Liverpool John Moores University

School of Engineering

Formal Safety Assessment of Marine Applications

By

Eleftherios Maistralis

A thesis submitted to Liverpool John Moores University in partial fulfilment of the requirements for the Degree of Doctor of Philosophy

February 2007

Dedicated to my loving parents George and Stella who stood up and supported me throughout my life in times of hardship. To my brother John who inspired me with his presence, and to my supervisor Prof. Jin Wang who didn't give up on me even in circumstances governed by uncertainty.

Abstract

This research has first established that it is based on multiple methodologies developed to tackle the areas of engineering cargo handling systems, both at port and on-board vessels, as well as in the area of organisational self-assessment. It continued in reviewing the current status and future aspects of marine safety assessment together with an examination of a few major accidents. The major problems identified in marine safety assessment in this research are associated with inappropriate treatment of uncertainty in data and human error issues during the risk modelling estimation process and the calculation of failure probabilities. Following the identification of the research needs, this thesis has developed several analytical models for the safety assessment of cargo handling systems and organisational assessment structure. Such models can be effectively integrated into a risk-based framework using the marine formal safety assessment, safety case concepts.

Bayesian network (BN) and evidential reasoning (ER) approaches applicable to cargo handling engineering systems have been proposed for systematically and effectively addressing uncertainty due to randomness and vagueness in data respectively. ER test cases for both a vessel selection process and a comparison of the safety maturity of different organisations in terms of self-assessment have been produced within a domain in which main and sub criteria have been developed for assessment reasons along with the combination of the proposed model with existing organisational models. BN test case for a Liquefied Petroleum Gas (LPG) reliquefaction plant has been produced within a cause-effect domain in which Bayes' theorem is the focal mechanism of inference processing. A methodology aiming in finding the probability of failure when having variables ruled by uncertainty is established using certain variable transformation methods through the First and Second order reliability methodologies. Form/Sorm produces a most likely failure point, which is demonstrated through the application at a port cargo handling crane system. The outcomes have the potential to facilitate the decision-making process in a risk-based framework. Finally, the results of the research are summarised and areas where further research is required to improve the developed methodologies are outlined.

Acknowledgements

During the course of the research described in this thesis, many individuals and organisations have provided considerable support in one way or another. The author is extremely grateful to the Liverpool John Moores University (LJMU) for the financial assistance provided, and to the Institute of Marine Engineering, Science and Technology (IMarEST) for their generous financial aid of the research. In particular, I would like to express my sincere gratitude to my supervisors, Prof. J. Wang and Dr. S. Bonsall, in the School of Engineering at LJMU for their stimulating suggestions, constructive comments and constant encouragement. I would like to record my sincere thanks to Interunity Management Corporation for assisting with the provision of all the technical data in the area of Liquefied Petroleum Cargoes, to the International Maritime Organization for providing me with an enormous amount of data support. Also, I would like to express my sincere thanks and pleasure working with my colleagues at the Marine and Offshore Technology Research Group of LJMU and I am ever so grateful for their wit that provided the critical forum for the research.

Last but not least, I would like to give special thanks to my best friend George for his encouragement, especially in times of hardship.

Eleftherios Maistralis

February 2006

CHAPTER 4: A MULTI-CRITERIA DECISION MAKING APPROACH, BASED ON A SYNTHESIZED FUZZY SET AND EVIDENTIAL REASONING METHODOLOGY

CHAPTER 5: MARINE SAFETY ASSESSMENT AND BAYESIAN NETWORKS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.1 General overview

The need for reliability in engineering systems became very apparent in the Second World War. Military equipment, in fields such as weapons, communications and transportation, experienced a rapid increase in complexity especially in terms of electronics and control systems. The Department of Defense (DOD) in USA realized that the complexity of the equipment would continue to increase dramatically. As a result they created the Advisory Group on the Reliability of Electronic Equipment (AGREE). A major part of the reliability theory development is based on the research made by the DOD [House of Lords, 1992], [Wang, 2000].

Along with the sectors of environmental and computer technology, safety, risk and reliability engineering have also met a significant percentage of development and expansion in the last forty years. In the early 1960s safety analyses were empirically based, the term risk analysis was totally unknown, and the word reliability was used only in isolated areas of the military and aerospace industry. The chemical industry, which was the world's largest industry at that time, first started to publish articles concerning reliability after 1966 [Barker & Campbell, 2000], [Birolini, 1993]. The issues of hazard and risk analysis were brought up from the European Union after the occurrence of the Seveso accident in 1976, which prompted the adoption of legislation aimed at the prevention and control of such accidents [U.N 96/82/EC, 1999]. Within the 1980s, offshore industry headed towards qualitative risk analysis in an attempt to break down the operational systems of offshore platforms to their respective components and conduct a preliminary hazard analysis trying to identify potential dangers. An industrial self regulative regime was operating in Norway and UK followed with a safety case regime. Risk analysis got towards the beginning of the 90s with the shipping industry entering a safety culture following a number of significant accidents which will be mentioned in this chapter but further explained in Chapter 2. Reaching the 21st century, risk assessment has been formalised and specific guidelines have been presented by International Maritime Organization (IMO).

Quality and reliability of complex engineering systems demanded a number of specific activities, from the initial design stage of the project to the operation phase [Villemeur,

1992], [Barker, 1990]. This includes the definition of targets, planning and performing analysis, selecting the appropriate components and materials, configuration management, control of production procedures and processes, aiming in a continuous development of reliability and quality during the production process [Birolini, 1993]. All these activities should be taken into account and executed correctly from the project's engineers in order to achieve the best performance in terms of reliability and quality of the scheduled targets. Before the 1960s adequate level of quality was achieved when the item was tested at final inspection, and found to be free of defects and failures after it left the manufacturer.

In the shipping industry the main concern of port designers, port-builders, port operators as well as vessel operators and vessel's personnel is the safety of the vessel and the safety of near-by installations or other vessels that may exist. A few serious accidents such as the sinking of Titanic, the capsize of the Herald of Free Enterprise, the Exxon Valdez grounding and the Esthonia ferry tragedy attracted greater attention to ship safety. There are significant consequences when an accident happens, in terms of deaths and injuries, damage to the environment and destruction of property. Further studies have been carried out, in order to find ways to prevent such unacceptable incidents. This has been reflected in the attention given to both the design improvements and to the port's operations conducted by educated and trained operators to the highest of industry's standards. The use of formalized procedures to estimate risks and to make decisions based on risk estimation has been changing within the maritime industry [Wang, 2000]. The risk levels existing in the maritime transportation can be initially estimated based on accident statistics. These studies allow the identification of time evolution of the levels of safety in global activity, and differentiation of safety in the different types of ships as far as size and age are concerned. The adoption of the safety case approach in the UK offshore industry has also encouraged marine safety analysis to look at the possibility of using similar methods to the wider marine industry [Guedes & Teixeira, 2001], [Wang, 2000].

