Pergamon

Journal of Safety Research
33 (2002) 81–115

JOURNAL OF
SAFETY
RESEARCH

www.elsevier.com/locate/jsr

Offshore safety case approach and formal safety assessment of ships

J. Wang*

School of Engineering, Liverpool John Moores University, Byron Street, Liverpool L3 3AF, UK

Received 25 April 2001; accepted 1 August 2001

Abstract

Problem: Tragic marine and offshore accidents have caused serious consequences including loss of lives, loss of property, and damage of the environment. **Method:** A proactive, risk-based "goal setting" regime is introduced to the marine and offshore industries to increase the level of safety. **Discussion:** To maximize marine and offshore safety, risks need to be modeled and safety-based decisions need to be made in a logical and confident way. Risk modeling and decision-making tools need to be developed and applied in a practical environment. **Summary:** This paper describes both the offshore safety case approach and formal safety assessment of ships in detail with particular reference to the design aspects. The current practices and the latest development in safety assessment in both the marine and offshore industries are described. The relationship between the offshore safety case approach and formal ship safety assessment is described and discussed. Three examples are used to demonstrate both the offshore safety case approach and formal ship safety assessment. The study of risk criteria in marine and offshore safety assessment is carried out. The recommendations on further work required are given. **Impact on industry:** This paper gives safety engineers in the marine and offshore industries an overview of the offshore safety case approach and formal ship safety assessment. The significance of moving toward a risk-based "goal setting" regime is given. © 2002 National Safety Council and Elsevier Science Ltd. All rights reserved.

Keywords: Formal safety assessment; Marine safety; Offshore safety; Risk assessment; Safety case

---

* Tel.: +44-151-231-2445; fax: +44-151-231-2453.
E-mail address: j.wang@livjm.ac.uk (J. Wang).

PII: S0022-4375(02)00005-1

1. Current status of offshore safety assessment

Following the public inquiry into the *Piper Alpha* accident (Department of Energy, 1990), the responsibilities for offshore safety regulations were transferred from the Department of Energy to the Health and Safety Commission (HSC) through the Health and Safety Executive (HSE) as the single regulatory body for offshore safety. In response to the accepted findings of the *Piper Alpha* inquiry, the HSE Offshore Safety Division launched a review of all offshore safety legislation and implemented changes. The changes sought to replace legislation that was seen as prescriptive with a more "goal setting" regime. The mainstay of the regulations is the Health and Safety at Work Act. Under that act, a draft of the offshore installation (safety case) regulations was produced (Health and Safety Executive (HSE), 1992). It was then modified, taking into account comments arising from public consultation. The regulations came into force in two phases: (a) at the end of May 1993 for new installations and (b) on November 1993 for existing installations. The regulations require operational safety cases to be prepared for all offshore installations. Both fixed and mobile installations are included. Additionally, all new fixed installations require a design safety case. For mobile installations, the duty holder is the owner.

The HSE framework for decisions on the tolerability of risk is shown in Fig. 1, where there are three regions: (a) intolerable, (b) as low as is reasonably practicable (ALARP), and (c) broadly acceptable. Offshore operators must submit operational safety cases for all existing and new offshore installations to the HSE Offshore Safety Division for acceptance. An installation cannot legally operate without an accepted operational safety case. To be acceptable, a safety case must show that hazards with the potential to produce a serious accident have been identified and that associated risks are below a tolerability limit and have been

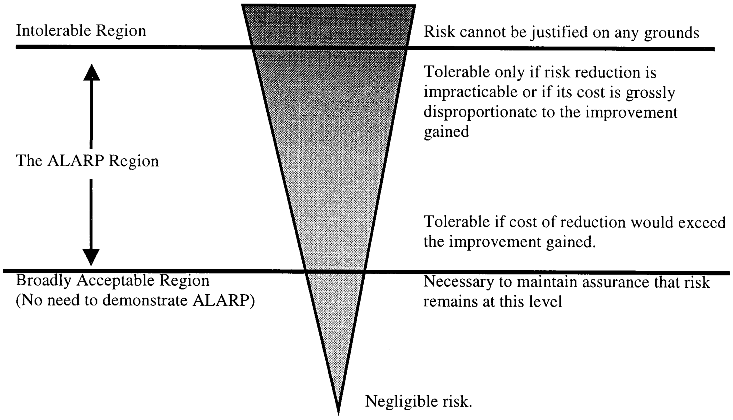


Fig. 1. The HSE framework for decisions on the tolerability of risk.

reduced ALARP. For example, the occurrence likelihood of events causing a loss of integrity of the safety refuge should be less than 10^{-3} per platform year (Spouse, 1997) and associated risks should be reduced to an ALARP level. It should be noted that the application of numerical risk criteria may not always be appropriate because of uncertainties in inputs. Accordingly, acceptance of a safety case is unlikely to be based solely on a numerical assessment of risk.

Fires and explosions may be the most significant hazards with potential to cause disastrous consequences in offshore installations. Prevention of fire and explosion and emergency response regulations (PFEER) were developed in order to manage fire and explosion hazards and the corresponding emergency responses that protect persons from their effects. A risk-based approach is used to deal with problems involving fire and explosion and emergency response. PFEER supports the general requirements by specifying goals for preventive and protective measures to manage fire and explosive hazards, to secure effective emergency response, and to ensure compliance with regulations by the duty holder. Management and administration regulations (MAR) were introduced to cover areas such as notification to the HSE of changes of owner or operator, functions, and powers of offshore installation managers. MAR is applied to both fixed and mobile offshore installations (excluding subsea offshore installations). The importance of safety of offshore pipelines has also been recognized. As a result, pipeline safety regulations (PSR) were introduced to embody a single integrated, goal-setting, risk-based approach to regulations covering both onshore and offshore pipelines.

After several years of experience of employing the safety case approach in the UK offshore industry, the safety case regulations were amended in 1996 to include verification of safety-critical elements, and the offshore installations and wells (design, construction, etc.) regulations (DCR) were introduced to deal with various stages of the life cycle of the installation. From the earliest stages of the life cycle of the installation, the duty holder must ensure that all safety-critical elements be assessed. Safety-critical elements are parts of an installation and of its plant (including computer programs) or any part whose failure could cause or contribute substantially to or whose purpose of which is to prevent or limit the effect of a major accident (Health and Safety Executive (HSE), 1996c). In DCR, (a) a verification scheme is introduced to ensure that a record is made of the safety-critical elements; (b) comment on the record by an independent and competent person is invited; (c) a verification scheme is drawn up by or in consultation with such person; (d) a note is made of any reservation expressed by such person; and (e) such scheme is put into effect (Health and Safety Executive (HSE), 1996c). All such records are subject to the scrutiny of the HSE at any time. More detailed information about the DCR can be found in Health and Safety Executive (HSE 1996a, 1996b, 1996c). DCR allows offshore operators to have more flexibility to tackle their own offshore safety problems. Offshore duty holders may use various safety assessment approaches and safety-based decision-making tools to study all safety-critical elements of offshore installations and wells to optimize safety. This may encourage offshore safety analysts to develop and employ novel safety assessment and decision-making approaches and to make more efforts to deal with offshore safety problems.

The relationships between such typical offshore safety regulations can be seen in Fig. 2, where the core regulations are the safety case regulations and others closely related to them.

Compliance with current offshore safety regulations is achieved by applying an integrated risk-based approach, starting from feasibility studies and extending through the life cycle of the installation. Design for safety is considered to be the most important. This is achieved through stages of hazard identification (HAZID) for the life cycle of installation from concept design to decommissioning and the use of state-of-the-art risk assessment methods (Janardhanan & Grillo, 1998). In a risk-based approach, early considerations are given to those hazards that are not foreseeable to design out by progressively providing adequate measures for prevention, detection, control, and mitigation and further integration of emergency response.

The main feature of the new offshore safety regulations in the UK is the absence of a prescriptive regime, which defines specific duties of the operator and adequate means. The regulations set forth high-level safety objectives, while leaving the selection of particular hazard arrangements in the hands of the operator. This is because hazards related to an installation are specific to its function and site conditions.

Recently, the industrial guidelines on a framework for risk-related decision support were produced by the UKOOA (1999). In general, the framework could be usefully applied to a wide range of situations. Its aim is to support major decisions made during the design, operation, and abandonment of offshore installations. In particular, it provides a sound basis for evaluating the various options that need to be considered at the feasibility and concept selection stages of a project, especially with respect to "major accidents hazards" such as fire, explosion, impact, and loss of stability. It can also be combined with other formal decision-making aids such as Multi-Attribute Utility Analysis (MAUA), Analytical Hierarchy Process (AHP), or decision trees if a more detailed or quantitative analysis of the various decision alternatives is desired.

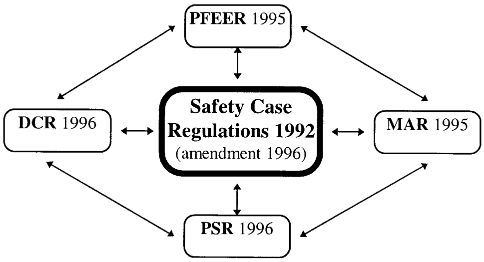


Fig. 2. Relationships between offshore safety regulations.

It should be noted that there can be significant uncertainties in the information and factors that are used in the decision-making process. These may include uncertainties in estimates of the costs, time scales, risks, safety benefits, the assessment of stakeholder views and perceptions, and so forth. There is a need to apply common sense and ensure any uncertainties are recognized and addressed.

