Journal of
Ship&Ocean Technology

SOTECH Vol. 5, No. 3, pp. 1~13, 2001

Towards Safety Based Design Procedure for Ships

Marijn Bakker[1], Hotze Boonstra[2], Wim Engelhard[3] and Bart Daman[4]

[1]Delft University of Technology, presently Royal Schelde Shipyards, Flushing
[2]Delft University of Technology; E-mail: H.Boonstra@WbMT.TUDelft.nl
[3]Safety Service Center BV, Apeldoorn
[4]Anthony Veder Shipowners, Rotterdam

Abstract

Present-day rules and regulations for the design and construction of ships are almost without exemption of a prescriptive and deterministic nature. Often it is argued that this situation is far from ideal; it does no right to the advances, which have been made during the past decades in engineering tools in marine technology, both in methodology and in computational power. Within IMO this has been realized for some time and has resulted in proposals to use Formal Safety Assessment(FSA) as a tool to improve and to modernize the rule making process. The present paper makes use of elements of the FSA methodology, but instead of working towards generic regulations or requirements, a Risk Assessment Approach, not unlike a 'safety case'; valid for a certain ship or type of ship is worked out. Delft University of Technology investigated the application of safety assessment procedures in ship design, in co-operation with Anthony Veder Shipowners and safety experts from Safety Service Center BV. The ship considered is a semi-pressurized-fully refrigerated LPG carrier. On the basis of the assumption that a major accident occurs, various accident scenarios were considered and assessed, which would impair the safety of the carrier. In a so-called Risk Matrix, in which accident frequencies versus the consequence of the scenarios are depicted, the calculated risks all appeared to be in the ALARP('as low as reasonable practicable') region. A number of design alternatives were compared, both on safety merits and cost-effectiveness. The experience gained with this scenario-based approach will be used to establish a set of general requirements for safety assessment techniques in ship design. In the view that safety assessment results will be most probably presented in a quasi-quantified manner, the requirements are concerned with uniformity of both the safety assessment. These requirements make it possible that valid comparison between various assessment studies can be made. Safety assessment, founded on these requirements, provides a validated and helpful source of data during the coming years, and provides naval architects and engineers with tools experience and data for safety assessment procedures in ship design. However a lot of effort has to be spent in order to make the methods applicable in day-to-day practice.

Keywords: safety-based design, formal safety assessment, risk assessment approach, accidents scenario of LPG ships

1 Introduction

Safety in shipping is related to a very wide range of aspects, for instance operational procedures on board, human factors, management at various levels, equipment, redundancy of equipment and systems, 'lines of defense', maintenance, infrastructure, communications, etc., to mention just a few. The present paper addresses just one of these: the design of the ship as a 'system'. This means that human factors, operational procedures, etc. are touched upon only when there is a relation with design aspects such as installation of equipment, lay-out etc.

Until recently safety aspects related to the design and construction of ships were, almost without exemption, of a prescriptive and deterministic nature. Often designers have argued that this situation is far from ideal. It enhances conservatism and it does no right to the advances, which have been made during the past decades in engineering tools in marine technology, both in methodology and in computational power.

Within IMO this has been realized for some time and has resulted in proposals to use Formal Safety Assessment(FSA) as a tool to improve and to modernize the rule making process(IMO 1996, IMO 1997). In some cases attempts have been made to implement safety aspects in the design procedure of a specific ship type; see for instance Sen et al(1997). Whereas the FSA methodology as proposed by IMO has much in common with recent developments in the safety approach in the Offshore Industry, there is a major difference. In the Offshore Industry one is obliged to perform for a new field development a so called Safety Case study in order to prove that within reasonable boundaries of technological possibilities and economical constraint safety of the installation is 'as low as reasonably practical'. See for instance HSE(1998). In the shipping industry IMO proposes that safety aspects are analyzed for a certain type of ship (or a 'generic' ship) and the outcome is translated into proposals for safety regulations. The decision to analyze safety in a generic situation is generally substantiated by the fact that there is no necessity to consider each aspect separately for each individual ship as ships of a certain type do have much in common. Also it is argued that a full FSA would costs too much effort and time for one single ship. However we believe that there are considerable disadvantages in the 'generic' FSA as well. For instance, when using a generic ship concept no distinction can be made between different design options. Furthermore within a certain generic ship type large differences in the installation and lay-out can be found; an LPG carrier can be fully-refrigerated or fully-pressurized, leading to completely different containment systems with different safety characteristics.