The issue of a more scientific approach to the subject of ship safety was first highlighted by Lord Carver's report on the investigation of the capsize of Herald of Free Enterprise in 1992 [House of Lords, 1992]. Lord Carver's report recommends that more emphasis should be given to the subject of ship safety by focusing on a performance based regulatory method. Significant improvements in maritime and specifically vessel's safety could be achieved using a Formal Safety Assessment (FSA) approach with possible application to ship design

and the operation of new technology. After the publication of Lord Carver's report the UK Maritime and Coastguard Agency (MCA) showed serious concerns over the improvement of ship safety and in 1993 proposed to the IMO that FSA method should be applied to ship design and operation in order to ensure safety and pollution prevention either in ports or in the open sea [MSA, 1993]. The IMO followed the MCA's proposal for FSA submission, and since then continuing efforts have been made to reach greater safety standards through specific methodologies. The FSA methodology adopted from IMO, progresses through the completion of five steps [MSA, 1996]. The five steps of FSA are:

1. The identification of hazards related to a case examined (engineering system or operational process).
2. The assessment of risk(s) associated with the identified hazards.
3. The control measures that need to be applied so that the assessed risk(s) can be managed.
4. The cost-benefit assessment of the proposed control measures.
5. The decisions which eventually lead to the best combination of risk controls in terms of cost benefit assessment for reduction of the overall risk factor to an acceptable level.

In general terms, within the last few years the application of FSA has been significantly progressed [Wang, 2002]. This is demonstrated by the successful case studies dealing with high speed crafts and bulk carriers, which were analysed and approved by the IMO, supporting a risk-based rule-making process [Wang, 2000]. Using FSA as a complete safety framework there are a number of advantages that come with it in terms of:

1. It creates a framework which is characterized by consistency and integration in all safety aspects examined.
2. It tries to get the best possible cost saving solution, through careful cost benefit analysis, without omitting the essence for performing safety analysis.
3. It changes the current status of approach from reactiveness to pro-activeness, thus enabling the easier identification of hazards that have not given rise to concerns yet.
4. The confidence of applying the proper risk control measures is increased, therefore staying in line with all regulatory requirements.
5. It gives the freedom to address and point out future developments in high risk areas that appear due to the ever-changing nature of marine industry.

The above mentioned five advantages, can be utilized in order for a shipping company to improve its performance by keeping risk levels as low as reasonably practicable (ALARP) [Wang, 2001]. It is worth mentioning that the only possible disadvantage of FSA is the fact that there are areas where methodologies need to be further developed in order to have accurate estimation results within an FSA framework

Safety assessment in ship/port design and operation offers great advantages including:

1. It ensures the quality and reliability of new vessels and installations like loading docks, loading arms and cranes. It measures the performance and the efficiency of operations, and based on the performance measurements, improves them.
2. All experiences gained from field work and all the lessons learned from any incidents that have occurred can be incorporated in a safety framework applied to port and ship operation.
3. It helps develop methodologies for estimation and control of possible scenarios that may result in undesirable incidents.

Understandably, there has been some concern over the likely impact of risk-based rule making on behalf of ship owners and vessel operators [Wang, 1997]. A change in what is considered to be established patterns of operations is never to the liking of many, as it creates problems in terms of time management, resources, additional training and doubt if at the end, the newly proposed methodologies are going to work and offer advantages over the existing status. Risk analysis follows a progressive path. It existed as guidance at the beginning but gradually it evolved to become part of the management decision making process. Although scepticism governs the majority of marine companies, others have realized the potential for development and adopted the newly proposed methodology aiming at improving their overall performance through the described safety analysis framework.

As marine industry is still an uncharted area relatively to shore industries in terms of safety assessment, methodologies and techniques need to be further developed to accommodate a number of questions raised. Generic FSA methodologies are able to facilitate safety at a reasonable accuracy degree in terms of results, leaving out details that cannot be accommodated within them. Vessels and ports are parted by a number of complex engineering and operational systems. There is lack of data and an uncertainty degree

involved when it comes to information concerning these systems separately, even more when trying to assess the reliability and safety of their individual components [Wang & Ruxton, 1997]. To date, comparatively little use of safety and reliability assessment methods has been made in connection with merchant shipping. Lloyd's Register of Shipping has for a long period, collected information relating to failures and has carried out development work to investigate the application of such methods to the classification of ships. Apart from this, some consultancy work has also been carried out on behalf of ship owners. Engineering systems and operational processes require a number of specific methodologies, being able to facilitate performance measurements and reliability assessment during operation, as well as being able to locate and identify any further problematic areas that traditional methods cannot efficiently tackle. Cases of risk estimation and decision making governed by uncertainty or lack of data need to be examined [Wang et al., 1996]. Rule-based decision making is an area where further research and development is required in order to make rational decisions. This thesis seeks to explore these identified gaps and propose means, through the development of a number of methodologies, to accommodate uncertainty and decision making processes in the areas of engineering reliability safety and organisational safety.

1.2 Aim and objectives of this thesis

This thesis is called upon to develop a number of risk-based methodologies to assess the reliability and safety of marine engineering systems as well as establish a pattern for self-assessment at organizational level within the marine sector in cases where vagueness and uncertainty of data exist. This aim is achieved through the generation of various risk-based models, novel for the maritime industry.

In order to achieve the main aim set, the following objectives have to be met throughout the course of the presented chapters:

- To critically review the current status of safety in the marine and port industry.
- To identify any key risk analysis techniques currently implemented in the sector.
- To examine formal safety assessment and its implementation to vessels.

- To demonstrate that Bayesian networks can be a very powerful tool in the process of assessing the reliability of an engineering system.
- To demonstrate that the combination of fuzzy logic with evidential reasoning can create a powerful tool in the decision making process for the maritime sector.
- To demonstrate the aid of evidential reasoning as a self-assessment tool when a company is trying to assess its own performance and benchmarked against others.
- To show through Form/Sorm method a better approximation of risk estimation.

These goals are established analytically through the course of this thesis.

