INTERNATIONAL MARITIME ORGANIZATION
4 ALBERT EMBANKMENT
LONDON SE1 7SR

Telephone: 020 7735 7611
Fax: 020 7587 3210
Telex: 23588 IMOLDN G

IMO

E

Ref. T1/3.02
T5/1.01

MSC/Circ.1023
MEPC/Circ.392
5 April 2002

GUIDELINES FOR FORMAL SAFETY ASSESSMENT (FSA) FOR USE IN THE IMO RULE-MAKING PROCESS

1 The Maritime Safety Committee, at its seventy-fourth session (30 May to 8 June 2001), and the Marine Environment Protection Committee, at its forty-seventh session (4 to 8 March 2002), approved Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process as set out at annex.

2 FSA is a rational and systematic process for assessing the risks relating to maritime safety and the protection of the marine environment and for evaluating the costs and benefits of IMO's options for reducing these risks. The use of FSA is consistent with, and should provide support to, the IMO decision-making process. It provides a basis for making decisions in accordance with resolutions A.500(XII) "Objectives of the Organization in the 1980's", A.777(18) "Work Methods and Organization of Work in Committees and their Subsidiary Bodies" and A.900(21) “Objectives of the Organization in the 2000s”.

3 Application of FSA may be particularly relevant for proposals for regulatory measures which have far reaching implications in terms of costs to the maritime industry or the administrative or legislative burdens which may result. This is achieved by providing a clear justification for proposed regulatory measures and allowing comparison of different options of such measures to be made. This is in line with the basic philosophy of FSA in that it can be used as a tool to facilitate a transparent decision-making process. In addition, it provides a means of being proactive, enabling potential hazards to be considered before a serious accident occurs.

4 Member Governments and non-governmental organizations are invited to apply FSA, when it is deemed necessary, in accordance with the annexed Guidelines and to submit the results thereof to the Organization in accordance with the Standard Format for Reporting shown in appendix 8 of the Guidelines.

5 This circular supersedes MSC/Circ.829-MEPC/Circ.335 on Interim Guidelines for the application of Formal Safety Assessment (FSA) to the IMO rule-making process.

***

ANNEX

GUIDELINES FOR FORMAL SAFETY ASSESSMENT (FSA) FOR USE IN THE IMO RULE-MAKING PROCESS

Table of Contents

List of figures

List of appendices

GUIDELINES FOR FORMAL SAFETY ASSESSMENT (FSA) FOR USE IN THE IMO RULE-MAKING PROCESS

1 INTRODUCTION

1.1 Purpose of FSA

1.1.1 Formal Safety Assessment (FSA) is a structured and systematic methodology, aimed at enhancing maritime safety, including protection of life, health, the marine environment and property, by using risk analysis and cost benefit assessment.

1.1.2 FSA can be used as a tool to help in the evaluation of new regulations for maritime safety and protection of the marine environment or in making a comparison between existing and possibly improved regulations, with a view to achieving a balance between the various technical and operational issues, including the human element, and between maritime safety or protection of the marine environment and costs.

1.1.3 FSA is consistent with the current IMO decision-making process and provides a basis for making decisions in accordance with resolutions A.500(XII) "Objectives of the Organization in the 1980's", A.777(18) "Work Methods and Organization of Work in Committees and their Subsidiary Bodies" and A.900(21) “Objectives of the Organization in the 2000s”.

1.1.4 The decision makers at IMO, through FSA, will be able to appreciate the effect of proposed regulatory changes in terms of benefits (e.g. expected reduction of lives lost or of pollution) and related costs incurred for the industry as a whole and for individual parties affected by the decision. FSA should facilitate the development of regulatory changes equitable to the various parties thus aiding the achievement of consensus.

1.2 Scope of the Guidelines

These Guidelines are intended to outline the FSA methodology as a tool, which may be used in the IMO rule-making process. In order that FSA can be consistently applied by different parties, it is important that the process is clearly documented and formally recorded in a uniform and systematic manner. This will ensure that the FSA process is transparent and can be understood by all parties irrespective of their experience in the application of risk analysis and cost benefit assessment and related techniques.

1.3 Application

1.3.1 The FSA methodology can be applied by:

.1 a Member Government or an organization in consultative status with IMO, when proposing amendments to maritime safety, pollution prevention and response-related IMO instruments in order to analyse the implications of such proposals; or

.2 a Committee, or an instructed subsidiary body, to provide a balanced view of a framework of regulations, so as to identify priorities and areas of concern and to analyse the benefits and implications of proposed changes.

1.3.2 It is not intended that FSA should be applied in all circumstances, but its application would be particularly relevant to proposals which may have far-reaching implications in terms of either costs (to society or the maritime industry), or the legislative and administrative burdens which may result. FSA may also be useful in those situations where there is a need for risk reduction but the required decisions regarding what to do are unclear, regardless of the scope of the project. In these circumstances, FSA will enable the benefits of proposed changes to be properly established, so as to give Member Governments a clearer perception of the scope of the proposals and an improved basis on which they take decisions.

2 BASIC TERMINOLOGY

The following definitions apply in the context of these Guidelines:

Accident:	An unintended event involving fatality, injury, ship loss or damage, other property loss or damage, or environmental damage.
Accident category:	A designation of accidents reported in statistical tables according to their nature, e.g. fire, collision, grounding, etc.
Accident scenario:	A sequence of events from the initiating event to one of the final stages.
Consequence:	The outcome of an accident.
Frequency:	The number of occurrences per unit time (e.g. per year).
Generic model:	A set of functions common to all ships or areas under consideration.
Hazard:	A potential to threaten human life, health, property or the environment.
Initiating event:	The first of a sequence of events leading to a hazardous situation or accident.
Risk:	The combination of the frequency and the severity of the consequence.
Risk contribution tree (RCT):	The combination of all fault trees and event trees that constitute the risk model.
Risk control measure (RCM):	A means of controlling a single element of risk.
Risk control option(RCO):	A combination of risk control measures.
Risk evaluation criteria:	Criteria used to evaluate the acceptability/tolerability of risk.

3 METHODOLOGY

3.1 Process

3.1.1 Steps

3.1.1.1 FSA should comprise the following steps:

.1 identification of hazards;

.2 risk analysis;

.3 risk control options;

.4 cost benefit assessment; and

.5 recommendations for decision-making.

3.1.1.2 Figure 1 is a flow chart of the FSA methodology. The process begins with the decision makers defining the problem to be assessed along with any relevant boundary conditions or constraints. These are presented to the group who will carry out the FSA and provide results to the decision makers for use in their resolutions. In cases where decision makers require additional work to be conducted, they would revise the problem statement or boundary conditions or constraints, and resubmit this to the group and repeat the process as necessary. Within the FSA methodology, step 5 interacts with each of the other steps in arriving at decision-making recommendations. The group carrying out the FSA process should comprise suitably qualified and experienced people to reflect the range of influences and the nature of the "event" being addressed.

3.1.2 Screening approach

3.1.2.1 The depth or extent of application of the methodology should be commensurate with the nature and significance of the problem. However, before starting the detailed application, a coarse application is suggested for the relevant ship type or hazard category, in order to include all aspects of the problem under consideration. Whenever there are uncertainties, e.g. in respect of data or expert judgment, the significance of these uncertainties should be assessed.

3.1.2.2 Characterization of hazards and risks should be both qualitative and quantitative, and both descriptive and mathematical, consistent with the available data, and should be broad enough to include a comprehensive range of options to reduce risks.

3.1.2.3 A hierarchical screening approach may be utilized. This would ensure that excessive analysis is not performed by utilising relatively simple tools to perform initial analyses, the results of which can be used to either support decision-making (if the degree of support is adequate) or to scope/frame more detailed analyses (if not). The initial analyses would therefore be primarily qualitative in nature, with a recognition that increasing degrees of detail and quantification will come in subsequent analyses as necessary.

3.1.2.4 A review of historical data may also be useful as a preparation for a detailed study. For this purpose a loss matrix may be useful. An example can be found in figure 2.

3.2 Information and data

3.2.1 The availability of suitable data necessary for each step of the FSA process is very important. When data are not available, expert judgment, physical models, simulations and analytical models may be used to achieve valuable results. Consideration should be given to those data which are already available at IMO (e.g. casualty and deficiency statistics) and to potential improvements in those data in anticipation of an FSA implementation (e.g. a better specification for recording relevant data including the primary causes, underlying factors and latent factors associated with a casualty).

3.2.2 Data concerning incident reports, near misses and operational failures may be very important for the purpose of making more balanced, proactive and cost-effective legislation. A judgement on the value of data which can be collected should be carried out in order to identify uncertainties and limitations, and to assess the degree of reliance that should be placed on the available data.

3.3 Incorporation of the human element

3.3.1 The human element is one of the most important contributory aspects to the causation and avoidance of accidents. Human element issues throughout the integrated system shown in figure 3 should be systematically treated within the FSA framework, associating them directly with the occurrence of accidents, underlying causes or influences. Appropriate techniques for incorporating human factors should be used.

3.3.2 The human element can be incorporated into the FSA process by using human reliability analysis (HRA). Guidance for the use of HRA within FSA is given in appendix 1 and diagrammatically in figure 4. To allow easy referencing the numbering system in appendix 1 is consistent with that of the rest of the Guidelines.

3.4 Evaluating regulatory influence

It is important to identify the network of influences linking the regulatory regime to the occurrence of the event. Construction of Influence Diagrams may assist (see appendix 3).

4 PROBLEM DEFINITION

4.1 Preparation for the study

The purpose of problem definition is to carefully define the problem under analysis in relation to the regulations under review or to be developed. The definition of the problem should be consistent with operational experience and current requirements by taking into account all relevant aspects. Those which may be considered relevant when addressing ships (not necessarily in order of importance) are:

.1 ship category (e.g. type, length or gross tonnage range, new or existing, type of cargo);

.2 ship systems or functions (e.g. layout, subdivision, type of propulsion);

.3 ship operation (e.g. operations in port and/or during navigation);

.4 external influences on the ship (e.g. Vessel Traffic System, weather forecasts, reporting, routing);

.5 accident category (e.g. collision, explosion, fire); and

.6 risks associated with consequences such as injuries and/or fatalities to passengers and crew, environmental impact, damage to the ship or port facilities, or commercial impact.

4.2 Generic model

4.2.1 In general, the problem under consideration should be characterized by a number of functions. Where the problem relates for instance to a type of ship, these functions include carriage of payload, communication, emergency response, manoeuverability, etc. Alternatively, where the problem relates to a type of hazard, for instance fire, the functions include prevention, detection, alarm, containment, escape, suppression, etc.

4.2.2 For application of FSA, a generic model should therefore be defined to describe the functions, features, characteristics and attributes which are common to all ships or areas relevant to the problem in question.

