© Marine Technology, Vol. 39, No. 2, April 2002, pp. 77–85

A Brief Review of Marine and Offshore Safety Assessment

J. Wang[1]

This paper reviews some typical marine and offshore accidents in terms of major causes and resulting actions. The lessons learned from previous marine and offshore accidents are discussed in terms of the change of the safety culture in both the marine and offshore industries. The concepts of initiating events and safety system responses in an accident sequence are described. The provision of risk analysis and prevention of accidents are discussed. The offshore safety case approach and formal ship safety assessment of ships are described in detail. The future aspects in marine and offshore assessment are also discussed.

1. Review of major marine and offshore accidents

TRAGIC accidents such as the *Herald of Free Enterprise, Derbyshire* and *Piper Alpha,* together with environmental disasters such as the *Amoco Cadiz* and *Exxon Valdez,* have focused world opinion on maritime safety and operation. Unfortunately, it is a fact of life that design for safety and safety operational practices are only appreciated after serious marine accidents have occurred. A proactive safety regime is required for both the marine and offshore industries.

Several typical marine and offshore accidents are described in the following to highlight the safety problems in the marine and offshore industries.

Some typical marine accidents

The *Amoco Cadiz* accident 1978—The *Amoco Cadiz,* a very large crude carrier (VLCC) departed from Kharg on March 16, 1978 for a scheduled voyage to Rotterdam. While off the coast of Brittany in France, her hydraulic steering gear failed and the vessel drifted in heavy seas. The vessel grounded on Portsall Rocks when the tug *Pacific* attempted to tow it out of the sea. The vessel broke in two parts and the entire cargo was lost, extensively polluting the French coast. The Amoco International Oil Company (AIOC) was asked why the steering gear failed. Judge McGarr, in his report, found that the AIOC was responsible. The conclusion of the report stated "The failure of *Amoco Cadiz*'s steering gear is directly attributable to an improperly designed, constructed and maintained steering gear system, and AIOC knew or should have known of the unseaworthy condition. The negligence of AIOC in failing reasonably to perform its obligations of maintenance and repair of the steering gear system was an approximate cause of the breakdown of the system on the 16th March 1978, the grounding of the vessel and the resulting damage" (McGarr Memorandum 1984).

With the *Amoco Cadiz* disaster, new requirements for tanker regulations were developed by the International Maritime Organization (IMO). The results of the inquiry into the *Amoco Cadiz* accident have contributed to the implementation of the Protocol of 1978—Tanker Safety and Pollution Prevention of SOLAS (International Convention for the Safety of Life at Sea 1974). All tankers of 10 000 grt and above shall have two remote steering gear control systems, each operable separately from the navigating bridge (IMO 2001). The main steering gear of new tankers of 10 000 grt and above shall comprise two or more identical power units, and shall be capable of operating the rudder with one or more power units.

The wreck of the *Derbyshire* 1980—The *Derbyshire* was a very large ship with overall length 294.1 m, extreme breath 44.3 m, maximum draft 18.4 m, gross tonnage 91 645.5 and net tonnage 67 428.5. She was owned by Bibby Line, built by Swan Hunter at Haverton Hill Shipyard, Teeside, and classed by Lloyd's Register of Shipping. During a typhoon in the Pacific on the September 9, 1980, the *Derbyshire,* of 169 044 dwt, disappeared in a mysterious circumstance when she was on route to Kawasaki, Japan with a cargo of iron ore concentrates. The tragedy cost 44 lives (42 crew and 2 wives).

It may be the case that the *Derbyshire* was unprepared to take the rigors of the typhoon seas. It can be explained that the cargo holds (1, 2 and perhaps 3) in the bow flooded through an opening, ventilators, and an air pipe after the covers were washed away. The remaining holds, hatch covers and other intact compartments, were destroyed by the successive implosion/explosion during the process of sinking. Water flooded into the holds, which contained thousands of tons of iron ore. With the force of explosion being equivalent to 17 tons of TNT (BBC 1998), the surveyors found "a picture of almost total destruction with parts of this huge ship ripped apart lying torn and crumpled on the sea bed" (*Derbyshire* . . . 1987).

The *Derbyshire* was designed in compliance as to freeboard and hatch cover strength with the regulations made by the UK Government in 1968—the Load Line Rules—which gave effect to most of the provisions of the International Load Line Convention 1966 (ILLC66). Minimum hatch cover strength requirements laid down for forward hatches in ILLC66 in conjunction with the prescribed minimum permissible freeboard for bulk carriers of similar size to the *Derbyshire* are seriously deficient in the context of present-day concepts of acceptable safety levels.

The *Herald of Free Enterprise* disaster 1987—The *Herald of Free Enterprise* was operated by Townsend Car Ferries Ltd., and her normal routes were Dover–Calais and Dover–Zeebrugge. On March 6, 1987, four minutes after leaving the Harbour of Zeebrugge, she capsized. As a result, at least 150 passengers and 38 crew members lost their lives (DTp 1987).

The capsizing of the *Herald of Free Enterprise* was caused by a combination of adverse factors. Those which have been positively identified were the trim by the bow, the bow door being left open and the speed of the vessel just before capsize. Their combined effect was to cause a quantity of water to

[1] School of Engineering, Liverpool John Moores University, Liverpool, Byrom Street, L3 3AF, U.K.