1.3 Why various and not single methodology were adopted through the thesis

This thesis incorporates multiple models, each one dealing with a different element. Each model is based on a custom proposed methodology, along with its respective test case. A brief outline of the generic structure for each of the following chapters includes:

1. A brief literature review within the sector that the chapter is dealing with. Critical evaluation of other people's work and proposed models is made in Chapter 2 of this thesis. The review within each chapter exists mainly to support the ideas of the author as far as information is concerned in the identification of existing gaps in the industry.
2. Background information on the theory that each model is based upon. Key elements of the theory are to be identified and presented so as to explain the mechanism that each theory works on. After the presentation of the framework, all modifications and novelties are presented along with the proposed methodological steps.
3. After proposing the methodology a test case is required to demonstrate its applicability. Test cases from within the marine industry are chosen so as to give a more advanced, though practical, when applicable, approach. Engineering systems from liquefied petroleum gas (LPG) vessels and container cranes are some of the cases that the proposed methodologies are applied to. It is the author's intention to demonstrate that theory and applicability within the marine industry are not so far apart.
4. All chapters end with a discussion of the key points raised throughout the chapter examined. The findings are assessed and a conclusion is drawn.

It is the combination of the methodologies developed within this thesis that when applied together can derive rational results when examining the engineering reliability or risk factors imposed to large engineering systems such as complete vessels or full dock loading/unloading facilities. The proposed methodologies when applied by experts can formulate, according to the case examined, a platform which can facilitate risk modeling and decision making when data is governed by vagueness or fuzziness or incompleteness.

As it can be seen from the aim and objectives of this thesis, there is the need to cover several aspects within the marine industry using the application of formal safety assessment that forces the implementation of a different methodology in each particular case. A unified methodology would not be applicable in all cases and it was not the intention to provide a single path, but multiple solutions to the number of different cases examined.

1.4 Scope of work

The safety analysis and decision support methodologies developed and described within this thesis have been applied to specific test cases. Their nature though, is such that they are applicable to a great variety of cases either in the operational or the design fields. They can also be utilized by other disciplines of engineering in cases where safety related data is lacking or vague. All these methodologies can be used in conjunction with the traditional methods in safety assessment for engineering products.

The paragraphs presented next, give the reader a "road map" of the content of each individual chapter.

Chapter 2 outlines the generic development of formal safety assessment within the marine industry and its current status. It shows the progress from a reactive approach usually used after a major accident towards a pro-active approach trying to minimize the overall risk factor existing in a system or a task. The adoption of FSA from the UK MCA as a means to improve safety is also included. A number of key lessons raised from accidents are outlined and briefly discussed. A critical overview of several models developed is made and gaps that have been omitted are identified so as to show the applicability of this thesis.

Chapter 3 presents the fundamental risk assessment methods used within the risk analysis framework, explaining their key points in such a way that they can be utilized along with the proposed methodologies in the chapters further up the thesis. This chapter does not intend to be a textbook chapter, but merely to show the interconnection of basic methodologies and the way they can be linked with more advanced risk estimation models. Methods like fault tree, event tree, risk matrix modeling and others are explained in this section of the thesis.

Chapter 4 shows that when dealing with multiple attribute decision analysis, the decision maker is often required to process simultaneous data containing both qualitative and quantitative values. The main aim of the decision-making process is to be able to derive rational decisions from uncertain or incomplete data contained in the total package of information. In this chapter a multilevel decision-making technique is developed based on the Dempster-Shafer theory, and is used in different areas of engineering, safety, management and design selection. The basic functions of evidential reasoning are also analysed and further developed in order to improve the process of dealing with attributes containing uncertainty or attributes with lack of information. A numerical example of a vessel selection process is examined using a proposed form of evidential reasoning approach. The sequence of the numerical steps followed to assess vessels is indicated so as to demonstrate the implementation of the procedure.

Chapter 5 indicates that along with the economic growth within the marine industry the need for sufficient safety levels has been increased throughout the past years, in view of optimising them for the years to come. Decisions made must ensure that adequate safety levels are achieved. What is more, to ensure that decisions are taken on a rational basis, a number of uncertainties need to be taken into consideration before any results are produced. Bayesian networks and influence diagrams provide the means of analysis in such a case. The intention of this chapter is to demonstrate their potential as a modelling technique, which can provide features not always available through conventional methods. The literature review and the background theory of Bayesian networks are analysed along with a proposed methodology and a test case to prove the value of the method.

Chapter 6 presents the Form/Sorm method, also known as most-likely failure point (MLFP), It is a method for estimating the probability P_f that a value of a calculated quantity would exceed (or, alternatively, be less than) a certain limit, given that a number of the input data

values, on which the calculation is based, is uncertain. This chapter contains a brief introduction to the background of the method, an explanation of its use and a proposed change in the way that variables are handled. Finally, a test case is presented to demonstrate the usage of the modified Form/Sorm method.

Chapter 7 shows that human and organisational performances are the main factors within a management framework used to either self-assess the progress of a company or compare it with other companies operating in the same field. Organisations that are safety oriented are often required to produce a self-assessment regime under which performance and safety analysis are divided into a number of main criteria. Some of these assessment criteria contain sub-criteria. This chapter presents a method incorporating the evidential reasoning algorithm, which can be equally used for self-assessment as well as for comparing two or more companies by an independent assessment source. The criteria used are presented, analysed and brought into a common utility plane so that comparisons can be carried out. All linguistic variables used as assessment grades, are the result of consultation with experts such as academics and engineers. A test case of assessment between four companies is also presented to demonstrate the applicability of the method within the marine industry.

Chapter 8 gives an overview of the thesis presented. A discussion is presented following the key points raised through the thesis. The safety analysis methodologies in the form presented in this thesis are capable of dealing with a number of questions and problems concerning engineering systems along with any topics raised within a safety assessment organizational framework. Suggestions for future work are made. A number of publications arising from this thesis can be found in journals and conferences as well as being referenced in this thesis.

Figure 1.1 shows a graphical representation of the structure of this thesis.