4.2.3 The generic model should not be viewed as an individual ship in isolation, but rather as a collection of systems, including organizational, management, operational, human, electronic and hardware aspects which fulfill the defined functions. The functions and systems should be broken down to an appropriate level of detail. Aspects of the interaction of functions and systems and the extent of their variability should be addressed.

4.2.4 A comprehensive view, such as the one shown in figure 3, should be taken, recognizing that the ship's technical and engineering system, which is governed by physical laws, is in the centre of an integrated system. The technical and engineering system is integrally related to the passengers and crew which are a function of human behaviour. The passengers and crew interact with the organizational and management infrastructure and those personnel involved in ship and fleet operations, maintenance and management. These systems are related to the outer environmental context, which is governed by pressures and influences of all parties interested in shipping and the public. Each of these systems is dynamically affected by the others.

4.3 Results

The output of the problem definition comprises:

.1 problem definition and setting of boundaries; and

.2 development of a generic model.

5 FSA STEP 1 - IDENTIFICATION OF HAZARDS

5.1 Scope

The purpose of step 1 is to identify a list of hazards and associated scenarios prioritized by risk level specific to the problem under review. This purpose is achieved by the use of standard techniques to identify hazards which can contribute to accidents, and by screening these hazards using a combination of available data and judgement. The hazard identification exercise should be undertaken in the context of the functions and systems generic to the ship type or problem being considered, which were established in paragraph 4.2 by reviewing the generic model.

5.2 Methods

5.2.1 Identification of possible hazards

5.2.1.1 The approach used for hazard identification generally comprises a combination of both creative and analytical techniques, the aim being to identify all relevant hazards. The creative element is to ensure that the process is proactive and not confined only to hazards that have materialized in the past. It typically consists of structured group reviews aiming at identifying the causes and effects of accidents and relevant hazards. Consideration of functional failure may assist in this process. The group carrying out such structured reviews should include experts in the various appropriate aspects, such as ship design, operations and management and specialists to assist in the hazard identification process and incorporation of the human element. A structured group review session may last over a number of days. The analytical element ensures that previous experience is properly taken into account, and typically makes use of background information (for example applicable regulations and codes, available statistical data on accident categories and lists of hazards to personnel, hazardous substances, ignition sources, etc.). Examples of hazards relevant to shipboard operations are shown in appendix 2.

5.2.1.2 A coarse analysis of possible causes and outcomes of each accident category should be carried out by using established techniques (examples are described in appendix 3), to be chosen according to the problem in question.

5.2.2 Ranking

The identified hazards and their associated scenarios relevant to the problem under consideration should be ranked to prioritize them and to discard scenarios judged to be of minor significance. The frequency and consequence of the scenario outcome requires assessment. Ranking is undertaken using available data, supported by judgement, on the scenarios. A generic risk matrix is shown in figure 5. The frequency and consequence categories used in the risk matrix have to be clearly defined. The combination of a frequency and a consequence category represents a risk level. Appendix 4 provides an example of one way of defining frequency and consequence categories, as well as possible ways of establishing risk levels for ranking purposes.

5.3 Results

The output from step 1 comprises:

.1 a list of hazards and their associated scenarios prioritized by risk level; and

.2 a description of causes and effects.

6 FSA STEP 2 - RISK ANALYSIS

6.1 Scope

6.1.1 The purpose of the risk analysis in step 2 is a detailed investigation of the causes and consequences of the more important scenarios identified in step 1. This can be achieved by the use of suitable techniques that model the risk. This allows attention to be focused upon high risk areas and to identify and evaluate the factors which influence the level of risk.

6.1.2 Different types of risk (i.e. risks to people, the environment or property) should be addressed as appropriate to the problem under consideration. Measures of risk are discussed in appendix 5.

6.2 Methods

6.2.1 The construction and quantification of fault trees and event trees are standard risk assessment techniques that can be used to build a risk model (see appendix 3). An example of a conceptual risk model is the Risk Contribution Tree (RCT) as shown in figure 6. Whilst the example makes use of fault and event tree techniques, other established methods could be used if appropriate.

6.2.2 Quantification makes use of accident and failure data and other sources of information as appropriate to the level of analysis. Where data is unavailable, calculation, simulation or the use of recognized techniques for expert judgement may be used.

6.3 Results

The output from step 2 comprises the identification of the high risk areas which need to be addressed.

7 FSA STEP 3 - RISK CONTROL OPTIONS (RCOs)

7.1 Scope

7.1.1 The purpose of step 3 is to propose effective and practical RCOs comprising the following four principal stages:

.1 focusing on risk areas needing control;

.2 identifying potential risk control measures (RCMs);

.3 evaluating the effectiveness of the RCMs in reducing risk by re-evaluating step 2; and

.4 grouping RCMs into practical regulatory options.

7.1.2 Step 3 aims at creating risk control options that address both existing risks and risks introduced by new technology or new methods of operation and management. Both historical risks and newly identified risks (from steps 1 and 2) should be considered, producing a wide range of risk control measures. Techniques designed to address both specific risks and underlying causes should be used.

7.2 Methods

7.2.1 Determination of areas needing control

The purpose of focusing risks is to screen the output of step 2 so that the effort is focused on the areas most needing risk control. The main aspects to making this assessment are to review:

.1 risk levels, by considering frequency of occurrence together with the severity of outcomes. Accidents with an unacceptable risk level become the primary focus;

.2 probability, by identifying the areas of the risk model that have the highest probability of occurrence. These should be addressed irrespective of the severity of the outcome;

.3 severity, by identifying the areas of the risk model that contribute to highest severity outcomes. These should be addressed irrespective of their probability; and

.4 confidence, by identifying areas where the risk model has considerable uncertainty either in risk, severity or probability. These uncertain areas should be addressed.

7.2.2 Identification of potential RCMs

7.2.2.1 Structured review techniques are typically used to identify new RCMs for risks that are not sufficiently controlled by existing measures. These techniques may encourage the development of appropriate measures and include risk attributes and causal chains. Risk attributes relate to how a measure might control a risk, and causal chains relate to where, in the "initiating event to fatality" sequence, risk control can be introduced.

7.2.2.2 RCMs (and subsequently RCOs) have a range of attributes. These attributes may be categorized according to the examples given in appendix 6.

7.2.2.3 The prime purpose of assigning attributes is to facilitate a structured thought process to understand how an RCM works, how it is applied and how it would operate. Attributes can also be considered to provide guidance on the different types of risk control that could be applied. Many risks will be the result of complex chains of events and a diversity of causes. For such risks the identification of RCMs can be assisted by developing causal chains which might be expressed as follows:

causal factors → failure → circumstance → accident → consequences

7.2.2.4 RCMs should in general be aimed at one or more of the following:

.1 reducing the frequency of failures through better design, procedures, organizational polices, training, etc;

.2 mitigating the effect of failures, in order to prevent accidents;

.3 alleviating the circumstances in which failures may occur; and

.4 mitigating the consequences of accidents.

7.2.2.5 RCMs should be evaluated regarding their risk reduction effectiveness by using step 2 methodology including consideration of any potential side effects of the introduction of the RCM.

7.2.3 Composition of RCOs

7.2.3.1 The purpose of this stage is to group RCMs into a limited number of well thought out practical regulatory options. There is a range of possible approaches to grouping individual measures into options. The following two approaches, related to likelihood and escalation, can be considered:

.1 "general approach" which provides risk control by controlling the likelihood of initiation of accidents and may be effective in preventing several different accident sequences; and

.2 "distributed approach" which provides control of escalation of accidents, together with the possibility of influencing the later stages of escalation of other, perhaps unrelated, accidents.

7.2.3.2 In generating the RCOs, the interested entities, who may be affected by the combinations of measures proposed, should be identified.

7.3 Results

The output from step 3 comprises:

.1 a range of RCOs which are assessed for their effectiveness in reducing risk; and

.2 a list of interested entities affected by the identified RCOs.

8 FSA STEP 4 - COST BENEFIT ASSESSMENT

8.1 Scope

8.1.1 The purpose of step 4 is to identify and compare benefits and costs associated with the implementation of each RCO identified and defined in step 3. A cost benefit assessment may consist of the following stages:

.1 consider the risks assessed in step 2, both in terms of frequency and consequence, in order to define the base case in terms of risk levels of the situation under consideration;

.2 arrange the RCOs, defined in step 3, in a way to facilitate understanding of the costs and benefits resulting from the adoption of an RCO;

.3 estimate the pertinent costs and benefits for all RCOs;

.4 estimate and compare the cost effectiveness of each option, in terms of the cost per unit risk reduction by dividing the net cost by the risk reduction achieved as a result of implementing the option; and

.5 rank the RCOs from a cost-benefit perspective in order to facilitate the decision-making recommendations in step 5 (e.g. to screen those which are not cost effective or impractical).

8.1.2 Costs should be expressed in terms of life cycle costs and may include initial, operating, training, inspection, certification, decommission etc. Benefits may include reductions in fatalities, injuries, casualties, environmental damage and clean-up, indemnity of third party liabilities, etc. and an increase in the average life of ships.

8.2 Methods

8.2.1 Definition of interested entities

8.2.1.1 The evaluation of the above costs and benefits can be carried out by using various methods and techniques. Such a process should be conducted for the overall situation and then for those interested entities which are the most influenced by the problem in question.

8.2.1.2 In general, an interested entity can be defined as the person, organization, company, coastal State, flag State, etc. who is directly or indirectly affected by an accident or by the cost effectiveness of the proposed new regulation. Different interested entities with similar interests can be grouped together for the purpose of applying the FSA methodology and identifying decision-making recommendations.

8.2.2 Calculation indices for cost effectiveness

There are several indices which express cost effectiveness in relation to safety of life such as Gross Cost of Averting a Fatality (Gross CAF) and Net Cost of Averting a Fatality (Net CAF) as described in appendix 7. Other indices based on damage to and affect on property and environment may be used for a cost benefit assessment relating to such matters. Comparisons of cost effectiveness for RCOs may be made by calculating such indices.

8.3 Results

The output from step 4 comprises:

.1 costs and benefits for each RCO identified in step 3 from an overview perspective;

.2 costs and benefits for those interested entities which are the most influenced by the problem in question; and

.3 cost effectiveness expressed in terms of suitable indices.

9 FSA STEP 5 - RECOMMENDATIONS FOR DECISION-MAKING

9.1 Scope

9.1.1 The purpose of step 5 is to define recommendations which should be presented to the relevant decision makers in an auditable and traceable manner. The recommendations would be based upon the comparison and ranking of all hazards and their underlying causes; the comparison and ranking of risk control options as a function of associated costs and benefits; and the identification of those risk control options which keep risks as low as reasonably practicable.

9.1.2 The basis on which these comparisons are made should take into account that, in ideal terms, all those entities that are significantly influenced in the area of concern should be equitably affected by the introduction of the proposed new regulation. However, taking into consideration the difficulties of this type of assessment, the approach should be, at least in the earliest stages, as simple and practical as possible.