2. Current status of formal ship safety assessment

Due to serious concerns over the safety of ships all over the world, the International Maritime Organization (IMO) continuously deals with safety problems in the context of operation, management, survey, ship registration, and the role of the administration. Improving safety at sea is highly stressed. The international safety-related marine regulations are guided by lessons learned from serious marine accidents that have happened. These lessons were first observed from the accidents. Then, the regulations and rules were produced to prevent similar accidents from occurring. For example, the capsize of the *Herald of Free Enterprise* in 1987 greatly affected the rule-developing activities of the IMO (Cowley, 1995; Sekimizu, 1997). The accident certainly raised serious questions on operation requirements and the role of management, which stimulated discussions in those areas at the IMO. This finally resulted in the adoption of the International Management System (ISM) Code. The *Exxon Valdes* accident in 1989, which was a large-scale oil spill, seriously damaged the environment. It facilitated the implementation of the international convention on Oil Pollution Preparedness, Response and Cooperation (OPRC) in 1990. Double hull or mid-deck structural requirements for new and existing oil tankers were subsequently applied (Sekimizu). The *Scandinavian Star* disaster in 1990 resulted in the loss of 158 lives. Furthermore, the catastrophic disaster of the *Estonia*, which capsized in the Baltic Sea in September 1994, caused more than 900 people to lose their lives. Those accidents highlighted the role of human error in marine casualties, and as a result, the new Standards for Training, Certificates and Watchkeeping (STCW) for seafarers were subsequently introduced.

After Lord Carver's report on the investigation of the capsize of the *Herald of Free Enterprise* was published (House of Lords, 1992), the UK Maritime and Coastguard Agency [previously named Marine Safety Agency (MSA)] quickly responded and in 1993 proposed to the IMO that formal safety assessment should be applied to ships to ensure a strategic oversight of safety and pollution prevention. The UK MCA also proposed that the IMO should explore the concept of formal safety assessment and introduce formal safety assessment in relation to ship design and operation. The IMO reacted favorably to the UK's formal safety assessment submission. Since then, substantial work (including demonstrating its practicality by a trial application to high-speed catamaran ferries and bulk carriers) has been done by the UK MCA. In general, for the last several years, the application of formal safety assessment has significantly progressed. This is demonstrated by the successful case studies of a high-speed craft and a bulk carrier and by the IMO approval of the application of a formal safety assessment for supporting rule-making process (MCA, 1997, 1998a, 1998b, 1998c; Wang, 2001).

Safety assessment in ship design and operation offers great potential incentives. Application of it may:

1. Improve the performance of the current fleet and make it possible to measure the performance change and ensure that new ships are good designs;
2. Ensure that experience from the field is used in the current fleet and that any lessons learned are incorporated into new ships; and
3. Provide a mechanism for predicting and controlling the most likely scenarios that could result in incidents.

Possible benefits have already been realized by many shipping companies. For example, P&O Cruises in the UK reviewed the implementation of risk assurance methods as a strategic project and proposed short/medium- and long-term objectives (Vie & Stemp, 1997). Its short/medium-term objectives are (a) to provide a reference point for all future risk assurance work, (b) to develop a structure chart that completely describes vessel operation, (c) to complete a meaningful HAZID as the foundation of the data set, (d) to enable identification of realistic options for vessel improvement, (e) to be a justified record of modifications adopted or rejected, and (f) to be capable of incorporating and recording field experience to ensure that the knowledge is not lost. Its long-term objectives are (a) to provide a mechanism for understanding the effect of modifications on total vessel performance, (b) to be capable of future development, (c) to provide a basis for total valuation of identified improvements using cost benefit analysis (CBA), (d) to generate a meaningful risk profile for vessel operation, and (e) to provide a monitor for evaluation of modification effectiveness. The idea of formal safety assessment may well be fitted to the above objectives in order to improve the company's performance.

3. Offshore safety assessment

The format of safety case regulations was advocated by Lord Robens in 1972 when he emphasized the need for self-regulation and pointed out the drawbacks of a rule book approach to safety. The concept of the safety case was derived and developed from the application of the principles of system engineering for dealing with the safety of systems or installations for which little or no previous operational experience exists (Kuo, 1998). The five key elements of the safety case concepts are illustrated in Fig. 3. A discussion of these follows:

1. *HAZID*. This step is to identify all hazards with the potential to cause a major accident.

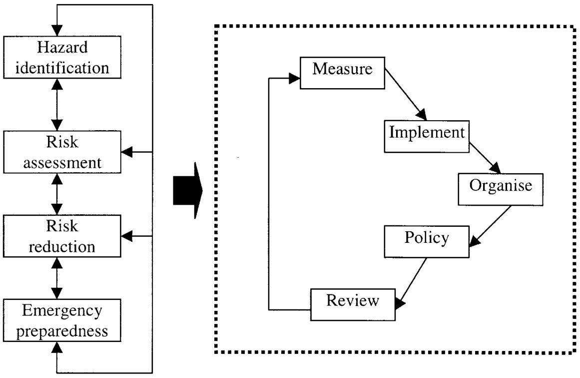


Fig. 3. The five key elements of the safety case concepts.

2. *Risk estimation*. Once the hazards have been identified, the next step is to determine the associated risks. Hazards can generally be grouped into three risk regions known as the intolerable, tolerable, and negligible risk regions as shown in Fig. 1.
3. *Risk reduction*. Following risk assessment, it is required to reduce the risks associated with significant hazards that deserve attention.
4. *Emergency preparedness*. The goal of emergency preparedness is to be prepared to take the most appropriate action in the event that a hazard becomes a reality so as to minimize its effects and, if necessary, to transfer personnel from a location with a higher risk level to one with a lower risk level.
5. *Safety management system* (SMS). The purpose of a safety management system is to ensure that the organization is achieving the goals safely, efficiently, and without damaging the environment. One of the most important factors of the safety case is an explanation of how the operator's management system will be adapted to ensure that safety objectives are actually achieved.

A safety case is a written submission prepared by the operation of an offshore installation. It is a stand-alone document that can be evaluated on its own but has cross-references to other supporting studies and calculations. The amount of detail contained in the document is a matter of agreement between the operator and the regulating authority. In general, the following elements of an offshore installation are common for many safety cases:

1. A comprehensive description of the installation.
2. Details of hazards arising from the operation installation.
3. Demonstrations that risks from these hazards have been properly addressed and reduced to an ALARP level.

4. Description of the safety management system, including plans and procedures in place for normal and emergency operations.
5. Appropriate supporting references.

The following activities characterize the development of a safety case:

1. Establish acceptance criteria for safety, including environment and asset loss, if possible. These may be both risk based and deterministic.
2. Consider both internal and external hazards using formal and rigorous HAZID techniques.
3. Estimate the frequency or probability of occurrence of each hazard.
4. Analyze the consequences of occurrence of each hazard.
5. Estimate the risk and compare with criteria.
6. Demonstrate ALARP.
7. Identify remedial measures for design, modification, or procedure to avoid the hazard altogether, reduce the frequency of occurrence, or mitigate the consequences.
8. Prepare the detailed description of the installation including information on protective systems and measures in place to control and manage risk.
9. Prepare a description of the safety management system and ensure that the appropriate hazard procedures are identified.

In offshore safety analysis, safety-based design/operation decisions are expected to be made at the earliest stages in order to reduce unexpected costs and time delays. A risk reduction measure that is cost effective at the early design stage may not be ALARP at the late stage. HSE regulations aim to have risk reduction measures identified and in place as early as possible when the cost of making any necessary changes is low. Traditionally, when making safety-based design/operation decisions for offshore systems, the cost of a risk reduction measure is compared with the benefit resulting from reduced risks. If the benefit is larger than the cost, then it is cost effective, otherwise it is not. This kind of CBA based on simple comparisons has been widely used in offshore safety analysis.

Conventional safety assessment methods and CBA approaches can be used to prepare a safety case. As the safety culture in the offshore industry changes, more flexible and convenient risk assessment methods and decision-making approaches can be employed to facilitate the preparation of a safety case. The UKOOA framework for risk-related decision support can provide an umbrella under which various risk assessment and decision-making tools are employed.

The guidelines in the UKOOA framework set out what is generally regarded in the offshore industry as good practice. These guidelines are a living document. Experience changes the working practices (both the business and social environment), and new technology may cause them to be reviewed and updated to ensure that they continue good practice. It should be noted that the framework produced by the UKOOA is only applicable to risks falling within the ALARP region shown in Fig. 1.

The life cycle approach manages the hazards that affect offshore installations (offshore safety study has to deal with the boundaries of other industries such as marine operations and aviation). In offshore safety study, it is best to obtain the optimum risk reduction solution for the total life cycle of the operation or installation, irrespective of the regulatory boundaries (UKOOA, 1999). The basic idea is to minimize/eliminate the source of hazard rather than place extremely high reliance on control and mitigatory measures. To reduce risks to an ALARP level, the following hierarchical structure of risk control measures (RCMs) should be followed:

- Elimination and minimization of hazards by "inherently safer" design
- Prevention
- Detection
- Control
- Mitigation of consequences

Decisions evolve around the need to make choices, either to do something or not to do something, or to select one option from a range of options. These can either take the form of rigid criteria that must be achieved or of goals or targets that should be aimed for but which may not be met. The UK offshore oil and gas industry operates in an environment where safety and environmental performances are key aspects of successful business. The harsh marine environment and the remoteness of many of the installations also provide many technical, logistic, and operational challenges. Decision-making can be particularly challenging during the early stages of design and sanction of new installations where the level of uncertainty is usually high.

In many situations, there may be several options that satisfy the requirements. It may also be difficult to choose a particular option that is obviously the best. If this is the case, there is a need to consider what is or may be "reasonably practicable" from a variety of perspectives and to identify and assess more than just the basic costs and benefits. The decision-making process can be set up to (UKOOA, 1999):

- Define the issue,
- Examine the options,
- Make the decision, and
- Implement, communicate, and review the decision.