Manuscript received at SNAME headquarters December 3, 2001.

enter G deck, thus reducing the vessel's stability. Another factor which may have contributed to the tragedy was the location of the ship's center of gravity, which is critical to the stability of the vessel. The containment of any one of these factors would have reduced the chances of capsizing.

The findings of the inquiry clearly demonstrated the contributions of human actions and decisions to the accident. These ranged from weakness in the management of safety to human errors, caused by various factors, including a heavy work load. The basic roll-on/roll-off (RO/RO) ferry design was questioned, in particular the single-compartment standard for G-deck. There are no watertight bulkheads at all on this deck to prevent shipped water from spreading along the full length of the vessel. This is a common feature of most RO/RO designs.

The public inquiry into the capsize of the *Herald of Free Enterprise,* led by Lord Carver, was a milestone in ship safety. It has resulted in changes of marine safety-related regulations, demonstrated by the adoption of the enhanced damage stability and watertight closure provisions in SOLAS '90, the introduction of the International Safety Management (ISM) Code and the development of the formal safety assessment framework of ships.

The *Estonia* accident 1994—The Estonian-flagged RO/RO passenger ferry *Estonia* departed from Tallinn, the capital of Estonia, on the September 27, 1994, at 1915 hours for a voyage to Stockholm, Sweden. She carried 989 people, 803 of whom were passengers. She sank in the northern Baltic Sea in the early hours of September 28, 1994. Only 137 passengers survived. According to the Accident Commission, the cause of the accident was that the design and manufacture of the bow visor locks were wrong, resulting in the locks being too weak. During bad weather conditions the locks were broken and the visor fell off and pulled open the inner bow ramp. Water flooded the main RO/RO deck and the vessel lost stability and sank. *Estonia,* on her last voyage, was not seaworthy and she did not fulfill the SOLAS requirements. The crew also made mistakes which partially contributed to the loss of so many lives.

The *Estonia* tragedy also resulted in a surge of research into the phenomenon of RO/RO damage survivability and was instrumental in the adoption of the North European Regional Damage stability standard in SOLAS '95 and the Stockholm Agreement. These standards require the upgrading of virtually every passenger RO/RO ship operating in Northern Europe (Channel, North Sea, Irish Sea, and Baltic Sea).

The loss of *Flare* 1998—MV *Flare* was built in Japan in 1972, as a single-deck, dry bulk cargo vessel of all-welded steel construction. It was of a type noted for its much thicker steelwork than most ships constructed in the 1980s (Brewer 1998a). On January 16, 1998, the Cypriot-registered a 29 222 dwt bulk carrier *Flare* owned by ABTA Shipping, was on the scheduled route from Rotterdam, the Netherlands, to Montreal, Quebec (ITF 2000), when she split in two during rough weather conditions approximately 45 miles Southwest of the French Islands of St. Pierre and Miquelon (off the Newfoundland coast in the Gulf of St. Lawrence). The vessel appeared to have snapped three holds forward of the accommodation block. The bow and midship sections of the ship drifted on the surface for days before finally sinking. From a crew of 25, 21 were lost.

Investigations focused on the operation of the vessel, the quantity and distribution of ballast, maintenance of the vessel, survival equipment on board and the search and rescue operation. The vessel was not fitted with a hull stress monitoring system, nor was one required by regulation. Following an underwater inspection of the ship and interviews with the survivors, a progress report on the Transport Safety Board (TSB) of Canada investigation into the disaster indicated that the vessel might have suffered several days of punishment from heavy seas before she sank. Information currently available would indicate that the *Flare* was subject to slamming and pounding for several days and the hull failure was most likely initiated by brittle fracturing which resulted in the loss of longitudinal structural integrity (Brewer 1998b). Rapid progression of the fractures in the upper part of the hull would have resulted in excessive compression stresses on the bottom structure, leading to sudden failure and complete hull separation. The TSB report concludes that (ITF 2000):

- The sinking was due to inadequate ballasting of the vessel that made the vessel vulnerable to pounding and slamming in the seaway (the *Flare* was without cargo when she sank).
- The owners failed to carry out structural repairs to the vessel—a contributing factor to the sinking. The owner could have completed critical repairs in Rotterdam before the *Flare*'s fatal voyage, but instead attempted to carry them out at sea using riding crews with welding equipment.
- The vessel's emergency radio beacon and other distress equipment failed to activate, which caused the rescue operation to take several hours to locate the vessel. Many seafarers perished in the freezing sea; miraculously four survived after several hours in the water.
- The master and the majority of the crew were new to the vessel, having joined in Rotterdam. No proper training or lifeboat drills took place and the crew were not familiar with abandon ship procedures. This resulted in the crew being unable to release the lifeboats after the vessel broke in two.

The report does highlight the owners' failure to maintain and operate a safe ship, which served to increase the death toll.

The multinational crewing of vessels is a long established practice. Where English is the common and working language of the ship, problems may arise when non-English speaking crew do not fully understand instructions. Such language differences can lead to uncertainty, misunderstanding, and a lack of control. That this problem existed on board the *Flare* was evident.