9.2 Methods

9.2.1 Scrutiny of results

Recommendations should be presented in a form that can be understood by all parties irrespective of their experience in the application of risk and cost benefit assessment and related techniques. Those submitting the results of an FSA process should provide timely and open access to relevant supporting documents and a reasonable opportunity for, and a mechanism to, incorporate comments.

9.2.2 Risk evaluation criteria

There are several standards for risk acceptance criteria, non as yet universally accepted. While it is desirable for the Organization and Member Governments which propose new regulations or modifications to existing regulations to determine agreed risk evaluation criteria after wide and deep consideration, those used within an FSA should be explicit.

9.3 Results

The output from step 5 comprises:

.1 an objective comparison of alternative options, based on the potential reduction of risks and cost effectiveness, in areas where legislation or rules should be reviewed or developed; and

.2 feedback information to review the results generated in the previous steps.

10 PRESENTATION OF FSA RESULTS

10.1 To facilitate the common understanding and use of FSA at IMO in the rule-making process, each report of an FSA process should:

.1 provide a clear statement of the final recommendations, ranked and justified in an auditable and traceable manner;

.2 list the principal hazards, risks, costs and benefits identified during the assessment;

.3 explain the basis for significant assumptions, limitations, data models and inferences used or relied upon in the assessment or recommendations;

.4 describe the sources, extent and magnitude of significant uncertainties associated with the assessment or recommendations; and

.5 describe the composition and expertise of the group that performed the FSA process.

10.2 The standard format for reporting the FSA process is shown in appendix 8.

FIGURE 1

FLOW CHART OF THE FSA METHODOLOGY

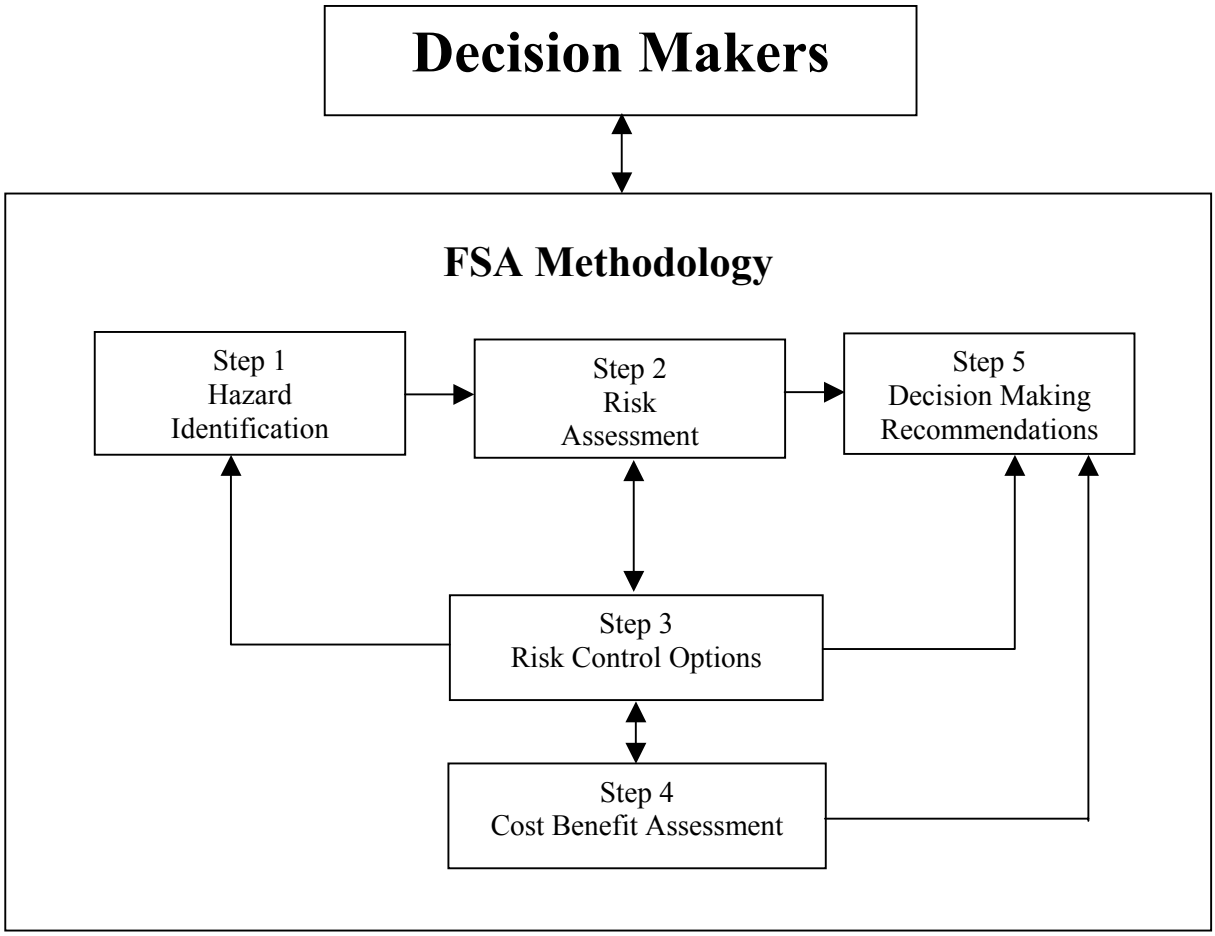


FIGURE 2

EXAMPLE OF LOSS MATRIX

Ship Accident Loss (£ per ship year)					
Accident Type	Ship accident cost	Environmental damage and clean up	Risk to life	Risk of injuries and ill health	Total cost
	£	£/tonne x number of tonnes	Fatalities x £ X m	DALY x £ Y	£
Collision Contact Foundered Fire/explosion Hull damage Machinery damage War loss Grounding Other ship accidents Other oil spills Personal accidents					
TOTAL					

DALY = Disabled Adjourned Life Years
(The World Health Report 2000; www.who.int)