Delft University of Technology investigated the application of safety assessment procedures in ship design, in co-operation with Anthony Veder Shipowners and safety experts from Safety Service Center BV. It is the intention to use the experience gained with this scenario-based approach to establish a set of general requirements for safety assessment techniques in ship design. In the view that safety assessment results will be most probably presented in a quasi-quantified manner, the requirements are concerned with uniformity of both the safety assessment approach and the evaluation criteria, as well as uniformity of the data used for the assessment.

Safety assessment, founded on these requirements, provides a validated and helpful source of data during the coming years, and provides naval architects and engineers with tools, experience and data for safety assessment procedures in ship design. However much effort has to be spent in order to make the methods applicable in day-to-day practice.

2 Safety assessment in general

In industry it is widely accepted to assess safety in the design process in order to explicitly reduce or eliminate serious risks. Design for safety may be defined as a process aimed at minimizing personnel injury or death, product damage or destruction, degradation of the environment or missing performance. Different methods have been developed to determine risks in a quantitative and qualitative way.

In general, safety risks are assessed in the following way:

- Identify the hazards
- Assess the consequences of each hazard
- Assess the likelihood of a hazard, taking into account the safeguards
- Determine the risks and assess whether the risks are acceptable
- Identify the risk control options, if risks are not acceptable
- Change design, if risks remain unacceptable

In designing often the term 'ALARP'(=As Low As Reasonable Practicable) is used. This means that the full assessment is carried out, all alternatives have been examined and possibilities to further decrease the risk have been balanced with the associated costs.

Risks can be determined in a qualitative way by the multiplication of the probability/frequency and the consequences of the occurrence. However, it is not always possible to find sufficient and/or reliable data to determine frequencies. In that case the qualitative approach is followed, so with engineering judgement and operational experience a rather good picture can be obtained of the risks.

In some branches of industry a lot of data has become available about incidents which can occur. In the Gas&Oil industry serious accidents have occurred in the past, which initiated the systematic collection of failure data of equipment and investigation of risks. If failure data is available the risks can be quantified and other types of studies are possible, like reliability and availability studies. Also expected value of costs and even risk-based inspection belongs to the possibilities. In general, quality of comparison of designs can be improved and optimized.

All kind of methods can be applied to perform hazard and risk analysis, each of which have advantages and disadvantages, depending on the nature of the product and the stage in the safety analysis process in which they are to be employed. In terms of increased detail of analysis these methods may be classified as follows, see e.g. Kumamoto and Henley(1996), Sen(1997):

- Preliminary Hazard Analysis(PHA)
- Fault and Event Tree Analysis(FTA/ETA)
- Cause-Consequences Analysis(CCA)
- Failure Mode, Effects and Criticality Analysis(FMECA)
- Hazard and Operability Analysis(HAZOP)

The most widely applied method to estimate risks is by means of a Risk Matrix, which is still based on the relationship of probability and the consequence. It is simple in use and does not need much explanation. It only requires an estimate of the consequences and the probability of the hazardous event. Criteria can be defined in such risk matrix, which may not be exceeded and the ALARP' region. The company can either define the boundaries of the criteria, by the legislator or by other authorities. Today, goal setting legislation is applied in a number of countries and will place the responsibility by the companies. Also risks to assets, environment and financial risks and reputation of a company may now be determined.

3 Safety assessment in shipping

Risk assessment techniques are gaining terrain in the shipping industry. This is especially true for reliability and availability studies and risk-based classification for machinery systems which are in full development. However, safety issues are generally not assessed using hazard identification and risk assessment methods. Safety issues in ship design are generally solved within the prescriptive regulatory framework.

