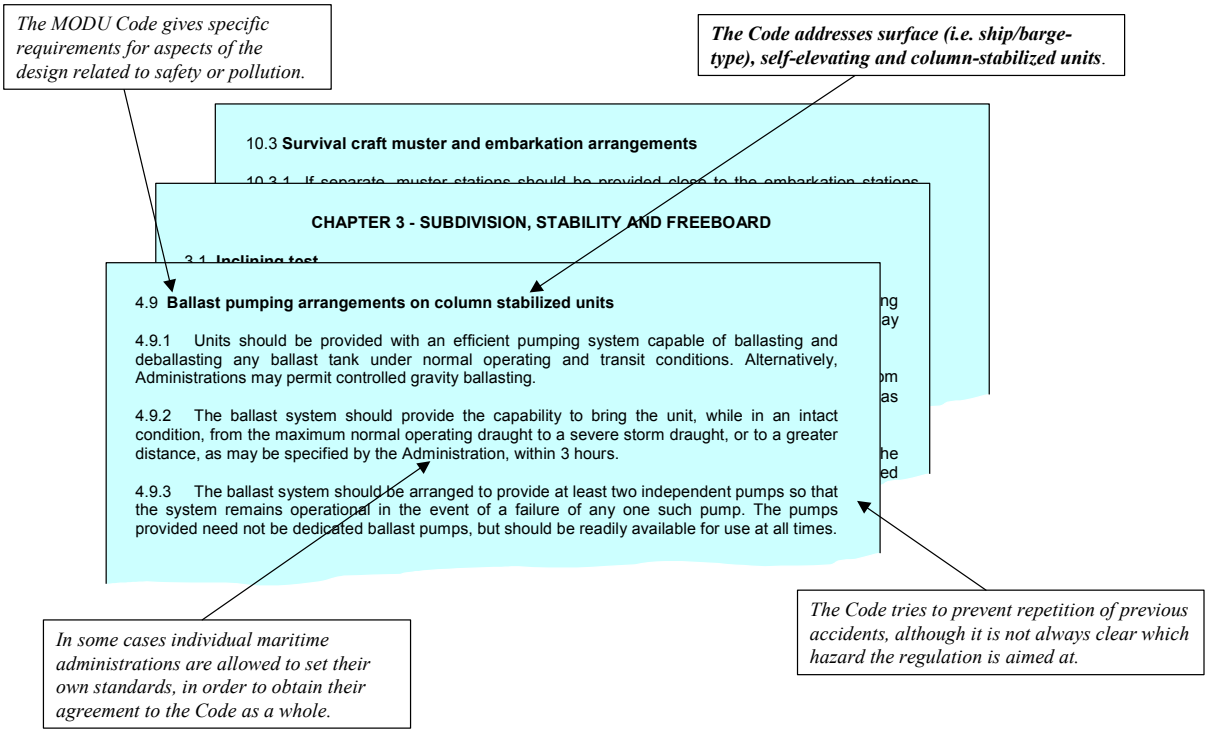
The advantage of marine regulations is that they encapsulate the accumulated wisdom from accident experience and from the judgement of many experts world-wide who have contributed to refining and improving them. The disadvantage when performing a risk assessment is that the accident experience and anticipated hazards that underpinned each rule are not recorded, and so it is very difficult to tell how safety-critical a particular rule might be for a particular installation.

1.4.2 IMO Legislation

The International Maritime Organization (IMO) is a specialised agency of the United Nations, which develops international conventions and codes for the promotion of safety at sea and the prevention of pollution. In order to establish common international standards, it works by consensus, and its regulations do not go into effect until they have been ratified by a sufficient number of maritime states. Each ratifying state must enact the regulations in its own domestic legislation (e.g the Merchant Shipping Act in the UK), and its own inspectors (e.g. the Maritime & Coastguard Agency in the UK) then enforce them. In the interim, IMO issues codes, which are widely used on a voluntary basis, although they are not legally enforceable.

The IMO Code for the Construction and Equipment of Mobile Offshore Drilling Units 1989 (MODU Code) is the main IMO instrument for mobile offshore installations. It recommends design criteria, construction standards and other safety measures for MODUs so as to minimise the risk to such units, to the personnel on board, and to the environment. Figure 1.1 illustrates some of the detailed requirements set out by the IODU Code.

Figure 1.1 Extract from IMO MODU Code



1.4.3 Classification Society Rules

Classification societies are independent organisations that issue rules for the safety of ships and offshore installations, performing on-going surveys and inspections to ensure that these rules are being followed. Their main purpose is to protect the ship and its cargo, and the rules apply primarily to the structural strength of the hull and the reliability of its essential machinery and equipment. They were originally set up by marine insurers to evaluate the quality of ships, but they have gradually transformed into certification organisations, with the task of ensuring that ships conform to classification rules and IMO regulations (Boisson 1999). The main classification societies active on the UKCS are Lloyd's Register, Det Norske Veritas, Bureau Veritas and American Bureau of Shipping.

As they have accumulated offshore experience, classification societies have introduced specific rules for individual installation types, such as column-stabilised units, self-elevating units, ship-shaped units (including floating production systems, floating storage units, drill ships, well stimulation/intervention vessels etc) and tension leg platforms. These rules are in general modifications of the ship rules, taking account of specific design requirements, such as the need to remain on location for extended periods, and in-service experience. However, there may be insufficient research or experience to ensure that the rules provide adequate protection against particular hazards, such as "green-water" and wave slamming on floating production systems (PAFA 2000).

Most traditional classification rules are detailed prescriptive requirements for specific types of equipment or designs that must be adopted, or functional requirements that must be attained, on all installations classed under the rules. This gives very clear instructions on how to design these aspects of the installation. It implies that the responsibility for safety in these areas rests mainly with the classification society, since the designer is simply required to satisfy the applicable rules. In general, such rules have been developed by expert judgement, responding to previous accident experience. They are only rarely based on risk assessment, and do not by themselves satisfy the requirement to perform a risk assessment.

In some areas, classification rules are relatively modern goal-setting requirements, notably for structural strength, the most complex of the areas addressed by classification. For example, Figure 1.2 illustrates the Lloyd's Register rules, which require a structural analysis of the individual installation under specified loading conditions, in order to demonstrate that it meets defined acceptance criteria for stress levels. Hence these rules in effect require a type of risk analysis, addressing certain specific hazards.

Figure 1.2 Example Rules on Structural Analysis
(Source: Lloyd's Register Rules and Regulations for the Classification of Mobile Offshore Structures)

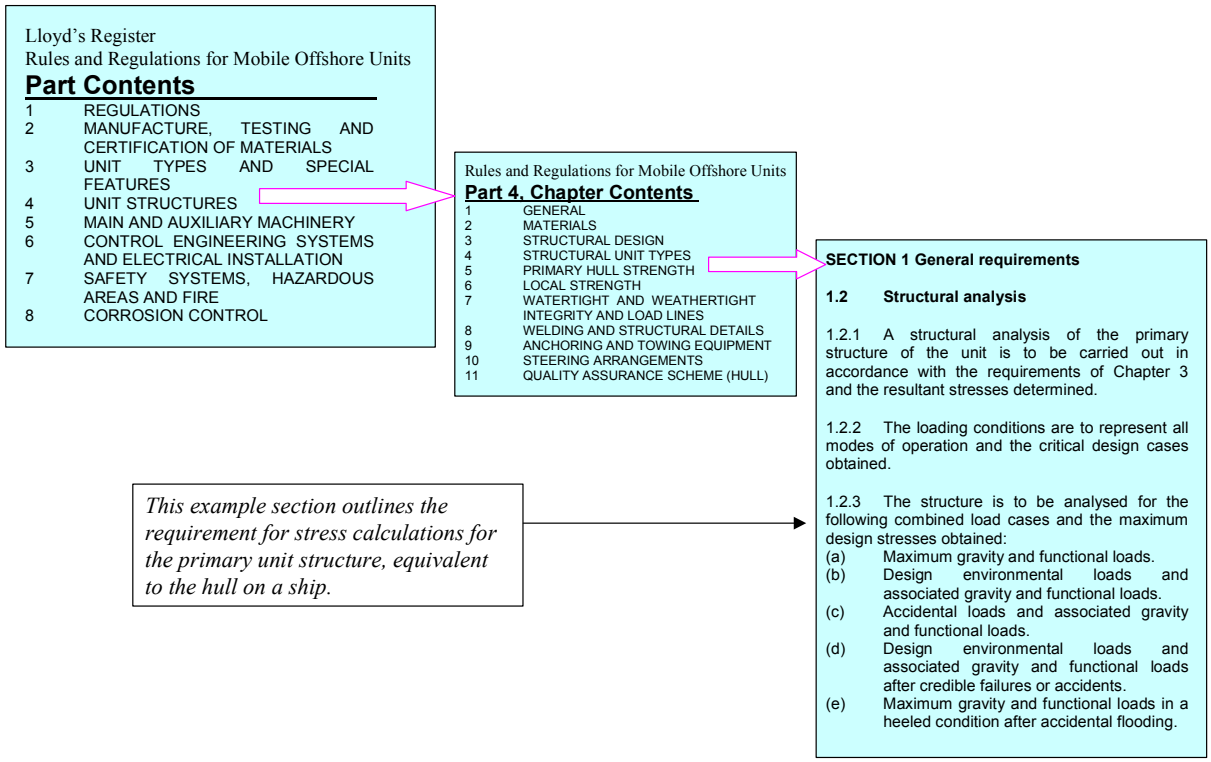


Figure 1.3 illustrates a more unusual instance of classification rules explicitly requiring a type of risk assessment. This is appropriate where the variety of possible design solutions make it impossible to anticipate all the hazards that might arise and specify safeguards against them. However, this type of rule is very unusual, as it is difficult to verify within the traditional scope of classification services.

Figure 1.3 Example Rules on Dynamic Positioning Systems
(Source: Det Norske Veritas Rules for Mobile Offshore Units)

600 Failure Mode and Effect Analysis (FMEA).

601 Documentation of the reliability and availability of the DP-system may be required in the form of a failure mode and effect analysis (FMEA).

602 The purpose of an FMEA is to give a description of the different failure modes of the equipment referred to in its functional task. Special attention is to be paid to the analysis of systems where an item may enter a number of failure modes and this may induce a number of different effects on the DP-system performance.

1.5 Risk Management and Decision-Making

1.5.1 HSE Tolerability of Risk Approach

HSE's views on decision-making on safety issues have most recently been explained in a "*Reducing Risks, Protecting People*" (HSE 1999a). This is at present a discussion document, subject to revision following comments.

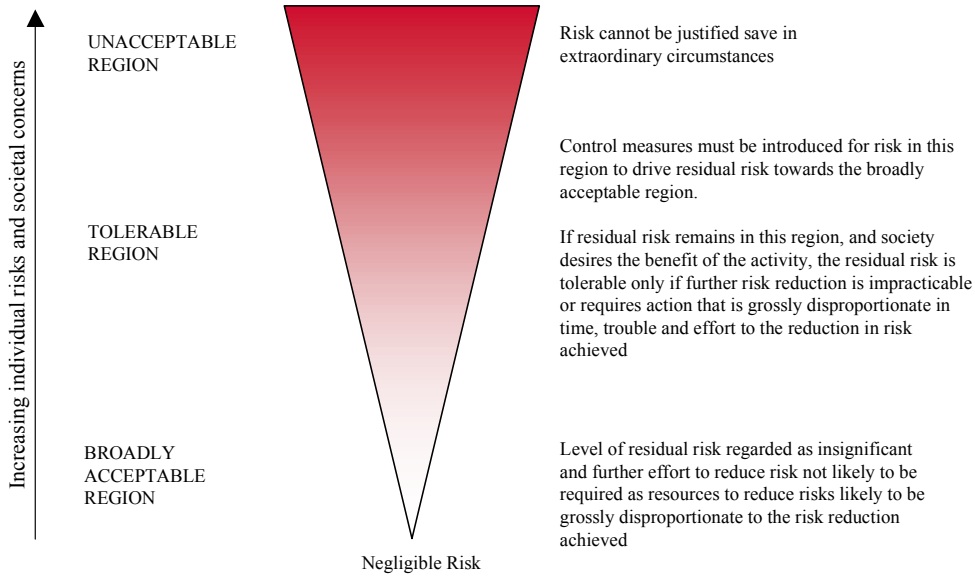
HSE's approach is based on a tolerability of risk (TOR) framework (Figure 1.4). It applies to risk in a broad sense, including not just the risks of harm (individual and societal risks), but also the perception of hazards and associated ethical and social considerations ("societal concerns"), such as aversion to large multiple-fatality accidents. It divides risk into 3 regions:

- Unacceptable - risks regarded as unacceptable except in extraordinary circumstances (such as wartime), whatever their benefits. Activities causing such risks would be prohibited, or would have to reduce the risks whatever the cost.

- Tolerable - risks that are tolerated in order to secure benefits. In this region, risks are kept as low as reasonably practicable (ALARP), by adopting reduction measures unless their burden (in terms of cost, effort or time) is grossly disproportionate to the reduction in risk that they achieve.

- Broadly acceptable - risks that most people regard as insignificant. Further action to reduce such risks is not normally required.

Figure 1.4 Tolerability of Risk Framework (HSE 1999a)

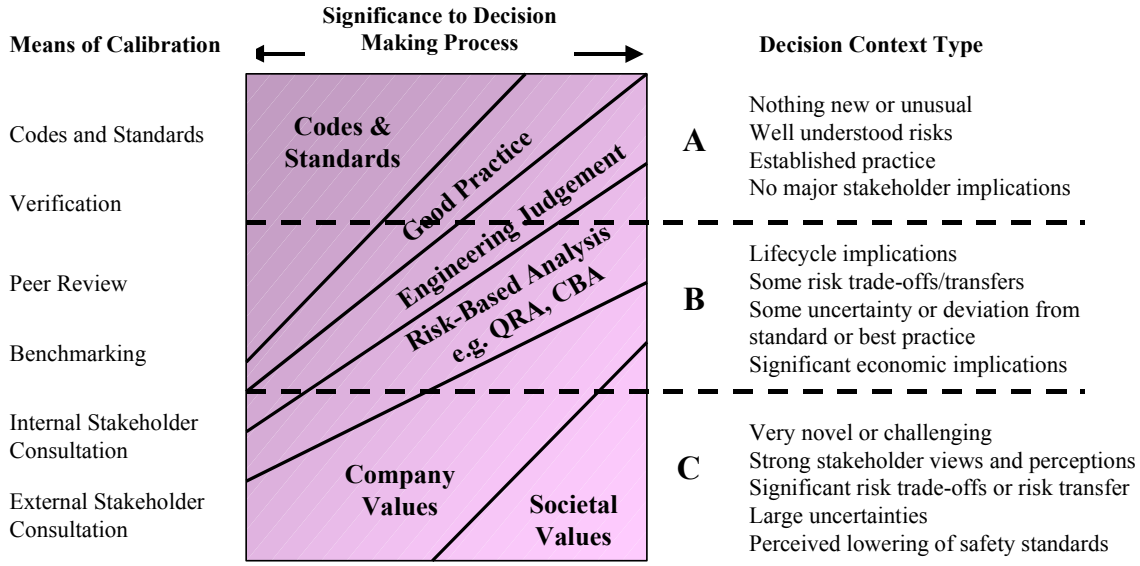


This approach has been adopted widely, and is appropriate for offshore installations. In order to apply it, the duty holder must first ensure that the risks are not unacceptable, and must then show that the risks are either ALARP or broadly acceptable. HSE has specified risk criteria (or "tolerability limits") to indicate the boundaries between the zones. Although these are intended to be guidelines, not rigid criteria to be complied with in all cases, in practice most offshore operators have adopted criteria based closely on them.

1.5.2 UKOOA Framework for Risk Related Decision Support

The UK offshore oil and gas industry has developed a framework to assist risk-related decision-making (UKOOA 1999), which helps decision-makers choose an appropriate basis for their decisions.

Figure 1.5 Risk-Related Decision Support Framework (UKOOA 1999)



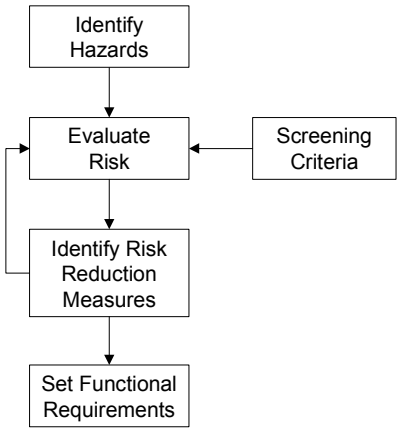
The framework (Figure I.5) takes the form of a spectrum of decision bases, ranging from those decisions dominated by purely engineering concerns to those where company and societal values are the most relevant factors. Down the right-hand edge of the framework are typical characteristics which indicate the decision context; these can be used to help the user determine the context for a specific decision. Once this level has been identified, reading horizontally across the framework shows the suggested balance of decision bases to be taken into account in the decision. Some means of calibrating or checking the decision basis are shown on the left-hand side of the framework (UKOOA 1999).

To relate the UKOOA framework to the current guide, "risk assessment" may be considered to consist of structured engineering judgement and risk-based analysis. This approach shows that risk assessment has a major input to Type B decisions, involving some uncertainty, deviation from standard practice, risk trade-offs etc. In Type A and C decisions, risk assessment is still relevant but is likely to be much less influential in reaching the final decision. IMO regulations and classification rules are representatives of "codes & standards", and are a major input to Type A decisions, with less influence on Type B and C.

1.5.3 ISO Offshore Risk Management Process

A draft International Standard 17776 (ISO 1999) on identification and assessment of hazardous events for offshore production installations gives a more conventional indication of how risk assessment fits into a wider risk management process (Figure 1.6).

Figure 1.6 The Process of Risk Management (ISO 1999)

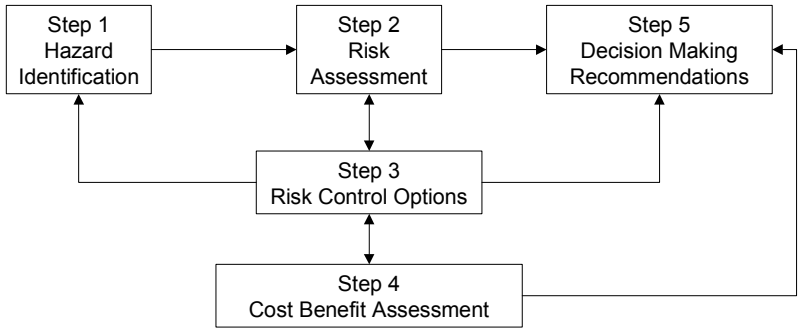


The first step of risk assessment is to identify the hazards that are present. Then the risks arising from them are evaluated either qualitatively or, if appropriate, quantitatively. Risk reducing measures are introduced if the risks exceed "screening criteria" (known in this guide as "risk evaluation criteria" - Section 3). Once the necessary measures have been identified, the functional requirements of these measures should be defined.

1.5.4 IMO Formal Safety Assessment

IMO is carrying out trial applications of formal safety assessment (FSA) as a proactive, transparent and systematic means of developing new safety regulations (IMO 1997). As defined by IMO, FSA consists of a 5-step process, involving hazard identification, risk assessment, development of risk control options, cost-benefit assessment, and making recommendations for decision-making (Figure 1.7). The purpose of FSA is to help develop risk-based regulations, and hence it should not be confused with risk assessment used in support of a safety case, although it uses many of the same techniques. FSA is applied to generic types of ship, and is seen as an alternative to a safety case approach, since it is widely believed that the shipping industry in not yet ready for the safety case approach.

Figure 1.7 Flowchart for Formal Safety Assessment (IMO 1997)



The importance of FSA for offshore installations is that in the future it may form a transparent risk-based justification for IMO regulations and classification society rules. However, at present such a basis does not exist.

1.6 Conclusions

Risk assessment approaches are increasingly commonly used for the assessment of major hazards and the demonstration that risks have been controlled to an ALARP standard. Attitudes have changed in the oil industry from an initial position of scepticism to good support for the simpler approaches, and for the clarity of focus this brings to controlling hazards, but with still some question as to the effectiveness of QRA.

The regulations applying to offshore operations in the UK, including HSWA, MHSWR and SCR, require operators to undertake risk assessment in order to identify appropriate measures to protect people against accidents, so far as is reasonably practicable. SCR includes a specific requirement for QRA, but this does not apply to marine hazards, i.e. hazards connected with the interface between the installation and the marine environment. Perhaps as a consequence, the risk assessments of marine hazards in the safety cases submitted to date have been less thorough than the treatment of hazards from fire and explosions.

The safety of offshore installations against marine hazards has traditionally relied on IMO legislation and classification society rules. These rules have been developed by expert judgement, responding to previous accident experience, and in general prescribe specific design solutions. They are only rarely based on risk assessment, and do not by themselves satisfy the requirement to perform a risk assessment.

Modern risk management approaches make clear that risk assessment has an important role to play in many risk-related decisions, particularly for decisions involving uncertainty, deviation from standard practice and risk trade-offs, for which marine regulations are less appropriate. The UKOOA decision support framework provides a suitable basis for such decision-making. The HSE tolerability of risk framework shows how risk assessment can contribute to such decisions.

2. RISK ASSESSMENT METHODOLOGIES

2.1 Choice of Approach

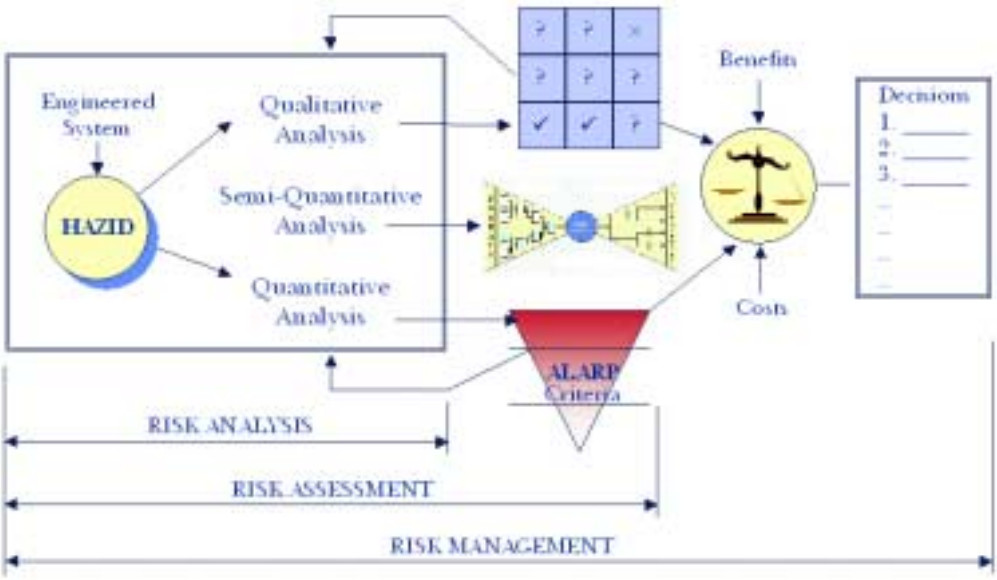
2.1.1 Definitions

The terminology for risk studies is:

- Risk analysis - the estimation of risk from the basic activity "as is".
- Risk assessment - a review as to acceptability of risk based on comparison with risk standards or criteria, and the trial of various risk reduction measures.
- Risk management - the process of selecting appropriate risk reduction measures and implementing them in the on-going management of the activity

These basic approaches are illustrated in Figure 2.1. The figure shows that hazard identification (HAZID) is an essential component of all three types of study.

Figure 2.1 Risk Assessment Approaches



2.1.2 Types of Risk Assessment

Risk assessment can be applied in approaches described as Qualitative, Semi-Quantitative and Quantitative, and the project manager needs to decide which is the right approach for the job. The basic aim is risk reduction and the key test is one of reasonable practicability.

In general, qualitative approaches are easiest to apply (least resource demands and least additional skill sets required) but provide the least degree of insight. Conversely quantitative approaches (QRA) are most demanding on resources and skill sets, but potentially deliver the most detailed understanding and provide the best basis if significant expenditure is involved. Semi-quantitative approaches lie in between these extremes.