Making risk-based decisions can be very difficult because it can be difficult to:

- Ensure that the choices have been properly selected and defined;
- Find ways to set out criteria and objectives;

- Identify risk issues and perceptions;
- Assess the performance of options against aspects that may not be quantifiable or that may involve judgments and perceptions that vary or are open to interpretation;
- Establish the relative importance of often widely different types of objectives and factors;
- Deal with uncertainties in estimates, data, and analyses;
- Deal with conflicting objectives and aspects of performance;
- Deal with differences in resolution of estimates, data, and analyses (these may not provide a fair reflection of the actual differences between the options being considered); and
- Deal with or avoid hidden assumptions or biases.

A narrow view in the decision-making process may result in decisions creating problems in other areas at a later time. For example, in a life cycle view of the project or installation, decisions made during design to decrease engineering and installation costs may lead to higher operating costs, reducing the overall profitability of the venue.

Safety and risk factors in the decision-making process include risk transfer, risk quantification, CBA, risk levels and gross disproportion, risk aversion, perception, risk communication, stakeholders, and uncertainties. As decision-making moves from the prescriptive nature to the descriptive nature, technology-based decision-making begins to include values. The hierarchical structure of the decision context is as follows (UKOOA, 1999):

- Prescription
- Well-established solution
- Well-understood risks
- Very novel
- Significant trade-offs or uncertainties
- Strong views and perceptions

The factors that affect offshore safety-based decision-making include degree of novelty versus well-understood situation or practice, degree of risk trade-offs and uncertainties, strength of stakeholder views and risk perceptions, and degree of business and economic implications (UKOOA, 1999). Decision calibration changes with design context. As the design context moves from prescription to strong views and perceptions, means of calibration change from codes and standards to external stakeholder consultation through verification, peer review, benchmarking, and internal stakeholder consultation.

The framework proposed by the UKOOA is also capable of reflecting the differences between the design of safety approaches for fixed offshore installations operating in the UK continental shelf versus mobile offshore installation

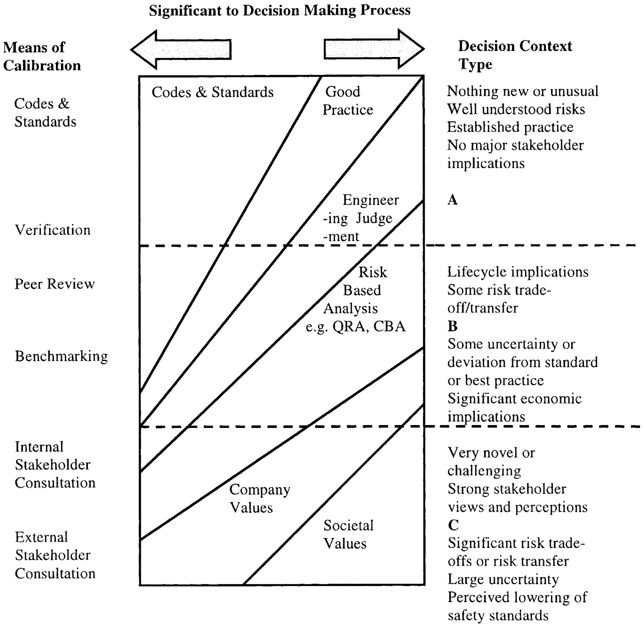


Fig. 4. The detailed UKOOA framework.

operating in an international market. Fixed offshore installations in the UK continental shelf are usually uniquely designed and specified for the particular duty and environment, and their design basis can be set against very specific hazards and specific processing and operation requirements. Many of the more complex design decisions therefore often fall into the Type B context in the detailed framework shown in Fig. 4. Mobile offshore installations have to operate in very different environments and tackle a wide range of operational activities and reservoir conditions. Specific codes and rules need to be applied. Therefore, many mobile offshore installation design decisions fall into the Type B context. Where neither codes and rules cannot be effectively applied nor traditional analysis cannot be carried with confidence, such installation may be categorized as Type C.

4. Formal ship safety assessment

Formal safety assessment is a new approach to maritime safety that involves using the techniques of risk and cost benefit assessment to assist in the decision-making process. There is a significant difference between the safety case approach and formal safety assessment. A safety case approach is applied to a particular ship, whereas formal safety assessment is designed to be applied to safety issues common to a ship type (such as high-speed passenger vessel) or to a particular hazard (such as fire). The philosophy of formal safety assessment is essentially the same as the one for the safety case approach. Many shipowners have begun to develop their own ship safety cases. The major difference between such ship specific applications of the approach and its generic application by regulators is that while features specific to a particular ship cannot be taken into account in a generic application, the commonalities and common factors that influence risk and its reduction can be identified and reflected in the regulator's approach for all ships of that type (Institute of Marine Engineers and MCE, 1998). This should result in a more rational and transparent regulatory regime. Use of formal safety assessment by an individual owner for an individual ship on the one hand and by the regulator for deriving the appropriate regulatory requirements on the other hand is entirely consistent (Institute of Marine Engineers and MCE, 1998).

It has been noted that many leading classification societies including Lloyds Register of Shipping and American Bureau of Shipping are moving toward a risk-based regime. It is believed that the framework of formal safety assessment can facilitate such a move.

A formal ship safety assessment framework that has been proposed by the UK MCA consists of the following five steps:

1. The identification of hazards
2. The assessment of risks associated with those hazards
3. Ways of managing the risks identified
4. Cost benefit assessment of the options
5. Decisions on which options to select

The above framework was initially studied at the IMO Maritime Safety Committee (MSC) Meeting 62 in May 1999. At the 65th meeting of the MSC in May 1995, strong support was received from the member countries and a decision was made to make formal safety assessment a high priority item on the MSC agenda. Accordingly, the UK decided to embark on a major series of research projects to further develop an appropriate framework and conduct a trial application on the chosen subject of high-speed passenger catamaran ferries. The framework produced was delivered to MSC 66 in May 1996, with the trial application programmed for delivery to MSC 68 in May 1997. An international formal safety assessment working group was formulated at MSC 66 and 67 where draft international guidelines were generated, including all key elements of the formal safety assessment framework developed by the UK.

Formal safety assessment involves much more scientific aspects than previous conventions. The benefits of adopting formal safety assessment as a regulatory tool include the following (Marine Safety Agency, 1993):

1. A consistent regulatory regime that addresses all aspects of safety in an integrated way;

2. Cost effectiveness, whereby safety investment is targeted to where it will achieve the greatest benefit;
3. A proactive approach enabling hazards that have not yet given rise to accidents to be properly considered;
4. Confidence that regulatory requirements are in proportion to the severity of the risks;
5. A rational basis for addressing new risks posed by ever-changing marine technology.

4.1. Identification of hazards

This step aims at identifying and generating a selected list of hazards specific to the problem under review. In formal ship safety assessment, a hazard is defined as "a physical situation with potential for human injury, damage to property, damage to the environment, or some combination" (Marine Safety Agency, 1993). HAZID is concerned with using the "brainstorming" technique involving trained and experienced personnel to determine the hazards. In formal ship safety assessment, an accident is defined as "a status of the vessel, at the stage where it becomes a reportable incident that has the potential to progress to loss of life, major environmental damage, and/or loss of the vessel" (Marine Safety Agency, 1993). The accident categories include (a) contact or collision, (b) explosion, (c) external hazards, (d) fire, (e) flooding, (f) grounding or stranding, (g) hazardous substances, (h) loss of hull integrity, (i) machinery failure, and (j) loading and unloading related failure. Human error issues should be systematically dealt with in the formal safety assessment framework. Significant risks can be chosen in this step by screening all the identified risks. Various scientific safety assessment approaches, such as Preliminary Hazard Analysis (PHA), Failure Mode, Effects and Criticality Analysis (FMECA), and HAZard and OPerability (HAZOP) study, can be applied in this step.

4.2. Assessment of risks

This step aims at assessing risks and factors influencing the level of safety. Risk assessment involves studying how hazardous events or states develop and interact to cause an accident. Shipping consists of a sequence of distinct phases between which the status of ship functions changes. The major phases include (a) design, construction, and commissioning; (b) entering port, berthing, unberthing, and leaving port; (c) loading and unloading; (d) dry-docking; and (e) decommissioning and disposal. A ship is made up of a set of systems such as machinery, control system, electrical system, communication system, navigation system, piping and pumping system, and pressure plant. A serious failure of a system may cause disastrous consequences. Risk assessment can be carried out with respect to each phase of shipping and each marine system. The likelihood of occurrence of each failure event and its possible consequences can be assessed using various safety assessment techniques such as an influence diagram, which is a combination of fault tree analysis and event tree analysis (Marine Safety Agency, 1993). An influence diagram can be used to deal with the escalation of an accident and mitigation aspects, such as the evaluation of people and containment of oil pollutants. Generic data or expert judgments can be used in risk assessment.

4.3. Risk control options

This step aims at proposing effective and practical risk control options. High-risk areas can be identified from the information produced in risk assessment. Then, the identification of RCMs can be initiated. In general, RCMs have a range of the following attributes:

1. Those relating to the fundamental type of risk reduction (i.e., preventative or mitigating).
2. Those relating to the type of action required and therefore to the costs of the action (i.e., engineering or procedural).
3. Those relating to the confidence that can be placed in the measure (i.e., active or passive and single or redundant).

RCMs can reduce frequency of failures and/or mitigate their possible efforts and consequences. Structural review techniques may be used to identify all possible RCMs for cost benefit decision-making.