If safety assessment studies are performed, they are mainly concerned with a practical ship specific problem. The assessment most often focuses on one particular ship system. The approach is based on common hazard identification techniques, supported with engineering judgement and operational experience. The results of these assessments are presented in a qualified manner in order to support decision-making concerning which design alternative to choose or to illustrate that the safety issue is within certain acceptance margins. The assessment is determined to be qualitative of nature while currently insufficient or reliable data is available to quantify risks of safety issues. The availability of reliable accident data is a less compelling argument, if the risk of safety issues is qualified intolerable. Then, regardless of the accuracy of the data used, immediate risk mitigating measures have to be taken.

Interest for safety assessment in shipping is still growing, both for the assessment of ship specific safety issues, as well as for a structured integral safety assessment approach. In this paper a safety assessment with a scenario-based approach is presented, taking into account various accident types and interaction between accident scenarios. This integral approach ensures that a wide range of hazards is analyzed. The process converges to those accident events with high risk.

4 The ship and system description

This paper describes the risk assessment study as performed on an existing LPG Carrier of a widely used type. The type under consideration is a semi-pressurized-fully refrigerated LPG carrier. The vessel is designed and constructed for the transport of liquefied gases as LPG, Ammonia, and VCM. The cargo capacity of the ship is $4200m^3$ divided over two independent type C tanks, one bi-lobe and one cylindrical tank. Figure 1 gives the General Arrangement of the vessel.

Prior to the risk assessment itself, a system description of the LPG carrier is made, in order to provide the risk assessment of the necessary information. The system description consists of a description of the ship particulars and relevant systems that are essential for the operation and survivability of the vessel.

The operational phase and the type of cargo carried influence the occurrence and the conse-

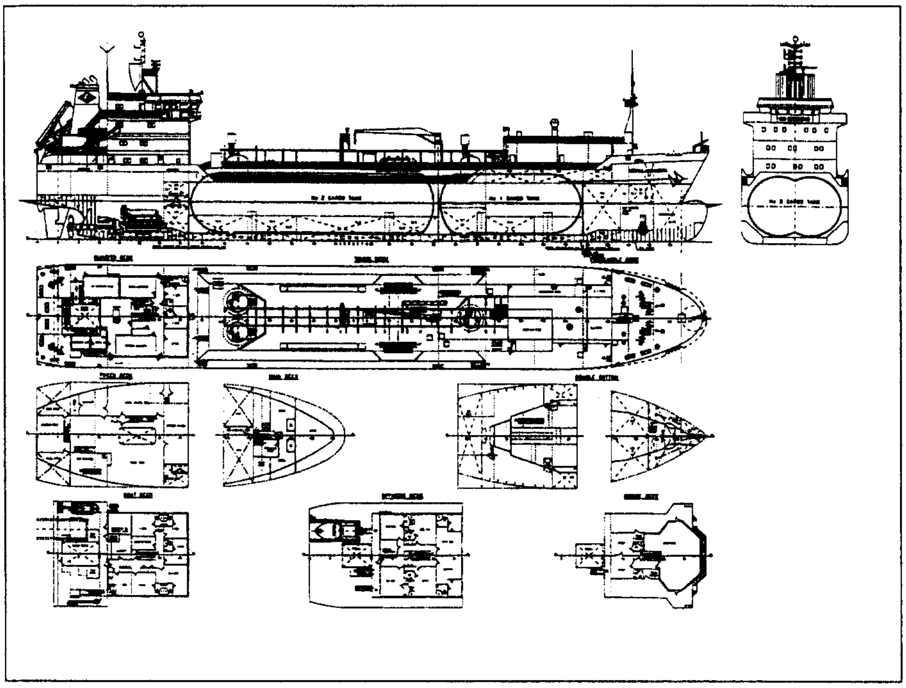

Figure 1: General arrangement of the ship

quences of hazardous events. Therefore, so-called system phases were introduced prior to the risk assessment. These system phases consist of a combination of the ship's operational phases(at sea, manoeuvring in port, moored at jetty) and of two principal liquefied gases(ammonia or propane)

5 Risk assessment approach

The risk assessment consists of a scenario-based approach, using elements of the Formal Safety Assessment methodology(FSA) as proposed by the IMO. The objectives of the assessment of the LPG carrier are related to the design of the carrier and the risk to capital assets. Accident scenarios that could impair the safety of the carrier are considered and assessed.