As can be seen, the process allows project teams wide variety in approach, although all are in principle equivalent. Sections 2.3 to 2.5 provide some guidance as to the strengths of each approach and factors that would suggest one over the others

In broad terms the hazard identification technique selection can be quite separate from the subsequent risk assessment approach. Thus a coarse hazard identification can support both qualitative or semi-quantitative risk assessments, whereas a detailed hazard identification can support any level of risk assessment.

2.1.3 Selection of Approach

Given the different approaches to risk assessment and the many different specific methods involved, it is not always obvious which to select. Whilst there is no single correct approach for a specific activity, there are approaches that are more suitable than others, and a decision framework is helpful in the selection process.

It is not possible to create a simple flowchart, with Yes-No branches, to define a suitable approach to risk assessment. But there are broad factors that can be used to aid the selection of a suitable risk assessment approach. These key factors include:

- Lifecycle stage
- Major hazard potential
- Risk decision context – novelty / uncertainty / stakeholder concern (eg. UKOOA)

These are key drivers for several reasons. **Lifecycle** is a driver as the lifecycle stage implies greater or lesser flexibility to change design elements, the knowledge of specific design and operational details, and the availability of historical records. Lesser design or operational knowledge will limit the approach to risk assessment to coarser methods. **Major Hazard Potential** is relevant as the greater the potential exposure to total loss or multiple fatality, the less desirable it is to use only conventional rule-based approaches for decision-making. Finally the **Risk Decision Context** (see the UKOOA framework in Section 1.5.2) with higher elements of novelty, uncertainty or stakeholder concern will also push towards more thorough risk assessment.

Once these drivers are defined, it is then feasible to select amongst the wide range of methods for risk assessment. These include:

- Hazard identification tools
  - Judgement
  - FMEA – Failure Modes and Effects Analysis
  - SWIFT – Structured What-If Checklist Technique
  - HAZOP – Hazard and Operability Study

- Risk Assessment approaches
  - Rules based approaches: regulations, approved codes of practice, Class Rules
  - Engineering judgement
  - Qualitative risk assessment
  - Semi-quantitative risk assessment
  - Quantitative risk assessment
  - Value-based approaches

- Risk Assessment techniques
  - Qualitative (risk matrix)
  - Semi-Qualitative use of structured tools (fault trees, events trees) – Bow-Tie approach
  - Quantitative risk assessment (coarse and detailed levels)
  - Stakeholder consultations

- Hierarchy of Options approaches for risk reduction
  - Eliminate the hazard
  - Prevent the occurrence
  - Mitigate the consequences
  - Escape, Evacuation, Rescue and Recover

- Decision making
  - Level within organisation and tools (design team, senior management, judgement, cost benefit analysis)

Several worked examples appear in the Case Study Section.

2.1.4 Lifecycle Implications

Risk assessment should be an on-going process throughout the lifecycle of an installation, from feasibility study through to abandonment, as an integral part of its risk management. The different stages of the lifecycle offer different opportunities for risk assessment, and hence the approach may be different in each:

- **Feasibility studies and concept selection stage.** Before the concept design is fixed, any risk assessment must be relatively simple and broad-brush. However, they should be broad in scope, addressing the complete lifecycle. Suitable techniques include hazard review, SWIFT and risk matrix (see below), performed at a high level. Simple lifetime QRAs are possible, using the number of people exposed and generic FARs (see below). An example of this might be a comparison of FPSO and pipelines. Incorporation of inherent safety is easiest at this concept selection stage.

- **Concept or front-end design.** Many concept designs are based closely on previous designs, and similarly concept risk assessments are often modifications of similar studies on previous designs. This allows them to learn from previous experience at modest cost. Suitable techniques include SWIFT, event trees and bow tie (see below). Quantitative "concept safety evaluations" have been widely used at this stage. However, for standard concepts, such as jack-up drilling rigs, quantification of risks may contribute relatively little at this stage, whereas for unusual concepts it may be essential to evaluate major risk reduction measures.

- **Detailed design.** The detailed design phase provides sufficient information for specific risk assessments, using techniques such as HAZOP, SWIFT, FMEA, FTA, QRA and EERA, and is usually the main focus of risk assessment work, although the opportunity to influence the design rapidly diminishes as the design progresses. In this phase, the risk assessment is used as a check that safety levels are acceptable, to evaluate additional safety measures, and to advise on major procedural safeguards.

- **Operation.** Once the installation is in operation, practical experience provides a good basis to update key aspects of the design risk assessments, such as HAZOP, SWIFT, QRA and EERA as part of the on-going risk management of the installation. There may also be opportunities to eliminate much of the complexity of the risk assessment of the detailed design.

- **Abandonment.** The abandonment raises new issues of safety and environmental protection, which may not have been considered in earlier risk assessments. Suitable techniques include hazard review, SWIFT and event trees. The novel and politically sensitive nature of abandonment mean that societal values may be particularly important in the decision-making (see Section I.5.2).

The goal of "inherent safety" in design involves avoiding or limiting hazards at source rather than relying on add-on safety features or management procedures to control them (Mansfield, Poulter & Kletz, 1996). Measures to promote "inherently safer" design include minimising hazardous inventories, avoiding complex processes, minimising exposure of personnel, separation of hazardous areas from accommodation etc. Opportunities to incorporate inherent safety are greatest at the earliest stages of design, when the design is most flexible and the costs of changes are low. It might be expected that such measures would be identified automatically by the consideration of cost-effective risk reduction measures required for the ALARP demonstration. However, they are often overlooked until the design is fixed, and by then their cost-effectiveness may be greatly reduced. It is therefore important that the risk assessment should actively search for an inherently safer design.

2.2 Hazard Identification

2.2.1 Definitions

A **hazard** is defined as a situation with a potential for causing harm to human safety, the environment, property or business. It may be a physical situation (e.g. a shuttle tanker is a hazard because it may collide with the production installation), an activity (e.g. crane operations are a hazard because the load might drop) or a material (e.g. fuel oil is a hazard because it might catch fire). In practice, the term "hazard" is often used for the combination of a physical situation with particular circumstances that might lead to harm, e.g. a shuttle tanker collision, a dropped load or a fuel oil fire. The essence of a hazard is that it has a *potential* for causing harm, regardless of how likely or unlikely such an occurrence might be.

Hazard identification (HAZID) is the process of identifying hazards, which forms the essential first step of a risk assessment. There are two possible purposes in identifying hazards:

- To obtain a list of hazards for subsequent evaluation using other risk assessment techniques. This is sometimes known as "failure case selection".

- To perform a qualitative evaluation of the significance of the hazards and the measures for reducing the risks from them. This is sometimes known as "hazard assessment".

The same techniques can be used for both, but the emphasis and conclusions will be different.

2.2.2 General Approach

Hazard identification is usually a qualitative exercise based primarily on expert judgement. Most HAZID techniques involve a group of experts, since few individuals have expertise on all hazards, and group interactions are more likely to stimulate consideration of hazards that even well-informed individuals might overlook.

Hazards are diverse, and many different methods are available for hazard identification. While some methods have become standard for particular applications (e.g. FMEA for ballast system failures), it is not necessary or desirable to specify which approach should be adopted in particular cases. The methodology should be chosen by the HAZID leader to meet the objectives as efficiently as possible given the available information and expertise. It may be a standard technique, following an established protocol, a modification of one, or a combination of several.

The following features are essential in any HAZID:

- The HAZID should be creative, so as to encourage identification of hazards not previously considered.
- It should use a structured approach, in order to obtain comprehensive coverage of relevant hazards without skipping less obvious problem areas.
- It should make use of accident experience, where available, so as to capture the lessons from previous accidents.
- The scope of the HAZID should be clearly defined, so as make clear which hazards should be included and which have been excluded.

For group-based HAZIDs (such as HAZOP and SWIFT), the following are also essential:

- They should draw on the expertise of people from different disciplines and backgrounds, including practical experience in the activity under study where possible.
- The leader should be independent of the team (i.e. an external consultant, a risk assessment specialist or an experienced leader from another department), and has the responsibility of preventing "group think" suppressing creative ideas.
- Conclusions and recommendations should be discussed and documented during the group session, so that they represent the views of the group rather than an individual.

CCPS (1992) gives detailed descriptions of the various HAZID techniques used in the process industry. CMPT (1999) summarises HAZID techniques that are available for offshore installations. Ambion (1997) summarises the HAZID techniques that are actually used in offshore safety cases. The following sections give a brief outline of the main techniques suitable for marine hazards on offshore installations.

2.2.3 Hazard Review

A hazard review (also known as a hazard survey or safety review) is a mainly intuitive, qualitative review of an installation to identify the hazards that are present and to gain qualitative understanding of their significance. It is one of the most commonly used HAZID techniques for MODUs (Ambion 1997).

A hazard review should address issues such as:

- Previous safety assessments - What is other people's assessment of the hazards? For many types of installation, previous HAZIDs and risk assessments may be sufficient give an outline appreciation of the hazards.

- Survey of previous accidents - Have similar installations suffered accidents in the past? This is one of the easiest (and most frequently overlooked) ways of identifying hazards. It provides a simple intuitive warning of the types of accidents that may occur, although it cannot be comprehensive, especially for new types of installation. Nevertheless, this is a very important first step, and ensures that the lessons from previous accidents are not overlooked. Some regulations in other industries require operators to provide 5-year accident histories for their companies, to underpin the risk assessment.

- Previous experience - If the installation already exists, has it suffered any near-misses or operating problems? Operating staff are likely to have ideas on potential accidents based on their own experience. Visual inspection of the installation by may suggest hazards, and this can be conducted as part of a safety audit.

- Hazardous materials data - What hazardous materials will be handled on the installation? The intrinsic hazards of common materials handled offshore such as oil, gas, condensate, H_2S, diesel oil etc have a major impact on the risks of the installation as a whole.

- Guidelines and Codes of Practice - Does the installation conform to good engineering practice and classification rules? Codes of practice for design, operation and certification of offshore installations include lessons learned from previous accidents. Complying with these documents therefore ensures a common level of safety for a standard installation. However, because they are written as guides for design, operation or certification, these documents usually do not specify the hazards that each measure is intended to control, and therefore are difficult to use for identifying hazards.

Good access to information is critical for a hazard survey. Public-domain information sources are reviewed by CMPT (1999).

The strengths of a hazard review are:

- It makes use of existing experience from a wide range of sources.
- It can be performed by a single analyst at low cost.
- It requires minimal information about the installation, and so is suitable for concept design.

Its weaknesses are:

- Its lack of structure makes it difficult to audit.
- It is limited to previous experience, and thus has limited value for novel installations.
- It does not produce a list of failure cases for a QRA.

Overall, this type of hazard review is an appropriate starting point for a hazard identification process, but is insufficient on its own except for simple studies of concepts that have been studied previously in detail.

2.2.4 Hazard Checklists

A hazard checklist is a written list of questions intended to prompt consideration of a full range of safety issues. They are used to check a design and confirm that good practice is incorporated

The American Petroleum Institute has developed a range of checklists for offshore activities, mainly addressing process and drilling risks (eg. API 14C, 14E, 14F, 14G, 14J) and a safety and environment management checklist in API RP75. These 14 series checklists are prescriptive in style and very detailed and are not focused on marine issues. The nearest marine equivalent might be instructions to surveyors in marine classification surveys.

Other types of checklists are widely used in offshore risk assessments. Generic hazard checklists consist of standard lists of hazards, or hazard categories. Although superficially similar to API-type checklists, their focus is more to assist the risk assessment than to check the design. They can be created from previous risk assessments, and provide an efficient means of generating a list of standard hazards suitable for HAZID of concept designs.

Table 2.1 gives an example generic checklist of major accident hazards for offshore installations. Excluding blowouts, riser/pipeline leaks, process leaks, transport accidents and personal accidents gives a list of marine major accident hazards. This is applicable to standard offshore installations, and may be incomplete for unusual installations.

Table 2.2 gives a generic list of keywords that can be used to prompt consideration of such hazards on any type of offshore installation. It includes some example hazards, not intended to be comprehensive.

A further type of checklist is used in SWIFT studies (see below). Checklists within SWIFT are more open-ended and designed to ensure the HAZID team addresses key areas, but are not so prescriptive or detailed that the team is inhibited from brainstorming novel failures.

Table 2.1 Example Generic Hazard Checklist (CMPT 1999)

Blowouts
- Blowout in drilling
- Blowout in completion
- Blowout in production (including wirelining etc)
- Blowout during workover
- Blowout during abandonment
- Underground blowout

Also covered under blowouts are:
- Well control incidents (less severe than blowouts)
- Fires in drilling system (e.g. mud pits, shale shaker etc)

Riser/pipeline leaks - leaks of gas and/or oil from:
- Import flow-lines
- Export risers
- Sub-sea pipelines
- Sub-sea wellhead manifolds

Process leaks - leaks of gas and/or oil from:
- Wellhead equipment
- Separators and other process equipment
- Compressors and other gas treatment equipment
- Process pipes, flanges, valves, pumps etc
- Topsides flowlines
- Pig launchers/receivers
- Flare/vent system
- Storage tanks
- Loading/unloading system
- Turret swivel system

Non-process fires
- Fuel gas fires
- Electrical fires
- Accommodation fires
- Methanol/diesel/aviation fuel fires
- Generator/turbine fires
- Heating system fires
- Machinery fires
- Workshop fires

Non-process spills
- Chemical spills
- Methanol/diesel/aviation fuel spills
- Bottled gas leaks
- Radioactive material releases
- Accidental explosive detonation

Marine collisions - impacts from:
- Supply vessels
- Stand-by vessels
- Other support vessels (diving vessels, barges etc)
- Passing merchant vessels
- Fishing vessels
- Naval vessels (including submarines)
- Flotel
- Drilling rig

Continued…

- Drilling support vessel (jack-up or barge)
- Offshore loading tankers
- Drifting offshore vessels (semi-subs, barges, storage vessels)
- Icebergs

For each vessel category, different speeds of events, such as powered and drifting may be separated.

Structural events
- Structural failure due to fatigue, design error, subsidence etc
- Extreme weather
- Earthquakes
- Foundation failure (including punch-through)
- Bridge collapse
- Derrick collapse
- Crane collapse
- Mast collapse
- Disintegration of rotating equipment

Marine events
- Anchor loss/dragging (including winch failure)
- Capsize (due to ballast error or extreme weather)
- Incorrect weight distribution (due to ballast or cargo shift)
- Icing
- Collision in transit
- Grounding in transit
- Lost tow in transit

Dropped objects - objects dropped during:
- Construction
- Crane operations
- Cargo transfer
- Drilling
- Rigging-up derricks

Transport accidents - involving crew-change or in-field transfers
- Helicopter crash into sea/platform/ashore
- Fire during helicopter refuelling
- Aircraft crash on platform (inc military)
- Capsize of crew boats during transfer
- Personal accident during transfer to boat
- Crash of fixed-wing aircraft during staged transfer offshore
- Road traffic accident during mobilisation

Personal (or occupational) accidents

Construction accidents - accidents occurring during:
- Construction onshore
- Marine installation
- Construction offshore
- Hook-up & commissioning
- Pipe laying

Attendant vessel accidents

Diving accidents

Table 2.2 Example Generic Keyword Checklist (Ambion 1997)

Key Word used in HAZID	Example of Hazard
Direct fire	Ignited blow-out Ignited process fire Fire in paint store
Loss of breathable atmosphere	Smoke ingress from HVAC Asphyxiation
Direct toxic	Toxic gas release
Explosion overpressure	Explosion from process gas leak
Dropped objects	Dropped load from crane Swinging load hit to process
Vehicle collision	Helicopter crash Ship collision to legs
Structural collapse	Crane collapse Leg failure in design load Extreme weather
Mechanical failure	Gas turbine rotor blade failure
Electrocution	Occupation accident
Pressure/loss of containment	Air receiver failure Unignited process vessel failure
Water/drowning	Deluge in process Man overboard
Direct chemical	Drilling chemical leak Lab chemical exposure
Occupational accidents	Trips, falls
Hydrocarbon leak general	Diesel tank failure Process leak

The strengths of a generic hazard checklist are:

- It makes use of experience from previous risk assessments.
- It helps to prevent past accidents from recurring
- It promotes standard hazard categories, and facilitates comparison between HAZIDs
- It can be prepared by a single analyst at low cost
- It requires minimal information about the installation, and so is suitable for concept design

Its weaknesses are:

- It is limited to previous experience, and thus may not anticipate hazards in novel designs or novel accidents from existing designs
- It does not encourage intuitive / brainstorming thinking, and so gives less insight into the nature of the hazards on the installation.

Overall, a generic hazard checklist is useful for most risk assessments, but should not be the only HAZID method, except for standard installations whose hazards have been studied in more detail elsewhere.

2.2.5 HAZOP

A hazard and operability (HAZOP) study is a method of identifying hazards that might affect safety and operability based on the use of guidewords. A team of experts in different aspects of the installation, under the guidance of an independent HAZOP leader, systematically considers each sub-system of the process in turn, typically referring to process and instrumentation diagrams (P&IDs). They use a standard list of guidewords to prompt them to identify deviations from design intent. For each credible deviation, they consider possible causes and consequences, and whether additional safeguards should be recommended. They record their conclusions in a standard format during the sessions.

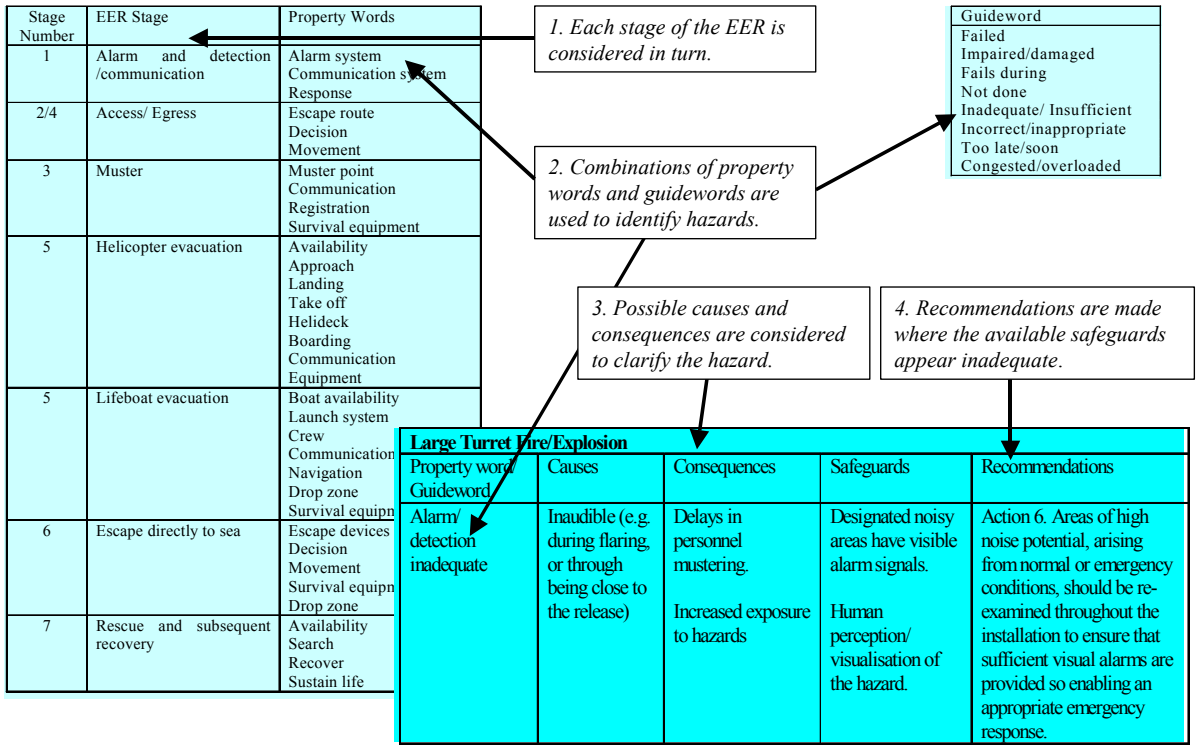
Guidance on HAZOP is given by CIA (1977), CCPS (1992) and Kletz (1992). Although these refer to onshore process industries, HAZOP of offshore process equipment is essentially the same. HAZOP is one of the most commonly used HAZID techniques in the offshore industry (Ambion 1997). However, its classic form is intended for continuous chemical processes as expressed in P&IDs and is not efficient for marine hazards.

The HAZOP technique can be modified to apply to non-process hazards, but there is a danger that changes to the guidewords will result in some hazards being overlooked. Hence, standard modifications are preferred to ad-hoc variations. These include:

- Drillers' HAZOP, for HAZID of offshore drilling operations (Comer et al 1986).
- EER HAZOP, for HAZID of evacuation, escape and rescue (RM Consultants 1995).

Figure 2.2 shows an example extract from an EER HAZOP, covering a single hazard in a single evacuation scenario.

Figure 2.2 Example EER HAZOP (Boyle & Smith 2000)



The strengths of HAZOP are:

- It is widely-used and its advantages and disadvantages are well-understood
- It uses the experience of operating personnel as part of the team
- It is systematic and comprehensive, and should identify all hazardous process deviations.
- It is effective for both technical faults and human errors.
- It recognises existing safeguards and develops recommendations for additional ones.
- The team approach is particularly appropriate to marine hazards in offshore operations requiring the interaction of several disciplines or organisations.

Its weaknesses are:

- Its success depends on the facilitation of the leader and the knowledge of the team.
- It is optimised for process hazards, and needs modification to cover other types of hazards.
- It requires development of procedural descriptions which are often not available in appropriate detail. However, the existence of these documents may benefit the operation.
- Documentation is lengthy (for complete recording).

Overall, HAZOP has become a standard tool for process plant design offshore, and is procedural HAZOP is widely used for simultaneous operation sand assessment of evacuation systems. However, other HAZID techniques may be more efficient for many marine hazards.

2.2.6 FMECA

A failure modes, effects and criticality analysis (FMECA) (or its simpler form, FMEA) is a systematic method of identifying the failure modes of a mechanical or electrical system. Typically, one or two analysts consider each component in turn, subjectively evaluating the effects and criticality (i.e. importance) of a failure there.

The analysis uses a form that begins with a systematic list of all components in the system, and typically includes:

- Component name.
- Function of component.
- Possible failure modes.
- Causes of failure.
- How failures are detected.
- Effects of failure on primary system function.
- Effects of failure on other components.
- Necessary preventative/repair action.
- Rating of frequency of failure.
- Rating of severity (i.e. consequence) of failure.

Failures are rated as critical if they have high frequency or severity ratings. In these cases, special protection measures may be considered.

An example extract from an FMEA of a ballast system is shown in Figure 2.3. The column headings are based on the US Military Standard Mli Std 1629A, but with modifications to suit the particular application. For example, the failure mode and cause columns are combined. The criticality of each failure is ranked as minor, incipient, degraded or critical.

Figure 2.3 Example Extract from an FMEA Work Sheet

Filling ballast tanks under gravity							
Ref.	**System /Equip. Failure**	**Cause**	**Effect**	**Detection**	**Mitigation-Compensation-System Response-Safeguards**	**Overall assessment**	**Overall criticality**
1BF	Sea Chest	1. Blocked	Tanks do not fill. Reduced stability, change of heel/trim increased hull stresses	* Valve position indicators. * Ballast tank level radar/sounding system. * If severe, angle of heel/trim.	i) Clean chest with steam. ii) Redundancy 3 other sea chests	In a worst case where failure was not acted upon quickly then a degraded state could arise where the ballasting operation of several tanks could be affected	D
1BF	Sea Chest	2. Loss of sea chest grid integrity.	Ingress of foreign bodies possible blockage of control valves and suction piping. Tanks do not fill. Build up of debris in system. Reduced stability, change of heel/trim increased hull stresses	* Valve position indicators. * Ballast tank level radar/sounding system. * If severe, angle of heel/trim.	i) Clean chest with steam. ii) Redundancy 3 other sea chests	In a worst case where failure was not acted upon quickly then a degraded state could arise where the ballasting operation of several tanks could be affected	D
2BF	Sea Chest	1. Partial Blockage	Reduced filling rate.	* Valve position indicator. * Ballast tank level radar/sounding system.	i) Clean chest with steam ii) Redundancy 3 other sea chests	Overall effect considered incipient due to detection ability and redundancy	I
3BF	Sea Chest	1. Leak at sea chest	Loss of ballast control in affected tank. Change of heel/trim	* Valve position indicator. * Ballast tank level radar/sounding system.	i) Continuously pumped to maintain correct level. ii) Isolate with sea chest blanks. iii) Equalises to exterior sea height in affected tank.	Loss of control in a tank is considered as degraded	D

The strengths of FMECA are:

- It is widely-used and well-understood
- It can be performed by a single analyst
- It is systematic and comprehensive, and should identify hazards with an electrical or mechanical basis
- It identifies safety-critical equipment where a single failure would be critical for the system

Its weaknesses are:

- Its benefit depends on the experience of the analyst.
- It requires a hierarchical system drawing as the basis for the analysis, which the analyst usually has to develop before the analysis can start.
- It is optimised for mechanical and electrical equipment, and does not apply to procedures or process equipment.
- It is difficult for it to cover multiple failures and human errors.
- It does not produce a simple list of failure cases.