FIGURE 3

COMPONENTS OF THE INTEGRATED SYSTEM

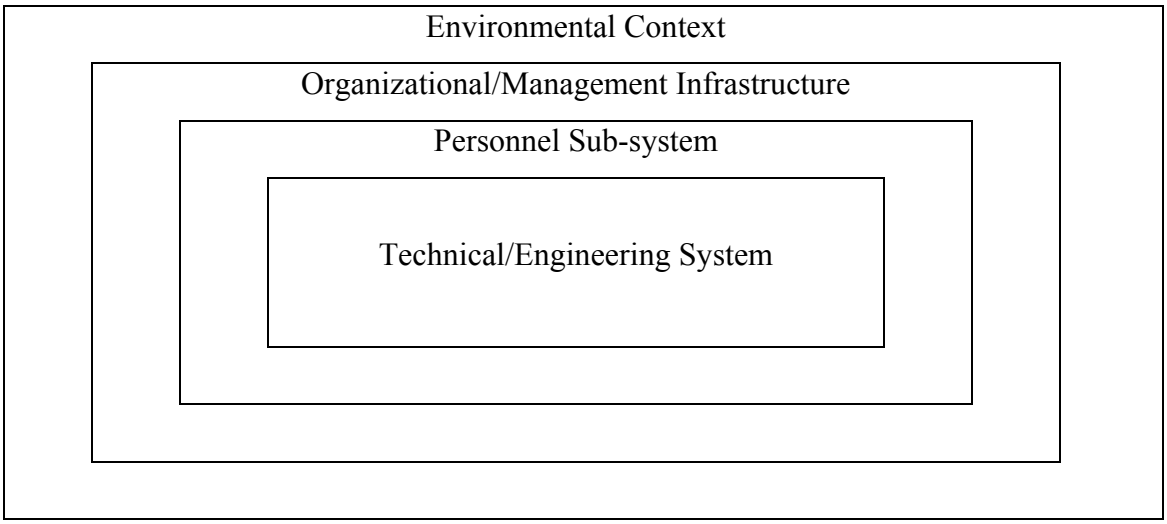


FIGURE 4

INCORPORATION OF HUMAN RELIABILITY ANALYSIS INTO THE FSA PROCESS

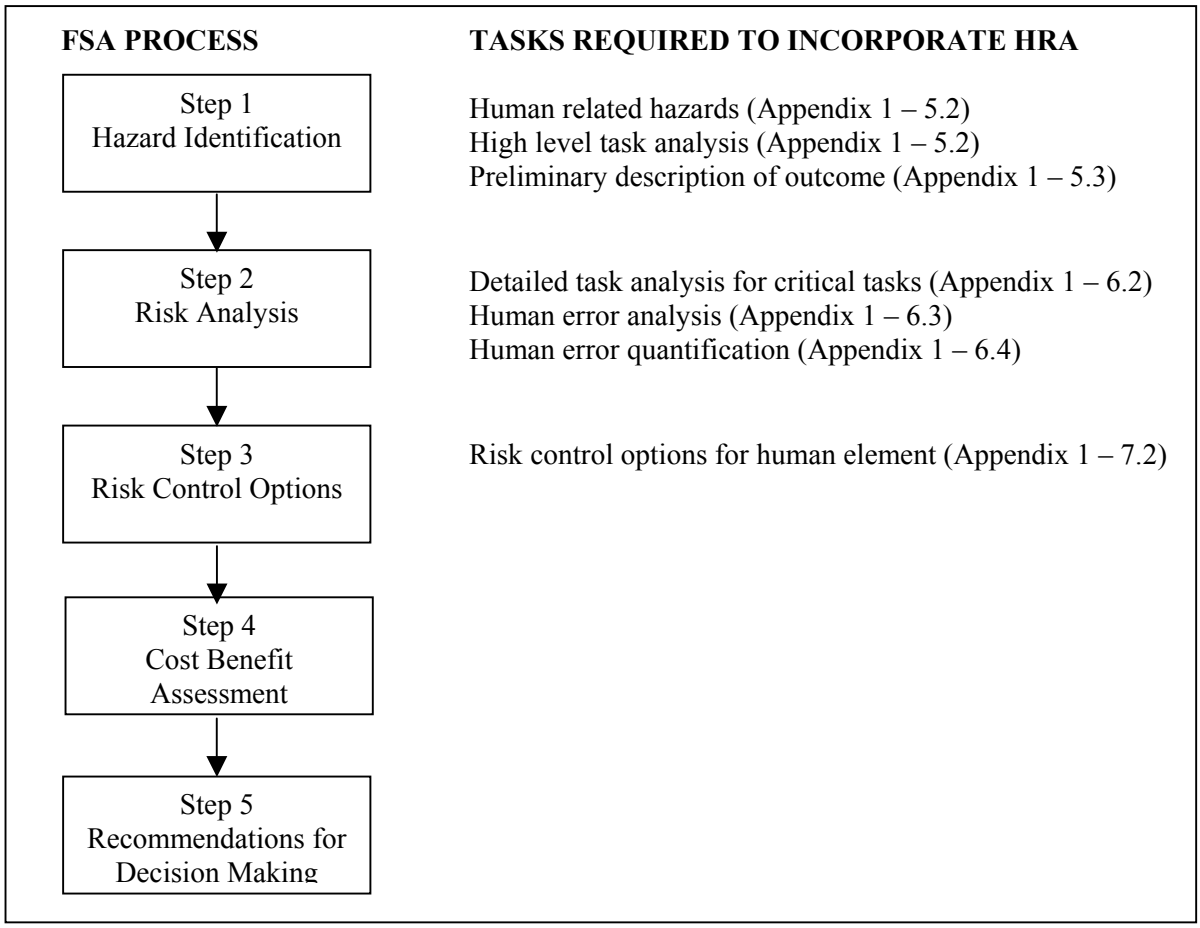


FIGURE 5

RISK MATRIX

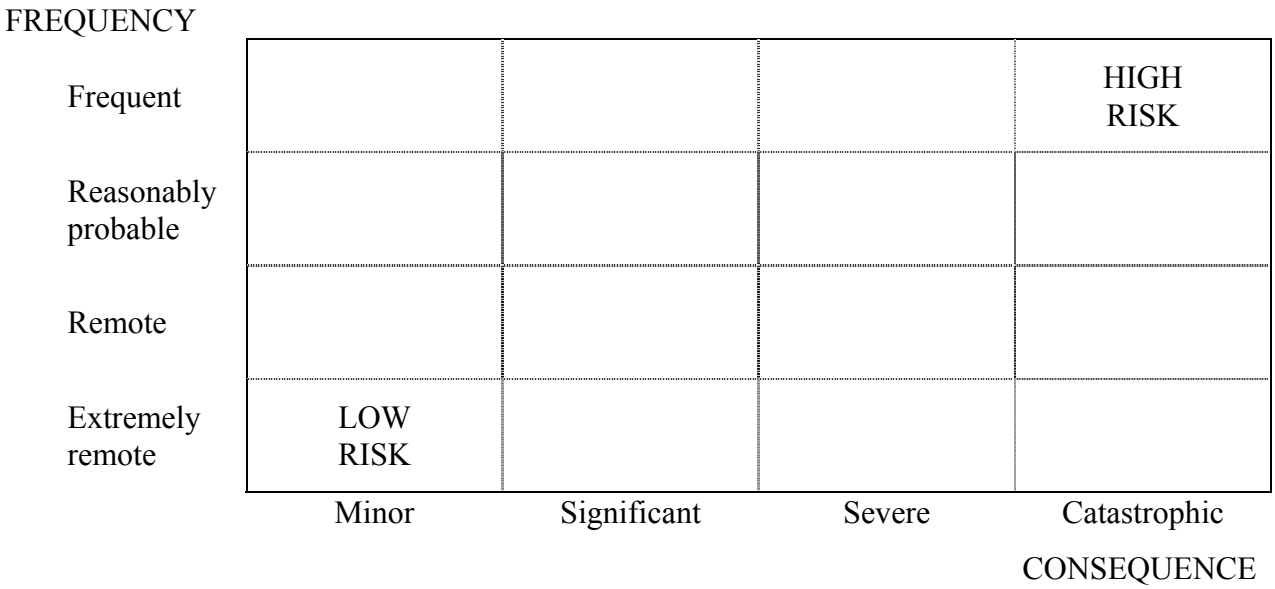
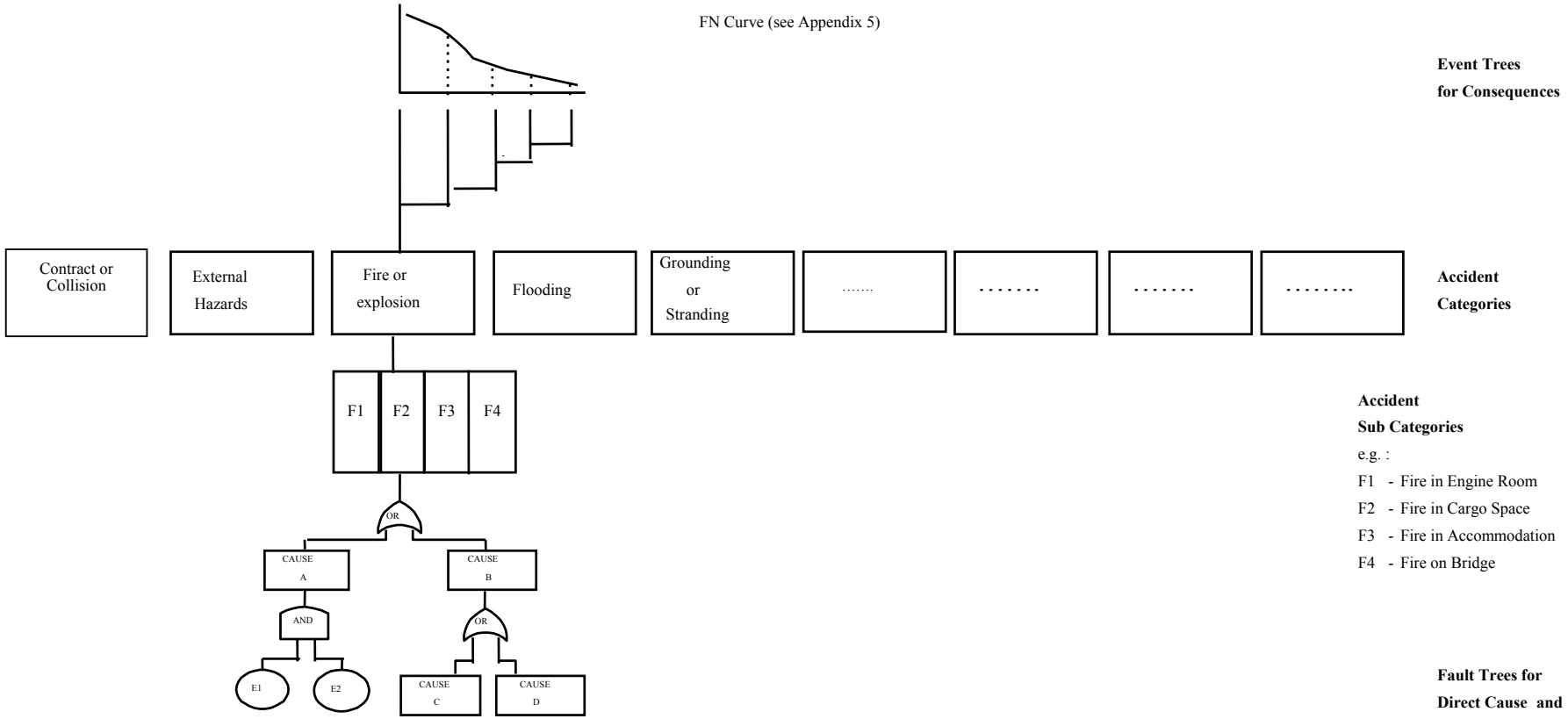


FIGURE 6

EXAMPLE OF A RISK CONTRIBUTION TREE*



* As defined in the context of these Guidelines.

APPENDIX 1

GUIDANCE ON HUMAN RELIABILITY ANALYSIS (HRA)

1 INTRODUCTION

1.1 Purpose of Human Reliability Analysis (HRA)

1.1.1 Those industries which routinely use quantitative risk assessment (QRA) to assess the frequency of system failures as part of the design process or ongoing operations management, have recognised that in order to produce valid results it is necessary to assess the contribution of the human element to system failure. The accepted way of incorporating the human element into QRA and FSA studies is through the use of human reliability analysis (HRA).

1.1.2 HRA was developed primarily for the nuclear industry. Using HRA in other industries requires that the techniques be appropriately adapted. For example, because the nuclear industry has many built-in automatic protection systems, consideration of the human element can be legitimately delayed until after consideration of the overall system performance. Onboard ships, the human has more degrees of freedom to disrupt system performance. Therefore, a high-level task analysis needs to be considered at the outset of an FSA.

1.1.3 HRA is a process, which comprises a set of activities and the potential use of a number of techniques depending on the overall objective of the analysis. HRA may be performed on a qualitative or quantitative basis depending on the level of FSA being undertaken. If a full quantitative analysis is required then Human Error Probabilities (HEPs) can be derived in order to fit into quantified system models such as fault and event trees. However in many instances a qualitative analysis may be sufficient. The HRA process usually consists of the following stages:

.1 identification of key tasks;
.2 task analysis of key tasks;
.3 human error identification;
.4 human error analysis; and
.5 human reliability quantification.

1.1.4 Where a fully-quantified FSA approach is required, HRA can be used to develop a set of HEPs for incorporation into probabilistic risk assessment. However, this aspect of HRA can be over-emphasised. Experienced practitioners admit that most benefit is derived from the early, qualitative stages of task analysis and human error identification. Effort expended in these areas pays dividends because an HRA exercise (like an FSA study) is successful only if the correct areas of concern have been chosen for investigation.

1.1.5 It is also necessary to bear in mind that the data available for the last stage of HRA, human reliability quantification, are currently limited. Although several human error databases have been built up, the data contained in them are only marginally relevant to the maritime industry. In some cases where an FSA requires quantitative results from the HRA, expert judgement may be the most appropriate method for deriving suitable data. Where expert judgement is used, it is important that the judgement can be properly justified as required by appendix 8 of the FSA Guidelines.

1.2 Scope of the HRA Guidance

1.2.1 Figure 4 of the FSA Guidelines shows how the HRA Guidance fits into the FSA process.

1.2.2 The amount of detail provided in this Guidance is at a level similar to that given in the FSA Guidelines, i.e. it states what should be done and what considerations should be taken into account. Details of some techniques used to carry out the process are provided in the appendices of this Guidance.

1.2.3 The sheer volume of information about this topic prohibits the provision of in-depth information: there are numerous HRA techniques, and task analysis is a framework encompassing dozens of techniques. Table 1 lists the main references which could be pursued.

1.2.4 As with FSA, HRA can be applied to the design, construction, maintenance and operations of a ship.

1.3 Application

It is intended that this guidance should be used wherever an FSA is conducted on a system which involves human action or intervention which affects system performance.

2 BASIC TERMINOLOGY

Error producing condition :	Factors that can have a negative effect on human performance.
Human error:	A departure from acceptable or desirable practice on the part of an individual or a group of individuals that can result in unacceptable or undesirable results.
Human error recovery:	The potential for the error to be recovered, either by the individual or by another person, before the undesired consequences are realised.
Human error consequence:	The undesired consequences of human error.
Human error probability:	Defined as follows: $HEP = \frac{Number\ of\ human\ errors\ that\ have\ occurred}{Number\ of\ opportunities\ for\ human\ error}$
Human reliability :	The probability that a person: (1) correctly performs some system-required activity in a required time period (if time is a limiting factor) and (2) performs no extraneous activity that can degrade the system. *Human unreliability* is the opposite of this definition.
Performance shaping factors:	Factors that can have a positive or negative effect on human performance.