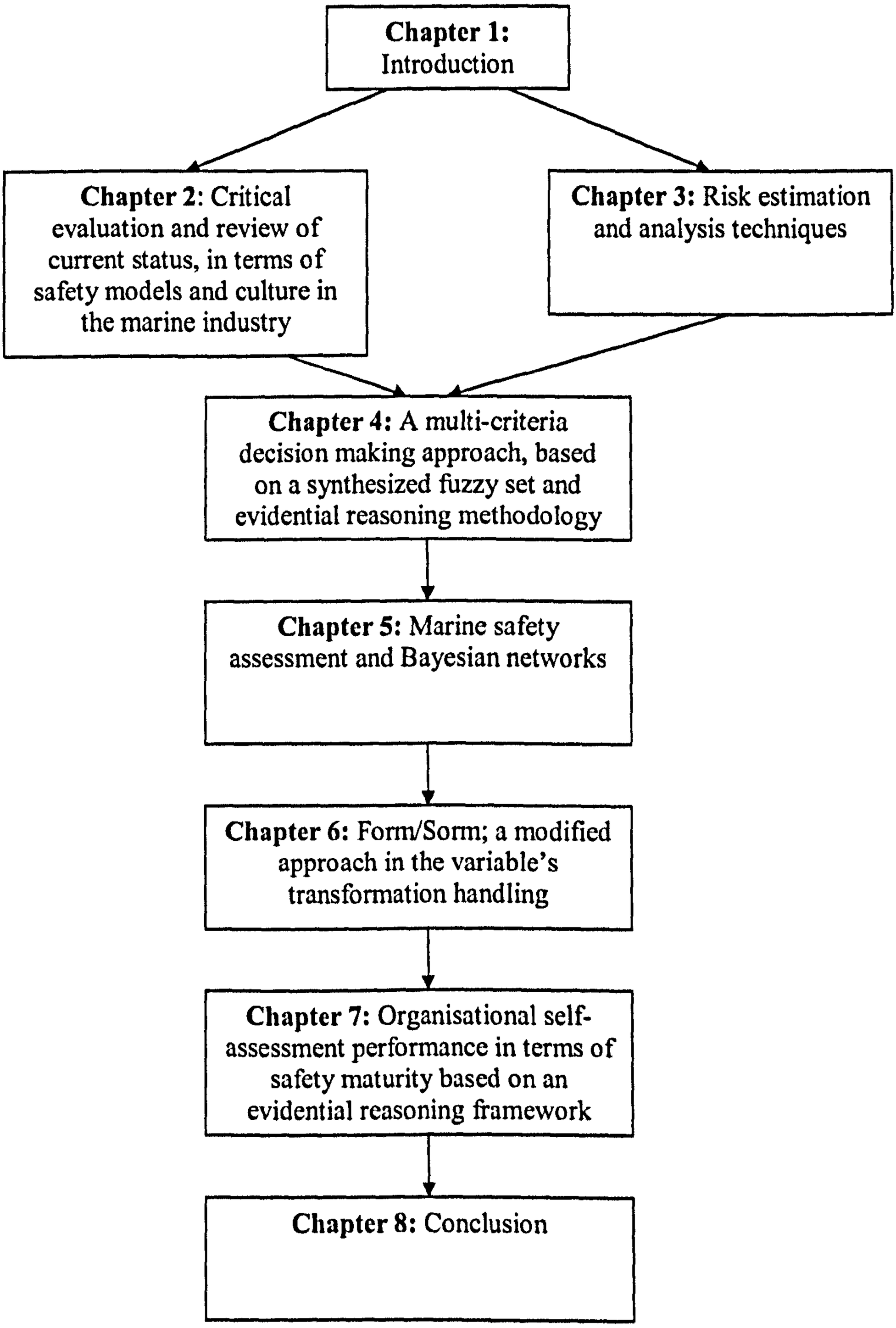


Figure 1.1 Thesis road map

CHAPTER 2: AN OVERVIEW OF FORMAL SAFETY ASSESSMENT

2.1 Introduction

In the maritime industry, over the recent years, quite a few serious accidents including the capsize of the Herald of Free Enterprise and the Exxon Valdez tragedy have shocked the public and attracted great attention to safety. The studies on how similar accidents may be prevented have been actively carried out at both the national and international levels. 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 (MCA) quickly responded and in 1993 proposed to the International Maritime Organization (IMO) that formal safety assessment (FSA) should be applied to ships to ensure a strategic control of safety and pollution prevention [MSA, 1993], [MSA, 1996]. The guidelines for the application of formal safety assessment have been recently approved for rule/regulation making purposes by the IMO. At the moment, one of the major concerns on the practical application of formal ship safety assessment is associated with the simplification of the approach and the study of trial test cases for producing more detailed guidelines to facilitate its application while human and organizational elements that significantly influence quality, safety, etc., also need to be addressed in detail accordingly. In the UK offshore industry, a safety case approach was introduced in 1993 following the public inquiry into the Piper Alpha accident of July 6, 1988. 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, 1998]. The main feature of the new offshore safety regulations in the UK is the absence of a prescriptive framework; defining specific duties of the operator as regard to what are adequate means. The regulations set higher safety standards 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 a complex engineering system such as a vessel or 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, 2002]. In general, the framework could be usefully applied to a wide range of

situations. 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. It can also be combined with other formal decision making aids such as Analytical Hierarchy Process (AHP).

As far as port safety is concerned, the guidelines indicating a general framework on port safety in the UK came from "Safety in Docks – Port regulations and guidance" [Health & Safety Commission, 1988]. The current status of port safety shows that there is a close relation between the MCA and the port authorities in order to ensure adequate levels of safety and pollution prevention in UK ports. It is again a case of leaving the operators to decide on the ways to deal with possible hazards instead of setting the path that they should follow in each case. What is needed is an application of formal safety assessment methods for handling situations arising in any kind of terminal with just minor modifications in the factors influencing them. This means that the methods applied in a chemical refinery dock when the vessel is undertaking loading or unloading of cargo, can be equally applied, with the domain knowledge, to a container or a Ro/Ro terminal. The "Port Marine Safety Code" recently produced by the DETR (Department of the Environment, Transport and the Regions, UK) introduces a national standard for every aspect of port marine safety in the UK [DETR, 2000]. Using it as a basis, further development and research can be targeted to engineering systems related to loading/unloading of cargo (such as cargo cranes) as well as in the logistics and transportation of goods within the port premises.

Many leading maritime organizations have started to move away from prescription, towards a risk based regime, to assist in maintaining capability throughout the life cycle of maritime products. Such a change will create new perspectives in risk modelling and safety based decision making. It is believed that a change from re-active to pro-active regime will gradually take place in the maritime industry [Sii & Wang, 2003]. This can certainly encourage safety engineers to develop and apply more flexible risk modelling and decision making approaches from the advances in general engineering and technology. Table 2.1 gives a brief overview of the current regulatory safety approach compared with the FSA proposed approach [Wang, 2002]. The differences are obvious as FSA focuses on pro-activeness whereas up until lately the lessons to be learned stood as the key players in the effort of improving marine safety.