Overall, FMECA is useful for safety-critical mechanical and electrical equipment, notably MODU ballast systems, but should not be the only HAZID method. Most accidents have a significant human contribution, and FMECA is not well suited to identifying these. As FMECA can be conducted at various levels, it is important to decide before commencing what level will be adopted as otherwise some areas may be examined in great detail while

others are examined at the system level without examining the components. If conducted at too deep a level, FMECA can be time consuming and tedious, but it leads to great understanding of the system.

2.2.7 SWIFT

The structured what-if checklist (SWIFT) technique is a method of identifying hazards based on the use of brainstorming. SWIFT is a more structured form of "What-if analysis" (CCPS 1992), but may be seen as a less rigorous and quicker alternative to HAZOP.

Like a HAZOP, SWIFT uses a team familiar with the installation, under the guidance of a specialist in the SWIFT technique. The main differences compared to a HAZOP are:

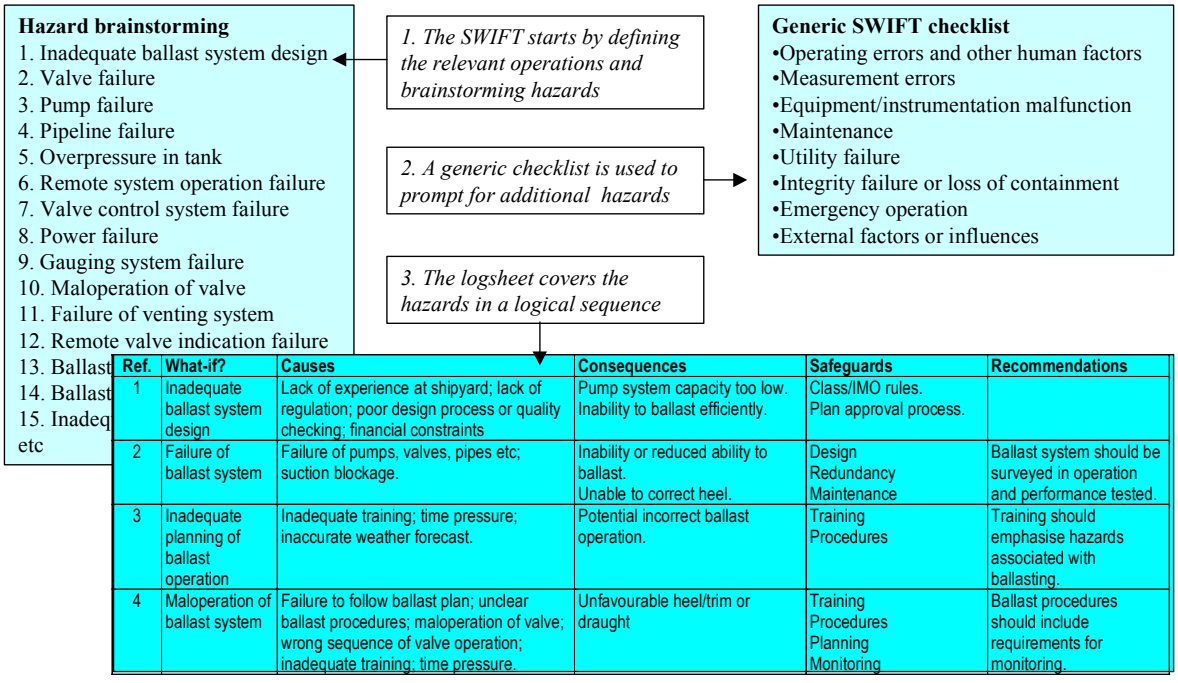
- The discussion proceeds systematically through the installation's modules or operations at the level of systems or procedures, rather than individual items or tasks.

- The method relies on brainstorming (i.e. creative thinking) and checklists to identify hazards, instead of a formal list of guidewords.

The discussions may begin with the words "What if", but other forms of initiating question may be "How could", "Is it possible" etc. It may be appropriate to pose all the questions in a brain-storming manner before trying to answer them.

Conclusions on each What-if are recorded in a standard format. An example worksheet is shown in Figure 2.4. This covers part of a ballast operation and illustrates how the SWIFT tends to cover high-level issues and human factors, in contrast to the FMEA in Figure 2.3.

Figure 2.4 Example SWIFT of Ballast System



Ref.	What-if?	Causes	Consequences	Safeguards	Recommendations
1	Inadequate ballast system design	Lack of experience at shipyard; lack of regulation; poor design process or quality checking; financial constraints	Pump system capacity too low. Inability to ballast efficiently.	Class/IMO rules. Plan approval process.	
2	Failure of ballast system	Failure of pumps, valves, pipes etc; suction blockage.	Inability or reduced ability to ballast. Unable to correct heel.	Design Redundancy Maintenance	Ballast system should be surveyed in operation and performance tested.
3	Inadequate planning of ballast operation	Inadequate training; time pressure; inaccurate weather forecast.	Potential incorrect ballast operation.	Training Procedures	Training should emphasise hazards associated with ballasting.
4	Maloperation of ballast system	Failure to follow ballast plan; unclear ballast procedures; maloperation of valve; wrong sequence of valve operation; inadequate training; time pressure.	Unfavourable heel/trim or draught	Training Procedures Planning Monitoring	Ballast procedures should include requirements for monitoring.

The strengths of SWIFT are:

- It is very flexible, and applicable to any type of installation, operation or process, at any stage of the lifecycle.
- It uses the experience of operating personnel as part of the team.
- It is quick, because it avoids repetitive consideration of deviations.

Its weaknesses are:

- As it works at system level, some hazards may be omitted, and it is difficult to audit.
- Adequate preparation of a checklist in advance is critical for the quality of the review.
- Its benefit depends on the experience of the leader and the knowledge of the team.

SWIFT/What-if analysis is rarely used offshore, but appears appropriate for many non-process activities.

2.2.8 Influence Diagrams

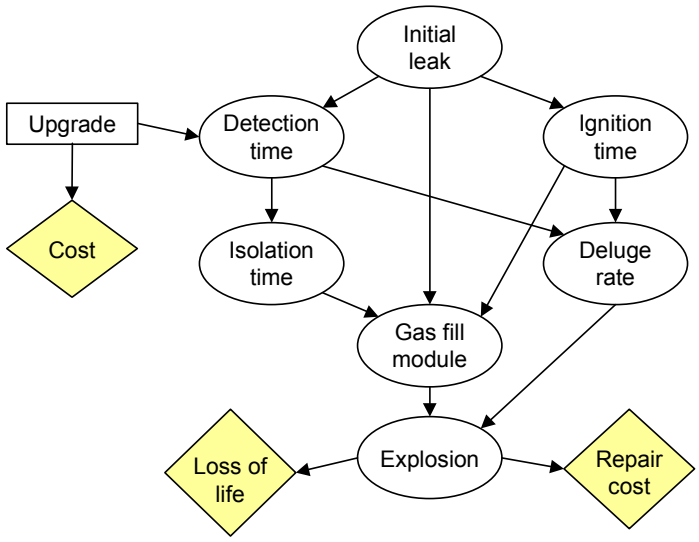
Influence diagrams are models for decision-making under uncertainty, developed in the field of decision analysis (Howard & Matheson 1980). An influence diagram is a graphical representation of the probabilistic dependence between the various factors that could influence the outcome of an event. The technique has been used in human reliability assessment (Humphreys 1995) and decision-making on explosion protection offshore (Bolsover & Wheeler 1999). Figure 2.5 shows a simple example

Figure 2.5 Example Influence Diagram for explosions

This influence diagram helps evaluate the decision whether to upgrade a gas detection system.

The diagram shows all the important issues, and uses arrows to represent how the issues influence each other. The ellipses represent issues that have some uncertainty (chance nodes). The rectangle represents the decision, and the diamonds represent associated costs and benefits (utilities).

Probability distributions (not shown here) can be assigned to the chance nodes and used to evaluate the expected benefits



Although they are not commonly used in hazard identification, influence diagrams have the potential to enhance the presentation of hazards identified using the techniques above, and may be an alternative to fault trees for this purpose.

2.2.9 Integrating HAZID in the Risk Assessment

Many hazard identification techniques are suitable not only for *identification* of hazards, but also for qualitative *evaluation* of their significance and consideration of risk reduction measures. In other works, they provide the basis for a complete qualitative risk assessment. Group based HAZIDs often provide great benefits for the participants and useful lists of recommendations, but their documentation can be difficult to understand for others who were not involved in the HAZID session. As a result, they are not always successfully integrated into ongoing safety management activities, which may result in hazards being forgotten, or the significance of safety measures being unclear.

The link between HAZIDs and quantitative risk assessments is provided by failure cases, which should in principle be developed from the HAZID (CMPT 1999). HAZIDs in later stages of the lifecycle should review the modelling of the failure cases in the QRA.

2.2.10 Integrating HAZID in Safety Management

The link between HAZIDs and ongoing safety management is typically provided by a hazard register. A hazard register records all the hazards that have been identified by the various HAZID techniques, showing representative causes, consequences and safeguards for each. Figure 2.6 shows part of a typical hazard register.

Figure 2.6 Example Hazard Register Extract

HAZARD CATEGORY	SYSTEM OR AREA	FAILURE CASE	CAUSE	EFFECTS	SAFEGUARDS	MAJOR ACCIDENT POTENTIAL	QRA EVENT ID
Blowout	Wireline	Well fluid release on main deck	Loss of well control during wireline	Fire, explosion, equipment damage, pollution	Wireline procedures, BOP	Yes	B009
Blowout	Production	Well fluid release in wellhead	Leak upstream of master valve	Fire, explosion, equipment damage, pollution	DHSV	Yes	B010
Process leak	Flowlines (3 off, WV to NRV)	Well fluid release in wellhead	Corrosion, human error, impact etc	Fire, explosion, escalation	ESD, fire/gas detection, open construction	Yes	P001

PFEER has promoted a movement towards a register of safeguards rather than hazards, since these have more specific management requirements. The HAZID techniques described above are well suited to identifying safeguards, especially safety-critical ones, as well as hazards.

2.3 Qualitative Methods

2.3.1 5 Steps

The booklet “5 Steps to Risk Assessment” (HSE 1998c) describes simple methods to document and evaluate risks, suitable for all employers and self-employed people. This requires a basic level of risk-based judgement, suitable for relatively minor hazards. These approaches may be appropriate for occupational risks in marine activities, but fall short of the analysis necessary to deal with major hazard risks.

2.3.2 Hazard Assessment

Some of the hazard identification techniques described in Section 2.2 are suitable for a qualitative evaluation of the significance of the hazards and the measures for reducing the risks from them. For example, FMECA includes a systematic evaluation of the criticality of each hazard. This is sometimes known as "hazard assessment", and is in effect a qualitative risk assessment. However, most HAZID techniques are not optimised for this, and normally require extension to use a more formalised technique such as risk matrices.

2.3.3 Risk Matrix Methods

Risk matrices provide a traceable framework for explicit consideration of the frequency and consequences of hazards. This may be used to rank them in order of significance, screen out insignificant ones, or evaluate the need for risk reduction of each hazard.

A risk matrix uses a matrix dividing the dimensions of frequency (also known as likelihood or probability) and consequence (or severity) into typically 3 to 6 categories. There is little standardisation in matters such as the size of the matrix, the labelling of the axes etc. To illustrate this, three different risk matrix approaches are presented below.

In each case, a list of hazards is generated by a structured HAZID technique, and each hazard is allocated to a frequency and consequence category according to qualitative criteria. The risk matrix then gives some form of evaluation or ranking of the risk from that particular hazard.

Sometimes risk matrices use quantitative definitions of the frequency and consequence categories. They may also use numerical indices of frequency and consequence (e.g. 1 to 5) and then add the frequency and consequence pairs to rank the risks of each hazard or each box on the risk matrix. In the terms of this guide, this does not constitute quantification (semi or full) and the technique is still classed as qualitative.

2.3.4 Defence Standard Matrix

A risk matrix that has been applied to marine activities derives from Defence Standard 00-56 "Safety Management Requirements For Defence Systems Part 1: Requirements" (1996). This sets out a 6 x 4 risk matrix based on frequency and consequence definitions as follows. A more detailed version is also provided in Part 2 of the standard, which applies more to reliability of technical systems.

The severity categories are defined as:

CATEGORY	DEFINITION
Catastrophic	Multiple deaths
Critical	A single death; and/or multiple severe injuries or severe occupational illnesses
Marginal	A single severe injury or occupational illness; and/or multiple minor injuries or minor occupational illness
Negligible	At most a single minor injury or minor occupational illness

The frequency categories are defined as:

ACCIDENT FREQUENCY	OCCURRENCE (During operational life considering all instances of the system)
Frequent	Likely to be continually experienced
Probable	Likely to occur often
Occasional	Likely to occur several times
Remote	Likely to occur some time
Improbable	Unlikely, but may exceptionally occur
Incredible	Extremely unlikely that the event will occur at all, given the assumptions recorded about the domain and the system

There are four decision classes:

RISK CLASS	INTERPRETATION
A	Intolerable
B	Undesirable and shall only be accepted when risk reduction is impracticable
C	Tolerable with the endorsement of the Project Safety Review Committee
D	Tolerable with the endorsement of the normal project reviews

The actual risk matrix (with the decision classes shown) is as follows:

	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	C	D	D	D

2.3.5 ISO Risk Matrix

An alternative, more up-to-date approach is given in the draft international standard 17776 (ISO 1999). This provides a 5 x 5 risk matrix with consequence and likelihood categories that are easier for many people to interpret (Figure 2.7).

The ISO 17776 matrix uses 4 types of consequence category: people, assets, environment and reputation reflecting current good practice in integrating safety and environmental risk decision making. The inclusion of asset and reputation risk is more for corporate well-being, but is useful as it makes the risk matrix central to the total risk decision process used by companies.

The ISO risk matrix uses more factual likelihood terminology (“has occurred in operating company”) instead of more general statements (“remote – likely to occur some time”). Whilst this makes it easier to apply, it also highlights the difficulty of these approaches for novel technology, with no operational reliability statistics.

Figure 2.7 ISO 17776 Risk Matrix

CONSEQUENCE					INCREASING PROBABILITY				
Severity Rating	People	Assets	Environ-ment	Reputation	A	B	C	D	E
					Rarely occurred in E&P industry	Happened several times per year in industry	Has occurred in operating company	Happened several times per year in operating company	Happened several times per year in location
0	Zero injury	Zero damage	Zero effect	Zero impact	Manage for continued improvement				
1	Slight injury	Slight damage	Slight effect	Slight impact					
2	Minor injury	Minor damage	Minor effect	Limited impact					
3	Major injury	Local damage	Local effect	Considerable impact					
4	Single fatality	Major damage	Major effect	Major national impact	Incorporate risk reducing measures				
5	Multiple fatalities	Extensive damage	Massive effect	Major international impact			Intolerable		

2.3.6 Risk Ranking Matrix

A risk matrix has been proposed for a revision of the IMO Guidelines on FSA (IMO 1997) to assist with hazard ranking. It uses a 7 x 4 matrix, reflecting the greater potential variation for frequencies than for consequences.

The severity index (SI) is defined as:

SI	SEVERITY	EFFECTS ON HUMAN SAFETY	EFFECTS ON SHIP	S (fatalities)
1	Minor	Single or minor injuries	Local equipment damage	0.01
2	Significant	Multiple or severe injuries	Non-severe ship damage	0.1
3	Severe	Single fatality or multiple severe injuries	Severe casualty	1
4	Catastrophic	Multiple fatalities	Total loss	10

The frequency index (FI) is defined as:

FI	FREQUENCY	DEFINITION	F (per ship year)
7	Frequent	Likely to occur once per month on one ship	10
5	Reasonably probable	Likely to occur once per year in a fleet of 10 ships, i.e. likely to occur several times during a ship's life	0.1
3	Remote	Likely to occur once per year in a fleet of 1000 of ships, i.e. 10% chance of occurring in the life of 4 similar ships	10^{-3}
1	Extremely remote	Likely to occur once in 100 years in a fleet of 1000 ships, i.e. 1% chance of occurring in the life of 40 similar ships	10^{-5}

Intermediate indices may be chosen if appropriate. Non-integer values may be used if more specific data is available.

If risk is represented by the product frequency x consequence, then an index of log(risk) can be obtained by adding the frequency and severity indices. This gives a risk index (RI) defined as:

$$RI = FI + SI$$

E.g. An event rated "remote" (FI=3) with severity "moderate" (SI=2) would have RI=5

The risk matrix is as follows (risk indices in bold):

		SEVERITY (SI)			
		1	2	3	4
FI	FREQUENCY	Minor	Moderate	Serious	Catastrophic
7	Frequent	**8**	**9**	**10**	**11**
6		**7**	**8**	**9**	**10**
5	Reasonably probable	**6**	**7**	**8**	**9**
4		**5**	**6**	**7**	**8**
3	Remote	**4**	**5**	**6**	**7**
2		**3**	**4**	**5**	**6**
1	Extremely remote	**2**	**3**	**4**	**5**

The risk index may be used to rank the hazards in order of priority for risk reduction effort. In general, risk reduction options affecting hazards with higher RI are considered most desirable.

2.3.7 Strengths and Weaknesses

The strengths of the risk matrix approach are:

- It is easy to apply and requires few specialist skills, and for this reason it is attractive to many project teams.
- It allows risks to people, property, environment and business to be treated consistently (using the ISO 17776 approach).
- It allows hazards to be ranked in priority order for risk reduction effort.

However, there are several problems with this approach, which are less apparent:

- Many judgements are required on likelihood and consequence and unless properly recorded the basis for risk decisions will be lost.
- The judgements must be consistent among different team members, which is difficult to achieve whether qualitative or quantitative definitions are used.
- Where multiple outcomes are possible (e.g. a fall on a slippery deck – consequence can range from nothing to a broken neck), it can be difficult to select the "correct" consequence for the risk categorisation. Many practitioners suggest using the more pessimistic outcome (in this case: broken leg) and not a very rare worst case nor the most likely trivial outcome.

- A risk matrix looks at hazards "one at a time" rather than in accumulation, whereas risk decisions should really be based on the total risk of an activity. Potentially many smaller risks can accumulate into an undesirably high total risk, but each smaller one on its own might not warrant risk reduction. As a consequence, risk matrix has the potential to underestimate total risk by ignoring accumulation.

- The risk matrix does not have a formal linkage to the HSE tolerability of risk framework (see Section 3). A key task if risk matrices are used for offshore safety cases is to ensure that the risk evaluation implicit in the matrix will conform to the HSE approach, and if this is not the case then the definitions should be altered appropriately. A good test is to verify that borderline decisions on risk reduction as determined from the matrix match current good maritime practice.

- Since the risk evaluation criteria are predefined, teams may (semi)consciously assign risks into an adjacent less onerous risk category, as this reduces project costs. The study leader must guard against this temptation.

- The lack of standardisation may cause confusion. The three examples above all have the high-frequency high-consequence combinations in different corners of the risk matrix.

Risk matrices are probably the most common approach used for risk assessment in marine activities, as they are appropriate for people new to risk assessment, being straightforward to apply and easy to understand. However, they suffer from several limitations, including difficulties in dealing with multiple differing outcomes, consistency in application, transparency of categorisation decisions, and dealing with novel hazards.

The depth of treatment of a risk matrix is appropriate for many hazards, in particular:

- If the vessel / activity is well established with good operational experience

- If there is a good track record of safe operations

- If there are relatively few possible catastrophic outcomes and good experience to suggest these are highly unlikely.

It is possible to use risk matrix for smaller well-known hazards, while using more in-depth analysis for novel hazards or a selection of major hazards.

2.4 Semi-Quantitative Methods

This approach is the next level up from risk matrix in terms of depth of analysis. As its name implies it uses techniques drawn from Quantified Risk Analysis (QRA), but does not actually quantify the results. Thus frequency may be analysed using a modelling technique such as Fault Tree Analysis (FTA) and consequences analysed using Event Tree Analysis (ETA). Other risk tools can also be used (see Lees 1996, CCPS 1989), but these are the most common.

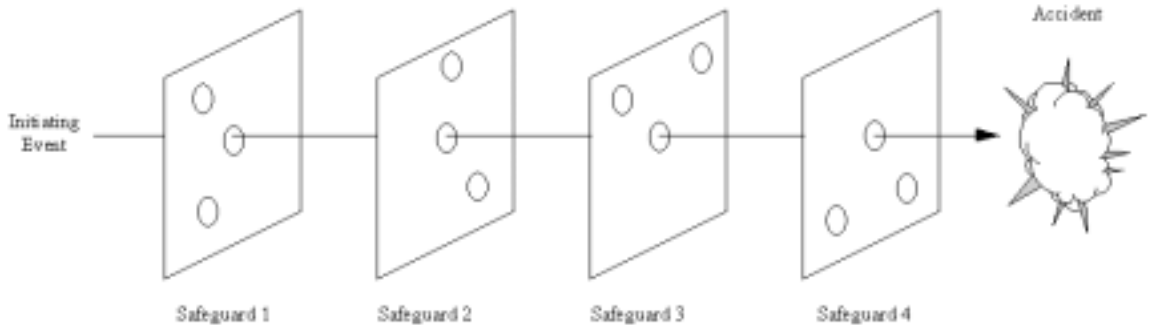
2.4.1 Fault Tree Analysis

Full details on Fault Tree Analysis are provided in a later section (2.6.6), and if the reader is unfamiliar with these then refer to that section before reading how it may be simplified.

The technique shows the means by which major hazard events occur through the escalation of smaller initiating events. The FTA shows the whole range of "initiating events" placing "demands" on the system and how the safeguards act to prevent escalation. Initiating events and safeguards can be anticipated conditions (e.g. storm), technical (e.g. propulsion systems) procedural (watch keeping rules) or human error related. In the semi-quantitative approach it is not necessary to evaluate likelihoods, the structure of the tree is sufficient to demonstrate the means by which major hazards arise. Teams can judge the adequacy of the safeguards (both number and quality) in judging acceptability.

A good analogy for accident causation is given by Reason (?) as shown in Figure 2.8. This so-called Swiss Cheese model shows challenges to the safety system as sticks poking through "holes" in each layer of defence (these are gaps or deficiencies in each safeguard). If there are insufficient safeguards or these have too many gaps, then a major accident becomes more likely.

Figure 2.8 Swiss Cheese Model of Accident Causation



Whilst the tree on its own can be useful for defining safeguards, on more complex trees this can be difficult to visualise or it may conceal common cause failures (a single failure defeating two or more safeguards, e.g. power failure). For these, a technique called "Minimal Cut Set Analysis" has been developed (Lees 1996). This technique assigns a unique label to every base event on the tree and shows all possible ways in which these can combine to lead to the major hazard event. These are often shown as letter combinations

eg A, B
CD, CE, CF
GHI
JKLMN

known as Single Event Cut Sets, Two Event Cut Sets, etc.

The significance of these is that single or two event cuts imply no or little safeguarding between the initiating event and the top event, whereas 4 and 5 event cut sets do have multiple redundancy. There are rules of thumb appropriate for major hazards that single or 2-event cut sets require additional mitigation / safeguarding, whereas 5 event cut sets and higher are probably adequate. Three and 4 event cut sets may require additional evaluation. Factors for evaluation include both the number of safeguards and their quality or reliability.