Some typical offshore accidents

The *Brava* accident 1977—In April 1977 a blowout occurred on the Ekofisk platform *Brava* in the North Sea. The blowout did not result in any loss of lives, injuries, explosion or fire but did cause a large environmental pollution due to an oil spill. The blowout was ascribed to human error. A contributing cause to the accident was attributed to simultaneous operations, that is, concurrent drilling and production operations. The accident received extensive worldwide press coverage. Following this accident, the Norwegian Petroleum Directorate issued guidelines for simultaneous operations which introduced specific restrictions and required specific approval prior to the commencement of such operations. At about the same time, the Norwegian Petroleum Directorate promulgated guidelines for the Concept Safety Evaluation (CSE) of the platform design. These guidelines required that the design be evaluated for potential accidents and that impairment frequency be at an acceptably low level (Norwegian Petroleum Directorate 1981).

The capsizing of the semisubmersible rig *Alexander Keilland* 1980—The *Alexander Keilland* was a semisubmersible rig comprising five large flotation pontoons. The whole structure was strengthened and stiffened by horizontal and diagonal bracing welded to each leg. The brace labeled D-6 was the trigger for the accident. On the March 27, 1980, the semisubmersible accommodation platform, *Alexander Keilland* capsized in the Ekofisk field in the Norwegian Sector. Of the 212 persons on board, 123 died (Strutt 1992).

The hydrophone was not part of the original design plan but had been put in during the construction phase. The installation of the hydrophone required the cutting of a hole, roughly in the bottom center of the brace, and the welding of a short flanged tube inserted in the hole. The decision for the modification was not checked with the design engineers as it had not been considered to be a structurally significant modification. The lowest quality flame cutting and welding had been employed. The investigators eventually proved that there had been a crack in the weld which had been there since the time of the modification. The crack had grown by a corrosion fatigue mechanism until it had propagated around the circumference of the brace, causing it to sever.

There was very little redundancy in the structural design of the *Alexander Keilland.* The remaining braces were not strong enough to withstand the loss of brace D-6.

A number of lessons were learned from this accident (Strutt 1992):

- The risk of losing a complete member was either not investigated or considered so unlikely that it was not designed against.
- The cracking at the hydrophone connection, leading to the subsequent brace failure, was not identified as a significant hazard when the hydrophone was added late in the rig construction process.
- The difficulty of evacuation from the accommodation and escape by lifeboats and life rafts in a severe list.
- The need to make allowances for human actions and omissions (e.g., leaving the watertight doors open, omission of inspection).
- The need to reassess risks when design changes are made.

This incident was largely the trigger for redevelopment of the Norwegian regulations in offshore safety.

The *Ocean Ranger* disaster 1982—The *Ocean Ranger* was a twin-pontoon semisubmersible drilling vessel with eight vertical columns. The vessel capsized off the eastern coast of Canada early in the morning of February 15, 1982 with the loss of the entire crew of 84. The fatal loss of stability was caused by the ingress of water into the forward ballast tank and the flooding of chain lockers and upper hull. The accident was caused by a chain of events. The key ones were the severe storm conditions and design flaws. Design flaws included the location of the ballast control room; the strength of the porthole windows; lack of protection for the control panel; lack of protection against flooding of chain lockers; and lack of facilities for pumping out water in the event of flooding (Government of Canada 1984).

The *Piper Alpha* accident 1988—Late in the evening of July 6, 1988, an explosion occurred aboard the *Piper Alpha* platform, triggering several subsequent explosions and enveloping the platform in a furious conflagration. The accident that destroyed the *Piper Alpha* rig claimed the lives of 165 of the 226 persons on board and 2 of the crew while engaged in rescue duties. The death toll was the highest in any accident in the history of offshore operations.

The initiation of the accident was attributed to poor communication between shifts of the platform operators. As a result, an inoperative condensate pump, from which the pressure safety valve had been removed, was started up. The escaping gas ignited and a chain of explosions took place to cause extensive damage to vital platform systems, including the platform internal communication system, making it impossible to issue an order to evacuate. Approximately 20 minutes after the first explosion, an incoming 18-in. high pressure gas pipeline riser was damaged, probably by falling debris. The escaping gas collected under the platform, resulting in an enormous explosion that destroyed most of the platform.

From the early stage in the inquiry it became clear that there were a number of features in the physical arrangements on and the management of the *Piper Alpha* which were such as to render it vulnerable to dangerous incidents, whether or not they contributed to the disaster. This led to a range of additional topics coming under consideration, including permit to work procedure and practice, active fire protection and preparation for emergencies.

The public inquiry, led by Lord Cullen, published its report in November 1990 (UK Department of Energy 1990). The inquiry covered the complete range of issues from hardware design and integrity through day-to-day safety management. The inquiry was a milestone to change the safety regime in the offshore industry in the U.K.

The Roncador disaster 2001—On March 15, 2001, three explosions rocked Petrobras' P-36 semisubmersible floating product platform as it worked in the company's Roncador field in the Campos basin off the Brazilian coast. The accident resulted in the deaths of 10 people in the explosions and the loss of an ultra-deepwater vessel in the rescue process. At the time of the accident P-36 was processing about 83 000 barrels of oil and 1.3 million m^3 of gas production per day [Von Flatern 2001].

What actually set off the explosions aboard P-36 is still a matter of conjecture. Petrobras has promised a report from an investigative committee.