Task analysis :	A collection of techniques used to compare the demands of a system with the capabilities of the operator, usually with a view to improving performance, e.g. by reducing errors.

3 METHODOLOGY

HRA can be considered to fit into the overall FSA process in the following way:

.1 identification of key human tasks consistent with step 1;

.2 risk assessment, including a detailed task analysis, human error analysis and human reliability quantification consistent with step 2; and

.3 risk control options consistent with step 3.

4 PROBLEM DEFINITION

Additional human element issues which may be considered in the problem definition include:

.1 personal factors, e.g. stress, fatigue;

.2 organizational and leadership factors, e.g. manning level;

.3 task features, e.g. task complexity; and

.4 onboard working conditions, e.g. human-machine interface.

5 HRA STEP 1 - IDENTIFICATION OF HAZARDS

5.1 Scope

5.1.1 The purpose of this step is to identify key potential human interactions which, if not performed correctly, could lead to system failure. This is a broad scoping exercise where the aim is to identify areas of concern (e.g. whole tasks or large subtasks) requiring further investigation. The techniques used here are the same as those used in step 2, but in step 2 they are used much more rigorously.

5.1.2 Human hazard identification is the process of systematically identifying the ways in which human error can contribute to accidents during normal and emergency operations. As detailed in paragraph 5.2.2 below, standard techniques such as Hazard and Operability (HazOp) study and Failure Mode and Effects Analysis (FMEA) can be, and are, used for this purpose. Additionally, it is strongly advised that a high-level functional task analysis is carried out. This section discusses those techniques which were developed solely to address human hazards.

5.2 Methods for hazard identification

5.2.1 In order to carry out a human hazard analysis, it is first necessary to model the system in order to identify the normal and emergency operating tasks that are carried out by the crew. This is

achieved by the use of a high-level task analysis (as described in table 2) which identifies the main human tasks in terms of operational goals. Developing a task analysis can utilise a range of data collection techniques, e.g. interviews, observation, critical incident, many of which can be used to directly identify key tasks. Additionally, there are many other sources of information which may be consulted, including design information, past experience, normal and emergency operating procedures, etc.

5.2.2 At this stage it is not necessary to generate a lot of detail. The aim is to identify those key human interactions which require further attention. Therefore, once the main tasks, subtasks and their associated goals have been listed, the potential contributors to human error of each task need to be identified together with the potential hazard arising. There are a number of techniques which may be utilised for this purpose, including human error HazOp, Hazard Checklists etc. An example of human-related hazards identifying a number of different potential contributors to sub-standard performance is included in table 3.

5.2.3 For each task and sub-task identified, the associated hazards and their associated scenarios should be ranked in order of their criticality in the same manner as discussed in section 5.2.2 of the FSA Guidelines.

5.3 Results

The output from step 1 is a set of activities (tasks and subtasks) with a ranked list of hazards associated with each activity. This list needs to be coupled with the other lists generated by the FSA process, and should therefore be produced in a common format. Only the top few hazards for critical tasks are subjected to risk assessment, less critical tasks are not examined further.

6 HRA STEP 2 - RISK ANALYSIS

6.1 Scope

The purpose of step 2 is to identify those areas where the human element poses a high risk to system safety and to evaluate the factors influencing the level of risk.

6.2 Detailed task analysis

6.2.1 At this stage, the key tasks are subjected to a detailed task analysis. Where the tasks involve more decision-making than action, it may be more appropriate to carry out a cognitive task analysis. Table 2 outlines the extended task analysis which was developed for analysing decision-making tasks.

6.2.2 The task analysis should be developed until all critical subtasks have been identified. The level of detail required is that which is appropriate for the criticality of the operation under investigation. A good general rule is that the amount of detail required should be sufficient to give the same degree of understanding as that provided by the rest of the FSA exercise.

6.3 Human error analysis

6.3.1 The purpose of human error analysis is to produce a list of potential human errors that can lead to the undesired consequence that is of concern. To help with this exercise, some examples of typical human errors are included in figure 1.

6.3.2 Once all potential errors have been identified, they are typically classified along the following lines. This classification allows the identification of a critical subset of human errors that must be addressed:

.1 the supposed cause of the human error;

.2 the potential for error-recovery, either by the operator or by another person (this includes consideration of whether a single human error can result in undesired consequences); and

.3 the potential consequences of the error.

6.3.3 Often, a qualitative analysis should be sufficient. A simple qualitative assessment can be made using a recovery/consequence matrix such as that illustrated in figure 2. Where necessary, a more detailed matrix can be developed using a scale for the likely consequences and levels of recovery.

6.4 Human error quantification

6.4.1 This activity is undertaken where a probability of human error (HEP) is required to input into a quantitative FSA. Human error quantification can be conducted in a number of ways.

6.4.2 In some cases, because of the difficulties of acquiring reliable human error data for the maritime industry, expert judgement techniques may need to be used for deriving a probability for human error. Expert judgment techniques can be grouped into four categories:

.1 paired comparisons;

.2 ranking and rating procedures;

.3 direct numerical estimation; and

.4 indirect numerical estimation.

It is particularly important that experts are provided with a thorough task definition. A poor definition invariably produces poor estimates.

6.4.3 Absolute Probability Judgement (APJ) is a good direct method. It can be used in various forms, from the single expert assessor, to large groups of individuals whose estimates are mathematically aggregated (see table 4). Other techniques which focus on judgements from multiple experts include: brainstorming; consensus decision-making; Delphi; and the Nominal Group technique.

6.4.4 Alternatives to expert opinion are historic data (where available) and generic error probabilities. Two main methods for HRA which have databases of human error probabilities (mainly for the nuclear industry) are the Technique for Human Error Rate Prediction (THERP) and Human Error Assessment and Reduction Technique (HEART) (See table 4).

6.4.5 Technique for Human Error Rate Prediction (THERP). THERP was developed by Swain and Guttmann (1983) of Sandia National Laboratories for the US Nuclear Regulatory Commission, and has become the most widely used human error quantitative prediction technique. THERP is both a human reliability technique and a human error databank. It models human errors using probability trees and models of dependence, but also considers performance shaping factors (PSFs) affecting action. It is critically dependent on its database of human error probabilities. It is considered to be particularly effective in quantifying errors in highly proceduralised activities.

6.4.6 Human Error Assessment and Reduction Technique (HEART). HEART is a technique developed by Williams (1985) that considers particular ergonomics, tasks and environmental factors that adversely affect performance. The extent to which each factor independently affects performance is quantified and the human error probability is calculated as a function of the product of those factors identified for a particular task.

6.4.7 HEART provides specific information on remedial risk control options to combat human error. It focuses on five particular causes and contributions to human error: impaired system knowledge; response time shortage; poor or ambiguous system feedback; significant judgement required of operator; and the level of alertness resulting from duties, ill health or the environment.

6.4.8 When applying human error quantification techniques, it is important to consider the following:

.1 Magnitudes of human error are sufficient for most applications. A 'gross' approximation of the human error magnitude is sufficient. The derivation of HEPs may be influenced by modelling and quantitative uncertainties. A final sensitivity analysis should be presented to show the effect of uncertainties on the estimated risks.

.2 Human error quantification can be very effective when used to produce a comparative analysis rather than an exact quantification. Then human error quantification can be used to support the evaluation of various risk control options.

.3 The detail of quantitative analysis should be consistent with the level of detail of the FSA model. The HRA should not be more detailed than the technical elements of the FSA. The level of detail should be selected based upon the contribution of the activity to the risk, system or operation being analysed.

.4 The human error quantification tool selected should fit the needs of the analysis. There are a significant number of human error quantification techniques available. The selection of a technique should be assessed for consistency, usability, validity of results, usefulness, effective use of resources for the HRA and the maturity of the technique.

6.5 Results

6.5.1 The output from this step comprises:

.1 an analysis of key tasks;

.2 an identification of human errors associated with these tasks; and

.3 an assessment of human error probabilities (optional).

6.5.2 These results should then be considered in conjunction with the high-risk areas identified elsewhere in step 2.

7 HRA STEP 3 - RISK CONTROL OPTIONS

7.1 Scope

The purpose of step 3 is to consider how the human element is considered within the evaluation of technical, human, work environment, personnel and management related risk control options.

7.2 Application

7.2.1 The control of risks associated with the human interaction with a system can be approached in the same way as for the development of other risk control measures. Measures can be specified in order to:

.1 reduce the frequency of failure;

.2 mitigate the effects of failure;

.3 alleviate the circumstances in which failures occur; and

.4 mitigate the consequence of accidents.

7.2.2 Proper application of HRA can reveal that technological innovations can also create problems which may be overlooked by FSA evaluation of technical factors only. A typical example of this is the creation of long periods of low workload when a high degree of automation is used. This in turn can lead to an inability to respond correctly when required or even to the introduction of 'risk taking behaviour' in order to make the job more interesting.

7.2.3 When dealing with risk control concerning human activity it is important to realise that more than one level of risk control measure may be necessary. This is because human involvement spans a wide range of activities from day-to-day operations through to senior management levels. Secondly, it must also be stressed that a basic focus on good system design utilising ergonomics and human factor principles is needed in order to achieve enhanced operational safety and performance levels.

7.2.4 In line with figure 3 of the FSA Guidelines, risk control measures for human interactions can be categorised into four areas as follows: (1) Technical/engineering sub-system, (2) Working environment, (3) Personnel sub-system and (4) Organisational/management sub-system. A description of the issues that may be considered within each of these areas is given in figure 3.

7.2.5 Once the risk control measures have been initially specified, it is important to reassess human intervention in the system in order to assess whether any new hazards have been introduced. For

example, if a decision had been taken to automate a particular task, then the new task would need to be re-evaluated.

7.3 Results

The output from this step comprises a range of risk control options categorised into 4 areas as presented in figure 3, easing the integration of human related risk into step 3.

8 HRA STEP 4 - COST BENEFIT ASSESSMENT

No specific HRA guidance for this section is required.

9 HRA STEP 5 - RECOMMENDATIONS FOR DECISION-MAKING

Judicious use of the results of the HRA study should contribute to a set of balanced decisions and recommendations of the whole FSA study.