The risk assessment approach consists of the following steps:

1. Accident event analysis
2. Quantified risk assessment
3. Risk control option identification and evaluation
4. Conclusions

Schematically the elements of this approach are shown in Figure 2.

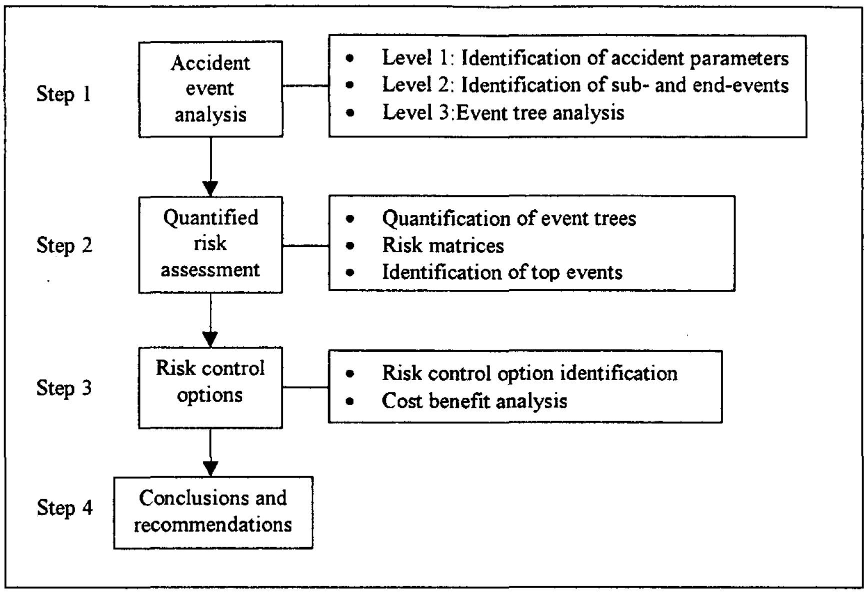

Figure 2: Schematic flow diagram of the risk assessment approach

5.1 Accident event analysis

The accident event analysis approach is based on the assumption that a main accident has occurred. The accident groups considered are: Collision, Contact, Grounding, Fire and Explosion.

The methods that are used in the accident event analysis are based on cause-consequences analysis and event tree analysis(ETA).

The aim is to identify hazardous events that are related to, or evolve from the occurrence of a specific accident. The accident event analysis forms the basis of the risk assessment study of the considered LPG carrier and introduces a scenario-base approach in the assessment. The results of the accident event analysis are used as input for a quantified risk assessment.

Within the accident event analysis different stages can be identified. The analysis starts with an "open-mind" towards possible hazardous events and related parameters following an initial main accident. The results converge to a set of accident events, which could impair the safe operation of the LPG carrier. This process has an iterative character and is supported by acquired knowledge from literature and expert judgement. The selected accident events are analyzed using an event tree analysis(ETA).

The system description of the LPG carrier provides for the analysis the information of the ship and of those systems that are subjected to, or influenced by the occurrence of accident events.

5.2 Quantified risk assessment

Prior to the quantified risk assessment so-called risk evaluation criteria were established to assess the risk of the events. Risk evaluation criteria is the collective term for frequency of occurrence, consequence and risk acceptance criteria. The presentation of risk, as a combination of frequency of occurrence and consequences, is done by means of a risk matrix.