4.4. Cost benefit assessment

This step aims at identifying benefits from reduced risks and costs associated with the implementation of each risk control option for comparisons. To conduct cost benefit assessment, it is required to set a base case that can be used as a reference for comparisons. A base case is the baseline for analysis reflecting the existing situation and what actually happens rather than what is supposed to happen. A base case reflects the existing levels of risk associated with the shipping activity before the implementation of risk control. Option costs and option benefits can be estimated. The Cost of Unit Risk Reduction (CURR) for each risk control option can then be obtained by dividing the net present value (NPV) of costs and benefits by the combined reduction in mortality and injury risks where 50 minor injuries are equivalent to 10 serious injuries or to one life. Those CURR values provide a relative ranking of the efficiency of alternative risk control options.

The evaluation of costs and benefits may be conducted using various methods and techniques. It should be initially carried out for the overall situation and then for those interested entities influenced by the problem consideration.

4.5. Decision-making

This step aims at making decisions and giving recommendations for safety improvement. The information generated can be used to assist in the choice of cost-effective and equitable changes and to select the best risk control option.

5. Risk criteria

Risk criteria are standards that represent a view, usually that of a regulator, of how much risk is acceptable/tolerable (Health and Safety Executive (HSE), 1995). In the decision-making process, criteria may be used to determine if risks are acceptable, unacceptable, or need to be reduced to an ALARP level. When Quantitative Risk Assessment (QRA) is performed, numerical risk criteria are required. The offshore industry has extensively used QRA and gained significant experience. The shipping industry has functioned reasonably well for a long time without consciously making use of risk criteria. Recently, QRA has been used extensively for ships carrying hazardous cargoes in port areas and for ships operating in the offshore industry (Spouse, 1997). In general, there are no quantitative criteria in formal safety assessment for a particular type of ship, although the MCA trial applications have used QRA to a certain extent. As time goes on, more QRA will be conducted in marine safety assessment. Therefore, numerical risk criteria in the shipping industry need to be dealt with in more detail.

As described previously in this paper, risk assessment involves uncertainties. Therefore, it may not be suitable to use risk criteria as inflexible rules. The application of numerical risk criteria may not always be appropriate because of uncertainties in inputs. Risk criteria may be different for different individuals. They would also vary between societies and alter with time, accident experience, and changing expectation of life. Risk criteria can therefore only assist judgments and be used as guidelines for decision-making.

In different industries, risk criteria are also different. For example, in the aviation industry, failure with catastrophic effects must have a frequency less than 10^{-9} per aircraft flying hour. In the nuclear industry, the basic principles of the safety policy recommended by the International Commission Radiological Protection (ICRP) are that no practice shall be adopted unless it has a positive net benefit; that all exposures shall be kept As Low As Reasonably Achievable (ALARA), taking economic and social factors into account; and that individual radiation doses shall not exceed specific criteria (International Commission on Radiological Protection, 1977). There are no explicit criteria used by ICRP.

For ships, the general risk criteria may include the following: (a) the activity should not impose any risks that can reasonably be avoided; (b) the risks should not be disproportionate to the benefits; (c) the risks should not be unduly concentrated on particular individuals; and (d) the risks of catastrophic accidents should be a small proportion of the total (Spouse, 1997). More specifically, individual risk criteria and social risk criteria need to be defined. For example, maximum tolerable risk for workers may be 10^{-6} per year according to the HSE industrial risk criteria. In the regions between the maximum tolerable and broadly acceptable levels, risks should be reduced to an ALARP level, taking costs and benefits of any further risk reduction into account (Wang, 2001).

6. Applications of offshore safety case approach and formal ship safety assessment

6.1. Formal safety assessment of a generic containership

Although there were not many major casualties, in terms of loss of lives, resulting from accidents involving containerships, this particular ship type has more of its fair share of losses due to incidents involving cargo damage, personal injury, collision, ship structural failure, and pollution (UK P&I Club, 1999; Wang & Foinikis, 2001). Major accidents in the last decade include the total loss of the *C/V Pioneer Container* in 1994 due to a collision in the South China Sea; the loss of the *C/V River Gurara* in 1996; the extensive damages suffered by the *C/V Toyama Maersk* in 1997 due to a collision with a Gas Carrier in the Singapore Strait; the loss of the *C/V MSC Carla* in 1998, which broke in two in bad weather conditions; and the extensive damages suffered by the *M/V APL China* in 1999 due to severe bad weather conditions. Statistics indicate that incidents involving containerships account up to about 7% of the total (Wang & Foinikis, 2001).

In terms of incident categories, containerships differ from most other ship types in that shore error accounts for a high percentage of all major incidents. The result is an equally high percentage of cargo damage. Although containerships follow the same pattern as the majority of cargo vessels, as far as the types of damages, they do differentiate in various aspects. The relative statistics available show that the percentage of incidents is higher in newer containerships, decreasing as they age, while in other cargo ship types, higher incident rates occur in their middle age. The same statistics show that a high percentage of all incidents caused by human error were due to shore-based personnel error, which is far higher than other cargo ship types. As far as ship size is concerned, the smaller ships of this type have fewer incidents (Wang & Foinikis, 2001).

Other operational characteristics of containerships, such as the fact that they very rarely travel in ballast condition and have few opportunities for overnight stay at ports, contribute to the overall performance of these vessels and their operators. At this point, it should be noted that although a relatively large amount of detailed data exists, organizations such as classification societies and private shipping companies possessing them are reluctant to release them. This is mainly due to the high competition in the market. On the other hand, either government agencies are not ready yet to dedicate the necessary resources for data collection, or the time period for which relevant government projects are run is not sufficient to produce reliable data.

6.1.1. *The generic containership*

The generic model of containership needs to be developed according to IMO Interim Guidelines (IMO, 1997), taking into consideration the particular systems and characteristics required for the transportation of containerized cargo. The generic containership is not a "typical" vessel but a hypothetical one consisting of all technical, engineering, operational, managerial, and environmental (physical, commercial, and regulatory) networks that interact during the transportation of containerized cargo. For a generic containership, the following assumptions are applied:

- The containership average lifetime: 25 years
- The average number of operational days per year: 330
- Operational hours per day: 24
- Major maintenance frequency: 1 every 2.5 years (30 months).

Containerships follow the general pattern that all international trading cargo ships do, but they differentiate in various aspects. The primary ones appear to be as follows:

6.1.1.1. Structure. The structure of a containership is typified by holds longitudinally divided in two sections (fore and aft), each being able to accommodate either one 40-ft unit or two 20-ft units. Holds are fitted with vertical "L"-shaped guides (cell guides) used to secure the units into their stowage position. Internal containership holds are box shaped surrounded by ballast, fuel tanks, and void spaces.

6.1.1.2. Strength and stability. Like most cargo vessels, containerships are equipped with means to calculate stability, shear forces (SF), and bending moments (BM). The differentiating feature of containerships is the additional need for the calculation of torsion moments (TM). This is necessary in cases where there is an uneven distribution of cargo because the vessel is partly loaded while proceeding to various ports before completing its loading.

Deck cargo reduces the stability of the vessel and calls for increased inherent or design stability of the vessel itself. It is not an uncommon phenomenon that a "metacentric height" (GM) is 6.5 m for a Panamax size containership in "light ship" condition. The use of high-speed diesel engines increases the fuel consumption rate, which imposes the need for large fuel tanks, usually located at, or close to, the midsection of the vessels. Thus, as fuel is consumed, bending moments and shearing forces are increasing. It is noteworthy that many modern containerships are equipped with real-time stress monitoring equipment allowing for automated correction of excessive values using ballast.

6.1.1.3. Cargo and ballast operations. This is one of the main differences between containerships and other cargo vessels. Loading and unloading cargo operations are carried out simultaneously and at very high rates. The cargo loaded and discharged is calculated based on the values declared by the shippers for each unit and by weighing the units upon their arrival at the terminal gate. Cargo operations are normally preplanned by terminal personnel in simulated conditions and are subject to evaluation and acceptance by the ship's personnel. Real-time follow-up of the operation is carried out both onboard and ashore and the final figures of stability, stresses, and cargo quantities are then calculated.

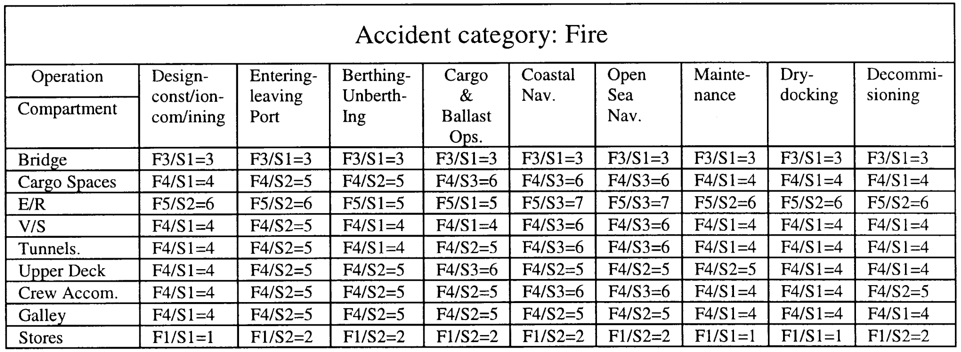
6.1.1.4. Maneuverability, power, and propulsion. Containerships are generally fitted with thrusters (bow and/or stern) and, in several cases, active rudders. This, coupled with the advanced hydrostatic features (i.e., block coefficient) of these vessels, produces a high level of maneuverability at all speed levels. High speeds, nevertheless, tend to reduce the time available for reaction by operators, adversely affecting the human reliability in close quarter situations.