FIGURE 1

TYPICAL HUMAN ERRORS

Physical Errors	*Mental Errors*
Action omitted Action too much/little Action in wrong direction Action mistimed Action on wrong object	Lack of knowledge of system/situation Lack of attention Failure to remember procedures Communication breakdowns Miscalculation

FIGURE 2

RECOVERY/CONSEQUENCE MATRIX

Consequence	**High**	**May need to consider**	**MUST CONSIDER**
	Low	**No need to consider**	**May need to consider**
		High	**Low**
		Recovery	

FIGURE 3

EXAMPLES OF RISK CONTROL OPTIONS

Technical/engineering sub-system

- ergonomic design of equipment and work spaces
- good layout of bridge, machinery spaces
- ergonomic design of the man-machine interface/human computer interface
- specification of information requirements for the crew to perform their tasks
- clear labelling and instructions on the operation of ship systems and control/communications equipment

Working environment

- ship stability, effect on crew of working under conditions of pitch/roll
- weather effects, including fog, particularly on watch-keeping or external tasks
- ship location, open sea, approach to port, etc.
- appropriate levels of lighting for operations and maintenance tasks and for day and night time operations
- consideration of noise levels (particularly for effect on communications)
- consideration of the effects of temperature and humidity on task performance
- consideration of the effects of vibration on task performance

Personnel sub-system

- development of appropriate training for crew members
- crew levels and make up
- language and cultural issues
- workload assessment (both too much and too little workload can be problematic)
- motivational and leadership issues

Organisational/management sub-system

- development of organization policies on recruitment, selection, training, crew levels and make up, competency assessment, etc.
- development of operational and emergency procedures (including provisions for tug and salvage services)
- use of safety management systems
- provision of weather forecasting/routeing services

TABLE 1

REFERENCES

1. Advisory Committee on the Safety of Nuclear Installations (1991*) Human Factors Study Group Second Report: Human reliability assessment - a critical overview*.
2. Annett, J. and Stanton, N.A. (1998) Special issue on task analysis. *Ergonomics*, 41(11).
3. Ball, P.W. (1991) The guide to reducing human error in process operations. *Human Factors in Reliability Group, SRDA – R3, HMSO.*
4. Gertman, D.I. and Blackman, H.S. (1994) *Human Reliability and Safety Analysis Data Handbook*. Wiley & Sons: New York.
5. Hollnagel, E. (1998) *Cognitive Reliability and Error Analysis Method*. Elsevier Applied Science: London.
6. Human Factors in Reliability Group (1995) *Improving Compliance with Safety Procedures–Reducing Industrial Violations*. HSE Books: London.
7. Humphreys, P. (ed.) (1995*) Human Reliability Assessor's Guide: A report by the Human Factors in Reliability Group:* Cheshire.
8. Johnson, L. and Johnson, N.E. (1987) A Knowledge Elicitation Method for Expert Systems Design. *Systems Research and Info. Science,* Vol.2, 153-166.
9. Kirwan, B. (1992) Human error identification in human reliability assessment. Part I: Overview of approaches. *Applied Ergonomics*, 23(5), 299-318.
10. Kirwan, B. (1997) A validation of three Human Reliability Quantification techniques - THERP, HEART and JHEDI: Part III - Results and validation exercise. *Applied Ergonomics*, 28(1), 27-39.
11. Kirwan, B. (1994) *A Guide to Practical Human Reliability Assessment*. Taylor & Francis: London.
12. Kirwan, B. and Ainsworth, L.K. (1992) *A Guide to Task Analysis. London*: Taylor & Francis.
13. Kirwan, B., Kennedy, R., Taylor-Adams, S. and Lambert, B. (1997) A validation of three Human Reliability Quantification techniques—THERP, HEART and JHEDI: Part II - Practical aspects of the usage of the techniques. *Applied Ergonomics*, 28(1), 17-25.
14. Lees, F. (1996) Human factors and human element. *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control.* Vol. 3. Butterworth Heinemann.
15. Pidgeon, N., Turner, B. and Blockley, D. (1991) The use of Grounded Theory for conceptual analysis in knowledge elicitation. *International Journal of Man-Machine Studies,* Vol.35, 151-173.
16. Rasmussen, J., Pedersen, O.M., Carino, A., Griffon, M., Mancini, C., and Gagnolet, P. (1981*) Classification system for reporting events involving human malfunctions. Report Riso-M-2240*, DK-4000. Roskilde, Riso National Laboratories, Denmark.
17. Swain, A.D. (1989) *Comparative Evaluation of Methods for Human Reliability Analysis*. Gesellschaft für Reaktorsicherheit (GRS) mbH.
18. Swain, A.D. and Guttmann, H.E. (1983) *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications: Final Report. NUREG/CR* - 1278. U.S. Nuclear Regulatory Commission.
19. Williams, J.C. (1986) *HEART - A proposed method for assessing and reducing human error. Proceedings, 9th Advances in Reliability Technology Symposium, University of Bradford*. NCRS, UKAEA. Culcheth, Cheshire.

TABLE 2

SUMMARY OF TASK ANALYSIS TYPES

1 High-level task analysis

1.1 High-level task analysis here refers to the type of task analysis which allows an analyst to gain a broad, but shallow, overview of the main functions which need to be performed to accomplish a particular task.

1.2 High-level task analysis is undertaken in the following way:

.1 describe all operations within the system in terms of the tasks required to achieve a specific operational goal; and

.2 consider goals associated with normal operations, emergency procedures, maintenance and recovery measures.

1.3 The analysis is recorded either in a hierarchical format or in tabular form.

2 Detailed task analysis

2.1 Detailed task analysis is undertaken to identify:

.1 the overall task (or job) that is done;

.2 subtasks;

.3 all of the people who contribute to the task and their interactions;

.4 how the work is done, i.e. the working practices in normal and emergency situations;

.5 any controls, displays, tools, etc. which are used; and

.6 factors which influence performance.

2.2 There are many task analysis techniques - Kirwan and Ainsworth (1992) list more than twenty. They note that the most widely used, hierarchical task analysis (HTA), can be used as a framework for applying other techniques:

.1 data collection techniques, e.g. activity sampling, critical incident, questionnaires;

.2 task description techniques, e.g. charting and network techniques, tabular task analysis;

.3 tasks simulation methods, e.g. computer modelling and simulation;

.4 task behaviour assessment methods, e.g. management and oversight risk trees; and

.5 task requirement evaluation methods, e.g. ergonomics checklists.

3 Extended task analysis (XTA)

3.1 Traditional task analysis was designed for investigating manual tasks, and is not so useful for analysing intellectual tasks, e.g. navigation decisions. Extended task analysis or other cognitive task analyses (see Annett and Stanton, 1998) can be used where the focus is less on what actions are performed and more on understanding the rationale for the decisions that are taken.

3.2 XTA is used to map out the logical bases of the decision-making process which underpin the task under examination. The activities which comprise XTA techniques are described in Johnson and Johnson (1987). In summary, they are:

.1 Interview. The interviewer asks about the conditions which enable or disable certain actions to be performed, and how a change in the conditions affects those choices. The interviewer examines the individual's intentions to make sure that all relevant aspects of the situation have been taken into account. This enables the analyst to build up a good understanding of what the individual is doing and why, and how it would change under varying conditions.

.2 Qualitative analysis of data. The interview is tape-recorded, transcribed and subsequently analysed. Methods for analysing qualitative data are well-established in social science and more recently utilised in safety engineering. The technique (called Grounded Theory) is described in detail by Pidgeon, *et al.* (1991).

.3 Representation of the analysis in an appropriate format. The representation scheme used in XTA is called systemic grammar networks - a form of associative network - see Johnson and Johnson (1987).

.4 Validation activities, e.g. observation, hypothesis.

TABLE 3

EXAMPLES OF HUMAN-RELATED HAZARDS

1 Human error occurs onboard ships when a crew member's ability falls below what is needed to successfully complete a task. Whilst this may be due to a lack of ability, more commonly it is because the existing ability is hampered by adverse conditions. Below are some examples (not complete) of personal factors and unfavourable conditions which constitute hazards to optimum performance. A comprehensive examination of all human-related hazards should be performed. During the 'design stage' it is typical to focus mainly on task features and on board working conditions as potential human-related hazards.

2 Personal factors

.1 Reduced ability, e.g. reduced vision or hearing

.2 Lack of motivation, e.g. because of a lack of incentives to perform well

.3 Lack of ability, e.g. lack of seamanship, unfamiliarity with vessel, lack of fluency of the language used onboard

.4 Fatigue, e.g. because of lack of sleep or rest, irregular meals

.5 Stress

3 Organizational and leadership factors

.1 Inadequate vessel management, e.g. inadequate supervision of work, lack of co-ordination of work, lack of leadership

.2 Inadequate ship owner management, e.g. inadequate routines and procedures, lack of resources for maintenance, lack of resources for safe operation, inadequate follow-up of vessel organisation

.3 Inadequate manning, e.g. too few crew, untrained crew

.4 Inadequate routines, e.g. for navigation, engine room operations, cargo handling, maintenance, emergency preparedness

4 Task features

.1 Task complexity and task load, i.e. too high to be done comfortably or too low causing boredom

.2 Unfamiliarity of the task

.3 Ambiguity of the task goal

.4 Different tasks competing for attention

5 Onboard working conditions

.1 Physical stress from, e.g. noise, vibration, sea motion, climate, temperature, toxic substances, extreme environmental loads, night-watch

.2 Ergonomic conditions, e.g. inadequate tools, inadequate illumination, inadequate or ambiguous information, badly-designed human-machine interface

.3 Social climate, e.g. inadequate communication, lack of co-operation

.4 Environmental conditions, e.g. restricted visibility, high traffic density, restricted fairway

TABLE 4

SUMMARY OF HUMAN ERROR ANALYSIS TECHNIQUES

The two main HRA quantitative techniques (HEART and THERP) are outlined below. CORE-DATA provides data on generic probabilities. As the data from all of these sources are based on non-marine industries, they need to be used with caution. A good alternative is to use expert judgement and one technique for doing this is Absolute Probability Judgement.

1 Absolute Probability Judgement (APJ)

1.1 APJ refers to a group of techniques that utilise expert judgement to develop human error probabilities (HEPs) detailed in Kirwan (1994) and Lees (1996). These techniques are used when no relevant data exist for the situation in question, making some form of direct numerical estimation the only way of developing values for HEPs.

1.2 There are a variety of techniques available. This gives the analyst some flexibility in accommodating different types of analysis. Most of the techniques avoid potentially detrimental group influences such as group bias. Typically the techniques used are: the Delphi technique, the Nominal Group Technique and Paired Comparisons. The number and type of experts that are required to participate in the process are similar to that required for Hazard Identification techniques such as HazOp.

1.3 Paired Comparisons is a significant, expert judgement technique. Using this technique, an individual makes a series of judgements about pairs of tasks. The results for each individual are analysed and the relative values for HEPs for the tasks derived. Use of the technique rests upon the ability to include at least two tasks with known HEPs. CORE-DATA and data from other industries may be useful.

1.4 The popularity of these techniques has reduced in recent times, probably due to the requirement to get the relevant groups of experts together. However, these techniques may be very appropriate for the maritime industry.

2 Technique for Human Error Rate Prediction (THERP)

2.1 THERP is one of the best known and most often utilised human reliability analysis techniques. At first sight the technique can be rather daunting due to the volume of information provided. This is because it is a comprehensive methodology covering task analysis, human error identification, human error modelling and human error quantification. However, it is best known for its human error quantification aspects, which includes a series of human error probability (HEP) data tables and data quantifying the effects of various performance shaping factors (PSFs). The data presented is generally of a detailed nature and so not readily transferable to the marine environment.