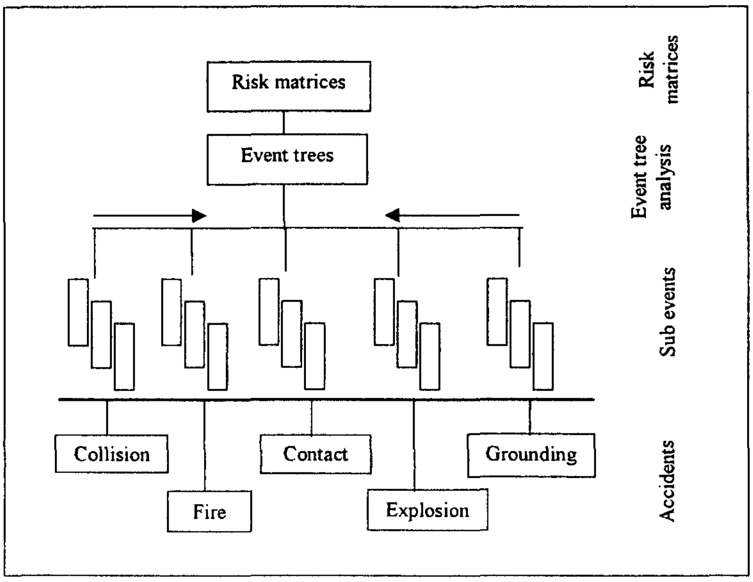

Figure 3: Accident event analysis and quantified risk assessment

The risk evaluation criteria are extracted from general used descriptions for consequence and occurrence. The evaluation of the risks is done by means of the ALARP principle. The ALARP boundaries are established by reviewing various sources that quantify accepted risk levels. The definition of the occurrence and consequence criteria is based on different sources that give values for these criteria, for instance IMO-MSC66(1996), HSE-UK(1998).

The occurrence criteria are described qualitatively and quantitatively and are composed of common accepted terms. The consequence criteria are described in a qualitative manner, while quantitative data in terms of costs are hard to obtain and not accurate enough.

The quantified risk assessment approach consists of the assessment of the event trees developed in the accident event analysis. The event tree analysis starts from an accident main group and is developed to specific sub-events and end-events. Thus, only a 'bottom up' approach is considered, quantifying the event trees which results in the risks of a number of events that are considered relevant for the safety of the LPG carrier. A sketch of the accident event analysis and of the QRA process is given in Figure 3.

The quantification of the event trees is done with the use of available accident data, and where needed estimations are made based on expert judgement. The results of the risk assessment are quasi-quantified. This means that the frequency of occurrence is quantified (given as numerical value), but the consequences are given in a qualitative manner. The results are concerned with the five main accident groups: Collision, Contact, Grounding, Fire and Explosion, and are placed in risk matrices.

As an example a number of possible events due to the accident group 'Collision' are presented in a Risk matrix in this paper. The events that are analyzed and assessed in the QRA of collision accidents are related to flooding of engine room, flooding of the cargo hold, loss of propulsion, loss of steering, damage to the cargo tanks, outflow of cargo. The risk matrix, as shown in Figure