2.4.2 Event Tree Analysis

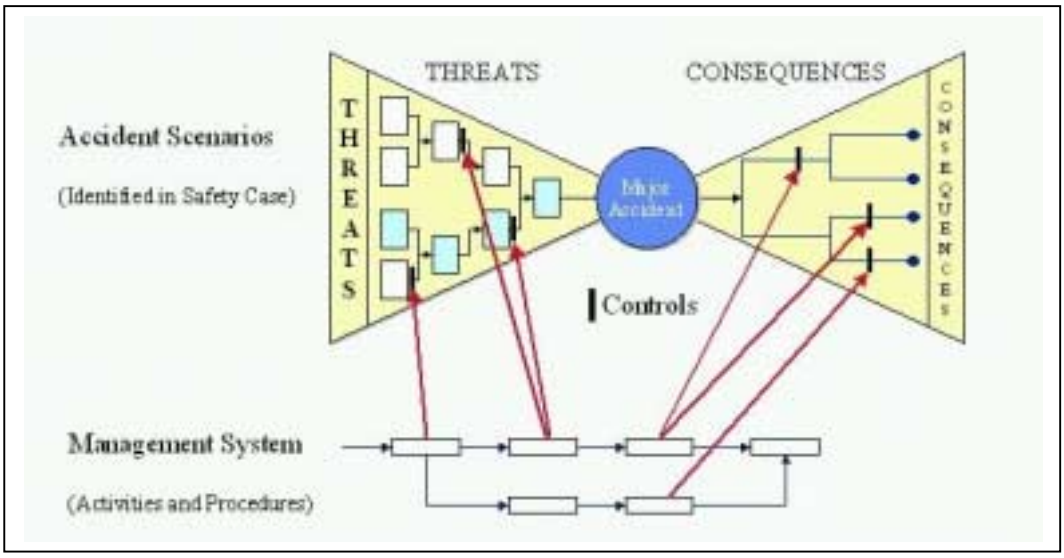
This technique is discussed more fully in Section 2.6.7. It is a branching technique (normally into pairs: YES / NO) tracing all possible outcomes of a major hazard event. Each branch itself branches and thus the event tree can expand exponentially. Fortunately many outcomes are the same, even if the route to get there differs.

The main qualitative use of event trees is to maintain the structure of the tree, but omit the stage of quantifying the branch probabilities. Establishing these probabilities can be time consuming, but the real value comes from the structure, that is understanding how event outcomes escalate and how safeguards are deployed to mitigate these outcomes.

2.4.3 Bow Tie Analysis

The Bow-Tie approach has been popularised recently in the Netherlands (EU Safety Case Conference, 1999) as a structured approach for risk analysis within safety cases where quantification is not possible or desirable. The idea is simple, to combine the cause and consequence analyses into a single diagram (preferably limited to A3 size paper) with the Fault Tree plotted sideways on the left and the Event Tree plotted sideways on the right. If the Major Accident is plotted as a large circle in the middle, this looks like a Bow Tie (see Figure 2.9).

Figure 2.9 Example Bow Tie Analysis



This diagram has several advantages for use in safety cases:

- the full range of initiating events is shown
- the intervening safeguards are clearly shown
- the actual way in which these combine and escalate is clearly shown
- the consequences side shows barriers in an equivalent manner
- the many possible consequence outcomes are defined
- the linkage of the barriers to the safety management system can be made explicit

Ideally these diagrams should be kept simple, as their main function is to demonstrate mechanisms and to allow staff and managers to understand how major hazard events can occur and what safeguards exist to prevent them. Short-hand notations make these diagrams much more compact and allow a complex tree to be captured on one page (Figure 2.10).

Figure 2.10 Short-Hand Notation for Bow Tie Diagram

One qualitative decision tool is to judge the qualitative risk and based on whether this is high, medium or low, then more or fewer safeguards are required. To ensure good balance, the approach demands equivalent safeguards on both sides of the Bow Tie. This conforms well to the HSE Hierarchy requirement (Eliminate – Prevent – Mitigate – Recover) as the first two are on the left and the latter two on the right. This ensures that prevention barriers as well as mitigation barriers both exist.

A good check is to list methodically every safeguard identified in the hazard identification and confirm that these appear on the Bow Tie relating to that major hazard. This helps link the hazard identification to the subsequent risk analysis. Once the diagram is completed it becomes visually obvious where there is insufficient safeguarding and conversely where there might be excess safeguarding. In a design situation, and assuming that it would not contravene current good practice, safeguarding resources can be diverted from the excess area to the insufficient to ensure good overall controls. In an operational situation, where there is insufficient safeguarding then additional hardware or procedural controls may be necessary.

This approach lends itself well to risk communication. The format is not overly complex and non-specialists can understand the approach. All safeguards relating to the hazard are shown explicitly and colour coding can be used to differentiate technical and procedural safeguards, and potentially the role of specific individuals or groups. The link to the safety management system depends on the safeguard type. If it is technical then it might link to the preventive maintenance portion, if it is procedural it might link to the training and qualification system, and both to the ongoing monitoring and audit program.

2.5 Quantitative Methods

2.5.1 Applicability

Quantitative risk analysis (QRA) is one of the most sophisticated techniques of risk assessment, but should only be used where it gives a clear benefit. UKOOA (1999) suggests that QRA is most appropriate for Type B decisions (Figure 1.5), involving risk trade-offs, deviation from standard practice or significant economic implications. Even for these decisions, QRA is only one of several inputs to the decision-making process, and must be balanced against other approaches such as engineering judgement and company values.

QRA as an engineering tool provides good understanding of the mechanisms of accidents and the role of safeguards in terminating accident sequences. It forces all assumptions to be explicit, and hence provides a better understanding of uncertainty than judgement-based approaches.

The Safety Case Regulations explicitly require QRA to show that the temporary refuge and means of evacuation make risks from fire and smoke ALARP (Section 1.3.2), but this does not apply to marine hazards. QRA has often been applied to ship-platform collision risks, and has proved influential in developing good risk management practices (Dovre Safetec 1999). It is possible to apply similar approaches to other marine hazards, although the techniques for this are much less highly developed than QRA of fire and explosions.

2.5.2 Frequencies and Consequences

QRA usually maintains a clear distinction between two important elements of risk:

- The frequencies of events, i.e. their likelihood in a given time period.
- The consequences of events, i.e. the fatalities, damage or pollution that they cause.

A hydrocarbon leak resulting in a fire or explosion is often considered the archetypal offshore accident scenario. This provides a clear distinction between the causes and likelihood of hydrocarbon leaks (frequencies) and the effects of fires and explosions on people, property and the environment (consequences). For most hydrocarbon leaks, the estimation of leak frequencies can be largely independent of the modelling of fires/explosions.

For marine hazards, such distinctions between frequencies and consequences are less clear, and each type of hazard must be considered separately. For example, the frequency of loss of position-keeping is clearly distinguished from its consequences. However, one of its consequences may be a contribution to the frequency of collision. Collisions themselves have their own consequences. For many marine hazards, such as loss of stability, it is difficult to consider the frequency without having defined the consequence. The risks may be determined by defining a range of consequences and estimating the frequency of each. Hence, for marine hazards, the frequencies and consequences are interdependent, and the major distinction is between the different types of hazards. Nevertheless, the methods of frequency analysis and consequence modelling are often applicable in principle to all hazards, and these are therefore considered separately below.

2.5.3 Failure Cases

Failure cases are specific hazards suitable for modelling in the risk assessment, forming discrete representations of the range of accidents that might occur in reality. For example, a hazard such as "ballast system failure" might be represented by two failure cases, (1) accidental ballasting of one compartment, and (2) accidental ballasting of two compartments. The QRA would then attempt to estimate the frequencies and consequences of these two events while neglecting all other types of ballast failure. Failure cases are sometimes known as "hazardous events", "accidental events", "top events", or more accurately as "equivalent discrete failures" and sometimes confusingly as "hazards".

The failure cases should form the link between the hazard identification and the QRA, but in practice the linkage is often weak and insufficiently documented.

The selection of failure cases has an important effect on the overall risk results. If too few failure cases are used, the risks and the benefits of risk control options may be unreliable. Benchmarking exercises have shown that the results from studies using too few failure cases may be several orders of magnitude higher or lower than more detailed studies. However, if too many failure cases are used, the QRA may be over-complex and difficult to check. CMPT (1999) gives further guidance on the selection of failure cases.

2.5.4 Frequency Methods

Frequency analysis involves estimating the likelihood of occurrence of each failure case. The main approaches to estimating frequencies are:

- Historical accident frequency data (Section 2.5.5). This uses previous experience of accidents. It is a simple approach, relatively easy to understand, but is only applicable to existing technology with significant experience of accidents and where appropriate records have been kept.

- Fault tree analysis (Section 2.5.6). This involves breaking down an accident into its component causes, including human error, and estimating the frequency of each component from a combination of generic historical data and informed judgement.

- Simulation. The frequencies of some types of accidents can be predicted using simulation models. An example of this is ship collisions, where time-domain simulation or analytical computation can be used to estimate the frequency of collisions from the range of ship movements in the area.

- Event tree analysis (Section 2.5.7). This is a means of showing the way an accident may develop from an initiating event through several branches to one of several possible outcomes. The technique is usually used to extend the initiating event frequency estimated by one of the above means into a failure case frequency suitable for combining with the consequence models.

- Human reliability analysis (Section 2.6.2). This is a means of modelling the contribution of human error to accidents, and may be used to generate inputs for fault tree analysis, theoretical models or event tree analysis.

- Judgemental evaluation. In some cases, it may be appropriate to select a frequency based on judgement of experienced personnel. This may be for simple assessments, for frequent events, for events having minimal risk, or for events where no better approach is available.

- Bayesian analysis. This is a systematic way of combining historical data with judgements, and includes a comprehensive treatment of uncertainties. It is used in structural reliability analysis (Section 2.5.8) but is rarely used in offshore QRA in the UK

In general, these techniques are used in combination.

2.5.5 Historical Data Analysis

Analysis of historical accident data forms the foundation of many QRAs. Frequencies are simply calculated by combining accident experience and population exposure, typically measured in terms of installation-years:

$$\text{Event frequency per installation year} = \frac{\text{Number of events}}{\text{Number of installations x Years of exposure}}$$

A prime source of data on offshore marine accidents is the Worldwide Offshore Accident Databank (WOAD). Figure 2.11 shows an example record from WOAD, illustrating the many indexing terms and the detailed free text description. CMPT (1999) reviews other available data sources for offshore QRA.

Figure 2.11 Example Record from WOAD

Acc. id. no.	**9605236**	Date of acc.	**960118**	Main operation	**MO**
Rev. date	**960730**	Time		Suboperation	**JU**
Name of unit	**ENSCO 69**	Duration	**2**	Acc. category	**A**
Unit id. no.	**76034**	Geogr. area	**AGM**	Main event	**ST**
Type of unit	**JU**	Shelf	**US**	Chain of events:	
Function	**DR**	Waterdepth	**100**	1	**ST**
Class. soc.	**AB**	Drilldepth		2	**LI**
Owner	**ENSCO**	Field/block	**ORANGE**	3	**FA**
Contractor	**ENSCO**	Syst./equipm. 1	**SL**	4	**PO**
Operator	**HALHOU**	Syst./equipm. 2	**DE**	5	
		Syst./equipm. 3	**UJ**	Hu. cause	
		Syst./equipm. 4		Eq. cause	**FP**
Wind	**99**	Fatalities	**0 / 0**		
Wave height	**99**	Injuries	**0 / 0**	Evacuation	**SU**
Air temp	**+1**	Downtime	**200**	Means 1	**SU**
Weather		Damage	**SE / 9999**	Means 2	
Light cond.		Release	**NO / 0**	Means 3	
Visibility	**IRRL**	Repair	**YA / 180**	# evacuated	**63**
		Ref. sources	**OI,OR,LL**		

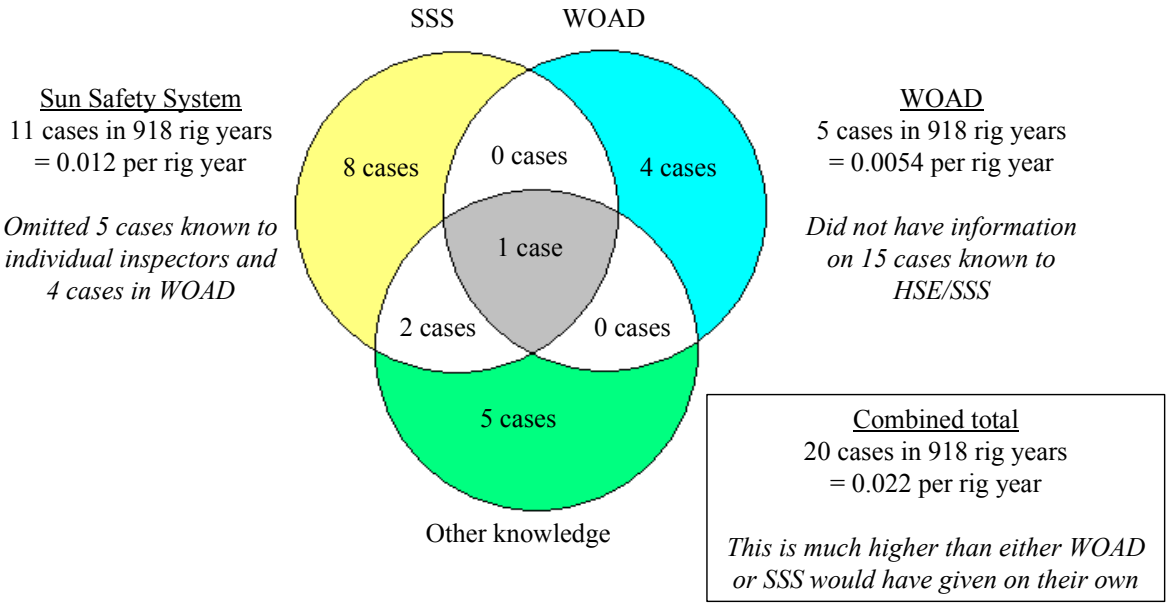
DESCRIPTION:
The jack-up was preparing to jack up on a new location when one of its legs sank 20 feet into the sea floor causing a severe list. The 63 persons on the platform were evacuated to an ENSCO supply vessel due to deteriorating weather conditions. The rig separated from its legs in heavy seas and high winds, heading south, adrift. At 1500 hrs the 19th, it was secured and inspection crew boarded the day after. Then the rig was taken to yard in Orange, TX and repairs are expected to take 3-6 months. The jack-up sustained damage to its hull, control house, derrick and jacking systems, in addition to losing the lower sections of its legs. The legs above the jacking tower were damaged, and one leg and the derrick collapsed onto the deck. Damaged equipment were removed and salvage of the leg sections (left on location when rig broke free) were initiated. In July the sheerlegs pontoon crane barge "Taklift 8" recovered the 3 lost legs which were in good condition and reusable. Rig owner expects the rig to be back in operation in July/August.

CCPS (1989) gives detailed guidance on collection and processing of frequency data for a QRA. CMPT (1999) gives simpler guidance with offshore examples.

A major challenge in historical data analysis arises from uneven reporting standards in most available accident databases. Accidents occurring in countries with open reporting cultures such as Norway are most likely to be included, but this rarely gives sufficient experience to obtain useful frequencies. Accidents elsewhere in the world may not be included unless they are very severe. Often, it is a matter of chance whether a particular accident is reported in the technical press and entered in the accident databases. Figure 2.12 illustrates the under-estimation of accident frequencies that may result. It compares the number of cases of flooding on semi-submersibles on the UKCS during 1970-97 in the HSE database "Sun Safety System", with cases included in WOAD and known by individual inspectors within HSE (DNV 1999). This shows that no single source is comprehensive, and emphasises the importance of combining different sources wherever possible. This uncertainty in historical accident frequencies must be borne in mind when interpreting the results.

Figure 2.12 Comparison of Different Sources for Flooding of Semi-Submersibles

This Venn diagram shows how many accidents were known to DNV's public-domain database WOAD, HSE's confidential database SSS, and individual inspectors within HSE. The outer parts of the circles show cases known only to one source. The intersections show cases known to two or more sources.



When only reports on major accidents (e.g. fatalities) are available, it is possible to estimate the frequency of less severe accidents from accident pyramids, which indicate typical ratios of fatalities, lost-time injuries, minor injuries, and near misses. This is desirable where it is intended to estimate the total cost of all accidents, for use in cost-benefit analysis. It may also be useful for estimating the frequency of serious accidents when only less serious ones have occurred. However, the ratios of the frequencies of these accidents are very sensitive to the nature of the installation and the definition of the accidents (HSE 1997a), so this approach should be used with caution.

The formal recording of major accidents and serious near misses, other than industrial injuries (RIDDOR), is increasingly mandated. All offshore leak events must be reported to the HSE, regardless of whether there was any consequence. The COMAH Directive requires major accidents or near misses involving specified quantities of materials to be reported to the HSE and thence onwards to the EU where a database is maintained (MARS). The USA Risk Management Plan legislation for process industry requires operators to report 5-year accident histories. Increasingly these data sources will provide good statistics for developing generic frequencies for use in risk analysis

Many QRA studies use existing generic accident frequencies instead of developing new ones. CMPT (1999) and E&P Forum (1996) provide extensive compilations of such generic frequencies.

The strengths of historical frequencies in QRA are:

- They are rooted in reality, so that the risk predictions arise directly from previous accident experience. This may be considered to be the most objective, least judgemental approach to frequency analysis. Cases are not limited by the imagination of a HAZID team.

- The events used to compile the frequencies can also be used to indicate the consequences, and thus can validate any consequence analysis, ensuring that the whole of the QRA is consistent with actual experience.

- Historical frequencies are relatively easy to understand, and hence to audit and update, compared to fault tree analysis or theoretical modelling.

The weaknesses include:

- The approach is most appropriate for relatively standard installations for which previous operating experience is relevant. However, it can be modified judgementally to apply to standard parts within a novel design.

- The approach often uses data from installations significantly different to the one in question, in order to obtain statistically significant accident frequencies. This inevitably introduces uncertainties, although generic frequency data is often independent of differences in environment

- Appropriate measures of exposure are often not available. For example, there are many sources of data on dropped load accidents, but few estimates of the numbers of loads lifted during the period of the data.

- Accidents may not be recorded in available sources. This may result in under-estimates of frequencies, as described above.

- Safety standards may have changed as a result of previous accidents, so that the conditions that led to historical accidents may be no longer valid. Recent experience is obviously the most appropriate.

- It is difficult for the approach to show the contribution of particular aspects (e.g. human error) to the accident frequency or the effect of many risk reduction measures. For these,

methods such as fault tree analysis and human reliability analysis are required, but these are usually calibrated against the historical accident frequencies.

Despite its limitations, historical experience is the basis of most offshore QRAs. Other methods, such as theoretical analysis and judgement may be appropriate where there is no accident experience, and human reliability analysis is a useful supplement to highlight the importance of human performance.

2.5.6 Fault Tree Analysis

Fault tree analysis (FTA) is a logical representation of the many events and component failures that may combine to cause one critical event (e.g. a system failure). It uses 'logic gates' (mainly AND or OR gates) to show how 'basic events' may combine to cause the critical 'top event'. The top event would normally be a major hazard such as "loss of position keeping". The possible consequences would be estimated separately.

FTA has several potential uses in offshore QRA:

- In frequency analysis, it is commonly used to quantify the likelihood of the top event occurring, based on estimates of the failure rates of each component. The top event may be an individual failure case, or a branch probability in a event tree.

- In risk presentation, it may also be used to show how the various risk contributors combine to produce the overall risk.

- In hazard identification, it may be used qualitatively to identify combinations of basic events that are sufficient to cause the top event, known as 'cut sets'.

Construction usually starts with the top event, and works down towards the basic events. For each event, it considers what conditions are necessary to produce the event, and represents these as events at the next level down. If any one of several events may cause the higher event, they are joined with an OR gate. If two or more events must occur in combination, they are joined with an AND gate. Lees (1996) gives a good review of this.

If quantification of the fault tree is the objective, downward development should stop once all branches have been reduced to events that can be quantified. If the tree is simple and each event only occurs once, the frequency of the top event can be determined manually using the appropriate formulae (e.g. CCPS 1989). More commonly, computer programs are used. CMPT (1999) gives sources for such programs.

The strengths of fault tree analysis are:

- It is widely used and well accepted.

- It is suitable for many hazards in QRA that arise from a combination of adverse circumstances.

- It is often the only technique that can generate credible likelihoods for novel, complex systems.

- It is suitable for technical faults and human errors.

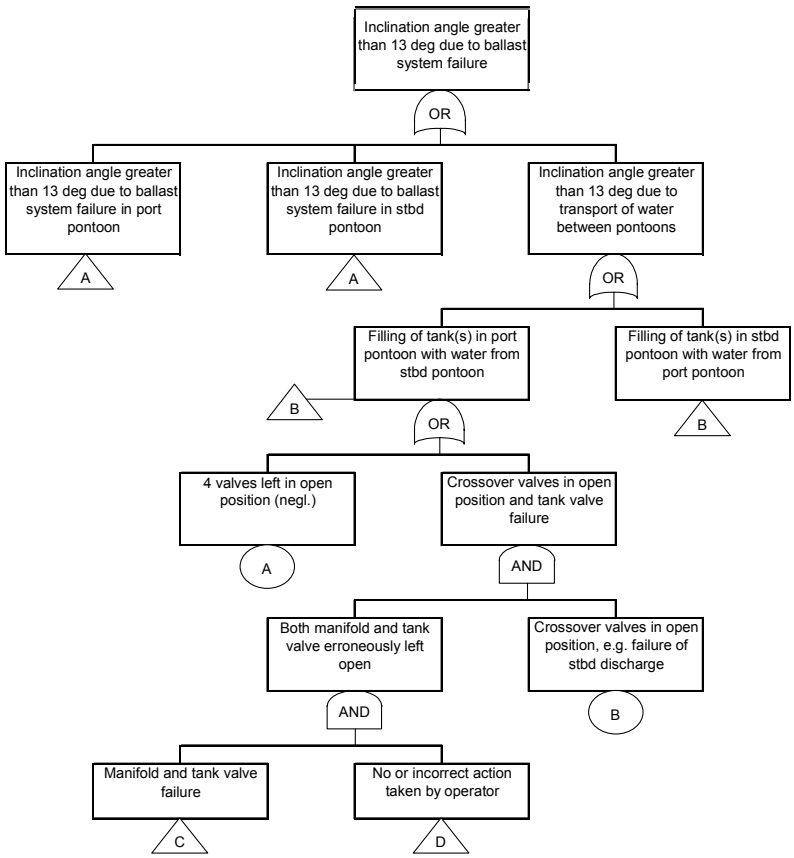
- It a clear and logical form of presentation.

Its weaknesses are:

- The diagrammatic format discourages analysts from stating explicitly the assumptions and conditional probabilities for each gate. This can be overcome by careful back-up text documentation.
- It soon becomes complicated, time-consuming and difficult to follow for large systems
- Analysts may overlook failure modes and fail to recognise common cause failures (i.e. a single fault affecting two or more safeguards) unless they have a high level of expertise and work jointly with the operator.
- All events are assumed to be independent.
- It loses its clarity when applied to systems that do not fall into simple failed or working states (e.g. human error, adverse weather etc).

FTA is a powerful technique, suitable for detailed analysis of individual systems. Figure 2.13 shows an example of FTA applied to a marine hazard.