2. Initiating events and accidents

One major objective of risk assessment is to reduce risks to a minimal level within both technical and economic constraints in order to achieve cost savings. To reduce risks, it is essential to know how an accident happens due to the occurrence of the initiating event(s). Figure 1 gives a sequence of how an initiating event develops into an accident.

From Fig. 1, it can be seen that a hazard can develop into an initiating event under certain conditions. The occurrence of an initiating event can cause some operational changes. The operational changes then cause unsafe conditions. At this stage, if safety systems (i.e., protection systems) respond accordingly, then possible serious consequences can be avoided and the incident is recorded. However, if safety systems fail to respond accordingly, a possible accident happens and serious consequences may be caused.

There are many types of initiating events. The typical ones include:

1. Machinery and equipment malfunctions (e.g., pumps, valves, instruments).
2. Containment failures (e.g., pipes, storage tanks, pressure vessels).
3. Human errors (e.g., in operation, maintenance, design, management).
4. External events (e.g., weather, obstacles).
5. Procedural or information (e.g., incorrect procedures, incorrect information).

The occurrence of an initiating event may cause certain operational changes with potential to cause possible consequences. The typical operational changes include:

1. Parameter deviations (e.g., pressure, temperature, flow rate).

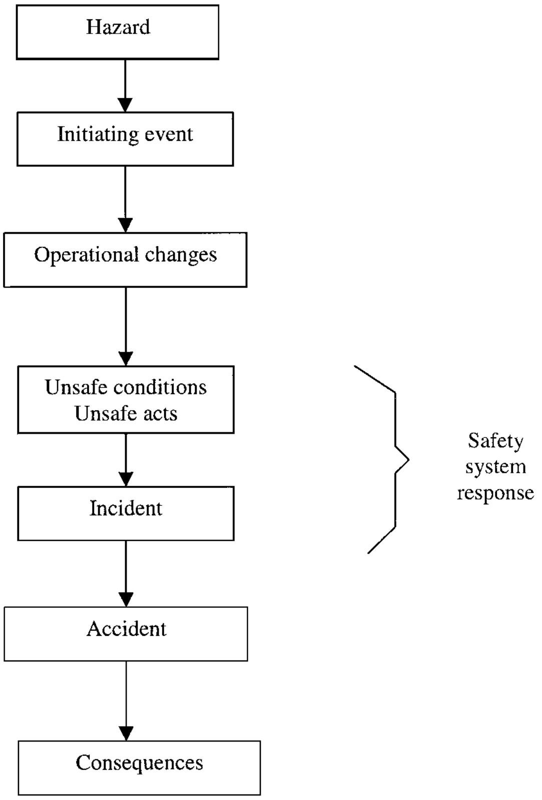

Fig. 1 Sequence of an accident

2. Material releases (e.g., combustibles, explosive materials, toxic materials).
3. Operator errors (e.g., observation, identification, choice/ execution of procedures).
4. External events (e.g., delayed warning, no warning).
5. Procedural or information (e.g., usefulness, timeliness).

It should be noted that the occurrence of an initiating event may also result in a combination of the above. When the operational changes happen, safety systems respond in order to mitigate possible consequences. There are various types of safety systems. The typical ones include:

1. Protection devices (e.g., relief valves, back up systems/ components, sprinklers).
2. Control system responses (e.g., closed loop control, open loop control, adaptive control).
3. Operator responses (e.g., planned or ad hoc).
4. Contingency operations (e.g., alarms, emergency, procedures, safety equipment, evacuations).
5. External events (e.g., early detection and warning).
6. Information (e.g., timing and applicability).

In a complex system there may be multiple safety systems (barriers) which can respond at different levels. A marine pollution control diagram in Fig. 2 shows how an initiating event breaches barriers to cause serious consequences. It can be seen that a hazard may cause operational changes. If safety systems respond accordingly (i.e., taking personnel measures, equipment measures, procedural measures), then the operating system can be back to the normal working conditions, otherwise errors will occur. If errors occur, safety systems can again respond to stop the propagation of failures, otherwise unsafe conditions remain there. At this stage, if safety systems do not respond accordingly, then an incident happens. If the incident breaks through the next barrier, then an accident happens. Accidents include collision, grounding, capsize, fire, explosion, structural failure, breakdown and cargo transfer error. At this stage, if the ship is double-bottomed and double-sided, possible marine pollution may be avoided, otherwise oil enters water (if the vessel's hull is damaged). If the spill containment and collection are conducted successfully, then possible pollution effects can be limited, otherwise the marine environment is damaged.

3. Provision of risk analysis and prevention of accidents

The above section describes how an initiating event develops into an accident. It can be found that in some cases several barriers need to be breached for an accident to happen. Risk assessment analyzes the causes leading to the occurrence of the initiating event and also how the initiating event causes possible consequences, in order to reduce the likelihood of occurrence and/or mitigate possible consequences. The process of maritime risk assessment can:

- Increase the understanding of safety through a systematic and logical development of accident sequences.
- Separate important accident sequences from unimportant ones.
- Provide a qualitative/quantitative measure of risk.
- Determine the importance of ship operator actions in coping with accidents.
- Identify cost effective designs or procedural changes for controlling risk.
- Improve the decision making (risk management process).
- Help clarify emergency planning needs.
- Provide assurance that state-of-the-art methods have been responsibly used to assess safety.