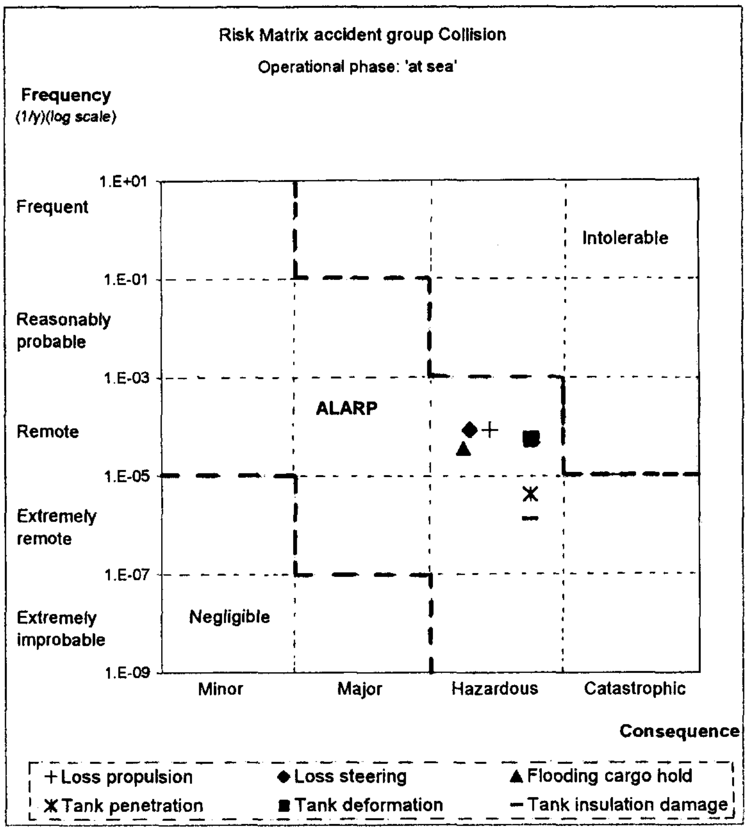

Figure 4: Risk matrix of events due to 'collision'

4, incorporates various events of the operational phase at sea.

During the quantification, various considerations concerning damage and occurrence distributions are taken into account:

- Distribution of collision damage extent.

- Distribution of damage location relative to the ship's length.

- The ship's system phase, i.e. sailing at sea, maneuvering in harbor, loading at jetty, etc.

Although all events are located in the ALARP region, the events presented in the risk matrix are relatively high compared to the other assessed events. The focus of the risk control option identification, with respect to collision, was therefore concentrated on these events. Reviewing the risks of collision events, the cargo containment system is likely to be damaged, although cargo release generally does not occur. Loss of propulsion and steering systems is likely to occur due to collision events in the engine room area. The safety and survivability of the LPG carrier is in danger if these events occur.

5.3 Risk control options(RCO)

The objective of the introduction of a risk control option is that the risk is lowered. Risks can be mitigated either by reducing the frequency of occurrence of an event or by reducing the consequences of an event, or even by a combination of the two. The identification of RCO's is based on the conclusions of the quantified risk assessment. The RCO are identified with respect to the consequences, rather than the causes, while the risk assessment was primarily concerned with effect of accidents rather than the causes of accidents (scenario-based approach). Therefore, the effects of the RCO are related to mitigate the consequences of events.

The analysis of the effectiveness of a potential introduction of a risk control option(RCO) is done by means of a cost benefit analysis(CBA). The suggested approach consists of four steps:

1. Assessment of the base case related to the risk control option
2. Assessment of risk control option benefits against base case
3. Assessment of the costs of the implementation of the RCO
4. Evaluation of results and decision making

Of the identified RCO's, one will be discussed here and evaluated with the use of a cost benefit analysis. The option discussed in this paper is an emergency propulsion and steering device (EPSD).

The EPSD is a device that could take over the propulsion and, or steering of the ship and was identified on the following events assessed in the QRA:

- Damage to propeller or rudder due to collision, contact or grounding.
- Flooding of the engine room due to collision, contact or grounding.
- Damage to main propulsion or steeling system due to collision, contact, grounding, fire or explosion.

The objectives of the EPSD are concerned with the ability to reduce risk to life, asset and environment. This can be accomplished with the EPSD while this device gives the LPG carrier the ability to continue the journey to the nearest safe haven or the ability to maintain some sort of control over the ship. This is important when the ship is e.g. drifting towards an unfavourable position(e.g.coast, traffic zone, grounding area).
Based on the objectives two possible configurations for an EPSD are a rotational pump-jet or Retractable, azimuthing bow thruster. These device can also perform the task of a conventional bow thruster in a transverse duct.

Step 1. Assessment of the base case related to the risk control option
The base case reflects the existing levels of risks assessed in the quantified risk assessment(QRA) before the implementation of the EPSD. In this step, the events associated with a figure implementation of the EPSD are categorized. The risk of these events is assessed in the QRA. The possible costs following the occurrence of these events are determined. Both the possible costs of direct associated events and those of possible escalating events are considered. Due to the fact that the costs evolving from the occurrence of these events is most often based on estimates, a sensitivity

Table 1: Summary of cost benefit analysis results

CBA step	Results
Base Case Costs	9.700 US$/year
Costs after implementation	8.400 US$/year
Gained Benefits of RCO	1.300 US$/year (positive)
Implementation costs Annual costs Capital costs	 3.000 US$/year 150.000 US$
NPV on investment(in 25 years)	-145.000 US$ (negative)

analysis is done to validate the results within a certain margin.