6.1.1.5. The cargoes carried. The majority of the cargoes carried are of high value, as opposed to bulk carriers and crude oil tankers, which tend to carry raw material of lower values. Containerized cargoes come in small parcels, while bulk cargoes (dry or liquid) come in larger ones. Goods traveling in a sealed container produce a problem of uncertainty as far as the characteristics of the cargo (i.e., quantity, quality security, and inherent hazards) are concerned. The information for such features is received by the documents accompanying the sealed unit and is rarely cross-checked. Only in cases of suspected existence of undeclared dangerous goods does the law provide for ship personnel to demand inspection of the unit's contents.

Due to the high loading rates and time pressure, most of the paperwork is received "in good faith" and the burden of avoiding, and in the worse case combating, hazardous situations falls on the ship personnel. Cases of undeclared hazardous substances and poorly maintained containers and tanks have been identified but are rarely reported to the authorities, usually following a compromising agreement between carriers and cargo owners (Transportation Safety Board of Canada [TSBC] 1999).

6.1.1.6. Cargo recipients (consignees). Another difference that containerships have is the one connected with the cargo recipients (consignees). Unlike other ship types (i.e., bulk carriers and tankers), the number of cargo consignees is highly increased. Even within the same unit, there may be more than one recipient. This fact, combined with the high value of the cargoes carried and their hazardous nature, increases both the exposure of the carriers for possible damage and the difficulty in coordination and cooperation between ship and cargo owners during contingency situations.

6.1.1.7. Ports and terminals. Container-handling ports and terminals have a distinct general layout and organization. Container terminals have the ability to concurrently carry out loading and discharging operations, while terminals



Accident category: Fire

Operation Compartment	Design-const/ion-com/ining	Entering-leaving Port	Berthing-Unberth-Ing	Cargo & Ballast Ops.	Coastal Nav.	Open Sea Nav.	Maintenance	Dry-docking	Decommisioning
Bridge	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3	F3/S1=3
Cargo Spaces	F4/S1=4	F4/S2=5	F4/S2=5	F4/S3=6	F4/S3=6	F4/S3=6	F4/S1=4	F4/S1=4	F4/S1=4
E/R	F5/S2=6	F5/S2=6	F5/S1=5	F5/S1=5	F5/S3=7	F5/S3=7	F5/S2=6	F5/S2=6	F5/S2=6
V/S	F4/S1=4	F4/S2=5	F4/S1=4	F4/S1=4	F4/S3=6	F4/S3=6	F4/S1=4	F4/S1=4	F4/S1=4
Tunnels.	F4/S1=4	F4/S2=5	F4/S1=4	F4/S2=5	F4/S3=6	F4/S3=6	F4/S1=4	F4/S1=4	F4/S1=4
Upper Deck	F4/S1=4	F4/S2=5	F4/S2=5	F4/S3=6	F4/S2=5	F4/S2=5	F4/S2=5	F4/S1=4	F4/S1=4
Crew Accom.	F4/S1=4	F4/S2=5	F4/S2=5	F4/S2=5	F4/S3=6	F4/S3=6	F4/S1=4	F4/S1=4	F4/S2=5
Galley	F4/S1=4	F4/S2=5	F4/S2=5	F4/S2=5	F4/S2=5	F4/S2=5	F4/S1=4	F4/S1=4	F4/S1=4
Stores	F1/S1=1	F1/S2=2	F1/S2=2	F1/S2=2	F1/S2=2	F1/S2=2	F1/S1=1	F1/S1=1	F1/S2=2

Fig. 5. Fire rankings using the "Risk Matrix Approach" expert judgement.

handling bulk cargoes tend to be specialized in either loading or discharging. In addition, cases where bulk carrier terminals can handle both loading and discharging, the two operations are never carried out simultaneously.

6.1.2. Formal safety assessment of a containership

In this paper, the test case is limited to one accident category only, namely "fire." In addition, mainly because only insufficient historical data are available, assumptions may be employed based on the experience in the field.

6.1.2.1. Step 1. Having identified the accidents, the causes are then grouped in terms of human error, hardware failures, external events, and so forth. The "fire" accident subcategories are listed as follows:

- Navigation bridge
- Cargo spaces
- Engine room
- Void spaces
- Tunnels
- Upper deck area
- Crew accommodation
- Galley
- Provisions' storage spaces (including bonded stores)

The screening process is carried out using the "Risk Matrix Approach" (Loughran, Pillay, Wang, Wall, & Ruxton, 2002). The combination frequency and severity rankings is used for the estimation of the Risk Ranking Number (RRN). The final ranking for the accident category of "fire" takes the form as presented in Fig. 5.

6.1.2.2. Step 2. In this step, the Potential Loss of Lives (PLL) and its distribution through the influence diagram will be determined. An illustration of the influence diagram for the accident category "fire" is in Fig. 6. Below the accident category level, the structure is a graphical representation of the accident subcategory, including all the combinations of relevant contributing factors for each accident subcategory. Above the accident category level is an event tree representation of the development of the accident category to its final outcome.

The study can then continue in order for the regulatory, commercial, and social/political influencing environments in each accident category to be deliberated and eventually quantified with regard to human and hardware failures and external events. The outcomes are shown in Fig. 7.

6.1.2.3. Step 3. The table constructed for the accident category "fire" is shown in Fig. 8. This figure shows that the areas requiring less consideration are clearly identifiable and appear to be the "provision stores" and "upper deck areas." For

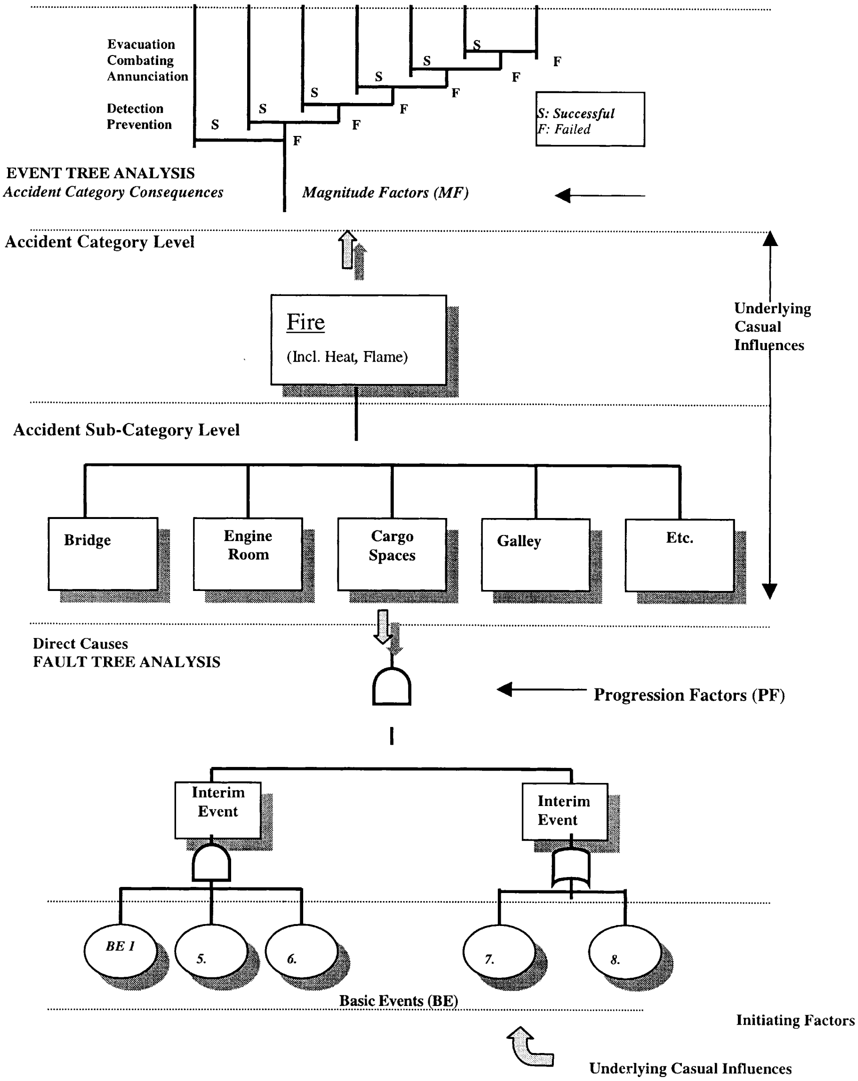


Fig. 6. Risk contribution tree for fire.

each of the remaining areas (subcategories), casual chains need to be constructed and risk reduction measures need to be identified.

Risk reduction measures are then grouped according to their effect on the system under consideration. The risk reduction measures (RCM) will then be evaluated, taking into account their effectiveness within the event trees or influence diagrams rather than their cost, utilizing once more expert judgments. The most effective RCM(s) can then be forwarded to the next step.

ACCIDENT CATEGORY: FIRE		
Compartment (Sub-Category)	% Incidents expected	Frequency (per vessel/year)
Navigation Bridge	2	1.4E-04
Cargo Spaces	6	4.3E-04
Engine Room	75	5.3E-03
Void Spaces	4	2.8E-04
Tunnels	4	2.8E-04
Upper Deck Areas	0.9	6.4E-05
Crew Accommodation	3	2.1E-04
Galley	5	5E-04
Provision Stores	0.1	7.1E-06
TOTAL	100	

Fig. 7. Incident database for fire.

6.1.2.4. Step 4. The most preferable featured of the CBA model construction is its use of nested computer spreadsheets to calculate the costs and benefits of each selected RCM. The quantification of the costs and benefits is achieved in terms of Net Present Value, which can be converted into a CURR value.

It is essential to carry out the above procedure for the overall situation as well as for each particular accident category. The CBA outcomes can then be listed according to their significance to the various stakeholders.