Table 2.1 Difference between FSA and current regulatory safety approach

Formal Safety Assessment			Current Approach
Step 1	What might go wrong?	Hazard identification	What did go wrong?
Step 2	How often, how likely? How bad?	Risk analysis Frequencies, probabilities Consequences Risk = probability x consequence	
Step 3	How can matters be improved?	Risk control options identification	How can matters be improved?
Step 4	How much? How much better?	Cost benefit evaluation	
Step 5	What actions are worthwile to take?	Recommendation	What actions are worthwhile to take?

In the following paragraphs an overview of major marine accidents is given. Among others, these accidents triggered the need for a pro-active safety framework and hence helped in the proposal and implementation of FSA. Following the accidents' review, FSA's structure and methodology is described.

2.2 Review of major marine and offshore accidents

2.2.1 The Amoco Cadiz

The Amoco Cadiz was a supertanker, owned by Amoco, that split in two after running aground on Portsall Rocks, three miles off the coast of Brittany, in March 16, 1978, resulting in one of the largest oil spills in history [NOAA, 1978]. En route from the Persian Gulf to Le Havre, France, the ship encountered stormy weather with gale conditions and high seas. A seemingly minor failure in its steering gear started a slow drift to the French coastline.

The entire cargo of 1,619,048 barrels spilled into the sea. A slick 18 miles wide and 80 miles long covered about 200 miles (320 km) of Brittany coastline. Beaches of 76 different Breton communities were oiled. The isolated location of the grounding and the rough seas at that time hampered clean-up efforts for two weeks after the incident occurred. Severe weather resulted in the complete breaking of the ship before any oil could be pumped out of the wreck.

As mandated in the "Polmar Plan", the French Navy was responsible for all offshore operations while the Civil Safety Service was responsible for shore clean-up activities. Although the total quantity of collected oil and water reached 100,000 tons, less than 20,000 tons of oil were recovered from this liquid after treatment in refining plants. After long negotiations on financial terms between the ship's captain and the master of a West German tugboat and two unsuccessful towing attempts, the towline finally broke during the argument and the ship drifted on the rocks [Conan, d'Ozouville & Marchand, 1978]. This accident was caused as seen mainly due to bad weather as well as due to multiple failures occurring in close time intervals.

Following the Amoco Cadiz disaster, new requirements for tanker regulations were developed by IMO. The results of the inquiry into the Amoco Cadiz accident have contributed to the implementation of the 1978 Protocol (Tanker Safety and Pollution Prevention) to the International Convention for the Safety of Life at Sea, 1974 (SOLAS) [IMO, 2001]. All tankers of 10000grt and above shall have two remote steering gear control systems, each operable separately from the navigating bridge. The main steering gear of new tankers of 10000grt and above shall comprise two or more identical power units and shall be capable of operating the rudder with one or more power units.

2.2.2 The Exxon Valdez

On March 23, 1989, the oil tanker Exxon Valdez departed from the Valdez oil terminal in Valdez, Alaska (on its 28th voyage), heading south through Prince William Sound, with a full load (52 million gallons) of oil. Captain Joseph Hazelwood radioed to the Coast Guard station that he would be changing course in order to avoid some growlers, small icebergs which had drifted into the sound from the Columbia Glacier [Galt, Lehr, & Payton, 1991]. The captain received permission to move into the northbound lane. Before retiring to his cabin, Captain Hazelwood instructed his third mate Gregory Cousins to "start coming back into the lanes" once the ship was abeam Busby Island Light, some 2 minutes ahead.

Although Cousins did give the instructions to the helmsman to steer the vessel to the right, the vessel was not turning sharply enough and at 12:04 a.m. on March 24, the

vessel hit Bligh Reef. It is not known whether Cousins gave the orders too late or the helmsman did not follow instructions properly.

The spilled oil affected 1,900 km of Alaskan coastline. Although Exxon's initial report of 10.8 million gallons (40,900 m^3) of oil spilled has been widely accepted, other sources estimate the spill at 35 million gallons (110,000 m^3) [Rice, Spies, Wolfe & Wright, 1996]. The Exxon Valdez supertanker was towed to San Diego, arriving on July 10 and repairs began in July 30, 1989. Approximately 1,600 tons of steel were removed and replaced. This accident was a typical example of human error and negligence.

2.2.3 The Piper Alpha

On 6 July 1988 there was a massive leakage of gas condensate which was ignited causing an explosion which led to large oil fires. The heat ruptured the riser of a gas pipeline from another installation [UKOOA, 2005]. This produced a further massive explosion and fireball that engulfed Piper Alpha. All this took just 22 minutes. The scale of the disaster was enormous. 167 people died, 62 people survived.

It is believed that the leak came from piping connected to a condensate pump. A safety valve had been removed from this piping for overhaul and maintenance. The pump itself was undergoing maintenance work. When the piping from which the safety valve had been removed was pressurised at start-up, it is believed the leak had occurred.

Lord Cullen chaired the official Public Inquiry into the disaster in two parts led by the Department of Energy (DOE) [DOE, 1990]. The first was to establish the causes of the disaster. The second part made recommendations as to the future safety regime. By 1993 all had been acted upon and substantially implemented. It is believed that this accident was the result of combined procedural defects and human error.

At the same time the HSE developed and implemented Lord Cullen's key recommendation, the making of regulations to require that the Operator/Owner of every installation should be required to submit to HSE, for their acceptance, a Safety case which demonstrated that the Company had adequate safety management systems,

had identified risks and reduced them to as low as reasonably practicable (ALARP), had put management controls in place, had provided for temporary safe refuge to be available and had made provisions for safe evacuation and rescue [DOE, 1990]. The Temporary Refuge is designed to provide a period of protection, allowing personnel to muster in safety while an accident is being assessed, and a decision is taken on whether or not to abandon the installation. The Temporary Refuge is equipped, amongst other things, with command, communication, monitoring, mustering and medical facilities. By November 1993 a safety case for every installation had been submitted to the HSE and by November 1995 all had had their Safety case accepted by the HSE.

The marine and offshore industry's accident frequency rates have improved significantly since 1988. There has been an overall reduction in accident frequency rates in the order of 50% [HSE, 2003]. Whilst the actual accident rates do not prove or disprove a safety regime or culture, they do provide a year on year or over a period of years, comparison to indicate an improving or worsening or level trend, provided that the statistics are compiled on the basis of a consistent methodology.

The marine and offshore industry agreed in 1992 to report to HSE on a voluntary basis, all offshore releases of hydrocarbons. From 1992 to 1994/95 the number of reported releases rose to a peak of [HSE, 2001]:

- 36 major releases.
- 170 significant releases.
- 111 minor releases.