Accidents may be prevented by procedures designed for:

- Safety prediction.
- Safety management.

In safety prediction, appropriate procedures are usually applied when new designs, equipment or tasks are being considered (Ruxton 1992). The purpose is to examine systems for new hazards, new potential accidents and new consequences. Specific safety prediction procedures may be needed for different applications.

The safety management procedures are designed to:

- Satisfy the requirements of rules and regulations.
- Meet the requirements of accepted standards.
- Allow the following of proven practices.
- Allow checklists and safety reviews (safety audits) to be used to identify deviations from accepted standards and good practice.

In marine and offshore design, it is required to reduce the likelihood of occurrence of hazards with potential to cause serious consequences in the first place. However, it is impossible to eliminate all hazards. Therefore, it is always possible that something would go wrong. If something does go wrong, it is required to minimize/mitigate possible consequences. This paper deals with all such problems.

4. Current status of marine and offshore safety assessment

Current status of offshore safety assessment

Following the public inquiry into the *Piper Alpha* accident (UK Department of Energy 1990), the responsibilities for offshore safety regulations were transferred from the Depart-

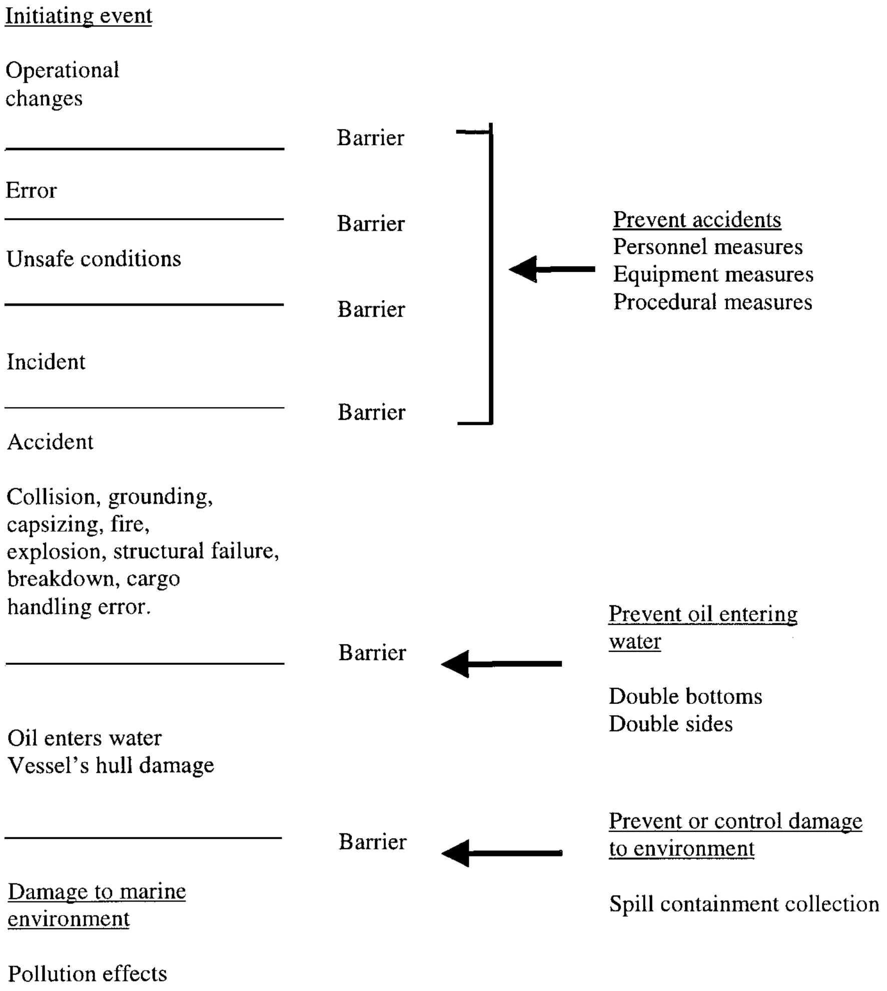

Fig. 2 Marine pollution control diagram

ment of Energy to the Health & Safety Commission through the Health & Safety Executive (HSE) as the single regulatory body for offshore safety. The safety case regulations came into force in two phases—at the end of May 1993 for new installations and 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 safety case regulations were amended in 1996 to include verification of safety-critical elements. The Offshore Installations and Wells (Design and Construction, etc.). Regulations 1996 (DCR '96) were introduced to deal with various stages of the life cycle of the installation (HSE 1996). DCR '96 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.

The main feature of the new offshore safety regulations in the U.K. is the absence of a prescriptive regime, defining specific duties of the operator and definition regarding what are adequate means. The regulations set forth high level safety objectives while leaving the selection of particular arrangements to deal with hazards in the hands of the operator. This is in recognition of the fact that 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 have been produced by the UK Offshore Operators Association (UKOOA) (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, loss of stability, etc. It can also be combined with other formal decision-making aids such as Multi-Attribute Utility Analysis if a more detailed or quantitative analysis of the various decision alternatives is desired.