6.1.2.5. Step 5. In this step, final decisions are made, taking into account each individual RCM's CURR value and PLL reduction capabilities, as determined and listed by the safety analysts.

Formal safety assessment can be feasibly applied to containerships, provided that several areas, causing uncertainties, are further deliberated. These areas influence both the general principles of formal safety assessment and the specific requirements for containerships, either directly or indirectly.

6.2. Formal safety analysis of a generic fishing vessel

The generic fishing vessel is a hypothetical vessel of any size and method of fishing. It includes all of the functions of operation that are necessary for any

ACCIDENT CATEGORY: FIRE			
Compartment (Sub-category)	Potential Loos of Life (PLL)	Frequency (Per vessel/year)	Severity (max. observed)
Navigation Bridge	2.2E-04	1.4E-04	1
Cargo Space	6.6E-04	4.3E-04	4
Engine Room	7.7E-03	5.3E-03	3
Void Spaces	4.4E-04	2.8E-04	3
Tunnels	4.4E-04	2.8E-04	3
Upper Deck Areas	9.9E-05	6.4E-05	3
Crew Accommodation.	3E-04	2.1E-04	3
Galley	5.5E-04	5E-04	2
Provision Stores	1.1E-05	7.1E-06	3

Fig. 8. Cumulative table for fire subcategories.

fishing vessel. Fishing, being a combined production and transport operation, is cyclic with the following distinct phases of life (Loughran et al., 2002):

- Design, construction, and commissioning
- Entering port, berthing, unberthing, and leaving port
- Fish loading and unloading
- Passage
- Dry dock and maintenance period
- Decommissioning and scraping

Fig. 9 shows the considerations when defining a generic fishing vessel for safety analysis purposes. These are the factors that will affect the safety and reliability of the vessel as the status of the ship function changes. A generic fishing vessel may also be thought of as being a combination of hard and soft systems as listed below:

- Communications
- Control
- Electrical
- Human
- Lifting
- Machinery
- Management system
- Navigation
- Piping and pumping
- Safety

The Fishing Vessel (Safety Provision) Rules of 1975 are still used by the fishing industry. Virtually all of the categories of accidents affecting humans directly are not specifically addressed in the 1975 Rules. This is because the 1975 Rules are

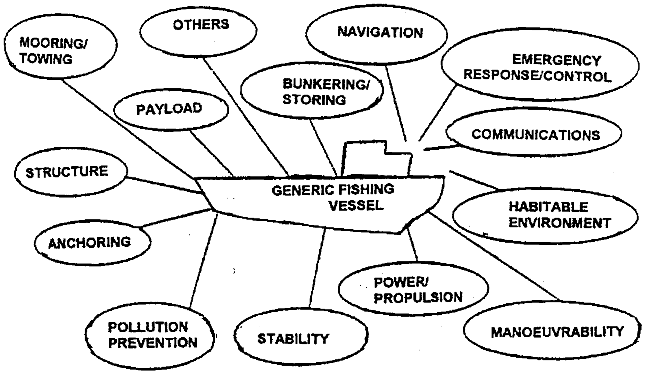


Fig. 9. Generic fishing vessel.

directed toward the safety of the vessel as a ship and nothing within the rules is particular to her role in fishing or to the act of fishing itself. The rules are primarily concerned with vessels over 12 m registered length. For some indeterminate reason, these rules do not concern themselves with the whole vessel but may be noted to consider the vessel from the deck and accommodation line downwards. The winches, wires, and fishing equipment are not covered by the rules.

In many reports of fishing vessel accidents, information is incomplete or totally lacking. This makes it difficult to analyze the events that lead to the accident. Accurate historical and current data on vessels, fishermen, professional experience, hours and nature of exposure, and safety performance of personnel and equipment are fundamental to assessing safety problems, monitoring results of safety programs, and measuring the effectiveness of safety improvement strategies. Very few data are regularly collected or published on these parameters. The limited data make it difficult to quantify safety problems, determine casual relations, and assess safety improvement strategies. However, the data that are available indicate that significant safety problems exist and that human error, vessel and equipment inadequacies, and environmental conditions all contribute to them (Loughran et al., 2002).

The literature survey found that safety assessment of fishing vessels had been limited to stability consideration and very little work has been carried out on the operational and equipment safety assessment. A full formal safety assessment application to a fishing vessel is yet to be carried out. In this paper, considering the current situation of fishing vessel safety, the formal safety assessment proposed by the MCA cannot be directly applied to a generic fishing vessel. It may be more appropriate to concentrate on the first two steps in the formal safety assessment proposed by the MCA. As a result, a formal safety analysis for a generic fishing vessel is proposed (Loughran et al., in press). The proposed formal safety analysis is based on the principle that formal safety assessment considers the characteristics of fishing vessels, addresses these areas, and identifies the high-risk areas that need design and/or operational attention. The formal safety analysis can be developed into five steps for ease of understanding as follows:

1. HAZID
2. Risk quantification
3. Risk ranking
4. Recommendations
5. Decision-making

Fig. 10 illustrates the proposed approach by means of a flowchart. A test case study on a generic fishing vessel as defined earlier is used to demonstrate the proposed formal safety analysis. The first step of the analysis is HAZID. This consists of determining which hazards affect the fishing vessels' activities under consideration using "brainstorming" techniques involving trained and experienced personnel. In the HAZID phase, the combined experience and insight of engineers is required to systematically identify all potential failure events at each

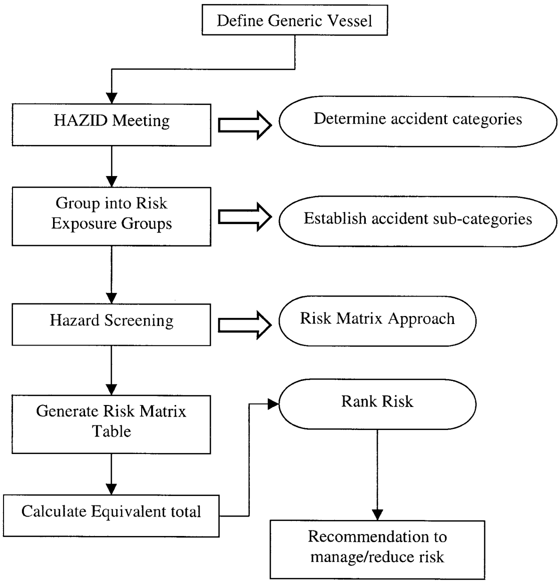


Fig. 10. The proposed approach.

required indenture level with a view to assessing their influences on system safety and performance. Various safety analysis methods may be used individually or in a combination to identify the potential hazards of a system.

Such typical methods include the following:

1. Preliminary hazard analysis (Henley & Kumamoto, 1992; Smith, 1993; Villemeur, 1992)
2. Fault tree analysis (Henley & Kumamoto, 1992; Smith, 1993; Villemeur, 1992)
3. Event tree analysis (Henley & Kumamoto, 1992; Smith, 1993; Villemeur, 1992)
4. Cause-consequence analysis (Henley & Kumamoto, 1992; Smith, 1993; Villemeur, 1992)
5. Failure mode, effects and criticality analysis (MIL STD)
6. Hazard and operability analysis (Henley & Kumamoto, 1992; Villemeur, 1992)
7. Boolean representation method (Wang, Ruxton, & Labrie, 1995)
8. Simulation analysis (Henley & Kumamoto, 1992; Villemeur, 1992)

Information produced from the HAZID phase will be processed to estimate risk. In the risk quantification phase, the likelihood and possible consequences of each system failure event will be estimated either on a qualitative basis or a quantitative basis (if the events are readily quantified). The level of potential consequences of a system failure event may be quantified in economic terms with regard to loss of lives/cargo/property and the degradation of the environment caused by the occurrence of the system failure event. The results produced from the risk quantification phase may be used through the risk-ranking phase to assist designers and operators in developing maintenance and operation policies to avoid the system failure events. Risk ranking can be undertaken on a qualitative basis if only qualitative safety information is available.

Accident categories that are considered in this analysis include the following:

- Foundering and flooding
- Stranding and grounding
- Collisions and contact
- Capsizing and listing
- Fires and explosions
- Machinery damage
- Heavy weather damage
- Missing vessels
- Others

Having identified the accident categories, the causes are then grouped into following risk exposure groups:

1. Human errors
Human performance
Communication
Navigation
Competency
Fishing
Anchoring
Mooring
Abandonment
Commercial pressures
Manning
Finance
Company or firm procedures
Onboard management
Systems management
Loading fish
Shore side systems
2. Hardware failures
Material of construction
Structure
Propulsion
Steering
Piping and plumbing
Control
Electrical
Refrigeration
Safety systems
Habitable environment
Emissions control
Bunkering and storage
Diagnostics systems
Maintenance systems
External events
Environment
Pollution prevention
Climatic variations
Payload
Fish handling, loading, and storage
Crane/lifting mechanisms
Berthing

In order to sort the large amount of information collected at the HAZID meeting, a set of accident subcategories is established as follows:

Collision and contact accident subcategory

- Berthed
- Starting up
- Loading and unloading in port
- Departing and maneuvering close to the berth
- Maneuvering in harbor and close to harbor
- Passage in open sea
- Loading fish at sea
- Entering harbor
- Arrival maneuvering close to the berth
- Shutdown
- Abnormal operation
- Maintenance
- Anchored
- Dry-docked

Fire accident subcategory

- Engine room
- Fish room space
- Wheelhouse
- Accommodation
- Galley

Loss of hull integrity accident subcategory

- Hull plating
- Framing
- Bulkheads
- Welds and joints
- Penetrations
- Seals
- Appendages
- Opening or failure of doors
- Opening or failure of scuttles
- Other

The Risk Matrix Approach is used in the hazard screening process. For each appropriate combination, an assessment has been made of the frequency (F) of the accident and the severity (S) of the consequences in terms of human injuries/deaths, property damage/loss, and the degradation of the environment. The corresponding RRN is then selected from the Risk Matrix Table. This method allows for expert judgments where detailed data are

		F1	F2	F3	F4	F5	F6	F7
S1	Minor Injuries	**1**	**2**	**3**	**4**	**5**	**6**	**7**
S2	Major injuries	**2**	**3**	**4**	**5**	**6**	**7**	**8**
S3	1 to 10 Deaths	**3**	**4**	**5**	**6**	**7**	**8**	**9**
S4	> 10 Deaths	**4**	**5**	**6**	**7**	**8**	**9**	**10**

Fig. 11. Risk matrix table.

unavailable. Fig. 11 shows the Risk Matrix Table, which gives (in a tabular format) a risk level related to the frequency and severity of an accident. RRN ranges from 1 (least frequent and least severe consequence) to 10 (most frequent and most severe consequence).