From 1994/95 to 1997/98 the number of releases have declined to:

- 22 major releases (39% reduction).
- 102 significant releases (43% reduction).
- 50 minor releases (55% reduction).

This reduction can be illustrated in Figure 2.1.

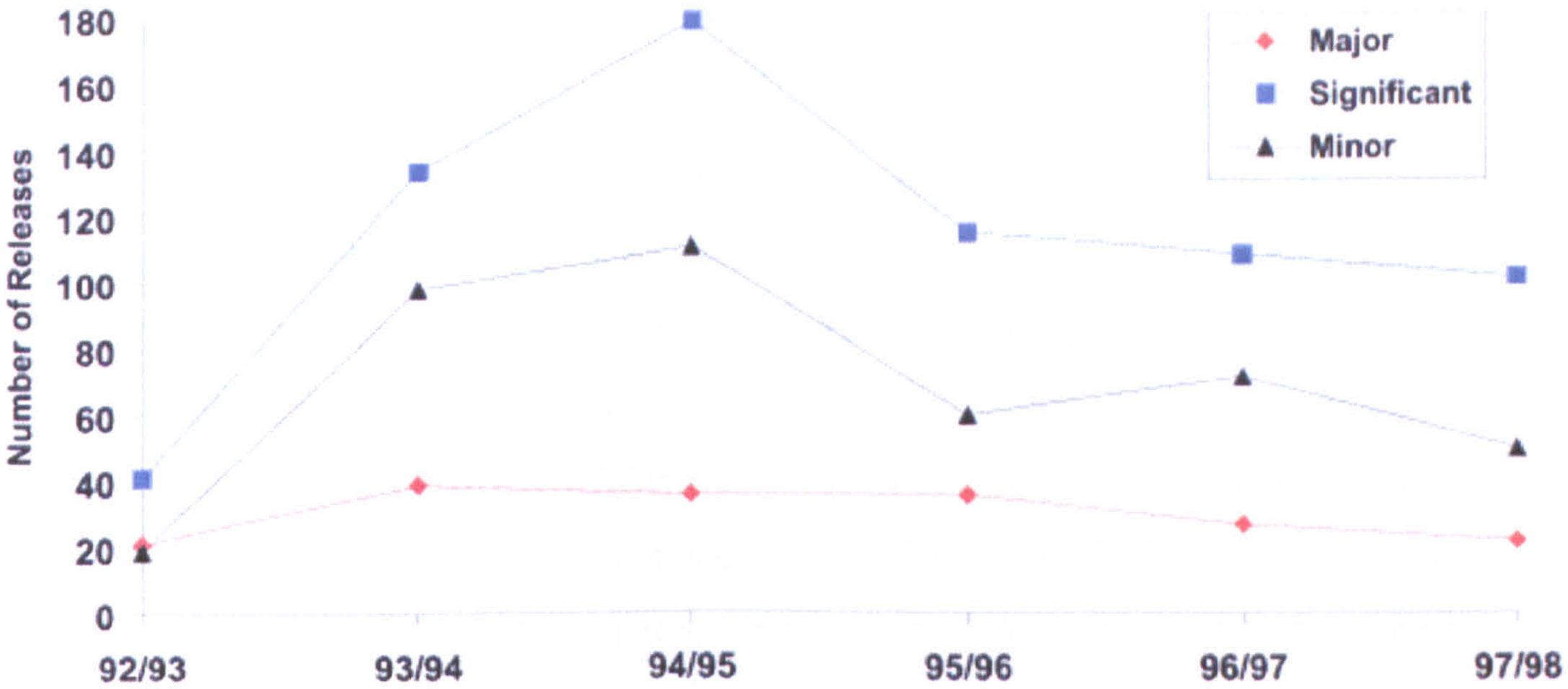


Figure 2.1 Reduction in the recorded release rates from 1992-1998

Similarly Figure 2.2 illustrates the descending number of fatalities and serious injuries which show that the industry has started to follow the road towards a safety oriented regime [HSE, 2001].