Figure 2.13 Extract from Fault Tree Analysis of Ballast System Failures (Veritec 1987)



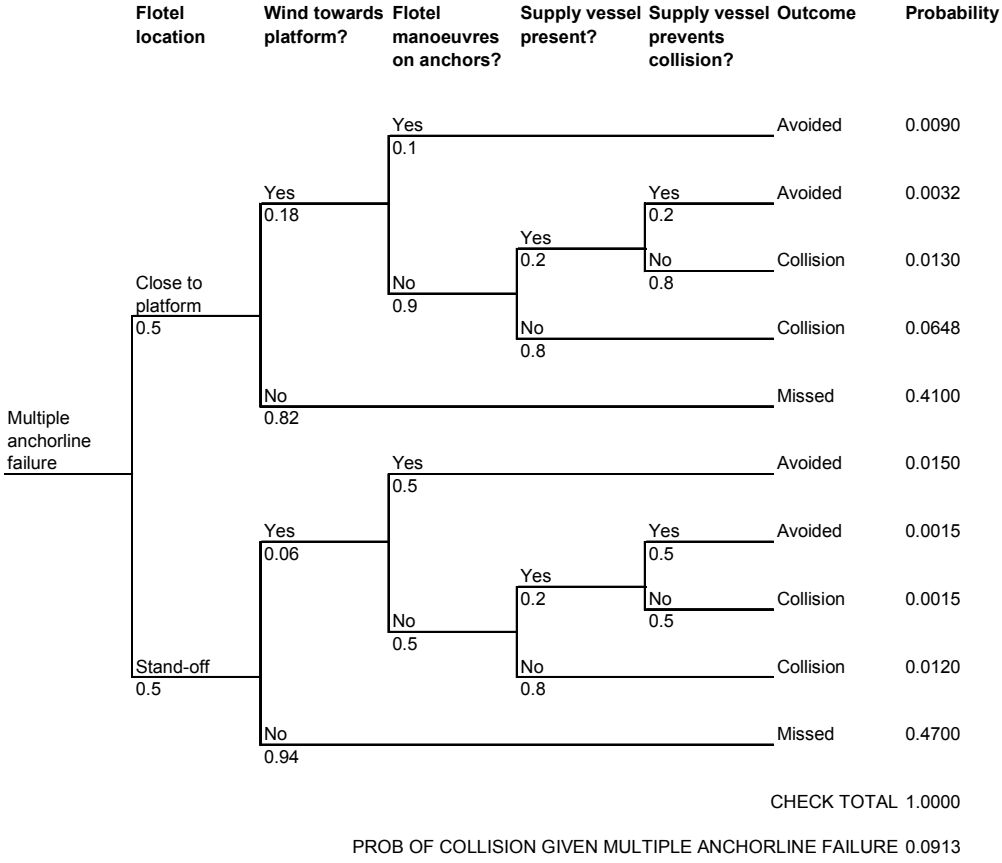
2.5.7 Event Tree Analysis

Event tree analysis (ETA) is a logical representation of the various events that may follow from an initiating event (e.g. a component failure). It uses branches to show the various possibilities that may arise at each step. It is often used to relate a failure event to various consequence models. It may also be used to quantify system failure probabilities, where several contributory causes can only arise sequentially in time.

Construction starts with the initiating event and works through each branch in turn. A branch is defined in terms of a question (e.g. 'Protective device fails?'). The answers are usually binary (e.g. 'yes' or 'no'), but there can also be multiple outcomes (e.g. 100%, 20% or 0% in the operation of a control valve). Each branch is conditional on the appropriate answers to the previous ones in the tree.

Usually an event tree is presented with the initiating events on the left and the outcomes on the right. The questions defining the branches are placed across the top of the tree, with upward branches signifying 'yes' and downward ones for 'no'.

Figure 2.14 Event Tree Analysis of Flotel-Platform Collision Probability (OCB/Technica 1988)



Quantification of an event tree is relatively simple, and is readily performed by hand, although spreadsheets or computer models are increasingly used to automate the multiplication task. A probability is associated with each branch, being the conditional probability of the branch (i.e. the answer 'yes' or 'no' to the branch question) given the

answers of all branches leading up to it. In each case, the sum of the probabilities of each branch must be unity. The probabilities of each outcome are the products of the probabilities at each branch leading to them. The sum of the probabilities for all outcomes must be unity as well. This provides a useful check on the analysis. Figure 2.14 shows an example of ETA applied to a marine hazard.

The strengths of event tree analysis are:

- It is widely used and well accepted.
- It is suitable for many hazards in QRA that arise from sequences of successive failures.
- It a clear and logical form of presentation.
- It is simple and readily understood.

Its weaknesses are:

- It is not efficient where many events must occur in combination, as it results in many redundant branches.

- All events are assumed to be independent.

- It loses its clarity when applied to systems that do not fall into simple failed or working states (e.g. human error, adverse weather etc).

ETA is a simple but effective technique, suitable for many applications.

2.5.8 Consequence Methods

Estimation of the consequences of each failure case is necessary to complete the analysis of the risks. The approach usually differs for each type of hazard. Guidance is given by CMPT (1999). Typical approaches include:

- Loss of position keeping - a range of consequences may be postulated and the possible routes to them identified by a frequency technique such as event tree analysis. Engineering calculations or drift modelling may be used to supply branch probabilities for the event tree (e.g. Figure 2.11).

- Loss of structural integrity - as above. In principle, the frequencies may be obtained from structural reliability analysis (SRA), but in practice even the failure probabilities from a fully probabilistic SRA are not adequately calibrated against actual experience to allow them to be combined with historical data for other hazards. Alternatively, SRA may be used to demonstrate that the design achieves structural reliability equivalent to existing designs. More commonly, offshore installations follow design codes and classification rules that have themselves been calibrated in this way. Either approach may be considered to justify the use of historical failure frequencies, even if these are based on different types of installations.

- Loss of stability - a range of consequences may be postulated and the possible routes to them identified by a frequency technique such as event tree analysis. Damage stability calculations may be used to provide branch probabilities.

- Loss of marine/utility systems - the consequences of such failures are usually minor by themselves unless they contribute to the frequency of more severe events such as collisions or loss of stability. Hence, they are normally included in the frequency model for these events, e.g. as event tree probabilities.

- Collisions - frequency methods for collisions usually give impact energies and collision geometries, which may be used as the basis of structural consequences modelling. This requires non-linear finite-element modelling, and is rarely used. More commonly, the consequences are based on judgemental interpretation of previous calculations, combined with evacuation modelling.

Event tree modelling is appropriate for most marine hazards. A range of damage consequences can be postulated for the installation, based on the HAZID, the possible routes to them presented by the event tree, and the branch probabilities determined by an appropriate combination of historical data, judgement and theoretical modelling. The fatality risk from each damage consequence can be determined by evacuation modelling (see below).

In some cases, major damage to the installation can result in hydrocarbon releases (e.g. blowouts, spills of stored oil, failures of flexible risers etc). These may cause environmental pollution, or may ignite to cause fires and explosions. Such escalation can be modelled using conventional offshore QRA techniques, which are outside the scope of this guide but are covered by CMPT (1999).

2.5.9 Evacuation Modelling

Most fatalities from marine hazards arise during an attempt to evacuate the installation (DNV Technica 1994). These risks are commonly addressed in an evacuation, escape and rescue analysis (EERA), which is a type of risk analysis first performed in response to a recommendation in the Cullen Report, but more recently used as a possible approach to the assessment required under PFEER. The EERA is usually qualitative, but quantitative approaches are necessary if the risks to personnel from marine hazards are to be quantified. EERA techniques are outside the scope of this guide but are covered by CMPT (1999).

2.5.10 Risk Presentation

The results from a QRA may be expressed as:

- Individual risks - the risk experienced by individuals on the installation. This usually refers to the risk of death, and may be expressed as an individual risk per annum (IRPA) or a fatal accident rate (FAR) per 100 million exposed hours. It may refer to the risk at a particular location on the installation for a hypothetical individual who is always there, or to the risk for a realistic individual, allowing for their movement around the installation and their time off-duty ashore. Hence, clear definition of the basis of the calculation is important when presenting the risk results.

- Group risks - the risk experienced by the whole group of personnel working on the installation or otherwise affected by it. This usually refers to the risk of death, and is usually expressed as an average number of fatalities per installation-year, known variously as annual fatality rate, potential loss of life (PLL), expectation value, rate of

death etc. Alternatively, it may be expressed as an FN curve, showing the cumulative frequency (F) of events involving N or more fatalities.

- Impairment frequencies - the frequency at which essential safety functions are made unusable by accidents. The main such safety function is the temporary refuge (TR). The Safety Case Regulations require the frequency of TR impairment from hydrocarbon hazards to be made ALARP. This allows personnel risks to be managed effectively without the need to quantify them directly. However, this approach is not normally used for marine hazards, because impairment frequencies are not simply comparable between different types of installations.

- Damage risks - the risk of damage to the installation. This may be expressed as the frequency per year of defined levels of damage (e.g. total loss, severe damage etc). Alternatively, if the damage levels are converted to financial losses, it may be expressed as an average damage cost per year. This is useful for cost-benefit analysis of risk reduction measures.

- Oil spill risks - the risk of oil spills from the installation. This can be expressed in forms equivalent to group risks for people, as either the average amount of oil spilled per year or as the cumulative frequency of different sizes of spills.

CMPT (1999) gives formulae defining how the results of each failure case should be combined to generate these measures. Figure 2.15 shows an example calculation of individual and group risks.

DNV Technica (1995) gives some benchmark risk estimates for mobile installations and marine hazards in the UKCS. The WOAD Statistical Report (DNV 1998) includes some benchmark frequencies of different severities of damage for mobile installations and marine hazards.

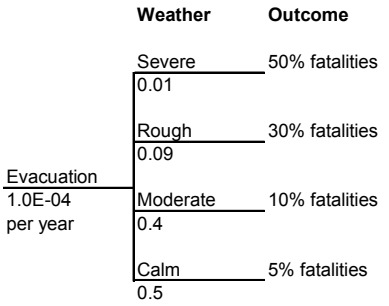
2.5.11 Uncertainties

Most of the inputs and all the outputs from a QRA are uncertain to some degree. In some cases, the uncertainties may be very large, and the conclusions of the QRA may be sensitive to possible variations in the inputs or modelling assumptions. These uncertainties form one of the main limitations of QRAs, and it is important that they are understood and accounted for explicitly. The HSE requires safety cases to "demonstrate that conclusions reached using QRA have taken uncertainty into account" (HSE 1998b).

UKOOA (2000) gives general guidance on how to take uncertainty into account in a QRA. This does not necessarily require a formal uncertainty analysis. In some cases, a conservative approach to the QRA and simple sensitivity analyses are sufficient to demonstrate that the QRA's conclusions are robust with respect to uncertainty in the inputs and assumptions. More detailed uncertainty analysis may be required if a critical decision is sensitive to uncertainties, or to the degree of conservatism in the QRA.

Analysis of uncertainties is itself one of the most uncertain areas in QRA. Most techniques of uncertainty analysis from conventional statistics are inappropriate for QRA, and much more empirical approaches are required, as outlined by CMPT (1999).

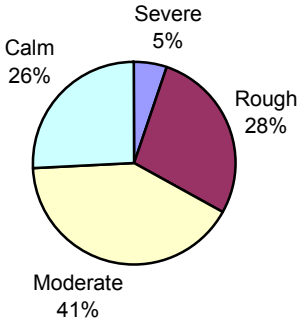
Figure 2.15 Example Risk Calculation

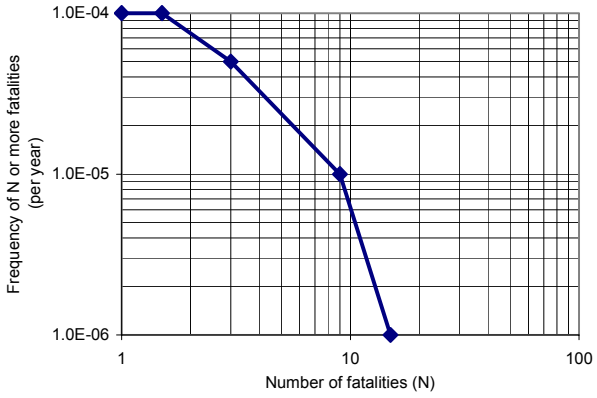


This example presents the risks in evacuation from an accident whose frequency is 10^{-4} per installation year. Four different weather cases are considered, with different probabilities of occurrence and outcomes ranging from 5% to 50% fatalities among the 30 people on board, as shown in the event tree (left). The spreadsheet (below) calculates the individual risk for a person continuously on board (LSIR = 9.7 x 10^{-6} per person year), the group risk (GR = 2.9 x 10^{-4} per installation year) and the cumulative frequencies (F) for the FN curve.

The pie chart (below left) shows the distribution of group risk by weather category. In this case, fatalities in moderate weather dominate the result. The FN curve is shown (below right).

Event frequency		1.0E-04	per year				
POB		30					
Weather	Weather prob	Fatality fraction	Fatalities (N)	Outcome freq	LSIR	GR	F
Severe	0.01	0.5	15	1.0E-06	5.0E-07	1.5E-05	1.0E-06
Rough	0.09	0.3	9	9.0E-06	2.7E-06	8.1E-05	1.0E-05
Moderate	0.4	0.1	3	4.0E-05	4.0E-06	1.2E-04	5.0E-05
Calm	0.5	0.05	1.5	5.0E-05	2.5E-06	7.5E-05	1.0E-04
Total	1.0			1.0E-04	9.7E-06	2.9E-04	





2.5.12 Further Information

For further information, Pitblado & Turney (1995) give an introduction to QRA for the process industries, including a section on offshore QRA. More detailed guides to QRA (notably CCPS 1989, and parts of Lees 1996) are useful in the area of basic techniques and consequence modelling, but do not cover many key areas specific to offshore installations. Aven (1992) provides detailed discussion of offshore QRA, focusing in particular on reliability analysis. CMPT (1999) gives more detailed guidance and source data specifically for offshore QRA, including marine hazards. E&P Forum (1996) provide a compilation of data for risk assessment of exploration and production activities, including marine hazards.

2.6 Human Element

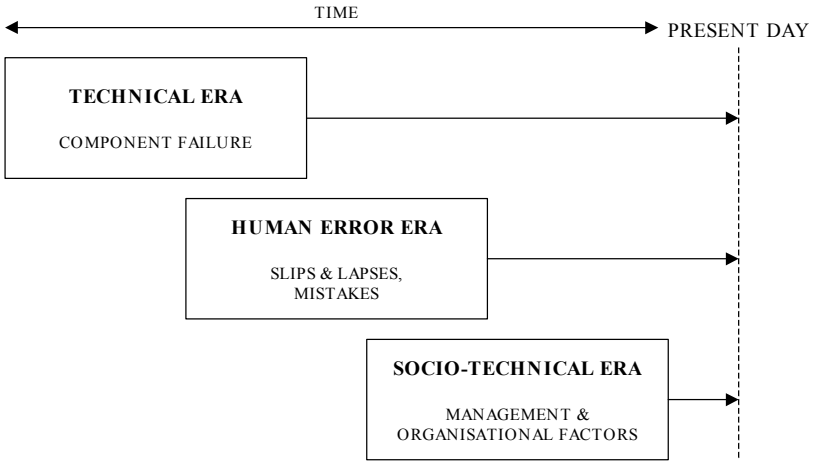
2.6.1 Human Factors

"Human factors" refer to environmental, organisational and job factors, and human and individual characteristics that influence behaviour at work in a way that can affect health and safety (HSE 1999b). It includes consideration of:

- The job - tasks should be designed in accordance with ergonomic principles to achieve a physical and mental match with people's capabilities.
- The individual - people should be recruited and trained so that they are competent in performing the job.
- The organisation - the company should establish a positive health and safety culture.

Reason (1991) interprets the development of interest in the human contribution to accidents in terms of three ages of safety concerns (Figure 2.16). First, the focus was on technical problems, and this still has its place. However, as technical systems became more reliable, the focus turned to the human causes, and many accidents were blamed on individuals directly involved in the operation. More recently, major accident investigations (e.g. *Piper Alpha*) have recognised that the root causes of failures of equipment and operators lie deeper in the organisation's safety management and safety culture.

Figure 2.16 Three Ages of Safety Concerns (Reason 1991)



Analyses of accident causes typically show that up to 80% of accidents may be attributed, at least in part, to the actions or omissions of people (HSE 1999b). For example, Tangen (1987) estimated that human error represented approximately 60% of all causes of shipping accidents, with procedural or administrative errors contributing a further 15%, and technical failures 25%. Of the human errors, only 20% were due to substandard acts by individual operators. The remaining 80% were attributed to factors over which management had direct control.

For a risk assessment to be comprehensive, it should take human factors into account. Given the dominance of human factors in accident causation, it is not surprising that measures to reduce human error are often among the most cost-effective ways of reducing risk. In order to

identify such measures, it is necessary to consider how people may contribute to causing accidents and how they may act to mitigate and escape from any accidents that do occur.

2.6.2 Human Errors

Nearly all accidents are initiated or exacerbated by human error. These errors include:

- Slips - making an unintended action through lack of attention or skill
- Lapses - unintended action through memory failures
- Mistakes - an intended but incorrect action
- Violations - a deliberate deviation from standard practice

Human errors in marine operations, such as towing or ballast system operation, tend to have immediate effects. They may be recovered with no harm done, or they may have some direct harmful impact. This may then require some form of emergency response to mitigate the impacts. Similarly, errors may occur during evacuation, with a direct effect, e.g. incorrect release of a lifeboat.

Errors can also occur during maintenance, and may then remain undiscovered (latent) until the equipment is required. These errors in effect cause equipment unavailability, and the significance of this depends on the system design. For example, this type of error may result in a ballast pump being unavailable when required.

2.6.3 Human Factors Assessment

The aim of human factors assessment is to consider in a systematic way the potential human factors problems in a particular activity, so as to identify possible risk reduction measures. In principle, it is desirable to consider human and technical factors in a holistic way, with the human factors assessment forming an integral part of the overall risk assessment. In practice, specialised human factors techniques may be applied efficiently in a separate sub-study.

The first stage of a human factors assessment is to make an inventory of all the operating tasks that are carried out in the activity under study. This is achieved through use of high-level task analysis, which identifies the main human tasks needed to meet the operational goals. It should consider not only in normal operations, but also emergency procedures, maintenance and recovery measures. It can be based on design information, operating procedures, past experience, observations or interviews with operators.

The second stage is to screen the task inventory to identify “safety-critical” tasks. These are the tasks that have the greatest impact on risk. Focussing the assessment on these tasks allows the level of detail in the assessment to be matched to the level of risk in the task. HRA (2000) outlines a method of assigning a criticality rating to offshore production and well operations tasks.

The next stage is to identify the specific human errors that may arise in the safety-critical tasks, together with their consequences. This may require a more detailed hierarchical task analysis, combined with a hazard identification technique such as hazard checklists, procedural HAZOP, or predictive human error analysis (HRA 2000). The errors can be classified in terms of the cause of the error, the potential for error-recovery (either by the operator or by another person) and the potential consequences of the error. The aim of this is to help focus on what can be done to reduce the risks.

In a qualitative assessment, the final stage is to select appropriate risk control measures, which will normally use expert judgement based on the identified error causes and consequences. Because human factors span a wide range of activities from daily operations through to senior management, risk control measures may be required at more than one level. This will include a basic focus on good ergonomic job design, the provision of competent individuals in the job, and the maintenance of good safety management and a positive safety culture.

2.6.4 Human Reliability Analysis

Human reliability analysis (HRA) consists of various techniques to estimate the probability of human error. It usually begins with a task analysis and human error analysis, and then uses various methods to estimate the probabilities of human error in the specific activity under study. The techniques of HRA are described by Humphreys (1998) and Kirwan (1994). It is appropriate for activities where large risks are sensitive to human errors, and where a quantitative treatment of human error is required for integration in a QRA. The human element is particularly important in emergency evacuation, and hence HRA may make a particularly important contribution to an EERA.

2.6.5 Training and Competence

On ships, requirements for crew training and qualifications are established by the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (IMO 1982). These state minimum international standards of competence and certification requirements for standard jobs on board ships. Individuals with the necessary certificates and experience are automatically considered competent for the specified job.

On offshore installations, where jobs are less standardised, it is appropriate to specify the required level of competence as part of the job description. The skills of each individual crew member should then be compared with the job requirements as part of their personal development plan, and an appropriate training programme should be developed for them. This process should be monitored and audited like any other aspect of safety management.

2.6.6 Safety Management Systems

The importance of managerial and organisational factors in accident causation has been shown in many disasters, notably *Piper Alpha*. It is widely acknowledged that well managed installations with comprehensive systems for training, safety reviews, operations and maintenance are generally more reliable and less prone to incidents than installations where the safety management system (SMS) is less developed.

The main elements that should be covered in the SMS were identified in the Cullen Report (Cullen 1990) including:

- Organisational structure
- Management personnel standards
- Training for operations and emergencies
- Safety assessment
- Design procedures

- Procedures for operations, maintenance, modifications and emergencies
- Management of safety by contractors
- The involvement of the workforce in safety
- Accident and incident reporting, investigation and follow-up
- Monitoring and auditing of the operation of the system
- Systematic re-appraisal of the system in the light of the experience of the operator and industry.

There are several published guidelines on good safety management practice, particularly in the chemical and marine industries (e.g. HSE 1997b). Most include lists of features similar to the above.

For offshore installations in UK waters, the Safety Case Regulations require the operator to have an adequate SMS in place, together with arrangements to audit it. The International Safety Management Code, adopted as part of the IMO Regulations on Safety of Life at Sea (SOLAS) will establish common international requirements on the SMS for mobile installations from 2002.

Risk assessments normally assume that an SMS is in place that will ensure safety management to a standard typical of similar installations. Some attempts have been made to reflect the actual safety management standard, as revealed by audits or minor incident experience, in the risk assessment of major accidents, but these are at an early stage of development and are rarely used.

3. DECISION MAKING

3.1 Overall Concept

The purpose behind almost any risk assessment is to support some form of decision making on safety matters. Decisions may be needed on issues such as:

- Whether or not an activity should be permitted.
- Whether measures are necessary to reduce its risks.
- Which of various options, involving different combinations of safety and expenditure, should be selected.
- How much should be invested in enhancing the safety of an installation.

To answer questions such as these, the decision-maker must decide when the activity or the installation is *safe enough*, i.e. when the risks are so low that further safety measures are not necessary.

The risks of accidents are not the only consideration when making decisions about safety standards on an installation. Operational, economic, social, political and environmental factors may be important too. The decision-making process must take account of the values of the company and the society, and may rely on engineering judgement, good practice and codes and standards. The importance of risk-based analysis to the decision depends on the decision context, as illustrated by the UKOOA decision support framework (Figure 1.5). This suggests that it has a significant role in many complex decisions, although rarely a dominant one.

Hence it is desirable for risk assessment to produce a clear view on the above issues, and on the question of "How safe is safe enough?" To answer this question, risk assessments use some form of "risk criteria". In the UK, these criteria are usually formulated within a framework of the ALARP principle.

3.2 The ALARP Principle

The ALARP principle originated as part of the philosophy of the UK Health and Safety at Work etc. Act 1974, which requires "every employer to ensure, so far as is reasonably practicable, the health, safety and welfare of all his employees". This remains the basis of the approach by the HSE for risk management in the UK.

The term "reasonably practicable" has a particular meaning drawn from legal precedent Asquith (1949):

> *"Reasonably practicable" is a narrower term than "physically possible" and implies that a computation must be made in which the quantum of risk is placed in the one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them - the risk being insignificant in relation to the sacrifice - the defendants discharge the onus on them [of proving that compliance was not reasonably practicable]. This computation falls to be made by the owner at a point of time anterior to the accident.*

In other words, employers are required to adopt safety measures unless the cost (in terms of money, time or trouble) is grossly disproportionate to the risk reduction. Once all such measures have been adopted, the risks are said to be ALARP.

Despite the references to "computation" in the legal judgement above, most decisions about reasonable practicability were based on subjective judgement of HSE inspectors, and on guidance published by the HSE to define what is reasonably practicable in specific areas. This arrangement was criticised in the Public Inquiry into siting a PWR at Sizewell (Layfield 1987):

> *The licence applicant often did not know what was expected of it, which could vary depending on the inspector concerned. Such inconsistency potentially leads to misallocation of resources, misunderstanding and confusion, and could mean that some aspects of the design are not as safe as they reasonably should be.*

In response, HSE published its tolerability of risk (TOR) framework, explaining its requirements as follows (HSE 1992):

> *Above a certain level, a risk is regarded as intolerable and cannot be justified in any ordinary circumstances. Below such levels, an activity is allowed to take place provided that the associated risks have been made as low as reasonably practicable. In pursuing any further safety improvements to demonstrate ALARP account can be taken of cost. It is in principle possible to apply formal cost-benefit techniques to assist in making judgements of this kind.*

In addition, the document suggested criteria to define the maximum tolerable and broadly acceptable individual risk levels, and presented a subtle concept of what is grossly disproportionate. These are discussed further in Sections 3.3 and 3.4 below.