Note that although the importance of such a safety case assessment has been widely recognized, it is not mandatory in the offshore industry worldwide. Note also that this offshore safety case philosophy has been already adopted on a mandatory basis by several countries, including Norway.

It should also 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, etc. There is a need to apply common sense and ensure that any uncertainties are recognized and addressed.

Current status of formal ship safety assessment

The international safety-related marine regulations have been governed by serious marine accidents that have happened. The lessons were first learned from the accidents and then the regulations and rules were produced to prevent similar accidents to occur.

After Lord Carver's report on the investigation of the capsize of the *Herald of Free Enterprise* was published in 1992, the UK Maritime & Coastguard Agency (UK MCA previously named as Marine Safety Agency) 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 it in relation to ship design and operation. The IMO reacted favorably to the U.K.'s formal safety assessment submission. Since then, substantial work, including demonstrating its practicability by trial application to the safety of high-speed catamaran ferries and a trial application to the safety of bulk carriers, has been done by the UK MCA. In general, for the past several years the application of formal safety assessment has reached an advanced stage. This is demonstrated by successful case studies on a high-speed craft and a bulk carrier and also that the IMO has approved the application of formal safety assessment for supporting the rule-making process (MSC 1997, 1998a,b,c, Wang 2001).

Note that 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 a high-speed passenger vessel), or to a particular hazard (such as fire). For a particular ship, its performance estimate can be easily obtained by including its special features given the formal safety assessment. The philosophy of formal safety assessment is essentially the same as the one of the safety case approach.

Formal safety assessment in ship design and operation may offer great potential incentives. The application of it may improve the performance of the current fleet, be able to measure the performance change and ensure that new ships are good designs; ensure that experience from the field is used in the current fleet and that any lessons learned are incorporated into new ships; and provide a mechanism for predicting and controlling the most likely scenarios that could result in incidents.

Risk criteria

Acceptance of risk is basically a problem of decision making, and is inevitably influenced by many factors such as type of activity, level of loss, economic, political and social factors, and confidence in risk estimation. A risk estimate, in the simplest form, is considered acceptable when below the level which divides the unacceptable from acceptable risks. The HSE framework for decisions on the tolerability of risk is shown in Fig. 3, where there are three regions: intolerable, ALARP (As Low As Reasonably Practicable), and broadly acceptable. Tolerability criteria are based on the principle that above a certain level, a risk is regarded as intolerable and cannot be justified in any ordinary circumstance. Below a certain level, the risk is considered as "broadly acceptable," but it is necessary to maintain assurance that risk remains below this level. Below these two levels is so called "tolerability region" within which an activity is allowed to take place provided that the associated risks have been made ALARP.

The term "reasonably practicable" implies that cost is considered in relation to risk reduction. A general interpretation of requiring risks to be ALARP is that the best that can be done in the prevailing circumstances must be done. It should be noted that in the U.K. health and safety legislation that the major accident risks are or will be ALARP. It is important to recognize that the demonstration of ALARP is required, and not the quantitative risk assessment (with the exception of the offshore industry). Therefore, ALARP can be demonstrated by historical data of low or acceptable levels of risk and by adoption of "best practice." The situation becomes more complicated with the new technologies for which there is no historical data, and good practice has not yet been established. In those situations, risk assessment becomes another useful tool in the search for an optimal solution.

It is also important to recognize that in a situation where a practicable risk reduction measure is identified, it should be implemented unless it can be shown robustly that the measure in question is not reasonably practicable. In other words, a measure should be put in place unless it is demon-

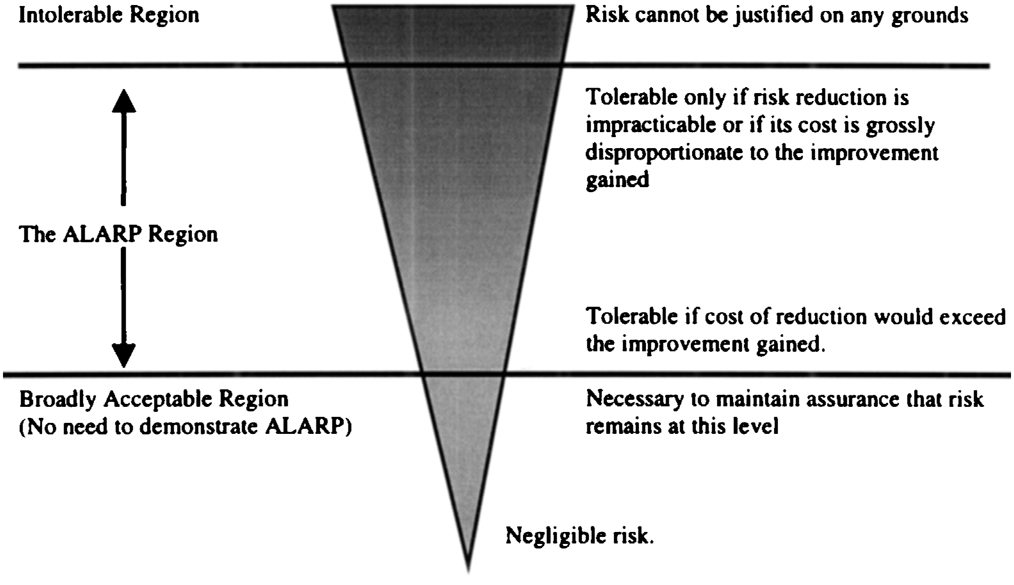
Intolerable Region
Risk cannot be justified on any grounds
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
The ALARP Region
Tolerable if cost of reduction would exceed the improvement gained.
Broadly Acceptable Region
(No need to demonstrate ALARP)
Necessary to maintain assurance that risk remains at this level
Negligible risk.