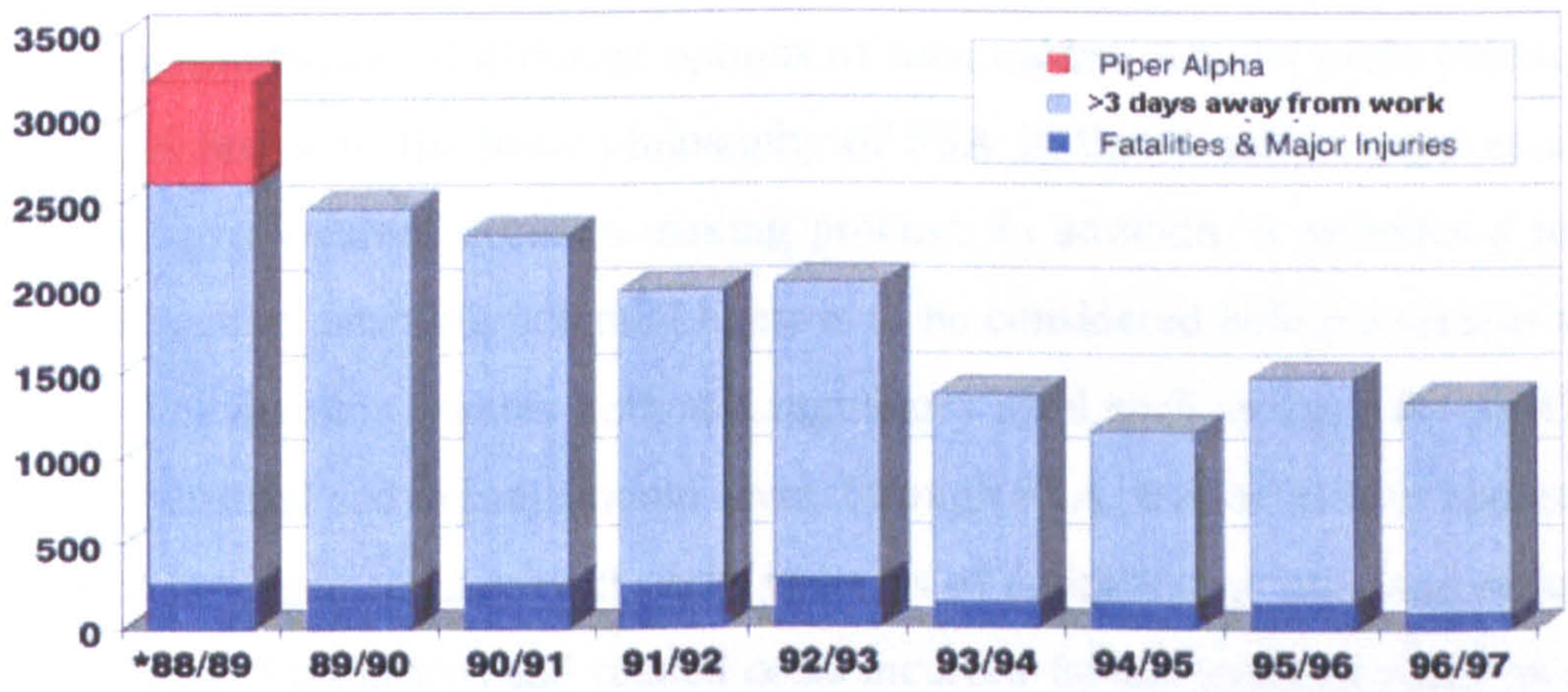


Figure 2.2 Reduction in fatalities and major accidents from 1988-1997

It is clear that it would be possible to prevent marine accident by proper design, correct operational training and procedures as well as an appropriate management system that performs regular reviews on the safety standards functioning. As the public concern regarding maritime safety increases, a lot of attention has been drawn to formal safety assessment as regulatory tool. It is believed that the adoption of such a tool both in the design and operation stages will reduce maritime risks to the ALARP level. Above this particular level systems and processes continue to operate without safety issues raised. The following paragraphs give an insight on the mechanism of operation of formal safety assessment.

2.3 Formal safety assessment

FSA is a rational and systematic process for assessing the risks relating to maritime safety and the protection of the marine environment and for evaluating the costs and benefits of the recommended risk control options for reducing these risks. The use of FSA is consistent with, and should provide support to, the IMO decision-making process. It provides a basis for making decisions in accordance with IMO resolutions A.500(XII) "Objectives of the Organization in the 1980s", A.777(18) "Work Methods and Organization of Work in Committees and their Subsidiary Bodies" and A.900(21) "Objectives of the Organization in the 2000s" [MSA, 1993].

Application of FSA may be particularly relevant for proposals for regulatory measures which have far reaching implications in terms of costs to the maritime industry or the administrative or legislative burdens which may result in. This is achieved by providing a clear justification for proposed regulatory measures and allowing comparison of different options of such measures to be made [MSA, 1996]. This is in line with the basic philosophy of FSA in that it can be used as a tool to facilitate a transparent decision-making process. In addition, it provides a means of being proactive, enabling potential hazards to be considered before a serious accident occurs. The decision makers both at a regulatory level such as the IMO [IMO, 1996] or at a industrial and organizational level, through FSA, will be able to appreciate the effect of proposed regulatory changes in terms of benefits (e.g. expected reduction of lives lost or of pollution) and related costs incurred for the industry either as a whole or just for the particular case examined and affected by the decisions they need to take.

2.3.1 FSA steps

FSA should consist of the following steps [IMO, 1997a]:

1. Identification of hazards.
2. Risk analysis.
3. Risk control options.
4. Cost-benefit assessment.
5. Recommendations for decision-making.

Figure 2.3 is a flow chart of the FSA methodology. The process begins with the decision makers defining the problem to be assessed along with any relevant boundary conditions or constraints. These are presented to the group who will carry out the FSA and provide results to the decision makers for use in their resolutions [IMO, 2002]. In cases where decision makers require additional work to be conducted, they would revise the problem statement or boundary conditions or constraints, and resubmit this to the group and repeat the process as necessary. Within the FSA methodology, step 5 interacts with each of the other steps in arriving at decision-making recommendations.