Fig. 12 gives the interpretation of the frequencies $F1-F7$ in terms of a generic fishing vessel based on the following estimations:

1. Vessel life expectancy: 25 years
2. Operational days per year: 250
3. Operational hours per day: 13
4. Major maintenance per year: 1

After identifying the high-risk areas and ranking them in order of importance, the next step is to make recommendations to manage/minimize the risk for the associated hazards. This could be achieved by applying the "brainstorming" method used earlier. The decision on which control option is most beneficial to implement is dependent on several factors such as cost, availability, and effectiveness. The formal safety analysis can be further developed to make it more elaborate and complete by using the MCA/IMO type of formal safety assessment for a generic vessel.

Likely to happen on a vessel once per Frequency	**General Interpretation**	**Generic fishing vessel Interpretation**
F1 10000 - 100000 years	Extremely remote to extremely improbable	Likely to happen every 20 yrs in the industry
F2 1000 – 10000 years	Remote to extremely remote	Likely to happen every 2 yrs in the industry
F3 100- 1000 years	Remote	Likely to happen 5 times per yr in the industry
F4 10 – 100 years	Reasonably probable to remote	Likely up to 3 times per vessel life
F5 1 – 10 years	Reasonably probable	Likely up to 30 times per vessel life
F6 Yearly	Reasonably probable to frequent	Likely annually per vessel
F7 Monthly	Frequent	Likely monthly per vessel

Fig. 12. Key to risk matrix table.

6.3. Safety case of an offshore installation

The following seven parts drawn from a safety case (Sii, 2001) are subjects that can be found in a typical safety case for the operations of an offshore installation:

6.3.1. Part I: Introduction and management summary

Part I of an operational safety case is an introduction and management summary. It will

(A) Describe the scope and structure of the safety case,
(B) Describe the ownership and operatorship of the installation, and
(C) Provide brief summaries of Parts II–VII, highlighting major conclusions.

A summary of all the key features contained in the safety case is outlined, including the following:

- Definition of the safety case
- Objectives
- Scope and structure of the seven parts of the safety case
- Usage of the safety case
- Custodian of the safety case
- Review periods and updates
- Application of the hazard management process to the operation
- Hazard analysis of the operation
- Remedial work
- Conclusions drawn concerning the safety of the operation

6.3.2. Part II: Operations safety management system

Part II is a concise description of the safety management system in evidence at the installation. It summarizes both the corporate and installation specific policies, organizational structures, responsibilities, standards, procedures, processes, controls, and resources that are in place to manage safety.

The six main sections of Part II cover the following:

(a) Policies and objectives
(b) Organization, responsibilities, and resources
(c) Standards and procedures
(d) Performance monitoring
(e) Audits and audit compliance
(f) Management review and improvement

6.3.3. Part III: Activities catalogue

Part III contains the activities catalog that lists all safety activities applicable to the operation in the activity specification sheet. The activity specification sheet describes the activity and the hazard management objectives of that activity, safety-related inputs and outputs, methods used to achieve the hazard management objectives, along with management controls applied and the accountability for meeting the stated objectives. Any areas of concern arising from these sheets are noted as deficiencies.

6.3.4. Part IV: Description of operations

Part IV describes the essential features of the installation in sufficient detail to allow the effectiveness of safety systems to be appreciated. As such, it describes the purpose of the installation and the processes performed there and its relationship to the location, reservoir, and other facilities. Operational modes and manning for the installation are described (e.g., normal operation, shut down configurations, maintenance modes, etc.).

The essence of Part IV is not to give a detailed physical description but to explain how the various systems relate to the safety of the installation and how their use can affect safety.

6.3.5. Part V: Hazard analysis, hazard register, and manual of permitted operations (MOPO)

Part V provides a description of the hazards, their identification, ranking, and assessment, the means by which they are to be controlled, and the recovery mechanisms. The design reviews and audits carried out to identify and assess hazards are also described.

It contains four sections:

(a) Hazard assessment
(b) Hazard register (including the hazard/activity matrix)
(c) Safety-critical operational procedures (SCOP)
(d) MOPO

The sections are constructed as follows:

(a) A summary of all hazard investigations, design reviews, and audits carried out, stating the major findings and recommendations from those investigations and the follow-up of recommended action items.
(b) The hazard register, which describes each hazard in terms of
  - The way it was identified,
  - The methods used to assess the possible dangers presented by the hazard,
  - The measures in place to control the hazard, and
  - The methods used to recover from any effects of the hazard.

It also contains the hazard/activity matrix that cross-refers the activities identified in Part III with their effects on the identified hazards.

(c) The MOPO defines the limits of safety operation permitted when the defenses are reduced, when operating conditions are unusually severe, or during accidental activities.
(d) A list of all safety-critical operations procedures identifying the key hazard controls and recovery procedures required for the installation.

6.3.6. Part VI: Remedial action plan

Part VI records any deficiencies identified during the studies that lead to Parts II–V and require action to be taken. The record known as the "remedial action plan" includes the following:

- A statement of each identified deficiency
- The proposed modifications to address the problem
- An execution plan to show action parties and planned completion dates

This remedial action plan is used as the basis of the improvement plan, and as such, the plan is regularly reviewed and updated annually.

6.3.7. Part VII: Conclusion and statement of fitness

Part VII includes summaries of the major contributors to risk, the acceptance criteria for such risks, deficiencies identified, and planned remedial actions.

Part VII ends with a "statement of fitness," which is the asset owner's statement that he/she appreciates and understands the hazards of the operation and considers that sufficient hazard control mechanisms are in place for the operation to continue. This statement is signed by the assess owner and approved by the signature of the operations directors.

7. Discussion and conclusion

An offshore installation/ship is a complex and expensive engineering structure composed of many systems and is usually different from others (Wang & Ruxton, 1997). Offshore installations/ships need to constantly adopt new approaches, new technology, new hazardous cargoes, and so forth, and each element brings with it a new hazard in one form or another. Therefore, safety assessment should cover all possible areas including those where it is difficult to apply traditional safety assessment techniques. Such traditional safety assessment techniques are considered to be mature in many application areas. Depending on the uncertainty level and/or the availability of failure data, different methods can be applied individually or in combination to deal with the situation. Lack of reliable safety data and lack of confidence in safety assessment have been the two major problems in safety analysis of various engineering activities. To solve such problems, further development may be required to develop novel safety assessment techniques for dealing with uncertainty properly and also to use decision-making techniques on a rational basis.

Safety assessment techniques currently used in offshore/ship safety assessment need to be further studied and the criteria for effective use of them need to be established in safety assessment. It is not feasible to apply one safety assessment method to identify and assess risks in a complete offshore installation/ship life cycle. An effective way is to use different safety assessment methods and apply them individually or in combination, depending on the particular situation, to assess risks with respect to each phase of the offshore installation/ship life cycle and each accident category (Wang & Ruxton, 1997). Existing safety assessment methods need to be studied regarding safety data flow and their interrelations to make full use of the advantages of each method. The conditions in which particular safety assessment methods are most effectively applied also need to be studied in the context of the full offshore installation/ship life cycle and accident categories.

7.1. Offshore safety

In offshore safety assessment, a high level of uncertainty in failure data has been a major concern, which is highlighted in the UKOOA's framework for risk-related decision support. Different approaches need to be applied with respect to different levels of uncertainty. UKOOA's framework also allows offshore safety operators to employ new risk modeling approaches and decision-making techniques in offshore safety assessment.

Novel decision-making techniques based on safety assessment are also required to make design and operation decisions effectively and efficiently. When operational aspects are considered in the decision-making process, it may be difficult to compare costs and benefits for all systems on a common basis since costs and benefits of systems vary differently with operational aspects. Furthermore, when more design parameters such as reliability are taken into account in the decision-making process, simple comparison of costs and benefits cannot be conducted. It may be required to develop an effective technoeconomic model that takes various costs and benefits into account (Wang, Yang, Sen, & Ruxton, 1996; Wang, Yang, & Sen, 1996). Formal Multiple Criteria Decision-Making (MCDM) techniques may be applied to process the mathematical model to determine where risk reduction actions are cost effective and how this is to be done (Wang et al., 1996; Yang & Sen, 1994).

Software safety analysis is another area where further research is required. In recent years, advances in computer technology have been increasingly used to fulfill control tasks to reduce human error and to provide operators with a better working environment in ships. This has resulted in the development of more and more software intensive systems. However, the utilization of software in control system has introduced new failure modes and created problems in the development of safety-critical systems. The DCR 1996 dealt with this issue in the UK offshore industry. In formal ship safety assessment, every safety-critical system also needs to be investigated to make sure that it is impossible or extremely unlikely that its behavior will lead to a catastrophic failure of the system and also to provide evidence for both the developers and the assessment authorities that the risk associated with the software is acceptable within the overall system risks (Wang, 1997).