Fig. 3 HSE framework for decisions on tolerability of risk

strated on "balance of probabilities" that the measure is not cost effective.

An offshore 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 reduced as low as is reasonably practicable. 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.

As far as risk criteria for ships are concerned, the general criteria may include: (1) the activity should not impose any risks which can reasonably be avoided; (2) the risks should not be disproportionate to the benefits; (3) the risks should not be unduly concentrated on particular individuals; and (4) 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 (HSE 1995).

5. Marine and offshore safety assessment

Offshore safety assessment

The concept of the safety case has been 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. 4. These elements are discussed as follows:

1. Hazard identification—This step is to identify all hazards with the potential to cause a major accident.

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, ALARP and negligible risk regions as shown in Fig. 3.

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—The purpose of a safety management system (SMS) 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.

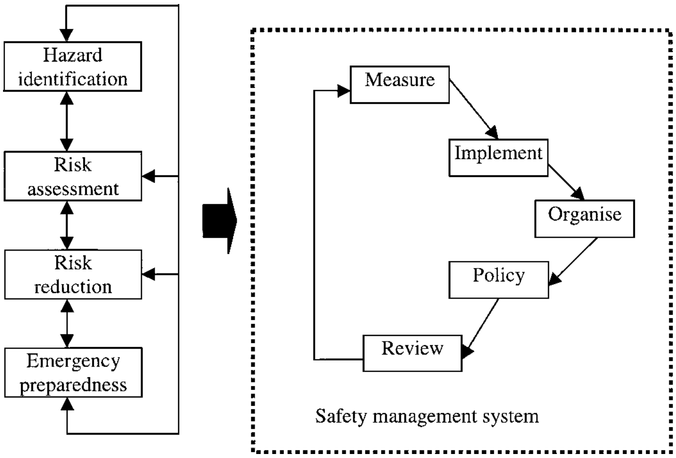

Fig. 4 Five key elements of safety case concepts

A safety case is a written submission prepared by the operator of an offshore installation. It is a stand-alone document which 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.

Safety-based design/operation decisions should be made at the earliest stages in order to reduce to a minimum unexpected costs and time delays regarding safety due to late modifications. It should be stressed that a risk reduction measure that is cost effective at the early design stage may not be ALARP at the late stage. HSE's 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 cost benefit analysis based on simple comparisons have been widely used as a general principle in offshore safety analysis.

Conventional safety assessment methods and cost benefit analysis 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. A life-cycle approach is required to manage the hazards that affect offshore installations. It should be noted that an offshore safety study has to deal with the boundaries of other industries such as marine operations and aviation. In an offshore safety study, it is desirable to obtain the optimum risk reduction solution for the total life cycle of the operation or installation, irrespective of the regulatory boundaries (UKOOA 1999). Decisions can either take the form of rigid criteria, which must be achieved, or take the form of goals or targets which should be aimed for, but which may not be met. The U.K. 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.

Formal ship safety assessment

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 which influence risk and its reduction can be identified and reflected in the regulator's approach for all ships of that type (*Proceedings* . . . 1999).

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, are entirely consistent (*Proceedings* . . . 1999).

A formal ship safety assessment framework that has been proposed by the UK MCA consisting of the following five steps: the identification of hazards; the assessment of risks associated with those hazards; ways of managing the risks identified; cost benefit assessment of the options; and decisions on which options to select.

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). Hazard identification is concerned with using the "brainstorming" technique involving trained and experienced personnel to determine the hazards. The accident categories include: (1) contact or collision; (2) explosion; (3) external hazards; (4) fire; (5) flooding; (6) grounding or stranding; (7) hazardous substances; (8) loss of hull integrity; (9) machinery failure; and (10) 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 the HAZard and Operability (HAZOP) study, can be applied in this step.

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: (1) design, construction and commissioning; (2) entering port, berthing, unberthing and leaving port; (3) loading and unloading; (4) dry docking; and (5) decommissioning and disposal. A ship consists 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 have disastrous consequences. Risk assessment may 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 described in Henley & Kumamoto (1992), Misra (1992), and Villemeur (1992).

An "influence diagram" can be constructed to study how the regulatory, commercial, technical and political/social environments influence each accident category and eventually quantify these influences with regard to human and hardware failure as well as external events (Marine Safety Agency 1993, UK MSC 1998a,b, Wang 2000, Billington 1999). In general, an "influence diagram" is a combination of fault trees and event trees. Each influence diagram is required to define the "best" and "worse" cases for each factor affecting the particular accident category under review. The whole process must cover each of those systems/compartments and include the escalation of the accident as well as the mitigation aspects such as evaluation of people, marine pollutants' containment, etc. Again, the various operational phases of the ship have to be taken into consideration and generic data or expert judgments are to be used.

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 and then the identification of risk control measures (RCMs) can be initiated. Risk control measures can reduce the likelihood of failures and/or mitigate their possible efforts and consequences. Structural review techniques may be used to identify all possible risk control measures for cost-benefit decision making.