Step 2. Assessment of risk control option benefits against base case
The implementation of EPSD mitigates the risk of the events associated with the objectives of the EPSD. The consequences and, or the frequency of occurrence is reduced due to the implementation of the RCO. In this step the reduction gained due to the RCO is determined by reconsidering the risk of associated events. Again, a sensitivity analysis is done to validate the results with a certain margin. In the present paper only the 'most probable' results are shown, not the results of the sensitivity analysis. Depending on the related events, the EPSD itself is also subjected to risk evolving out of the occurrence of accidents. These risks are also considered and adjusted within the benefits of the RCO.

Comparing the base case(no EPSD) with the reduced risks of events after implementation of the EPSD, the benefits of the risk control option can be obtained. These benefits are actually the reduction in possible costs of risk due to the implementation of the EPSD, in this case expressed in US$/year. The accidents considered are:

1. Grounding, resulting in damage to ship
2. Contact, resulting in damage to ship and/or jetty
3. Collision, resulting in damage to ship and/or damage to another ship
4. Drifting at sea and foundering of the ship due to severe weather
5. Release of cargo, with damage to health, loss of life, and/or environmental damage

The associated costs(both direct and indirect) of the events vary between US$ 20M and US$ 0.5M. However since the frequency of occurrence of the events is extremely low (between 10^{-4} and 10^{-7} per year), the probable cost per year are low as well. A summary of the base case costs and benefits of the implementation of the emergency propulsion and steering device are listed in Table 1. Concluding, in this particular case the total possible benefits gained by the implementation of the EPSD are calculated at 1.300 US$ per year.

Step 3. Assessment of the implementation costs the RCO
The implementation of EPSD involves an increase in costs relative to the existing situation. These

costs involve capital costs, operating costs and maintenance costs. In this step of the cost benefit analyse the various cost items are identified and quantified in order to determine the additional implementation cost of the EPSD compared with the base case. The results are again presented in Table 1.

step 4. Evaluation of results and decision making
The evaluation of the cost benefit analysis of the considered RCO should result in a motivated conclusion on which a decision can be made whether or not to implement the RCO. This is done by calculating the Net Present Value (NPV) of the risk control option EPSD, which is composed of the capital costs, the operational costs and its benefits. Over a 25-year period the NPV is minus 145.000 US$, see Table 1. Consequently the conclusion can be drawn that the installation of the EPSD system is not advisable under the present circumstances.

Future developments in risk assessment and the availability of accurate consequence and occurrence data could lead to results that justify the implementation of an EPSD.

5.4 Results of the risk assessment

Considering all assessed accident event evolving from the five main accident groups it can be concluded that the events with the highest risk levels can be summarized as follows.
Due to collision, contact and grounding:

- Flooding events.
- Loss of propulsion and steering.
- Damage to the cargo containment system, including damage to the cargo tank, damage to the insulation of the tank deformation of the tank wall and penetration of the tank wall. Cargo release only takes place in the event of tank wall penetration.

Due to fire and explosions:

- Engine room fire.
- Fire and escalating fire at the main deck of the cargo hold area.

The risks of these accidents are all within ALARP region. The risks are therefore acceptable, however risk control options for these adverse events should be considered. In this paper a possibility to reduce the probability of accidents due to loss of steering and loss off propulsion is worked out. With the currently available statistical data on accidents, resulting events and costs involved, the risk control option 'Emergency Propulsion and steering Device' is economically not advisable, as the net present value of the implementation is negative.

6 Conclusions and recommendations

The FSA methodology in its present form, as proposed by IMO, is less suitable for integration in ship design procedures. While FSA may be the right tool for the drafting of regulations, it is too generic to be of much value for a specific ship or a specific design and it does not sufficiently distinguish between different options in a particular design. Furthermore within a certain generic ship type large differences in the installation and lay-out can be found. For instance a LPG carrier can be fully-refrigerated, or fully-pressurized, leading to completely different containment systems with different safety characteristics.