7.2. Ship safety

The formal safety assessment philosophy has been approved by the IMO for reviewing the current safety and environmental protection regulations, studying any new element proposal by the IMO, and justifying and demonstrating a new element proposal to the IMO by an individual administration. Further applications may include the use of formal safety assessment for granting exemptions or accepting equivalent solutions for specific ships under the provisions of an individual administration, for demonstrating the safety of a specific ship and its operation in compliance with mandatory requirements to the acceptance of an individual owner, and as a management tool to facilitate the identification and control of risks as a part of the Safety Management System in compliance with the ISM Code by an individual owner. Several possible options regarding the application of formal safety assessments are currently still under investigation at the IMO. Among the possible application options, the individual ship approach may have the greatest impact on marine safety and change the nature of the safety regulations at sea since it may lead to deviation from traditional prescriptive requirements in the conventions toward performance-based criteria. This may be supported by ship type-specific information. However, this would raise concern due to the difficulty in the safety evaluation process by other administrations, particularly when acting as port states, although the merits of it may also be very significant. At the moment, unlike in the UK offshore industry, there is no intention to put in place a requirement for individual ship safety cases.

It is also very important to take into account human error problems in formal safety assessment. Factors such as language, education, and training, which affect human error, need to be taken into account. The application of formal safety assessment may also encourage the Flag States to collect operation data. Another important aspect that needs to be considered is the data problem. The confidence of formal safety assessment greatly depends on the reliability of failure data. If formal safety assessment is applied, it may facilitate the collection of useful data on operational experience that can be used for effective proactive safety assessment.

More test case studies also need to be carried out to evaluate and modify formal ship safety assessment and associated techniques and to provide more detailed guidelines for the employment of them. This would enable validation of them and can also direct the further development of suitable formal ship safety assessment techniques and facilitate technology transfer to industries.

It is clear that it would be possible to prevent marine accidents by good design, training, and operation in an appropriate systematic management system. As the public concern regarding maritime safety increases, more and more attention is directed to the application of formal safety assessments of ships as a regulatory tool. It is believed that the adoption of such a tool in ship design and operation will reduce maritime risks to a minimum level.

Acknowledgments

This work forms part of the projects jointly supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant References GR/M24967, GR/R30624, and GR/R32413 and by the Health and Safety Executive (HSE) under Grant Reference D3727.

References

Cowley, J. (1995). The concept of the ISM Code. In *Proceeding of management and operation of ships: practical techniques for today and tomorrow* (pp. 24–25). London: The Institute of Marine Engineers.

Department of Energy (1990). *The public inquiry into the Piper Alpha disaster*. London: Department of Energy (Cullen Report, ISBN 0 10 113102).

Health and Safety Executive (HSE). (1992). *The offshore installations (safety case) regulations 1992*. London: HSE Books (ISBN 00118820559).

Health and Safety Executive (HSE). (1995). *Generic terms and concepts in the assessment and regulation of industrial risks*. London: HSE Books (Discussion Document DDE2).

Health and Safety Executive (HSE). (1996a). *A guide to the integrity, workplace environment and miscellaneous aspects of the offshore installations and wells (design and construction, etc.) regulations*. London: HSE Books (ISBN 0717611647).

Health and Safety Executive (HSE). (1996b). *A guide to the installation verification and miscellaneous aspects of amendments by the offshore installations and wells (design and construction, etc.) regulations 1996 to the offshore installations (safety case) regulations 1992*. London: HSE Books (ISBN 0717611930).

Health and Safety Executive (HSE). (1996c). *The offshore installations and wells (design and construction, etc.). Regulations 1996*. London: HSE Books (ISBN 0-11-054451-X, No. 913).

Henley, E. J., & Kumamoto, H. (1992). *Probabilistic risk assessment, 1002*. New York: IEEE Press.

House of Lords (1992). *Safety aspects of ship design and technology, Select Committee on Science and Technology, 2nd Report*. HL Paper 30-I.

IMO. (1997, November). *IMO/MSC circular 829, interim guidelines for the application of formal safety assessment to the IMO rule-making process*. London: Author.

Institute of Marine Engineers and MCE (1998, December 4). *Proceeding of new safety culture*. London: Author.

International Commission on Radiological Protection (1977). *Recommendations of the ICRP*. Oxford: Pergamon (ICRP Publication 26).

Janardhanan, K., & Grillo, P. (1998). Latest UK offshore safety legislation. *The Journal of Offshore Technology*, 37–39.

Kuo, C. (1998). *Managing ship safety*. London: Lloyd's of London Press Ltd. (ISBN 1-85978-841-6).

Loughran, C., Pillay, A., Wang, J., Wall, A., & Ruxton, T. (2002). A preliminary study of fishing vessel safety. *Journal of Risk Research*, *5*(1), 3–21.

Marine Safety Agency (1993). *Formal safety assessment MSC66/14*. London: Marine Safety Agency (Submitted by the United Kingdom to IMO Maritime Safety Committee).

MCA (1997). *FSA trial application to high speed passenger Catamaran vessel (68/14/2 and 68/INF)*. London: Author.

MCA (1998a). *Notes on the experience gained on formal safety assessment*. Informal paper submitted by UK to IMO/MSC, 69th session, London, 12th February 1998 (IMO/MSC 69/INF14). London: Author.

MCA (1998b). *Formal safety assessment for bulk carriers (including annexes A-I)*. Informal paper submitted by UK to IMO/MSC, 70th session, London, 27th November 1998 (IMO/MSC 70/INF PAPER). London: Author.

MCA (1998c). *Trial application of FSA to the dangerous goods on passenger/Ro-Ro vessels*. 69/INF.24. Submitted by Finland IMO. London: Author.

Sekimizu, K. (1997). Current work at IMO on formal safety assessment. In *Proceeding of marine risk assessment: a better way to manage your business* (pp. 8–9). London: Author.

Sii, H. S. (2001). *Marine and offshore safety assessment*. PhD Thesis, Staffordshire University, UK.

Smith, D. J. (1993). *Reliability, maintainability and risk* (4th ed.). London: Butterworth-Heinemann Ltd.

Spouse, J. (1997). Risk criteria for use in ship safety assessment. In *Proceeding of marine risk assessment: a better way to manage your business*. London: The Institute of Marine Engineers.

TSBC (Transportation Safety Board of Canada) (1999). *Statistics and accident/incident reports for the period 1995–1999. Safety analysis and communications directorate*. Quebec, Canada: Author.

UK P&I CLUB (1999). *Analysis of major claims — ten years trends in maritime risk*. London: Author.

UKOOA (1999). *Industry guidelines on a framework for risk related decision-making*. London: UK Offshore Operators Association.

Vie, R. H., & Stemp, J. B. (1997). The practical application of risk assurance technology techniques to cruise vessel design and operation. In *Proceeding of marine risk assessment: a better way to manage your business*. London: The Institute of Marine Engineers.

Villemeur, A. (1992). *Reliability, availability, maintainability and safety assessment*. Chichester: Wiley.

Wang, J. (1997). A subjective methodology for safety analysis of safety requirements specifications. *IEEE Transactions on Fuzzy Systems*, *5*(3), 418–430.

Wang, J. (2001). Current status of future aspects of formal safety assessment of ships. *Safety Science*, *38*, 19–30.

Wang, J., & Foinikis, P. (2001). Formal safety assessment of containerships. *Marine Policy*, *21*, 143–157.

Wang, J., & Ruxton, T. (1997). A review of safety analysis methods applied to the design process of large engineering products. *Journal of Engineering Design*, *8*(2), 131–152.

Wang, J., Ruxton, T., & Labrie, C. R. (1995). Design for safety of marine engineering systems with multiple failure state variables. *Reliability Engineering and System Safety*, *50*(3), 271–284.

Wang, J., Yang, J. B., & Sen, P. (1996). Multi-person and multi-attribute design evaluations using evidential reasoning based on subjective safety and cost analysis. *Reliability Engineering and System Safety*, *52*(2), 113–128.

Wang, J., Yang, J. B., Sen, P., & Ruxton, T. (1996). Safety based design and maintenance optimisation of large marine engineering systems. *Applied Ocean Research*, *18*(1), 13–27.

Yang, J. B., & Sen, P. (1994). A general multi-level evaluation process for hybrid MADM with uncertainty. *IEEE Transactions on Systems, Man and Cybernetics*, *24*, 1457–1458.

Dr. Wang is Reader in Marine Engineering in the School of Engineering at Liverpool John Moores University, UK. He undertook two UK Engineering and Physical Sciences Research Council (EPSRC)-funded and one European Union (EU)-funded safety and reliability engineering research projects at Newcastle University, UK from 1990 to 1995. He has been involved in marine and offshore safety research for the past 12 years with support from the EPSRC, EU, HSE, etc. He has authored/coauthored over 100 technical papers related to marine and offshore safety in conference proceedings and international journals. He is a member of the Council of the UK Safety and Reliability Society (SaRS) and the Technical Papers and Conferences Committee of the Institute of Marine Engineers (IMarE). He is also a member of the Editorial Board of two journals. He is currently directing a research group of seven postdoctoral and doctoral research members in the areas of marine and offshore technology research.

Dr. Wang's major research interests include safety- and reliability-based design of large marine and offshore products, probabilistic and nonprobabilistic safety analysis and decision-making, and port safety assessment and analysis of safety-critical systems in the software domain.