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.

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.

6. Conclusion

This paper describes several major marine and offshore accidents. How an initiating event develops into an accident is also described. In the design process of large marine and offshore engineering products, it is required to minimize the occurrence of serious hazards and reduce/mitigate possible consequences. Many safety assessment and decision-making approaches need to be applied to achieve this.

In offshore safety assessment, a high level of uncertainty in failure data has been a major concern that 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 the costs and benefits of systems vary 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 techno-economic model which takes various costs and benefits into account (Wang et al 1996). To process such a model with multiple objectives, which usually have a conflicting nature, formal decision-making techniques may be best applied to process the mathematical model in order to determine where risk reduction actions are cost effective and how they can be carried out (Wang et al 1996a).

As far as ship safety is concerned, 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. Several possible options regarding the application of formal safety assessment 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 towards performance-based criteria.

Although trial studies on a high-speed craft and a bulk carrier have been carried out by the MCA as mentioned previously, 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 their employment and validation. This could also direct the further development of suitable formal ship safety assessment techniques and facilitate technology transfer to industries.

Acknowledgments

This work forms part of the projects supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant References GR/R30624 and GR/R32413. Thanks are also offered to the two anonymous referees for their useful comments.

References

BBC New Online 1998 U.K. *Derbyshire* sinking inquiry reopens. http://news1.thdo.bbc.co.uk/low/english/uk/newsid_64000/64828.std, March 12.

Billington, C. J. 1999 Managing risks in ports. *Managing Risk in Shipping,* The Nautical Institute, London, 57–69.

Brewer, J. 1998a *Flare* break-up renew bulker safety pressure. *Lloyds List,* January 20.

Brewer, J. 1998b Canada to examine older bulk carriers. *Lloyds List,* November 25.

Derbyshire—loss of sister ship leads to *Derbyshire* probe. *Motor Ship,* January 1987.

DTp 1987 MV *Herald of Free Enterprise*—fatal accident investigation. Sheen Report, Report of Court No. 8074, U.K. Department of Transport, HMSO.

Government of Canada 1984 Report one: the loss of the semisubmersible drill rig *Ocean Ranger* and its crew. Royal Commission Report, The Government of Canada, Council for Publication Citation, Ottawa.

Henley, E. J. and Kumamoto, H. 1992 *Probabilistic Risk Assessment,* IEEE Press, New York.

HSE 1995 Generic terms and concepts in the assessment and regulation of industrial risks. Discussion Document DDE2, HSE Books.

HSE 1996 The offshore installations and wells (design and construction, etc.) regulations 1996. ISBN 0-11-054451-X, No. 913.

ITF 2000 Transport Minister responds to TSB Report's recommendation on sinking of M. V. *Flare.* http://www.itf.org.uk/press/flare2.htm, News Release No. H064/00, September 5.

IMO 2001 International Convention for the Safety of Life at Sea (SOLAS), 1974—The Protocol of 1978 (Entry into force: May 1, 1981).

Kemeny, J. G. 1969 Report of the President's commission on the accident at the Three Mile Island.

Misra, K. B. 1998 *Reliability Analysis and Prediction.* Elsevier Science Publishers B.V., 1992.

Kuo, C. 1998 Managing ship safety. LLP, ISBN 1-85978-841-6.

Marine Safety Agency 1993 Formal safety assessment MSC66/14, submitted by the United Kingdom to IMO Maritime Safety Committee.

McGarr Memorandum 1984 Memorandum opinion and final judgment order on the issue of liability by United States District Judge Frank J. McGarr.

MSC 68/14/2 & 68/INF. 1997 FSA trial application to high-speed passenger catamaran vessel, U.K.

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

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

MSC 69/INF.24 1998c Trial application of FSA to the dangerous goods on passenger/Ro/Ro vessels. Submitted by Finland IMO.

Norwegian Petroleum Directorate 1981 Guidelines for safety evaluation of platform conceptional design. NPD, May.

Proceedings 1998 New safety culture. Organized by the Institute of Marine Engineers and the MCA, London, December 4.

Ruxton, T. 1992 Introduction to safety and risk. Presented at the International Workshop on Safety Analysis and Techniques Required for Formal Safety Assessments in the Shipping and Offshore Industries, Paper 12, London, Sponsored by IMarE et al, December 16–18, 42 pages.

Spouse, J. 1997 Risk criteria for use in ship safety assessment. *Proceedings,* Marine Risk Assessment: A Better Way to Manage Your Business, The Institute of Marine Engineers, London, April 8–9.

Strutt, J. 1992 Overview of major accidents offshore. Presented at the International Workshop on Safety Analysis and Techniques Required for Formal Safety Assessments in the Shipping and Offshore Industries, Paper 12, London, Sponsored by IMarE et al, December 16–18, 13 pages.

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

UKOOA 1999 Industry guidelines on a framework for risk related decision making. Published by the U.K. Offshore Operators Association, April.

Villemeur, A. 1992 *Reliability, Availability, Maintainability and Safety Assessment.* John Wiley & Sons, England.

Von Flatern, R. 2001 World awaits Roncador disaster report. *Offshore Engineer,* April, 12–13.

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

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