In the more recent discussion document (HSE 1999a), the TOR framework is described in different words but remains broadly equivalent (Figure 1.4):

> *When assessing compliance with duties qualified by all injunctions embodying the concept of 'reasonable practicability' such as SFAIRP (so far as is reasonably practicable), ALARP (as low as reasonably practicable), ALARA (as low as reasonably achievable), it is now taken for granted that such duties have not been complied with if the regime introduced to control risks fails the 'gross disproportion' test. This is usually achieved by weighing each opportunity for an incremental reduction in risks against the presumed benefits in terms of the avoidance of injury.*

The criteria for maximum tolerable and broadly acceptable individual risk levels were unchanged, but the concept of what is grossly disproportionate was simplified, as discussed in Section 3.4 below

3.3 Risk Criteria

3.3.1 Definitions

Risk criteria are the standards used to help evaluate the significance of the results of a risk assessment in order to help with decision-making. They are also known variously as "acceptability criteria", "decision criteria", "screening criteria", "tolerability criteria" and "acceptance criteria".

When criteria are used to judge a particular activity as acceptable, this raises the question, "Acceptable to whom?" The judgements in the criteria are intended to reflect a broad consensus of people in the society, or at least those who consider risk assessment a helpful basis for decision-making. To emphasise this, the TOR framework uses the term "broadly acceptable". In reality, the judgements are usually made by regulators or company management on behalf of the workforce or public, but should be seen as judgements that could be justified to the public, assuming the issues were adequately explained.

It is impossible to represent with precision what is or is not acceptable to the public. This varies between individuals, and alters with time, accident experience and changing expectations of life. It is therefore a political judgement, and a risk criterion can only provide a crude indication of how people might react to a given risk.

It should be noted that, while future risks may be "acceptable", any major accident that occurs is inevitably seen as "unacceptable", however infrequent it may be, and typically acts as a trigger for risk reduction actions. Public statements by business leaders and politicians may promise that cost will not limit such actions, but in reality the choice of risk reduction measures is usually limited by a pragmatic evaluation of their costs and benefits. It is decisions such as these that risk criteria attempt to predict.

3.3.2 Tolerability and Acceptability

There have been several interpretations of the terminology of risk criteria, in which the terms "acceptable", "tolerable" and "justifiable" sometimes refer to different levels of risk and sometimes are used interchangeably.

In many cases, risk criteria are seen as dividing "unacceptable" risks from "acceptable" ones. However, the term "acceptable risks" is often inappropriate in the English language, because it implies that the person exposed has consented to receive the risks, and even regards them with favour.

The HSE introduced the concept of "tolerability" to avoid this problem, and explained it as follows (HSE 1992):

> *"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 means that we do not regard it as negligible or something we might ignore, but rather as something we need to keep under review and reduce further if and as we can. For a risk to be "acceptable" on the other hand means that for purposes of life or work, we are prepared to take it pretty well as it is.*

The HSE's terminology in effect places the various terms into an order, as follows:

Unacceptable/Intolerable	Highest
Tolerable	↑
Broadly acceptable/Insignificant	↑
Negligible	Lowest

3.3.3 Qualitative Criteria

When risks are expressed in qualitative form, the criteria to help evaluate their significance are usually expressed on a risk matrix. Such criteria are presented in the risk matrices in Section 2.3 and will not be repeated here. For consistency with the TOR framework, they should divide the matrix into "unacceptable", "tolerable" and "broadly acceptable" regions. The precise positioning of the bands is rather arbitrary, since the qualitative definitions of the frequency and consequence scale are too. The important message is that both high frequency and consequence are undesirable, and that low risk is only achieved by making both low.

Semi-quantitative approaches to risks, such as bow-tie analysis (Section 2.4) are not normally suitable to evaluate the acceptability of the risks. They are optimised to highlight the safeguards that are in place, and to ensure that suitable safeguards are considered for each hazard. By themselves, they do not provide a framework to evaluate whether the selected safeguards are sufficient. This may be done using engineering judgement based on good practice and available codes and regulations, but is best documented through a hazard assessment technique such as SWIFT or HAZOP.

3.3.4 Individual Risk Criteria

Individual risk criteria are intended to ensure that individual workers are not exposed to excessive risks. They are particularly useful for evaluating the significance of fatality risks, because individual risks are largely independent of the number of workers exposed, and hence in principle are comparable across different situations. This means that individual risk criteria developed by the HSE for workers onshore can also be applied to workers on offshore installations and ships.

HSE's guidelines on tolerability limits (i.e. their individual risk criteria) are (HSE 1999a):

Maximum tolerable risk for workers	10^{-3} per person-year
Maximum tolerable risk for the public	10^{-4} per person-year
Broadly acceptable risk	10^{-6} per person-year

The HSE criteria have been proposed for application to average individual risk on offshore installations as follows (Schofield 1993):

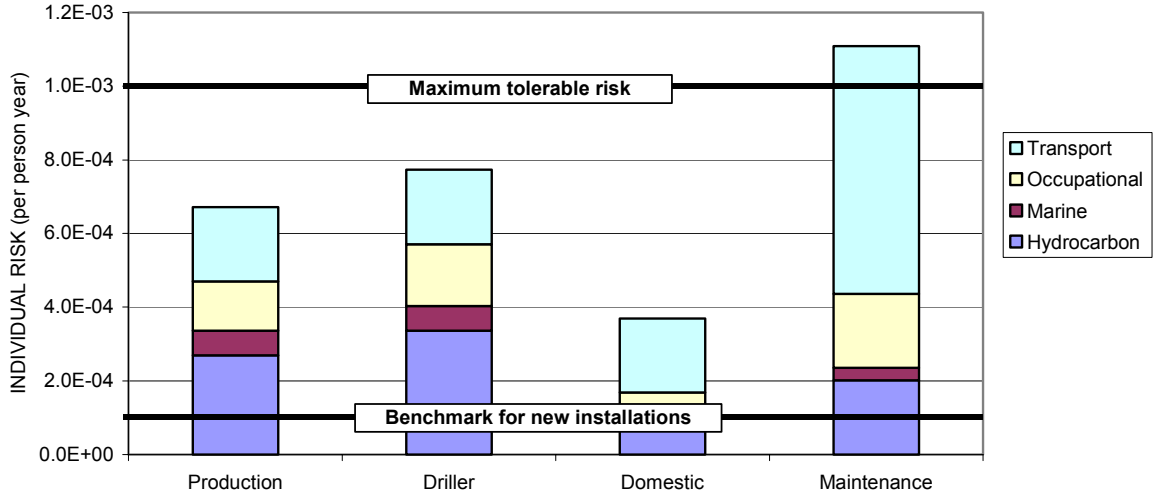
Maximum tolerable risk for installations in general	10^{-3} per person-year
Benchmark for new/modern installations	10^{-4} per person-year
Broadly acceptable for any installation	10^{-6} per person-year

To assist comparison with other criteria, these may be converted to FARs as described by CMPT (1999) for offshore workers:

Maximum tolerable risk for installations in general	30
Benchmark for new/modern installations	3
Broadly acceptable for any installation	0.03

Figure 3.1 illustrates how these criteria might be used to evaluate the risks from two different options.

Figure 3.1 Example Risk Evaluation



The bar chart shows risks for different individuals on a hypothetical installation. In this case the individual risk for maintenance workers exceeds the HSE tolerability limit. The breakdown shows that this is mainly due to transport and could not be corrected by reducing the marine risk. The risk for the other workers is within the ALARP region, but does not meet the benchmark for new installations.

It should be noted that none of the above are official HSE criteria for offshore installations. The assessment principles for offshore safety cases state (HSE 1998b):

> *Duty holders should set their own criteria for the acceptability and tolerability of total individual risk. However, it is common practice for the maximum tolerable level of individual risk of fatality to be set at 1 in 1000 per year, and for the broadly acceptable level of individual risk to be set in the range 1 in 100 000 to 1 in 1 million per year.*

The HSE (1998b) assessment principles clarify that the individual risk for comparison with the criteria should cover all risk contributors, including transport and occupational risk, as well as major accident hazards.

HSE (1998b) also state that the assessment should "take account of people exposed to exceptional risks". This means that the risks should be calculated for critical groups exposed to risks significantly higher than the average on the installation. They will evidently be more critical when evaluating the tolerability of risks than people with lower risks. This appears slightly more stringent than the R2P2 document (HSE 1999a), which states that the general tolerability limits refer to "any substantial category of workers for any large part of a working life", and hence might be exceeded by "fairly exceptional groups". It may be concluded that no workers in the offshore context are considered "fairly exceptional", since any hazardous

offshore occupations (e.g. divers, drillers, support vessel deck crew etc) are such "substantial" categories that 10^{-3} per year should be considered the maximum tolerable risk for them.

To show whether these are realistic criteria for offshore installations, they can be compared with actual offshore risks. The individual risks in the UK Sector averaged across all installations during 1977-91 were approximately 6×10^{-4} per year, with the 1991 level estimated to be somewhat lower at 4×10^{-4} per year (DNV Technica 1995). The individual risks on some installations averaged across all personnel on board approach (and sometimes exceed) 10^{-3} per year, but are well below this on most installations. Even allowing for variations in risk between different groups on an installation, the majority of people on the majority of installations should easily meet a criterion of 10^{-3} per year. The criterion might appear rather lenient for many installations. However, if used in combination with the ALARP requirement, few risks would actually approach this value.

3.3.5 Application to Marine Activities

The criteria above are intended to apply to the total risk to the worker while offshore, including hydrocarbon releases, marine hazards, transport accidents and occupational accidents. When considering marine hazards, it would be desirable to have a criterion to evaluate the risks from these alone, but unfortunately there is no acceptable level of risk from specific hazards - it depends entirely on what the total risk is. Clearly the risk would be unacceptable if the marine risk exceeded 10^{-3} per person-year, but it may also be unacceptable at much lower levels of marine risk if the other risk components are high. Even if the marine risk is 10^{-6} or less, it cannot be described as "acceptable", because this term applies only to the total risk.

If the other risks are unknown, a rough benchmark for marine risk can be obtained by using the proportion of risk from marine hazards in generic studies (e.g. DNV Technica 1995). However, this may be misleading, and at least a simple generic analysis of all other hazards is normally necessary before any judgement can be made about risk acceptability.

3.3.6 Group Risk Criteria

Group (or societal) risk criteria are intended to limit the total risk of death imposed by the installation on its workers and any third parties. If expressed on an FN diagram, group risk criteria may be used to limit the risk of major accidents involving large numbers of fatalities.

A difficulty arises if group risk criteria are applied to different sizes of development. A large installation, with a high production rate and many personnel on board (POB), usually has higher group risks than a smaller one. A constant group risk criterion would therefore be most strict for large installations, and might encourage dividing a development into several smaller installations, which might increase the total group risk.

The obvious solution to this difficulty is for the group risk criterion to take account of the benefits of the installation (in terms of energy production, jobs, tax revenues etc), but no suitable method of taking account of the value of an offshore installation has yet been developed. Schofield (1993) suggested a group risk criterion proportional to the POB. This in effect approximates the value of the installation by the number of personnel on board, and hence would be stricter for installations that achieve a large production with a minimum POB.

This above difficulties can be avoided if group risks are used for comparing alternatives for the same development. Then the production is the same for each option, and it is valid to prefer the one with the lowest group risks. This approach does not require any values for the criteria, but it does require a choice of form for comparing the group risks. In general, the annual fatality rate is used. In order to minimise high-fatality accident risks, FN diagrams might be preferred.

Overall, group risk criteria are desirable in principle, but in practice they are difficult to set. Most studies therefore use individual risk criteria together with cost-benefit analysis. Group risks are estimated and used in the cost-benefit analysis, but are not usually limited by specific group risk criteria.

3.3.7 Impairment Criteria

Impairment frequency criteria are a simple means of judging the risk to personnel on the platform, without requiring explicit fatality risk calculations. They are usually applied to safety evaluations of the concept design, where fatality risk estimates may not be available. They typically apply to impairment of the temporary refuge (TR) or other safety functions.

The HSE assessment principles for safety cases propose criteria as follows (HSE 1998b):

> *There should be sufficient evidence to demonstrate that the frequency with which accidental events will result in a loss of TR integrity within the minimum stated endurance time, does not exceed the order of 1 in 1000 per year. This frequency should be reduced to a lower level wherever this is reasonably practicable. Where the frequency is close to 1 in 1000 per year, there should be convincing arguments presented that it is not practicable to reduce it further*.

In the terminology of this guide, this is a maximum tolerable criterion of around 10^{-3} per year, with ALARP considerations applied below this level. This requirement only refers to impairment of the TR by fire, explosion, smoke and toxic gas, and hence does not appear to apply to marine hazards. However, it is considered applicable to any such fires etc resulting from marine hazards such as collisions or structural failures.

3.3.8 Strengths and Weaknesses of Risk Criteria

The strengths of risk criteria as a decision support tool are:

- They make interpretation of the results of a risk assessment explicit and traceable.
- They are widely used and discussed in different fields.

The weaknesses are:

- Quantitative criteria tend to be given undue weight in the decision-making, and it must be noted that they are only one input to it, and the final decision may not agree with the risk evaluation, once all relevant factors have been taken into account.

- Since the risk criteria are relatively well established, there may be a temptation to bias the results of the risk assessment in order to meet them. This is a particular danger when the regulator sets the criteria and the operator does the analysis. It is preferable for the operator to focus on using the assessment to support their own decision-making processes, rather than to justify residual risks to an external authority.

- The standard individual risk criteria refer only to the total risks, and are not applicable to the risks from individual hazards such as marine risks (see above).

- In most cases, the standard individual risk criteria show that the risks are tolerable if ALARP, and hence do not add much to the decision-making process.

3.4 Cost-Benefit Analysis

3.4.1 Purpose

Cost-benefit analysis (CBA) is a technique for comparing the costs and benefits of a project, developed to help appraise public sector projects. In safety assessment, it is usually used to assess *additional* safety measures on a project by comparing the cost of implementing the measure with the benefit of the measure, in terms of the risk-factored cost of the accidents it would avert.

The purpose of CBA is to show whether the benefits of a measure outweigh its costs, and thus indicate whether it is appropriate to implement the measure. CBA cannot provide a definitive decision, because factors other than risks and costs may be relevant, but it provides a useful guide.

Techniques of economic appraisal are available to estimate the costs of a measure. Normally, the time, effort and trouble involved can readily be expressed in cost units. Even measures that appear impracticable can often be represented by the cost of developing a practical implementation.

QRA allows an estimate of the benefits of safety measures, in terms of the risk-factored cost of the accidents they would avert. CBA now forms an important link between the QRA and general safety management.

3.4.2 Valuing Risks to Life

One of the most difficult issues in CBA of safety measures is how to balance costs with risks, when the two are in different units. Many types of risks can easily be expressed in monetary terms - for example, risks of property damage or business interruption. But risks to life are much more difficult to value. Risks of damage to the environment pose an even greater problem in this respect.

The standard approach to CBA of risks to life is to convert them into equivalent costs. The monetary valuation of risks to life is often described as placing a “value on life”. This phrase is convenient but distasteful, because no amount of money can compensate an individual for the loss of their life. In fact, CBA places a value on “averting a statistical fatality”. An averted statistical fatality may, for example, consist of a reduction in risk of death of 10^{-3} per year for each of 100 individuals over a period of 10 years. This distinction is important

because it is much more reasonable to place a value on small changes in risk than on death itself.

Figure 3.2 Example Calculation of Statistical Fatalities

A hypothetical risk reduction measure reduces the individual risk of 50 people on an installation from 5 x 10^{-4} per person-year to 4 x 10^{-4} per person-year. The lifetime of the installation is expected to be 20 years. How many statistical fatalities would the measure save?

The risk reduction is:
(5 x 10^{-4} - 4 x 10^{-4}) fatalities per person year x 50 people x 20 years = 0.1 statistical fatalities

Presentation of this difficult concept can be improved by using the term "value of preventing a statistical fatality" (VPF). This emphasises that what is being valued is the reduction in risk to many lives, rather than the actual lives that are at risk of being lost.

The advantage of this type of valuation is that the benefits of any safety measure (including reductions in risks to life, property, business interruption etc) can be expressed in common units, and subtracted from the costs of the measure in order to estimate the net financial saving. However, many people find this type of calculation distasteful, viewing risks to life as qualitatively different to financial risks, and not having simple monetary values.

An alternative approach, commonly adopted in modern risk assessments, is to express the risks and costs as a ratio, known as the implied cost of averting a fatality (ICAF), as follows:

$$\text{ICAF} = \frac{\text{Net cost of measure}}{\text{Reduction in fatality risks}}$$

This measure is dimensional, with units of £ spent per fatality averted (or equivalents in other currencies). This approach avoids "losing" the valuation of risks to life within the calculation, and keeps it explicit. But even so, a choice must still be made of an appropriate ICAF, in order to decide which measures to adopt.

3.4.3 Discounting Future Costs and Risks

In a conventional CBA, future costs and benefits are converted to present values, discounting those that occur in the future. Discounting financial quantities is justified because money is always more useful now than in the future, due to the opportunities to invest and make it grow. Discounting risks to life in the same way is much more questionable. It can be argued that it is better to reduce risks now than in the future, and so immediate risk reductions should be valued more highly than future ones. However, when considering the benefits of a given safety measure, it is not clear that the lives of present workers are any more valuable than the lives of future workers. In fact, given the progressive increase in real terms of the VPF used in decision-making, the reverse may be true. Discounting the cost of future fatalities is widely regarded as unethical.

In order to ensure a bias in favour of safety, it is preferable to calculate the ICAF from lifetime risk benefits (with no discounting) and the present value of costs (with conventional discounting):

$$\text{ICAF} = \frac{\text{Present value of lifetime cost of measure}}{\text{Reduction in lifetime statistical fatalities}}$$

In theoretical terms, this is rather inconsistent, but in practical terms it produces a reasonable solution to this difficult issue.

Figure 3.3 Example Calculation of Present Value

A hypothetical risk reduction measure has an initial capital cost of £100,000 and an annual maintenance cost of £5,000 per year. Its lifetime is expected to be 20 years. The company uses an internal real discount rate of 6% per annum. What is the present value cost of the measure?

The present value cost of a measure is:

$$PV = C_o + C_k (1 - (1 + r)^{-L})/r$$

where:

- PV = *present value of cost*
- r = *discount rate (per year)*
- L = *project life (years)*
- C_o = *initial cost*
- C_k = *cost in year k (for k=1 to L)*

In this case, the present value is

$$PV = £100,000 + £5000 \times 11.5 = £157,000$$

3.4.4 Gross Disproportion

Under the ALARP principle (Section 3.2), risk reduction measures should be adopted unless their cost is "grossly disproportionate" to the benefit gained.

In its original version of the tolerability of risk framework, HSE included the requirement that (HSE 1992):

> *In weighing the costs of extra safety measures the principle of reasonable practicability (ALARP) applies in such a way that the higher or more unacceptable a risk is, the more, proportionately, an employer is expected to spend to reduce it.*

In its more detailed guidance on CBA, HSE (1992) stated that gross disproportion "takes the form of a multiplier applied to the value of the health and safety benefits and increasing with the level of risk". HSE did not wish to specify what such multipliers should be, but suggested that the point of rapidly diminishing marginal returns should be intuitively obvious.

Although sound in principle, this concept is difficult to apply in practice, and very few companies have made use of it. In its latest discussion document, HSE has removed this concept from the TOR framework, and gives much more vague guidance as follows (HSE 1999a):

> *The test of 'gross disproportion' when weighing risks against costs implies that, at least, there is a need to err on the side of safety in the computation of safety costs and benefits. In short, case law requires that there should be a transparent bias on the side of health and safety. The acceptance of this bias is fundamental to conformity with the law. Moreover, the extent of the bias (i.e. the relationship between action and risk) has to be argued in the light of all the circumstances applying to the case and the precautionary approach that these circumstances warrant. Our general approach is that as a rule, whenever possible, standards should be improved or at least maintained.*

Practical interpretations of this are presented in the next section.

3.4.5 Cost-Benefit Criteria

When CBA is used to compare the costs and benefits of safety measures, the Department of the Environment, Transport and the Regions (DETR) uses a VPF up-rated annually in line with GDP per capita. In 1998 this had reached £1.0 million (DETR 1998).

This has been used by most other UK Government Departments. HSE uses the DETR value as a "benchmark", but "regard higher values as being appropriate for risks for which there is high aversion, e.g. those which give rise to high levels of societal concern or individual risk" (HSE 1999a). Elsewhere, HSE has argued that the VPF for major hazards that produce significant societal risks cannot be less than 3 times the VPF for individual risks (HSE 1996a). This is consistent with an earlier study (ACDS 1991), which used a VPF of £2m, adding a gross disproportion factor of 4 to the then road VPF of £0.5m. A similar approach based on the current DETR VPF would now give £4m.

In the offshore industry, VPFs for decision-making purposes have been in the range £1m - 10m, although few have been published:

- BP used a range of values of £0.6m to 6m (Beaumont 1995). Risk reduction measures costing less than £0.6m per life saved would proceed without question; between £0.6m and £6m a measure would only proceed if no better alternative were available.

- Shell adopted guidelines in the form of costs to avert a fatality that are linked to the individual risk levels. In general, risk reduction measures costing less than £5m per life saved are presented to management for consideration (Kennedy 1993).

CMPT (1999) suggested that if the ICAF were less than £1m, the measure would be cost-effective, and hence reasonably practicable even if individual risks were low, and would normally be adopted. If ICAF were in the range £1m to £10m, the measure would not be cost-effective, but might be considered reasonably practicable, especially if the individual risks were high in the ALARP zone. If the ICAF exceeded £10m, the measure would not be considered reasonably practicable, and the money could usually be spent more effectively on other safety measures.

Nevertheless, some safety measures that have been adopted in the past have involved ICAF values much higher than £10m. This may reflect higher VPFs, aversion to high-fatality accidents, or it may result from company or societal values dominating the decision.

Figure 3.4 Example Calculation of ICAF

A hypothetical risk reduction measure reduces the annual fatality rate on an installation by 0.01 statistical fatalities per year and has a present value cost of £2,000,000. The lifetime of the installation is expected to be 20 years. The maximum individual risk on the installation is 10^{-4} per year. Should the measure be implemented?

The implied cost of averting a fatality (ICAF) if the measure were implemented would be:

$$ICAF = \frac{£2,000,000}{0.01 \times 20} = £10 \text{ million per fatality averted}$$

A measure with ICAF £10 million would not normally be implemented unless the individual risk was at the top of the ALARP region, which it is not in this case. However, the decision should also take account of technical standards, established good practice, engineering judgement and company or societal values, any of which might provide over-riding justification for the measure.

3.4.6 Strengths and Weaknesses of Cost-Benefit Analysis

The strengths of cost-benefit analysis as a decision support tool are:

- CBA takes account of two of the most important factors in many decisions on safety measures, namely cost and safety. It makes the analysis of these factors explicit and traceable.
- CBA has been adopted to standardise investments on safety within the UK government, and by IMO and classification societies, as well as being widely used by offshore companies.
- CBA can be applied specifically to marine activities, since it is able to consider the costs and benefits of a specific measure without knowing the risks on the installation as a whole.

The weaknesses are similar to those for risk criteria (Section 3.3.8), but also include:

- Monetary valuation of risks to life is widely considered unethical, and presentation of CBA results may provoke antagonistic reactions.
- Many factors cannot be adequately converted into financial units, and it is important that these are given adequate weight in the decision-making process, alongside the CBA results.

3.5 Demonstration of ALARP

3.5.1 Choice of Approach

The approach needed to show whether risks are ALARP will depend on the decision type, as indicated in the UKOOA framework (Section 1.5.2). It is not necessary to use CBA or QRA to demonstrate whether risks are ALARP, but these are likely to have some degree of input to many decisions, and may be particularly important for decisions involving risk trade-offs.

3.5.2 Qualitative Approach

The quantitative approach to showing whether the risks on an installation or in an activity are ALARP involves the following steps:

1. Identify each hazard and ensure that appropriate safeguards are adopted. Provided that the installation/activity is based on established practice (UKOOA decision context Type A - Figure I.5) and follows applicable rules, codes and good safety management practices, the risks may be assumed tolerable if ALARP.

2. Identify a complete range of practicable risk reduction measures, based on best modern practice.

3. Each measure should be implemented unless it is demonstrated that the measure is not reasonable practicable. This demonstration must show that the money, time and trouble involved in implementing it would be grossly disproportionate to the benefit obtained. In the qualitative approach this argument must be based on structured judgement.

4. Once all measures have either been implemented (or the company is committed to implementing them) or demonstrated to be not reasonably practicable, the risks are ALARP.