The Quantified Risk Assessment(QRA) as discussed in this paper, concentrates on 'ship specific' (or 'ship-type specific') problems. The approach is based on common hazard identification techniques, supported with engineering judgement and operational experience. It takes into account various types of accidents and interaction between accident scenarios. This ensures that a wide range of hazards is analyzed. The process converges to those accident events with high risk.

This QRA is potentially better suited to be incorporated in ship design procedures than FSA.

- The QRA, contrary to FSA, makes a clear distinction between risks involving life, risks involving environment and risks involving asset. This makes a quick review and evaluation during hazard screening and hazard ranking possible.

- Whereas the FSA methodology is based on a generic ship or even a generic shipping model, in the QRA a specific ship is considered and one can even zoom in on a specific sub-system of a ship.

- The QRA has potentially capabilities to improve ship design procedures by introducing first principles in the analysis part of the design and by supporting unbiased decision procedures.

In the execution of the risk assessment, problems were encountered related to the validation of the risk assessment results. Therefore, interpretation of the results of the risk assessment of the LPG carrier has to be taken with some reservation. The occurrence frequencies and consequences of the various accident events incorporate a deviation and uncertainty. This is due to the following:

- The accident data that is used for the assessment gives limited insight in the factors that are related to the accident. Distribution of the damage extent and the damage location relative to the ship length cannot be filtered out of the actual accident data. Neither can certain accident factors or environmental factors be filtered out of the used accident data.

- Due to the difficulties in obtaining accident data that included damage distribution figures and the costs of events, the consequences can only be given in terms of qualitative descriptions. Thus the risk assessment has a quasi-quantified character while the occurrence is given as a numerical value, but the consequences are described qualitative.

Before QRA procedures can be introduced in practice, where decisions have to be made within a few days or even a few hours, considerable improvement and streamlining is required:

- statistical data on accidents, its causes and resulting(consequential) damage is often not at hand.

- It is questionable whether present-day databases, based on historical accidents will ever provide sufficient statistical information, as(luckily) accidents involving loss of life or damage to the environment do not happen that often.

- Therefore a database, containing(also) information on incidents('near misses') would be of great value.
- At present well defined criteria and coherence in qualitative descriptions of risk evaluation criteria is still lacking.

Abbrviations and acronyms

ALARP	= As Low As Reasonable Practicable
CBA	= Cost Benefit Analysis
EPSDETA	= Emergency Propulsion and steering Device
ETA	= Event Tree Analysis
FSA	= Formal Safety Assessment
IMO	= International Maritime Organisation
LPG	= Liquefied Petroleum Gas
NVP	= Net Present Value
QRA	= Quantified Risk Assessment
RCO	= Risk Control Option

References

DOBLER, I. P. 1994 The requirements for the publication of detailed global marine casualties statistics. MARIT. POL. MGMT, **21**, **1**, pp. 45-60

HSE 1998 Assessment principles for offshore safty cases. Health and Safety Executive HSG181, London, ISBN 0 7161 1238 4

IMO 1994 International code of safety for high speed craft. Resolution MSC.36(63), IMO-187E. London.

IMO 1996a Formal safety assessment. A methodology for formal safety assessment of shipping. IMO-MSC 66/INF.8, 66th session.

IMO 1997a Interim guidelines for the application of formal safety assessment to the IMO rule-making process. MSC/Circ.829 - MEPC/Circ.335.

KUMAMOTO, H. AND HENLEY, E. I. 1996 Probabilistic risk assessment and management for engineers and scientists. IEEE Press, New York, ISBN 0 7803 1004 7.

LLOYD'S REGISTER OF SHIPPING Casualty returns. Lloyd's Register of Shipping, London, published annually

MARINE ACCIDENT INVESTIGATION BRANCH 1997 Extract from the merchant shipping accident reporting and investigations. years 1995 to 1997, UK, (http://www.open.gov.uk/maib/)

SEN, P. ET AL 1997 A methodology for the integration of formal safety analysis into the design of lifeboats. IMDC'97 Newcastle