2.2 THERP contains a dependence model which is used to model the dependence relationship between errors. For example, the model could be used to assess the dependence between the helmsman making an error and the bridge officer noticing it. Operational experience does show that there are dependence effects between people and between tasks. Whilst this is the only human error model of its type, it has not been comprehensively validated.

2.3 A full THERP analysis can be resource-intensive due to the level of detail required to utilise the technique properly. However, the use of this technique forces the analyst to gain a detailed appreciation of the system and of the human error potential. THERP models humans as any other sub-system in the FSA modelling process. The steps are as follows:

.1 identify all the systems in the operation that are influenced and affected by human operations;

.2 compile a list and analyse all human operations that affect the operations of the system by performing a detailed task analysis;

.3 determine the probabilities of human errors through error frequency data and expert judgements and experiences; and

.4 determine the effects of human errors by integrating the human error into the PRA modelling procedure.

2.4 THERP includes a set of performance shaping factors (PSFs) that influence the human errors at the operator level. These performance factors include experience, situational stress factors, work environment, individual motivation, and the human-machine interface. The PSFs are used as a basis for estimating nominal values and value ranges for human error.

2.5 There are advantages to using THERP. First it is a good tool for relative risk comparisons. It can be used to measure the role of human error in an FSA and to evaluate risk control options not necessarily in terms of a probability or frequency, but in terms of risk magnitude. Also, THERP can be used with the standard event-tree/fault-tree modelling approaches that are sometimes preferred by FSA practitioners. THERP is a transparent technique that provides a systematic, well-documented approach to evaluating the role of human errors in a technical system. The THERP database can be used through systematic analysis or, where available, external human error data can be inserted.

3 Human Error Assessment Reduction Technique (HEART)

3.1 HEART is best known as a relatively simple way of arriving at human error probabilities (HEPs). The basis of the technique is a database of nine generic task descriptions and an associated human error probability. The analyst matches the generic task description to the task being assessed and then modifies the generic human error probability according to the presence and strength of the identified error producing conditions (EPCs). EPCs are conditions that increase the order of magnitude of the error frequency or probability measurements, similar in concept to PSFs in THERP. A list of EPCs is supplied as part of the technique, but it is up to the analyst to decide on the strength of effect for the task in question.

3.2 Whilst the generic data is mainly derived from the nuclear industry, HEART does appear amenable to application within other industries. It may be possible to tailor the technique to the marine environment by including new EPCs such as weather. However, it needs careful application to avoid ending up with very conservative estimates of HEPs.

4 CORE-DATA

4.1 CORE-DATA is a database of human error probabilities. Access to the database is available through the University of Birmingham in the United Kingdom. The database has been developed as a result of sponsorship by the UK Health and Safety Executive with support from the nuclear, rail, chemical, aviation and offshore industries and contains up to 300 records as of January 1999.

4.2 Each record is a comprehensive presentation of information including, e.g. a task summary, industry origin, country of origin, type of data collection used, a database quality rating, description of the operation, performance shaping factors, sample size and HEP.

4.3 As with all data from other industries, care needs to be taken when transferring the data to the maritime industry. Some of the offshore data may be the most useful.

APPENDIX 2

EXAMPLES OF HAZARDS

1 SHIPBOARD HAZARDS TO PERSONNEL

.1 asbestos inhalation
.2 burns from caustic liquids and acids
.3 electric shock and electrocution
.4 falling overboard
.5 pilot ladder/pilot hoist operation

2 HAZARDOUS SUBSTANCES ON BOARD SHIP

Accommodation areas:
.1 combustible furnishings
.2 cleaning materials in stores
.3 oil/fat in galley equipment

Deck Areas:
.4 cargo
.5 paint, oils, greases etc. in deck stores

Machinery spaces:
.6 cabling
.7 fuel and diesel oil for engines, boilers and incinerators
.8 fuel, lubricating and hydraulic oil in bilges, save alls, etc.
.9 refrigerants
.10 thermal heating fluid systems

3 POTENTIAL SOURCES OF IGNITION

General
.1 electrical arc
.2 friction
.3 hot surface
.4 incendiary spark
.5 naked flame
.6 radio waves

Accommodation areas (including bridge):
.7 electronic navigation equipment
.8 laundry facilities - irons, washing machines, tumble driers, etc.

Deck areas:
.9 deck lighting
.10 funnel exhaust emissions
.11 hot work sparking

Machinery spaces:

.12 air compressor units

.13 generator engine exhaust manifold

4 HAZARDS EXTERNAL TO THE SHIP

.1 storms

.2 lightning

.3 uncharted submerged objects

.4 other ships

APPENDIX 3

HAZARD IDENTIFICATION AND RISK ANALYSIS TECHNIQUES

1 Fault Tree Analysis

1.1 A Fault Tree is a logic diagram showing the causal relationship between events which singly or in combination occur to cause the occurrence of a higher level event. It is used in Fault Tree Analysis to determine the probability of a top event, which may be a type of accident or unintended hazardous outcome. Fault Tree Analysis can take account of common cause failures in systems with redundant or standby elements. Fault Trees can include failure events or causes related to human factors.

1.2 The development of a Fault Tree is by a top-down approach, systematically considering the causes or events at levels below the top level. If two or more lower events need to occur to cause the next higher event, this is shown by a logic "and" gate. If any one of two or more lower events can cause the next higher event, this is shown by a logic "or" gate. The logic gates determine the addition or multiplication of probabilities (assuming independence) to obtain the values for the top event.

2 Event Tree Analysis

2.1 An Event Tree is a logic diagram used to analyse the effects of an accident, a failure or an unintended event. The diagram shows the probability or frequency of the accident linked to those safeguard actions required to be taken after occurrence of the event to mitigate or prevent escalation.

2.2 The probabilities of success or failure of these actions are analysed. The success and failure paths lead to various consequences of differing severity or magnitude. Multiplying the likelihood of the accident by the probabilities of failure or success in each path gives the likelihood of each consequence.

3 Failure Mode and Effect Analysis (FMEA)

FMEA is a technique in which the system to be analysed is defined in terms of functions or hardware. Each item in the system is identified at a required level of analysis. This may be at a replaceable item level. The effects of item failure at that level and at higher levels are analysed to determine their severity on the system as a whole. Any compensating or mitigating provisions in the system are taken account of and recommendations for the reduction of the severity are determined. The analysis indicates single failure modes which may cause system failure.

4 Hazard and Operability Studies (HAZOP)

4.1 These studies are carried out to analyse the hazards in a system at progressive phases of its development from concept to operation. The aim is to eliminate or minimise potential hazards.

4.2 Teams of safety analysts and specialists in the subject system, such as designers, constructors and operators are formally constituted. The team members may change at successive phases depending on the expertise required. In examining designs they systematically consider deviations from the intended functions, looking at causes and effects. They record the findings and recommendations and follow-up actions required.

5 What If Analysis Technique

5.1 What If Analysis Technique is a hazard identification technique suited for use in a hazard identification meeting. The typical participants in the meeting may be: a facilitator leader, a recorder and a group of carefully selected experienced persons covering the topics under consideration. Usually a group of 7 to 10 persons is required.

5.2 The group first discusses in detail the system, function or operation under consideration. Drawings, technical descriptions etc. are used, and the experts may have to clarify to each other how the details of the system, function or operation work and may fail.

5.3 The next phase of the meeting is brainstorming, where the facilitator leader guides by asking questions starting with "what if?". The questions span topics like operation errors, measurement errors, equipment malfunction, maintenance, utility failure, loss of containment, emergency operation and external influences. When the ideas are exhausted, previous accident experience may be used to check for completeness.

5.4 The hazards are considered in sequence and structured into a logical sequence, in particular to allow cross-referencing between hazards.

5.5 The hazard identification report is usually developed and agreed in the meeting, and the job is done and reported when the meeting is adjourned.

5.6 The technique requires that the participants are senior personnel with detailed knowledge within their field of experience. A meeting typically takes three days. If the task requires long meetings it should be broken down into smaller sub-tasks.

5.7 SWIFT (Structured What If Technique) is one example of a What If Analysis Technique (http://www.dnv.nl/Syscert/training&consultancy.htm).

6 Risk Contribution Tree (RCT)

6.1 RCT may be used as a mechanism for displaying diagrammatically the distribution of risk amongst different accident categories and sub-categories, as shown in figure 6 of the FSA Guidelines. Structuring the tree starts with the accident categories, which may be divided into sub-categories to the extent that available data allow and logic dictates. The preliminary fault and event trees can be developed based on the hazards identified in step 1 to demonstrate how direct causes initiate and combine to cause accidents (using fault trees), and also how accidents may progress further to result in different magnitudes of loss (using event trees). Whilst the example makes use of fault and event tree techniques, other established methods could be used if appropriate.

6.2 Quantifying the RCT is typically undertaken in three stages using available accident statistics:

.1 categories and sub-categories of accidents are quantified in terms of the frequency of accidents;

.2 the severity of accident outcomes is quantified in terms of magnitude and consequence; and

.3 the risk of the categories and sub-categories of accidents can be expressed as F-N curves (see appendix 5) or potential loss of lives (PLL) based on the frequency of accidents and the severity of the outcome of the accidents. Thus, the distribution of risks across all the sub-categories of accidents is determined in risk terms, so as to display which categories contribute how much risk.

7 Influence Diagrams

The purpose of the Influence Diagram approach is to model the network of influences on an event. These influences link failures at the operational level with their direct causes, and with the underlying organizational and regulatory influences. The Influence Diagram approach is derived from decision analysis and, being based on expert judgements, is particularly useful in situations for which there may be little, or no empirical data available. The approach is therefore capable of identifying all the influences (and therefore underlying causal information) that help explain why a marine risk profile may show high risk levels in one aspect (or even vessel type) and low risk level in another aspect. As the Influence Diagram recognises that the risk profile is influenced, for example by human, organisational and regulatory aspects, it allows a holistic understanding of the problem area to be displayed in a hierarchical way.

APPENDIX 4

INITIAL RANKING OF ACCIDENT SCENARIOS

1 At the end of step 1, hazards are to be prioritized and scenarios ranked. Scenarios are typically the sequence of events from the initiating event up to the consequence, through the intermediate stages of the scenario development.

2 To facilitate the ranking and validation of ranking, it is generally recommended to define consequence and probability indices on a logarithmic scale. A risk index may therefore be established by adding the probability/frequency and consequence indices. By deciding to use a logarithmic scale, the Risk Index for ranking purposes of an event rated "remote" (FI=3) with severity "Significant" (SI=2) would be RI=5.

Risk = Probability x Consequence
Log (Risk) = log (Probability) + log (Consequence)

3 The following table gives an example of a logarithmic severity index, scaled for a maritime safety issue. Consideration of environmental issues or of passenger vessels may require additional or different categories.