3.5.3 Quantitative Approach

The quantitative approach to showing whether the risks on an installation or in an activity are ALARP involves the following steps:

1. Estimate the risks and compare with appropriate risk criteria. If they exceed the maximum tolerable criterion, then measures must be taken to make them tolerable; otherwise operations must cease. If they are broadly acceptable, the risks are ALARP and no further risk reduction measures need be considered, provided appropriate diligence is applied to maintain risks in this region. If they are in the ALARP region, continue as follows.

2. Identify a complete range of practicable risk reduction measures, based on best modern practice, focusing primarily on large risk contributors.

3. Each measure should be implemented unless it is demonstrated that the measure is not reasonable practicable. In the quantitative approach, this argument should be based on CBA. The demonstration should be robust against uncertainties in the risk estimates and in the treatment of aversion to high-fatality accidents (CMPT 1999).

4. Once all measures have either been implemented (or the company is committed to implementing them) or demonstrated to be not reasonably practicable, the risks are ALARP.

3.5.4 The Positive Use of QRA

The wording of the definition of ALARP and the approach to demonstrating it described above seem to suggest that QRA and CBA should be used primarily to demonstrate that measures that have not been adopted are not reasonably practicable. This negative approach sometimes results in QRA being used to explain why some safety measures are *not* adopted, while qualitative arguments are considered sufficient to explain why other measures *are* adopted. Such approaches have contributed to a loss of faith in the QRA process, and HSE (1998b) states that “particular attention should be paid to a safety case which uses QRA arguments to justify not implementing identified risk reduction measures”.

The suggested solution to this is that, where it is appropriate to use QRA, it should be used to evaluate all major safety measures, including those that are adopted as well as those that are not. This will avoid creating the negative impression described above. It will also show the ICAF of typical measures that are adopted on mainly judgemental grounds, and so make the decision-making process more transparent. When measures are rejected, based on a combination of quantitative and judgemental inputs, it will then give more authoritative support to the decision.

3.5.5 The Role of Technical Standards

Technical standards issued by classification societies, IMO, national authorities and industry bodies underpin the design of many aspects of most offshore installations. These standards have been developed, partly in response to accident experience, using the expertise of the industry, and represent the results of what is in effect a qualitative process of risk assessment. However, judged as a risk assessment, the process has been rather unstructured and there is rarely adequate documentation of why particular measures are specified and which rules are applicable to non-standard installations. In the future, these standards are likely to be based on FSA (Section 1.5.4), which may overcome some of these limitations.

The aim of the technical standards is to ensure that, provided the installation is used for a standard application under good safety management, the risks will be ALARP. However, it is an established part of good safety management to make use of risk assessment to identify hazards and minimise risks. Compliance with technical standards provides a sound design basis for standard offshore installations, but does not replace risk assessment altogether.

HSE (1996b) summarises the balance of technical standards and risk assessment required in the UK as follows:

> *It is expected that the design of the installation will be based on current good engineering practice. It should, however, be appropriately risk-based and compliance solely with existing codes, standards and guidance may not be sufficient to meet the regulatory requirements. Requirements for systematic and explicit consideration of risks have been introduced by MHSWR, SCR, PFEER and PUWER. These risk assessments can be expected to contribute to design considerations, for instance through the setting of risk-based performance standards Such risk assessments, however, may not need to be quantitative: qualitative assessments may be more appropriate in some circumstances, e.g. in the absence of appropriate failure or incident data.*

The requirement for at least qualitative risk assessment is also illustrated in the UKOOA framework (Figure 1.5). Even for Type A decisions, there is a role for engineering judgement (i.e. qualitative risk assessment), although technical standards provide the majority of the input to the decision. For Type B and C decisions, there is a greater role for risk-based analysis (i.e. QRA and CBA), and a reduced role for technical standards. Standard offshore installations, such as semi-submersible and jack-up drilling units, could be considered Type A. Many offshore marine installations, such as FPSOs are likely to be Type B. Some novel installations could be considered Type C.

Limits to the validity of technical standards can be determined where they are based on modern structured approaches, such as documented failure experience and safety studies for generic types of installation. If the installation under consideration deviates significantly from

the design of the generic type on which the rules were based, a detailed risk assessment should be carried out. This may be used to derive design accidental loads or performance standards to be used in the design, and to show that the installation as designed attains acceptable overall safety. In modern offshore classification rules, this type of risk assessment is explicitly recognised as a technique complementary to the use of technical standards.

3.6 Uncertainty in Decision-Making

The results of a risk assessment are inevitably uncertain. The choice of decision-making criteria is also uncertain in many cases. The combined uncertainty may be rather greater than the difference between the risk result and the decision criterion. How should this influence the evaluation of the risks?

There are two standard approaches to this question - a classical risk approach and a Bayesian approach. Although in concept the two approaches sound rather different, their practical results are the same in many cases.

A classical (or traditional) approach considers the best-estimates of risk and the preferred decision criteria, in order to obtain a basic evaluation of the risk. It then considers the uncertainty in the two, in order to evaluate how confident the analysts are in their conclusion. It might conclude, "the safety measure appears cost-effective, but this is very sensitive to certain key assumptions". The decision-maker would then be expected to take account of the fact that the uncertainties made the risk assessment unreliable, and would probably be forced to rely more on judgement.

A Bayesian approach considers uncertainty as an intrinsic component of the risk, which cannot be meaningfully separated from it. It might conclude, "there is a probability of 0.5 that the benefits of the safety measure will outweigh the costs". The quoted probability takes account of all relevant uncertainties and reflects the analyst's degree of belief in the conclusion. Again, such a conclusion would lead the decision-maker to rely on other inputs.

These examples show that considering uncertainty in the evaluation provides valuable additional information concerning the reliability of the risk assessment's input to the decision. This "reliability" may be considered the likelihood that an independent analysis of the same subject would reach the same conclusion. It indicates the weight that should be given to the risk assessment in the decision-making.

If uncertainties are not considered, and this information is not provided to decision-makers, there is a danger that they will consider it to be fully reliable. This may result in inappropriate decisions being made, and if further risk assessments are later performed, yielding different conclusions with apparently equal certainty, it may cause a loss of confidence in the risk assessment technique.

There is widely held concern about the opposite danger, that providing information about the reliability of a risk assessment, which is often rather low, will itself cause a loss of confidence in the technique. This may arise from a belief that risk assessment must give a clear-cut decision about safety measures, rather than contribute to a more complex decision, and from paying inadequate attention to the benefits of learning from the risk assessment process.

3.7 Benefits Beyond Decision-Making

It is a common experience in performing risk assessments that the *process* of performing a risk assessment yields greater benefits than the final risk results. The relatively small importance of the risk results arises from the uncertainties that are inevitably attached. The results tend to be more important in a novel application of risk assessment, where risk estimates have not previously been available. As more and more risk assessments of similar installations or activities are carried out, the differences in the risk results are often seen to arise more from differences in methodology than from actual differences in the installations, and their significance decreases.

The much larger importance of the risk assessment process arises from the creative yet systematic thought process that is necessary to produce risk estimates. Risk assessment imposes a discipline on the analysts to consider the safety of an installation or activity in great detail, to think about what might go wrong and what is available to prevent or mitigate it, and to consider the relevance of previous accident experience. Properly performed, this process yields a great understanding of the installation and its safety features, often with useful insights into ways that safety might be improved. Even if no new cost-effective safety measures are identified, the process provides reassurance that an important and reasonably practical step has been taken to anticipate what might go wrong and what could be done to prevent it.

A particular benefit arises from the consideration of the role of safeguards (i.e. risk reduction measures incorporated into the design) in achieving acceptable safety. Consideration of these is particularly important in the HAZID and in the semi-quantitative approach to risk, as well as some approaches to QRA, although it tends to be obscured in the approaches based on historical frequencies. This provides important input to the safety management system, for example by suggesting the performance standards required from key safeguards, highlighting training needs, providing input to emergency planning etc.

These benefits explain why most modern safety management systems include a requirement for a risk assessment, and why it is such an important component of the offshore safety regime.

3.8 Suitable and Sufficient Risk Assessment

In general, HSE require a risk assessment to be "suitable and sufficient". The meaning of this phrase varies slightly in different contexts, but the following definitions are considered appropriate for marine hazards.

"Suitable" means that "the assessment technique chosen should be appropriate to the assessment being made" (HSE 1998a).

"Sufficient" means that the assessment is adequate to show that risks are ALARP, and does not require further elaboration. In most HSE guidance, it requires the presentation of the risk assessment in the Safety Case to be sufficient for HSE to understand why particular safety measures have been adopted. The use of this term in the SCR (para 165) is slightly different and hardly distinct from "sufficient".

4. REFERENCES

ACDS (1991), "Major Hazard Aspects of the Transport of Dangerous Substances", Health and Safety Commission, Advisory Committee on Dangerous Substances, HMSO.

Ambion (1997), "Approaches to Hazard Identification", Ambion Consultants, Offshore Technology Report OTO 97 068, Health & Safety Executive, HSE Books.

Asquith, Lord Justice (1949) in Edwards v National Coal Board, 1 KB 704; 1949 1 All ER 743 p712 and p747, a case on the interpretation of S 102 (8) of the Coal Mines Act, 1911.

AUPEC (1999), "Evaluation of the offshore safety legislative regime", Aberdeen University Petroleum and Economic Consultants Ltd (AUPEC); Health and Safety Executive (HSE). Safety Policy Division.

Aven (1992), "Reliability and Risk Analysis", Elsevier Applied Science, London.

Beaumont, J. (1995), "Clyde & Seillean", presentation to Safety Case Preparation, The Industry Responds, Fire and Blast Information Group Technical Review Meeting, The Steel Construction Institute, Ascot, UK

Boisson, P (1999), "Safety at Sea: Policies, Regulations and International Law", Bureau Veritas, Paris

Bolsover, A.J. & Wheeler, M. (1999), "Decision-Making to Treat an Explosion Hazard", Conference on Safety on Offshore Installations.

Boyle, P. & Smith, E.J. (2000), "Emergency Planning using the HSE's Evacuation, Escape and Rescue (EER) HAZOP Technique", Hazards XV, Symposium Series No.147, Institution of Chemical Engineers, Rugby.

CCPS (1992), "Guidelines for Hazard Evaluation Procedure", 2nd edition, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

CCPS (1989), "Chemical Process Quantitative Risk Analysis", Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

CMPT (1999), "A Guide to Quantitative Risk Assessment for Offshore Installations", Centre for Maritime and Petroleum Technology, London. ISBN 1 870553 365.

Comer, P.J., Fitt, J.S. & Ostebo, R. (1986), "A Drillers' HAZOP Method", Paper SPE 15876, European Petroleum Conference, Society of Petroleum Engineers, London.

DETR (1998), "1998 Valuation of the Benefits of Prevention of Road Accidents and Casualties", Highways Economics Note No1: 1998, Department of the Environment, Transport and the Regions.

DNV Technica (1995), "An Overview of Risk Levels in the Offshore Industry on the UK Continental Shelf (1994)", HSE Offshore Technology Report OTH 94 458, HMSO.

DNV (1999), “Semi-Submersible Flooding Incident Data”, Offshore Technology Report OTO 1999 016, Health & Safety Executive.

DNV (1998), “Worldwide Offshore Accident Databank Statistical Report 1998), Det Norske Veritas, Høvik, Norway.

DNV Technica (1995), “An Overview of Risk Levels in the Offshore industry on the UK Continental Shelf”, Offshore Technology Report OTH 94 458, Health & Safety Executive.

Dovre Safetec (1999), “Effective Collision Risk Management for Offshore Installations”, Offshore Technology Report OTO 1999 052, Health & Safety Executive.

E&P Forum (1996), “Quantitative Risk Assessment Datasheet Directory”, Report 11.8/250, E&P Forum, London.

Howard, R.A. & Matheson, J.E. (1981), “Influence Diagrams”, SRI International, Menlo Park, California, USA. Reprinted in “Readings on the Principles and Applications of Decision Analysis”, Strategic Decisions Group, Stanford University, 1984.

HRA (2000), “Human Factors Assessment of Safety Critical Tasks”, Human Reliability Associates, Offshore Technology Report OTO 1999 092, Health & Safety Executive.

HSE (1999a), “Reducing Risks, Protecting People”, Discussion Document, Health & Safety Executive.

HSE (1999b), “Reducing Error and Influencing Behaviour”, HSG 48, Health and Safety Executive, HSE Books, Sudbury, UK.

HSE (1998a), “A Guide to the Offshore Installations (Safety Case) Regulations 1992”, Health & Safety Executive, HSE Books.

HSE (1998b), “Assessment Principles for Offshore Safety Cases”, HS(G)181, Health & Safety Executive, HMSO.

HSE (1998c), “Five Steps to Risk Assessment”, INDG163, Health and Safety Executive, HSE Books, Sudbury, UK.

HSE (1997a), “The Costs of Accidents at Work”, HSG 96, Health and Safety Executive , HSE Books, Sudbury, UK.

HSE (1997b), “Successful Health and Safety Management”, HSG 65, Health and Safety Executive , HSE Books, Sudbury, UK.

HSE (1996a), “The Use of Risk Assessment within Government Departments”, Health and Safety Executive, HMSO.

HSE (1996b), “A Guide to the Integrity, Workplace Environment and Miscellaneous Aspects of the Offshore Installations and Wells (Design and Construction, etc) Regulations 1996”, L85, Health and Safety Executive, HMSO.

HSE (1992), "The Tolerability of Risk from Nuclear Power Stations", Health and Safety Executive, HMSO.

Humphries, P. (1995), "Human Reliability Assessor's Guide", Human Factors in Reliability Group, Report SRDA - R11, AEA Technology.

IMO (1997), "Interim Guidelines for the Application of Formal Safety Assessment (FSA) to the IMO Rule-Making Process", Marine Safety Committee MCS/Circ.829, International Maritime Organization, London.

IMO (1982), "International Convention on Standards of Training, Certification and Watchkeeping for Seafarers 1987", International Maritime Organization, London.

ISO (1999), "Petroleum and Natural Gas Industries - Offshore Production Installations - Guidelines on Tools and Techniques for the Identification and Assessment of Hazardous Events", Draft International Standard ISO 17776, International Organization for Standardization.

Kennedy, B. (1993), "ALARP in Practice - An Industry View", Offshore Safety Cases Conference, HSE, Aberdeen.

Kirwan, B. (1994), "A Guide to Practical Human Reliability Assessment", Taylor & Francis, London.

Layfield, F. (1987), "Sizewell B Public Inquiry Report", HMSO.

Lees, F.P. (1996), "Loss Prevention in the Process Industries", 2nd edition, Butterworth-Heinemann, Oxford.

Mansfield, D., Poulter, L. & Kletz, T. (1996) "Improving Inherent Safety", Offshore Technology Report OTH 96 521, Health & Safety Executive, HSE Books.

OBB/Technica (1988), "Comparative Safety Evaluation of Arrangements for Accommodating Personnel Offshore", Report OTN 88 175, Department of Energy.

PAFA (2000), "Review of Greenwater & Waveslam Design & Specification Requirements for FPSO/FSUs", PAFA Consulting Engineers, Offshore Technology Report OTO 2000 004, Health & Safety Executive.

Pitblado, R. & Turney, R. (1995), "Risk Analysis in the Process Industries", European Federation of Chemical Engineers, Institution of Chemical Engineers, Rugby, UK.

Reason, J. (1991), "The Reliability of Management in Decision Making", Seminar Reliability, The Risk of Management, IMechE, London.

RM Consultants (1995), "A Methodology for Hazard Identification on EER Assessments", Offshore Technology Report OTH 95 466, Health & Safety Executive, HSE Books.

Schofield, S.L. (1993), "A Framework for Offshore Risk Criteria", Safety and Reliability, vol 13, no 2.

Tangen, H.D. (1987), “A Classification Society’s View of the Way Ahead”, Conference on Ro-Ro Safety & Vulnerability: The Way Ahead, RINA, London.

UKOOA (2000), “Guidelines for Quantitative Risk Assessment Uncertainty”, UK Offshore Operators Association, London.

UKOOA (1999), “A Framework for Risk Related Decision Support”, UK Offshore Operators Association, London.

APPENDIX I - GLOSSARY

Acceptability criteria - another term for risk criteria (q.v.).

Acceptable risks are risks considered insignificant and not justifying further effort to reduce them.

Accidental events - another term for failure cases (q.v.).

Accidents are sudden unintended departures from normal operating conditions in which some degree of harm is caused.

Annual fatality rate (AFR) is the long-term average number of fatalities per year.

As low as reasonably practicable (ALARP) describes the approach to health and safety management required by the UK Health & Safety at Work Act (Section 3.2)

Availability is the proportion of time that a component or system is performing as intended.

Basic events are fundamental inputs at the bottom of each branch of a fault tree.

Best-estimate refers to the most probable value of a parameter.

Broadly acceptable risks are risks considered acceptable by consensus among people in society, in particular those who find such concepts helpful in decision-making.

Conditional probability is the chance of an event occurring given that specified previous events have occurred.

Confidence range (or confidence interval) is the range within which the true value of a parameter might lie.

Consequences are the expected effects of an event occurring. In QRA, it usually means the size of the zone within which fatalities are expected, or the number of deaths.

Conservative refers to approaches tending to err on the side of high risk estimates.

Cost-benefit analysis (CBA) is a technique for comparing the costs and benefits of a measure, usually in financial terms (Section 3.4).

Decision criteria - another term for risk criteria (q.v.).

Escape may refer to movement on the platform away from the area affected by an incident, or the process of leaving the platform via the sea.

Evacuation is the planned method of leaving the installation in an emergency.

Evacuation, Escape and Rescue Analysis (EERA) is a type of risk analysis applied to evacuation etc.

Event is a non-specific term used to describe any incident, accident, failure case or outcome as appropriate.

Event tree analysis (ETA) is a technique to illustrate or quantify the various events that may follow from one initiating event (Section 2.6.7)

Failure is when a system fails to perform its intended function.

Failure cases are representations in a risk assessment of the range of possible accidents which might occur in reality.

Failure criteria define the conditions of heat and blast causing failure of items of structure or equipment.

Failure rate is the mean number of failures per unit time.

Failure modes and effects analysis (FMEA) - an earlier form of FMECA (q.v.).

Failure modes, effects and criticality analysis (FMECA) is a systematic review of a mechanical system, identifying failure modes and considering the effects of failures at each point (Section 2.3.6)

Fatal accident rate (FAR) is the number of fatalities per 10^8 exposed hours.

Fault tree analysis (FTA) is a technique to illustrate or quantify the various events and component failures that may combine to cause one critical top event (Section 2.6.6).

Frequency is the number of occurrences of an event per unit time. In QRA, it is usually expressed as the frequency per year.

Gross disproportion is a bias in favour of safety when assessing what is reasonable practicable (q.v.) (Section 3.4.4).

Group risk is the risk experienced by the whole group of people exposed to the hazard. It is often expressed as the relationship between the frequency and the number of people affected by an event.

Harm is the adverse impact of accidents, such as sickness, injuries, deaths, damage to property, degradation of the environment, or interruption of business.

Hazards are situations with a potential for causing harm (q.v.) (Section 2.3.1).

Hazard and operability study (HAZOP) is a method of identifying hazards that might affect safety and operability, using systematic critical group review structured by the use of guidewords, usually applied to a process plant design (Section 2.3.5).

Hazard assessment is sometimes treated as meaning the same as risk assessment, and sometimes as meaning the same as hazard analysis. In this guide, it is taken to mean a qualitative form of risk assessment (Section 2.3.1).

Hazard checklist is a written list of questions or designed to prompt consideration of safety issues.

Hazard identification (HAZID) is the process of identifying hazards (q.v.) (Section 2.3).

Hazardous activities are industrial processes, such as offshore installations, with inherent hazards.

Hazard register is a record of hazards identified by various HAZID techniques (Section 2.6).

Hazard review is a mainly intuitive hazard identification technique (Section 2.3.3).

Human reliability analysis (HRA) is the analysis of the human contribution to system failures (Section 2.7.2).

Hydrocarbons are mixtures of materials whose chemical structure is based on hydrogen and carbon. They include well fluid, gas, oil and condensate.

Hydrocarbon events are spills and releases of hydrocarbons. They include blowouts, riser leaks and process leaks.

Implied cost of averting a fatality (ICAF) is the expenditure on a safety measure divided by the number of statistical fatalities (q.v.) averted by it.

Incidents are relatively minor accidents, i.e. unintended departures from normal operating conditions in which little or no harm was caused.

Individual risk is the frequency (usually per year) at which a single individual is expected to suffer a given level of harm (usually death) due to specific hazards.

Influence diagrams are graphical representations of the probabilistic dependence between the various factors that influence the outcome of an event (Section 2.3.8).

Likelihood is the probability or frequency (q.v.) of an event occurring.

Major accidents are accidents involving several fatalities at once, severe damage to the installation, or major oil pollution.

Major hazards are hazardous activities with a potential for causing major accidents, i.e ones involving several fatalities at once, severe damage to the installation, or major oil pollution.

Marine hazards is a term used to describe the focus of the present guide on hazards on offshore installations other than those due to drilling, hydrocarbon releases, diving or transportation (Section 1.2).

Mitigation refers to measures of minimising the consequences of an accident after it has started. It is sometimes used loosely to refer to all types of risk reduction.

Negligible risks are risks so small that there is no cause for concern about them, and no reason to take action to reduce them.

Potential loss of life (PLL) is the predicted long-term average number of fatalities in a given time period. "PLL per year" is another term for annual fatality rate (q.v.).

Probability is the chance of an event occurring in specific circumstances. It is a number between 0 and 1.

Procedural HAZOP is a version of HAZOP (q.v.) applied to operational procedures.

Quantitative risk assessment (QRA) is a means of estimating and evaluating numerical risks from a particular hazardous activity such as an offshore platform. It involves identifying the hazards that are present, making numerical estimates of their frequencies and consequences, and evaluating the significance of the risk results.

Reasonably practicable means that the cost (in terms of money, time or trouble) involved in implementing a measure is not grossly disproportionate (q.v.) to the benefit gained (Section 3.2)

Reliability is the probability that a component or system is able to perform its required function for a given period of time or for a given demand.

Reliability analysis is a set of techniques for identifying possible failure modes in a system and for estimating the likelihood of failure.

Rescue is the process of picking up personnel from the sea and returning them to a safe place.

Risk is the combination of likelihood and consequence of hazards being realised, i.e. the chance of a specific event occurring within a specific period.

Risk analysis is the quantification of risks without making judgements about their significance. It involves identifying hazards and estimating their frequencies and consequences, so that the results can be presented as risks.

Risk assessment is a means of making a systematic evaluation of the risk from hazardous activities, and making a rational evaluation of their significance, in order to provide input to a decision-making process. This may be qualitative or quantitative.

Risk criteria are standards to help evaluate the significance of risk results. They relate quantitative risk estimates to qualitative value judgements about the significance of the risks.

Risk estimation - another term for risk analysis (q.v.)

Risk evaluation involves assessing the significance (and sometimes the acceptability) of the estimated risks. It may use risk criteria or cost-benefit analysis of possible risk reduction measures to show whether the risks are as low as reasonably practicable.

Risk management is the making of decisions concerning the risk, and the subsequent implementation of the decisions in the safety management system (Section 2.4).

Safety is the absence of risk. It usually refers to the safety of humans or property from acute hazards, i.e. accidents, and so excludes health hazards.

Safety case is a document demonstrating the adequacy of safety management arrangements for an installation.

Safety management system is the set of arrangements in place to manage the safety of a hazardous activity.

Sensitivity is the degree to which results of a calculation (such as a QRA) are affected by variations in the inputs.

Societal risk - another term for group risk (q.v.).

Statistical fatality is a small change in risk for many people amounting to an expectation of one fatality (Section 3.4.2).

Structured what-if checklist technique (SWIFT) is a method of identifying hazards using structured brainstorming (Section 2.3.7).

Sufficient means that the risk assessment and safety case are adequate to show that risks are ALARP, and do not require further elaboration.

Suitable means that the risk assessment technique chosen should be appropriate to the assessment being made.

Temporary refuge is a place on an offshore installation where people will be adequately protected from hazards while awaiting evacuation.

Tolerable risks are risks that the exposed people are expected to bear without undue concern, once all reasonably practicable reduction measures have been adopted (Section 3.3.2).