Severity Index				
SI	SEVERITY	EFFECTS ON HUMAN SAFETY	EFFECTS ON SHIP	S (Equivalent 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 damage	1
4	Catastrophic	Multiple fatalities	Total loss	10

4 The following table gives an example of a logarithmic probability/frequency index.

Frequency Index			
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 a few times during the ship's life	0.1
3	Remote	Likely to occur once per year in a fleet of 1000 ships, i.e. likely to occur in the total life of several similar ships	10^{-3}
1	Extremely remote	Likely to occur once in the lifetime (20 years) of a world fleet of 5000 ships.	10^{-5}

5 The following table gives an example of a risk matrix based on the tables above.

Risk Index (RI)					
		SEVERITY (SI)			
		1	2	3	4
FI	FREQUENCY	Minor	Significant	Severe	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**

APPENDIX 5

MEASURES AND TOLERABILITY OF RISKS

1 There are two fundamental measures of risk, individual risk and societal risk. It is necessary for the risk to be both tolerable to the individual and tolerable to society. Individual risk can be regarded as the risk to an individual in isolation while societal risk is the risk to society of a major accident. There is a clear perception in society that a single accident that kills 1,000 people is worse than 1,000 accidents that kill a single person. Therefore the tolerable level of societal risk is usually lower than the tolerable level of individual risk.

2 Individual risk is usually assessed by some form of a criticality matrix where the risk is assessed against frequency of occurrence (ranging from extremely remote to frequent) and severity of outcome (ranging from insignificant to catastrophic). Societal risk is usually assessed by a technique such as an FN curve where the acceptable level of frequency (F) of an accident is plotted against the number (N or more) of people killed by the accident.

3 When each risk assessment is made, it will be necessary also to determine which assessment method should be used. Generally, accidents that cause one or two fatalities are best assessed by individual risk considerations, while accidents that cause the loss of a crew or the passengers are best assessed by societal risk considerations.

4 Whichever assessment method is used, the uncertainties of quantitative risk assessment must be balanced against the potential risk reduction. It is necessary to consider the uncertainty in the process in order to avoid premature judgements about the benefits of a particular Risk Control Option.

5 The current best practice is to recognise that there are three levels of risk: Intolerable, As Low As Reasonably Practicable (ALARP) and Negligible.

6 "Intolerable" means that the risk cannot be justified except in extraordinary circumstances, "Negligible" that the risk has been made so small that no further precaution is necessary, and "ALARP" that the risk falls between these two states.

7 The risk when travelling on a ferry should therefore be made "ALARP". There are no exceptional benefits to a passenger to allow an "intolerable" risk and sea travel can clearly never be made so safe that the risk is "negligible" and no precautions need to be made.

8 The extent to which risk exposure is involuntary (as opposed to voluntary) may also be relevant in determining the acceptability of risk. For example, a lower level of risk might be appropriate for people living near a port and unaware of the risks that shipping operations impose upon them, compared with the risks experienced by crew members who choose to continue their employment in a particular shipping trade.

APPENDIX 6

ATTRIBUTES OF RISK CONTROL MEASURES

1 Category A attributes

1.1 **Preventive risk control** is where the risk control measure reduces the probability of the event.

1.2 **Mitigating risk control** is where the risk control measure reduces the severity of the outcome of the event or subsequent events, should they occur.

2 Category B attributes

2.1 **Engineering risk control** involves including safety features (either built in or added on) within a design. Such safety features are safety critical when the absence of the safety feature would result in an unacceptable level of risk.

2.2 **Inherent risk control** is where at the highest conceptual level in the design process, choices are made that restrict the level of potential risk.

2.3 **Procedural risk control** is where the operators are relied upon to control the risk by behaving in accordance with defined procedures.

3 Category C attributes

3.1 **Diverse risk control** is where the control is distributed in different ways across aspects of the system, whereas concentrated risk control is where the risk control is similar across aspects of the system.

3.2 **Redundant risk control** is where the risk control is robust to failure of risk control, whereas **single risk control** is where the risk control is vulnerable to failure of risk control.

3.3 **Passive risk control** is where there is no action required to deliver the risk control measure, whereas **active risk control** is where the risk control is provided by the action of safety equipment or operators.

3.4 **Independent risk control** is where the risk control measure has no influence on other elements.

3.5 **Dependent risk control** is where one risk control measure can influence another element of the risk contribution tree.

3.6 **Involved human factors** is where human action is required to control the risk but where failure of the human action will not in itself cause an accident or allow an accident sequence to progress. **Critical human factors** is where human action is vital to control the risk either where failure of the human action will directly cause an accident or will allow an accident sequence to progress.

3.7 Where a **critical human factor** attribute is assigned, the human action (or critical task) should be clearly defined in the risk control measure.

3.8 **Auditable** or **Not Auditable** reflects whether the risk control measure can be audited or not.

3.9 **Quantitative** or **Qualitative** reflects whether the risk control measure has been based on a quantitative or qualitative assessment of risk.

3.10 **Established** or **Novel** reflects whether the risk control measure is an extension to existing marine technology or operations, whereas novel is where the measure is new. Different grades are possible, for example the measure may be novel to shipping but established in other industries or it is novel to both shipping and other industries.

3.11 **Developed** or **Non-developed** reflects whether the technology underlying the risk control measure is developed both in its technical effectiveness and its basic cost. Non-developed is either where the technology is not developed but it can be reasonably expected to develop, or its basic cost can be expected to reduce in a given timescale. The purpose of considering this attribute is to attempt to anticipate development and produce forward looking measures and options.

APPENDIX 7

EXAMPLE OF CALCULATION OF INDICES FOR COST EFFECTIVENESS

The estimates given refer to Gross Cost of Averting a Fatality (Gross CAF) and Net Cost of Averting a Fatality (Net CAF). Their definitions are:

$$\text{Gross CAF} = \frac{\Delta C}{\Delta R}$$

and

$$\text{Net CAF} = \frac{\Delta C - \Delta B}{\Delta R}$$

where:

ΔC is the cost per ship of the risk control option.

ΔB is the economic benefit per ship resulting from the implementation of the risk control option (this may also include pollution prevented).

ΔR is the risk reduction per ship, in terms of the number of fatalities averted, implied by the risk control option.

APPENDIX 8

STANDARD FORMAT FOR REPORTING AN APPLICATION OF FORMAL SAFETY ASSESSMENT TO IMO

1 This standard format is intended to facilitate the compilation of the results of applications according to the "Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process" and the consistent presentation of those results to IMO.

2 Interested parties having carried out an FSA application should provide the most significant results in a clear and concise manner, which can also be understood by other parties not having the same experience in the application of risk assessment techniques.

3 The report of an FSA application should contain an executive summary and the following sections: definition of the problem, background information, method of work, description of the results achieved in each step and final recommendations arising from the FSA study.

4 The level of detail of the report depends on the problem under consideration. However, to facilitate the understanding and use of the results of the FSA application, the report should not exceed 20 pages, excluding figures and appendices.

5 Those submitting the results of the FSA application should provide the other interested parties with timely and open access to relevant supporting documentation and sources of information or data which are referred to in the above-mentioned report, as reflected in paragraph 9.2.1 of the FSA Guidelines.

6 The following section presents the standard format of FSA application reports. The subjects expected to be presented in each section of the report are listed in italic characters and reference is made, in brackets, to the relevant paragraph(s) of the FSA Guidelines.

STANDARD REPORTING FORMAT

1 TITLE OF THE TRIAL APPLICATION

2 SUMMARY (maximum 1/2 page)

2.1 Executive summary: scope of the application and reference to the paragraph defining the problem assessed and its boundaries.

2.2 Actions to be taken: type of action requested (e.g. for information or review) and summary of the final recommendations listed in section 7.

2.3 Related documents: reference to any supporting documentation.

3 DEFINITION OF THE PROBLEM (maximum 1 page)

3.1 Definition of the problem to be assessed in relation to the proposal under consideration by the decision-makers.

3.2 Reference to the regulation(s) affected by the proposal to be reviewed or developed (in an annex).

3.3 Definition of the generic model (e.g. functions, features, characteristics or attributes which are relevant to the problem under consideration, common to all ships of the type affected by the proposal).

(refer to paragraphs 4.1 and 4.2 of the FSA Guidelines)

4 BACKGROUND INFORMATION (maximum 3 pages)

4.1 Lessons learned from recently introduced measures to address similar problems.

4.2 Casualty statistics concerning the problem under consideration (e.g. ship types or accident category).

4.3 Any other sources of data and relevant limitations.

(refer to paragraph 3.2 of the FSA Guidelines)

5 METHOD OF WORK (maximum 3 pages)

5.1 Composition and level of expertise of those having carried out the application (name and expertise in an annex).

5.2 Description on how the assessment has been conducted in terms of number of meetings, organization of working groups, etc

5.3 Start and finish date of the assessment.

(refer to paragraph 3.1.1.2 of the FSA Guidelines)

6 DESCRIPTION OF THE RESULTS ACHIEVED IN EACH STEP
(maximum 10 pages)

For each step, describe:

.1 method and techniques used to carry out the assessment;

.2 assumptions or limitations, if any, and the basis for them; and

.3 outcomes of each step of the FSA methodology, including:

STEP 1 - HAZARD IDENTIFICATION: (refer to paragraph 5.3 of the FSA Guidelines)

- *prioritised list of hazards*
- *identified significant accident scenarios*

STEP 2 - RISK ANALYSIS: (refer to paragraph 6.3 of the FSA Guidelines)

- *types of risk (e.g. individual, societal, environmental, business)*
- *presentation of the distribution of risks depending on the problem under consideration*
- *identified significant risks*
- *principal influences that affect the risks*
- *sources of accident and reliability statistics*

STEP 3 - RISK CONTROL OPTIONS: (refer to paragraph 7.3 of the FSA Guidelines)

- *what hazards are covered by current regulations*
- *identified risk control options*
- *assessment of the control options as a function of their effectiveness against risk reduction*

STEP 4 - COST BENEFIT ASSESSMENT: (refer to paragraph 8.3 of the FSA Guidelines)

- *identified types of cost and benefits involved for each risk control option*
- *cost-benefit assessment for the entities which are influenced by each option*
- *identification of the cost effectiveness expressed in terms of cost per unit risk reduction*

STEP 5 - RECOMMENDATIONS FOR DECISION-MAKING
(refer to paragraph 9.3 of the FSA Guidelines)

- *objective comparison of alternative options*
- *discussion on how recommendations could be implemented by decision-makers*

7 FINAL RECOMMENDATIONS FOR DECISION MAKING (maximum 2 1/2 pages)

List of final recommendations, ranked and justified in an auditable and traceable manner.

(refer to paragraph 9.3 of the FSA Guidelines)

ANNEXES (as necessary)

.1 name and expertise of the experts involved in the application
.2 list of references
.3 sources of data
.4 accident statistics
.5 technical support material
.6 any further information