Top event is the critical event at the top of a fault tree.

Uncertainty is the degree of doubt about parameters or results in a QRA.

Uncertainty analysis is the process of quantifying the uncertainties in the risk results.

Value of statistical life (VOSL) is the expenditure that can be justified to prevent one statistical fatality (q.v.).

Value of preventing a statistical fatality (VPF) - another term for value of statistical life (q.v.).

ABBREVIATIONS

AFR	annual fatality rate
ALARP	as low as reasonably practicable
CBA	cost-benefit analysis
CCPS	Center for Chemical Process Safety
CMPT	Centre for Maritime and Petroleum Technology
EER	evacuation, escape and rescue
EERA	evacuation, escape and rescue analysis
ETA	event tree analysis
FAR	fatal accident rate
FMEA	failure modes and effects analysis
FMECA	failure modes, effects and criticality analysis
FN	frequency-number of fatalities
FPS	floating production system
FPSO	floating production, storage and off-loading
FSA	formal safety assessment
FTA	fault tree analysis
GDP	gross domestic product
HAZID	hazard identification
HAZOP	hazard and operability study
HMSO	Her Majesty's Stationery Office
HRA	human reliability analysis
HSE	Health & Safety Executive
HSWA	Health & Safety at Work etc Act 1974
ICAF	implied cost of averting a fatality
IMO	International Maritime Organisation
IR	individual risk
MODU	mobile offshore drilling unit
P&ID	piping and instrumentation diagram
PFEER	Prevention of Fire and Explosion and Emergency Response
PLL	potential loss of life
POB	people on board
PWR	pressurised water reactor
QRA	quantitative risk assessment
SCR	Offshore Installations (Safety Case) Regulations 1992
SMS	safety management system
SRA	structural reliability analysis
SWIFT	structured what-if checklist technique
TOR	tolerability of risk framework
TR	temporary refuge
UK	United Kingdom
UKCS	United Kingdom Continental Shelf
UKOOA	United Kingdom Offshore Operators Association
VOSL	value of statistical life
VPF	value of preventing a statistical fatality
WOAD	World-wide Offshore Accident Databank

APPENDIX II - WORKED EXAMPLES

Chapter 2 outlined the wide variety of risk assessment approaches that are in use in the marine industry. The selection of the right approach is important if the depth of treatment and accuracy is to match the requirement for a "suitable and sufficient" risk assessment.

In order to make the selection clearer, the five worked examples in this section cover several real marine problems as might be encountered at different stages of the life-cycle. The examples show for each which might be the best approach and give reasons.

The meaning of "suitable and sufficient" was defined in the Glossary. **Suitable** means that the risk assessment technique chosen should be appropriate to the assessment being made**. Sufficient** means that the risk assessment and safety case are adequate to show that risks are ALARP, and do not require further elaboration**.**

In this context then "suitable and sufficient" means that the operator has selected an approach that matches the data availability at that stage of the lifecycle, and has used this approach with adequate rigour to be able to demonstrate that risks are "as low as reasonably practicable". Additionally, the safety case description of the assessment undertaken should be of adequate detail so that a technically trained assessor can verify the approach as appropriate and the result as correct within acceptable uncertainty.

The overall framework diagram showing all the options is given in the figure below. In general, options towards the upper rows of this table are less detailed and options lower down are more detailed.

Key Drivers **Risk Assessment Approach Selection**

Lifecycle Stage	Major Hazard Potential	UKOOA Decision Context	Hazard Identification Technique	Risk Approach	Technique and ALARP Demo	Decision Making
Concept Design Operations Abandonmen	Catastrophic loss possible Significant number of people Significant environmental potential	Type A Nothing new Well understood Established practice Type B Lifecycle issues Some risk trade-offs Deviation from established practice Major cost issues Type C Very novel Stakeholder views Major risk trade-offs Perception of lowering stds	Judgement FMEA SWIFT HAZOP	Class Rules Design Std Engineering Judgement Risk Analysis a) Qualitative b) Semi-Quant c) Quantitative Value systems	Simple tabulation Risk Matrix QRA structure + Barriers QRA evaluation Historical data / FTA / ETA / Consequence Stakeholder Consultations	Design team Judgement Cost Benefit Analysis Senior Management Judgement

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. The following examples attempt to clarify these points.

Example 1: Concept stage: Decision to use Shuttle tanker vs Pipeline

At Concept Stage, most information relates to project parameters (eg. product pricing, flowrates, estimated lifetime, cost of money, etc) and little engineering detail is finalised. The different concepts can throw up significant safety issues, but these must be assessed at a simpler level, essentially demonstrating the concept can be made to work and be ALARP, but with the final details of how this would be achieved in practice postponed until Detail Design.

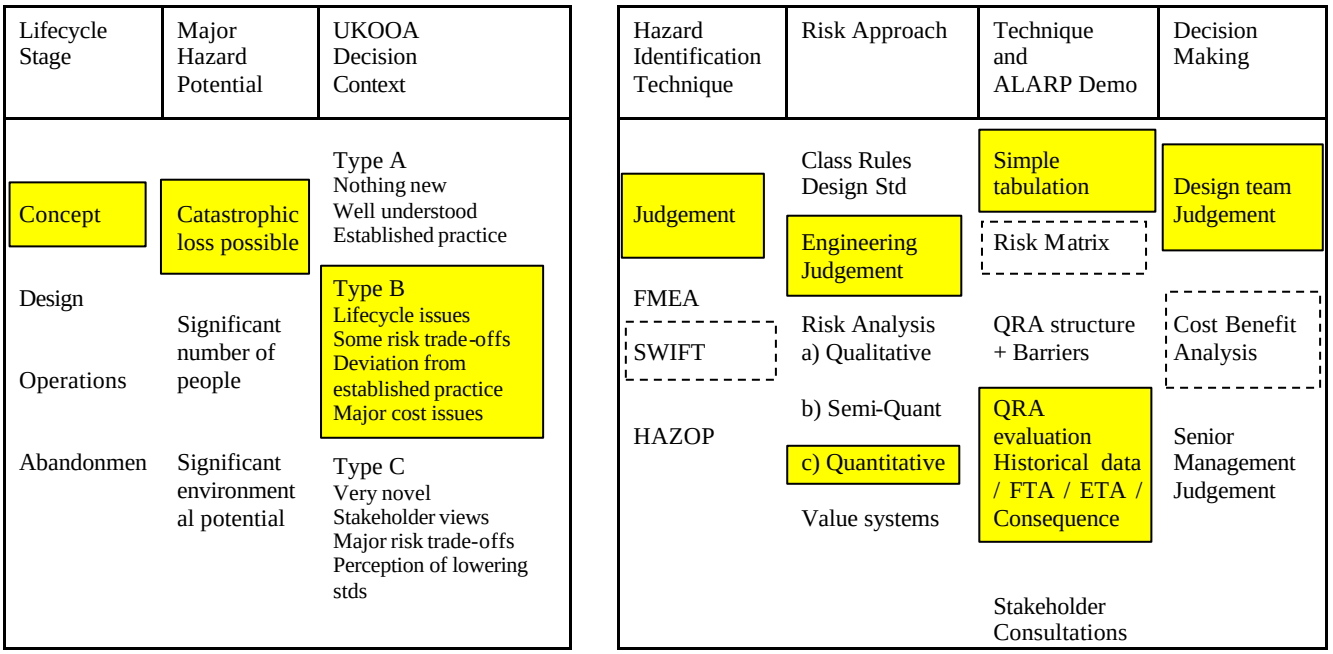
At its simplest, the Concept decision here is to select between two options: either to use a shuttle tanker or a pipeline to transport produced oil to onshore processing. The shuttle tanker option will normally require additional processing / stabilisation on the platform, and create greater risks associated with the extra processing, mooring, transfer, and subsequent voyage hazards. The pipeline option is more expensive and requires a suitable balance between flowrates and distance to become feasible, but risks generally are lower.

In order to select the optimum concept, it may be appropriate to consider refined options, such as a short pipeline to a remote tanker loading point. In principle, such a design may emerge naturally from the risk assessment process. For example, a high-level hazard identification of the shuttle tanker option may identify shuttle tanker collision as a key hazard, for which a solution might be using a submerged turret mooring. In practise, it is preferable that the concept options used as a basis for the decision should incorporate good current practice at the outset, otherwise a biased comparison may result.

The suggested approach meeting the suitable and sufficient test might be as follows:

Lifecycle Stage:	Concept stage
Major Hazard Potential:	Catastrophic loss possible - especially environmental risks associated with shuttle tanker.
Decision Context:	This would be Type B (in UKOOA terms) with Lifecycle issues with some risk clear trade-offs between the pipeline and shuttle options.
Hazard ID technique:	As no substantive engineering detail is available, the identification technique would most likely be judgement based, using where possible lessons from previous similar facilities. Techniques such as FMEA and HAZOP cannot be applied without engineering drawings, however SWIFT could be an option, and would enhance the documentation of the judgement based identification.
Risk Approach:	The risk approach could be judgement based due to the lack of detail. If so, the factors considered should be diverse - safety and environmental risks, reputation, costs, etc and be listed in a clear tabulation (a little like the Best Practicable Environmental Option approach of the Environment Agency). Alternatively, an outline quantitative analysis may be preferable.
Technique:	In a judgemental approach, the technique can be purely descriptive, although some operators might use qualitative risk ranking (risk matrix) and make explicit rough estimates for likelihood and consequences of each option. A quantitative approach would use generic risk data characteristic of the two concept options.

Decision Making: This would normally by a Design Team decision, with referral to the Senior Management for approval. As a catastrophic incident is possible with these options it could be that Senior Management involvement might be greater than normal. An outline cost-benefit analysis would be a possible way to evaluate the results of a quantitative approach where there is a risk-cost trade-off.



Example 2: Design Stage: Stability for MODU – concern about exposed Atlantic Frontier location (high wind and wave loadings)

The issues here are primarily technical in nature and address whether past designs, developed for less exposed waters, are suitable for the tougher conditions in the Atlantic Frontier. At this stage of the lifecycle, engineering design details will be readily available, and environmental conditions would be forecast and assessed. As stability is the particular issue, then catastrophic loss is a potential concern.

Lifecycle Stage: Design stage

Major Hazard Potential: Catastrophic loss of the MODU is possible if a stability issue arose.

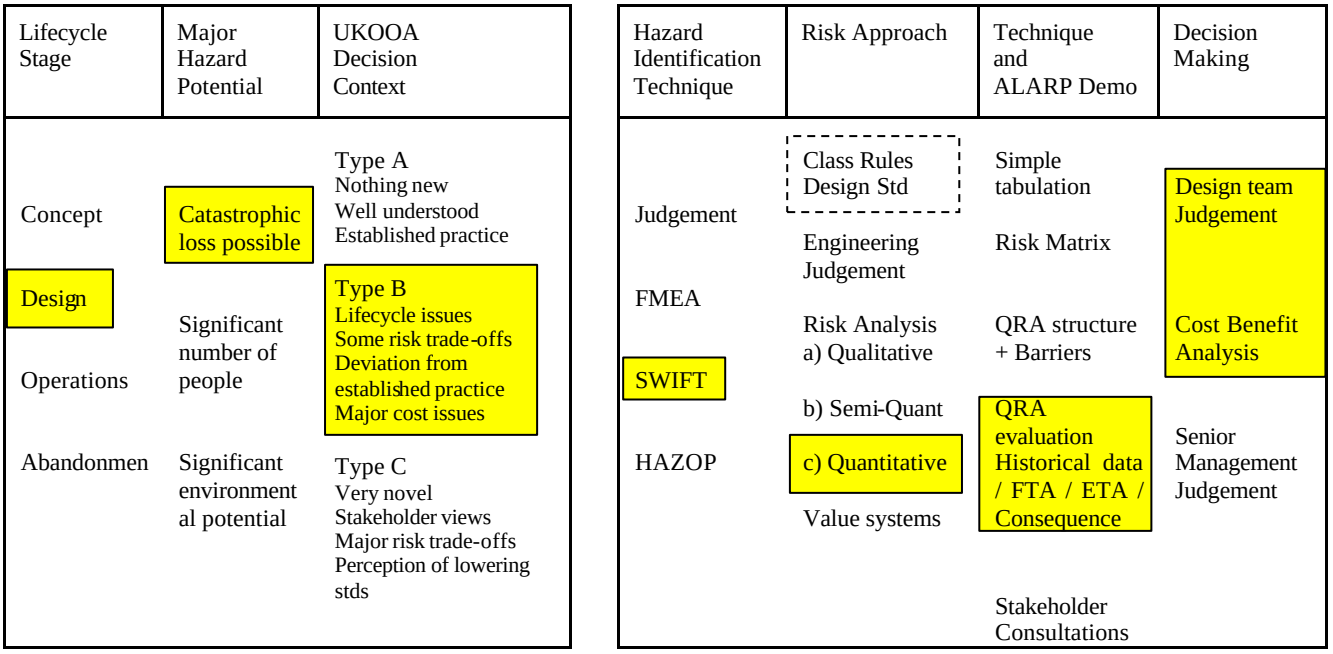
Decision Context: This would be Type B. It is clearly not Type A as issues for this location are not yet “established practice”, on the other hand they are not “very novel” either as the conditions and expected loads are reasonably predictable.

Hazard ID technique: The issues for Stability would best be addressed using a what-if checklist approach such as SWIFT, with the checklist addressing past accidents. Alternatives such as FMEA and HAZOP are not optimal for such stability problems.

Risk Approach: The risk approach would be based on Classification Rules and other design guidance (e.g. 4th Edition). As catastrophic loss is at issue, the residual risks in Class designs should be quantified. The input data is available in this case and a lesser approach, such as relying entirely on Class Rules, would not be considered sufficient balanced against the potential scale of loss.

Technique: The approach would emp loy QRA techniques, probably using historical data and some fault and event tree analysis to establish probabilities of defined MODU consequences (including catastrophic loss).

Decision Making: The decision here is technical and would normally be taken by the design team, using the QRA results as input to a cost-benefit analysis.



Example 3: Operations Phase - hardware issue: Mooring failure Southern North Sea (moderate loads, long experience)

This problem is related to the previous one, and again is primarily technical in nature - this time a mooring issue. The equipment has been in service for some time and the sea conditions in this area are well understood.

Lifecycle Stage: Operations stage

Major Hazard Potential: A loss of mooring could result in the vessel drifting into collision with nearby structures - with significant loss of life or environmental consequences.

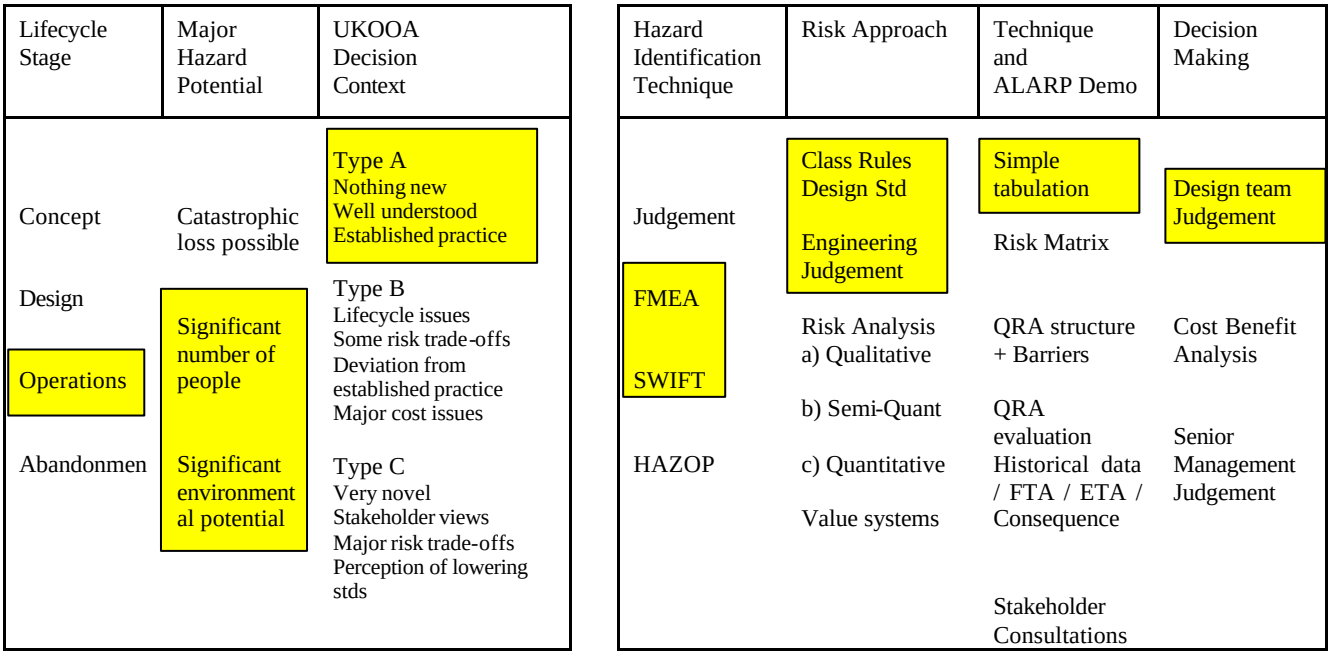
Decision Context: This is a well established operation and little that is new. This is a Type A decision in UKOOA terms.

Hazard ID technique: The issues in this problem relate mainly to technical matters. The technique will have access to good drawings and operational experience and ideally would be team based. The problem is not so well suited to HAZOP as it is to SWIFT or FMEA.

Risk Approach: Technical causes of mooring failure are covered well by Classification Rules and these would be the primary basis for the analysis. The operating environment is within normal Classification experience. The hazard identification may show that procedural failures are a major cause of in-service failures, and engineering judgement is needed to adopt appropriate safeguards

Technique: Simple tabulation of the measures taken and the Classification Rules followed will normally be sufficient.

Decision Making: The Design Team would do this. There is no special issue requiring the judgement of Senior Management.



Example 4: Operations Phase - organisational issue: Reduced manning, and enhanced evacuation arrangements, allows reduced number of TEMPSC for evacuation

This problem relates to an organisational change that reduces manpower and through better procedures allows for a reduction in lifeboats. The risk assessment must show that the changed arrangements do not adversely affect safety and that risks for the new arrangements are ALARP.

Lifecycle Stage: Operations stage

Major Hazard Potential: If arrangements do not work satisfactorily then there could be significant loss of life.

Decision Context:	The issues here relating to demanning do involve clear risk trade-offs and the impression of a lowering of existing standards as lifeboats are being removed. There is a need to involve stakeholders (here the workforce) and demonstrate to them the suitability of the revised arrangements. This makes this a UKOOA Type C decision.
Hazard ID technique:	The hazard identification technique should be formal and team based and either SWIFT or HAZOP would be appropriate. SWIFT is an obvious technique for this application and HAZOP has been applied increasingly for evacuation assessments. FMEA is poor for human factors issues and is unsuitable here.
Risk Approach:	The approach here should be a combination of QRA and Value-based assessment (involving stakeholders' views). Data is readily available allowing quantification, but a numerical approach alone would be inappropriate for this type of apparent safeguards reduction.
Technique:	This would be a combination of standard QRA tools (historical data, fault and event trees) and Stakeholder consultations.
Decision Making:	In view of the likely contentious nature of the lifeboats reduction, the decision making would be a combination of Cost-Benefit Analysis (based on the QRA results) and Senior Management Judgement to deal with the stakeholder views.

Lifecycle Stage	Major Hazard Potential	UKOOA Decision Context
Concept	Catastrophic loss possible	Type A Nothing new Well understood Established practice
Design	Significant number of people	Type B Lifecycle issues Some risk trade-offs Deviation from established practice Major cost issues
Operations		
Abandonmen	Significant environmental potential	Type C Very novel Stakeholder views Major risk trade-offs Perception of lowering stds

Hazard Identification Technique	Risk Approach	Technique and ALARP Demo	Decision Making
Judgement	Class Rules Design Std	Simple tabulation	Design team Judgement
FMEA	Engineering Judgement	Risk Matrix	
SWIFT	Risk Analysis a) Qualitative	QRA structure + Barriers	Cost Benefit Analysis
HAZOP	b) Semi-Quant	QRA evaluation Historical data / FTA / ETA / Consequence	Senior Management Judgement
	c) Quantitative Value systems	Stakeholder Consultations	

Example 5: Abandonment phase: Sailing into Portsmouth harbour for break-up by a contractor company (normally servicing the Royal Navy) and subsequent landfill

This problem is a mixture of two issues, one a relatively straightforward technical matter (the navigation and break-up) and the other a contentious disposal of potentially contaminated materials. There are clear risks associated with navigation of large offshore structures into busy southern ports unused to these activities and their break-up also by staff unfamiliar with these structures. However, the issues are well known and suitable prior planning based on well founded risk assessment should ensure risks are ALARP. The disposal aspect is not so easily addressed by purely technical analysis. Community trust needs to be established as there will be concerns about long term contamination issues. The risk assessment for this aspect needs stakeholder involvement - in this case the community.

Lifecycle Stage:	Abandonment stage
Major Hazard Potential:	As the marine structure is not in operation and will have been made safe for disposal, the main issue relates to environmental contamination.
Decision Context:	The disposal of offshore marine structures is very contentious in the UK after Brent Spar and the high degree of recycling achieved for disposal of the Viking platform. Disposal here to landfill would be seen as a lowering of standards and requiring major stakeholder consultations as to what level of disposal would be acceptable. This is therefore a UKOOA Type C decision.
Hazard ID technique:	The risks associated with the navigation and vessel break-up would be well reviewed using the SWIFT technique. This is a team-based checklist driven technique that can address the issues raised here. It could also be used to document the alternatives to landfill and identify risks associated with those alternatives.
Risk Approach:	The navigation and break-up risk assessment would be well handled using Engineering Judgement. The Value System review would be appropriate for the disposal aspects.
Technique:	Stakeholder discussions are the main activity in this category and this is to achieve a good understanding of what the community sensitivities would be in this case. Until more experience is gained there is no alternative to group discussions.
Decision Making:	The Design Team would decide on navigation and break-up alternatives. The disposal to landfill issue would necessarily involve Senior Management, who would base that decision on the outcome of the stakeholder interviews and an analysis of the alternative disposal options.

Lifecycle Stage	Major Hazard Potential	UKOOA Decision Context
Concept	Catastrophic loss possible	Type A Nothing new Well understood Established practice
Design	Significant number of people	Type B Lifecycle issues Some risk trade-offs Deviation from established practice Major cost issues
Operations		
Abandonment	Significant environmental potential	Type C Very novel Stakeholder views Major risk trade-offs Perception of lowering stds

Hazard Identification Technique	Risk Approach	Technique and ALARP Demo	Decision Making
Judgement	Class Rules Design Std	Simple tabulation	Design team Judgement
	Engineering Judgement	Risk Matrix	
FMEA	Risk Analysis a) Qualitative	QRA structure + Barriers	Cost Benefit Analysis
SWIFT	b) Semi-Quant	QRA evaluation Historical data / FTA / ETA / Consequence	Senior Management Judgement
HAZOP	c) Quantitative		
	Value systems		
		Stakeholder Consultations	

Conclusion

The meaning of "suitable and sufficient" risk assessment can be difficult as the degree of information available and the uncertainties vary through life and by the nature of the risk decision. The aim here has been to show that there needs to be a clear rationale for the approach adopted and this should balance the needs with the tools available.

The approach adopted should be appropriate to the problem with the aim of practicality and fit-for-purpose. For major hazard issues or ones which are contentious this is unlikely to be the simplest approach and may well involve stakeholder consultations. For lower hazard, well established problems with few novel features a simple approach will usually be the most effective.

Printed and published by the Health and Safety Executive
C0.50 4/02

MAIL ORDER
HSE priced and free
publications are
available from:
HSE Books
PO Box 1999
Sudbury
Suffolk CO10 2WA
Tel: 01787 881165
Fax: 01787 313995
Website: www.hsebooks.co.uk

RETAIL
HSE priced publications
are available from booksellers

HEALTH AND SAFETY INFORMATION
HSE InfoLine
Tel: 08701 545500
Fax: 02920 859260
e-mail: hseinformationservices@natbrit.com
or write to:
HSE Information Services
Caerphilly Business Park
Caerphilly CF83 3GG

HSE website: www.hse.gov.uk

OTO 2001/063

£ 15.00

ISBN 0-7176-2231-2