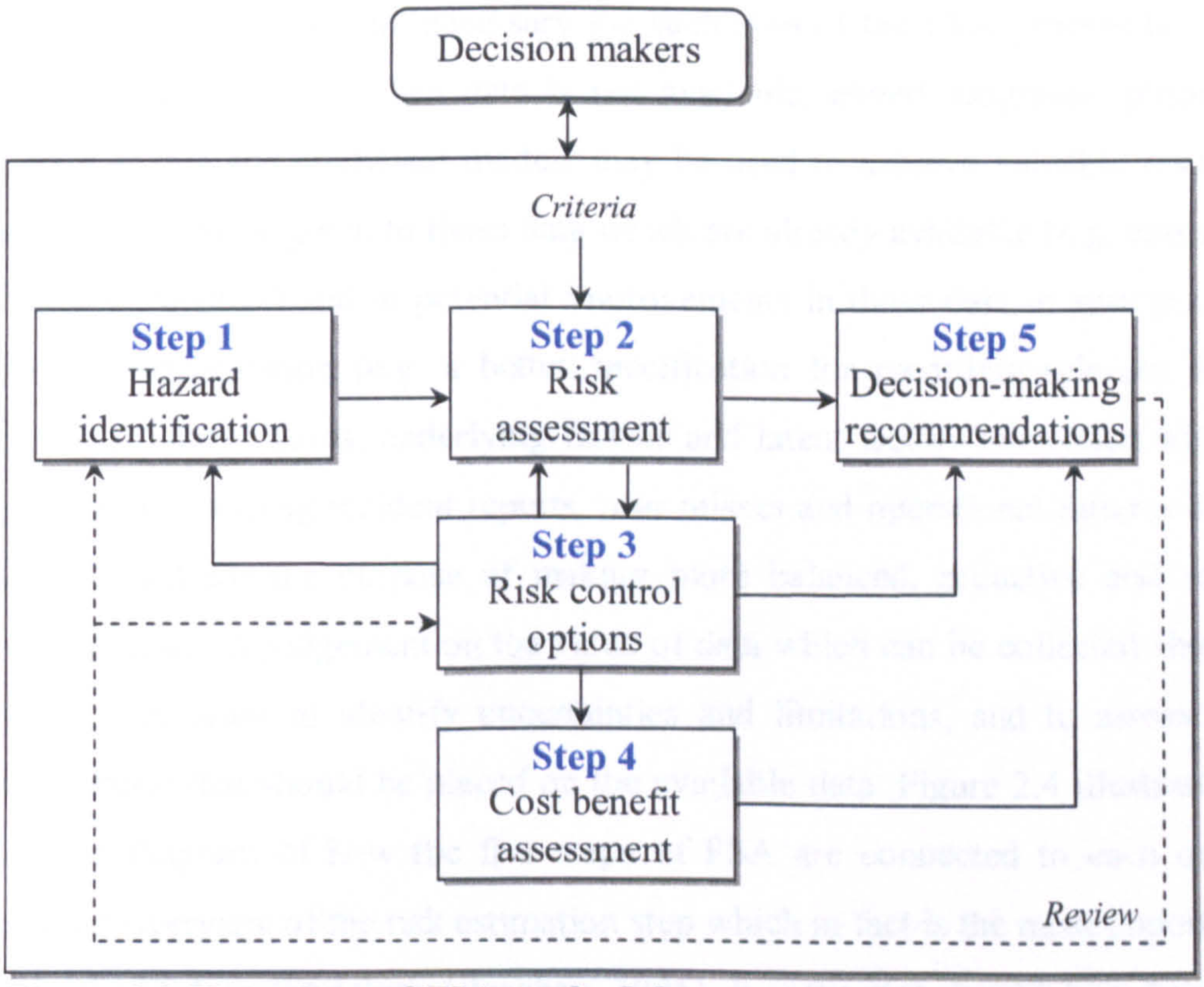


Figure 2.3 Flow chart of FSA methodology

The group carrying out the FSA process should consist of qualified and experienced people to reflect the range of influences and the nature of the "event" being addressed. The depth or extent of application of the methodology should be in-line with the nature and significance of the problem [IMO, 2004]. However, before starting the detailed application, a coarse application is suggested for the relevant ship type or hazard category, in order to include all aspects of the problem under consideration. Whenever there are uncertainties, e.g. in respect of data or expert judgment, the significance of these uncertainties should be assessed. Characterization of hazards and

risks should be both qualitative and quantitative, and both descriptive and mathematical, consistent with the available data, and should be broad enough to include a comprehensive range of options to reduce risks. A hierarchical screening approach may be utilized. This would ensure that excessive analysis is not performed by utilising relatively simple tools to perform initial analyses, the results of which can be used to either support decision-making (if the degree of support is adequate) or to scope/frame more detailed analyses (if not). The initial analyses would therefore be primarily qualitative in nature, with a recognition that increasing degrees of detail and quantification will come in subsequent analyses as necessary. A review of historical data may also be useful as a preparation for a detailed study.

The availability of suitable data necessary for each step of the FSA process is very important [Peachey, 1995]. When data is not available, expert judgment, physical models, simulations and analytical models may be used to achieve valuable results. Consideration should be given to those data which are already available (e.g. casualty and deficiency statistics) and to potential improvements in those data in anticipation of an FSA implementation (e.g. a better specification for recording relevant data including the primary causes, underlying factors and latent factors associated with a casualty). Data concerning incident reports, near misses and operational failures may be very important for the purpose of making more balanced, proactive and cost-effective legislation. A judgement on the value of data which can be collected should be carried out in order to identify uncertainties and limitations, and to assess the degree of reliance that should be placed on the available data. Figure 2.4 illustrates a more detailed diagram of how the five steps of FSA are connected to each other giving a better overview of the risk estimation step which in fact is the most important step within the FSA methodology [Peachey, 1995]. It is the step in which traditional and advanced risk estimation techniques are applied. What can be measured can be reduced.

Figure 2.4 Flow chart of FSA methodology concentrated on risk estimation

The human element is one of the most important contributory aspects to the causation and avoidance of accidents. Human element issues throughout an integrated system should be systematically treated within the FSA framework, associating them directly with the occurrence of accidents, underlying causes or influences. Additionally, appropriate techniques for incorporating human factors, such as the TESEO technique should be used. This technique uses a marking system based on different human related criteria and produces the outcome in terms of multiplication of all the respective factors. Thus can produce quantitative results in a case where qualitative variables are used.

2.3.1.1 FSA step 1 – Identification of hazards

The purpose of step 1 is to identify a list of hazards and associated scenarios prioritized by risk level specific to the problem under review. This purpose is achieved by the use of standard techniques to identify hazards which can contribute to accidents, and by screening these hazards using a combination of available data and judgement [Riding, 1997]. The hazard identification process should be undertaken in the context of the functions and systems generic to the ship type or problem being considered.

The approach used for hazard identification generally comprises a combination of both creative and analytical techniques, the aim being to identify all relevant hazards. The creative element is to ensure that the process is proactive and not confined only to hazards that have materialized in the past. It typically consists of structured group reviews aiming at identifying the causes and effects of accidents and relevant hazards [CCPS, 1992]. Consideration of functional failure may assist in this process. The group carrying out such structured reviews should include experts in the various appropriate aspects, such as ship design, operations and management and specialists to assist in the hazard identification process and incorporation of the human element. A structured group review session may last over a number of days. The analytical element ensures that previous experience is properly taken into account, and typically makes use of background information (for example applicable regulations and codes, available statistical data on accident categories and lists of hazards to personnel, hazardous substances, ignition sources, etc.). Examples of hazards relevant to shipboard operations are shown at Appendix I. A complete analysis of possible causes and outcomes of each accident category should be carried out by using established techniques (typical techniques are reviewed in Chapter 3), to be chosen according to the problem in question.

The identified hazards and their associated scenarios relevant to the problem under consideration should be ranked to prioritize them and to discard scenarios judged to be of minor significance. The frequency and consequence of the scenario outcome requires assessment. Ranking is undertaken using available data, supported by judgement, on the scenarios. The qualitative method named risk matrix is described in Chapter 3. The frequency and consequence categories used in the risk matrix have to be clearly defined. The product given by the likelihood of occurrence of an undesired event (frequency) and the severity of consequences imposed represents the derived risk level.

Therefore the output from step 1 consists of:

1. A list of hazards and their associated scenarios prioritized by risk level.
2. A description of causes and effects.

2.3.1.2 FSA step 2 - Risk analysis

The purpose of the risk analysis in step 2 is a detailed investigation of the causes and consequences of the more important scenarios identified in step 1. This can be achieved by the use of suitable techniques that model the risk. This allows attention to be focused upon high risk areas and to identify and evaluate the factors which influence the level of risk. Different types of risk [Henley & Kumamoto, 1992] (i.e. risks to people, the environment [EPA, 1996] or property) should be addressed as appropriate to the problem under consideration.

The construction and quantification of fault trees and event trees are standard risk assessment techniques that can be used to build a risk model (see Chapter 3). An example of a conceptual risk model is the Risk Contribution Tree (RCT) as shown in Figure 2.5 [IMO, 2002a]. Whilst the example makes use of fault and event tree techniques, other established methods could be used if appropriate. Quantification makes use of accident and failure data and other sources of information as appropriate to the level of analysis. Where data is unavailable, calculation, simulation or the use of recognized techniques for expert judgement may be used.

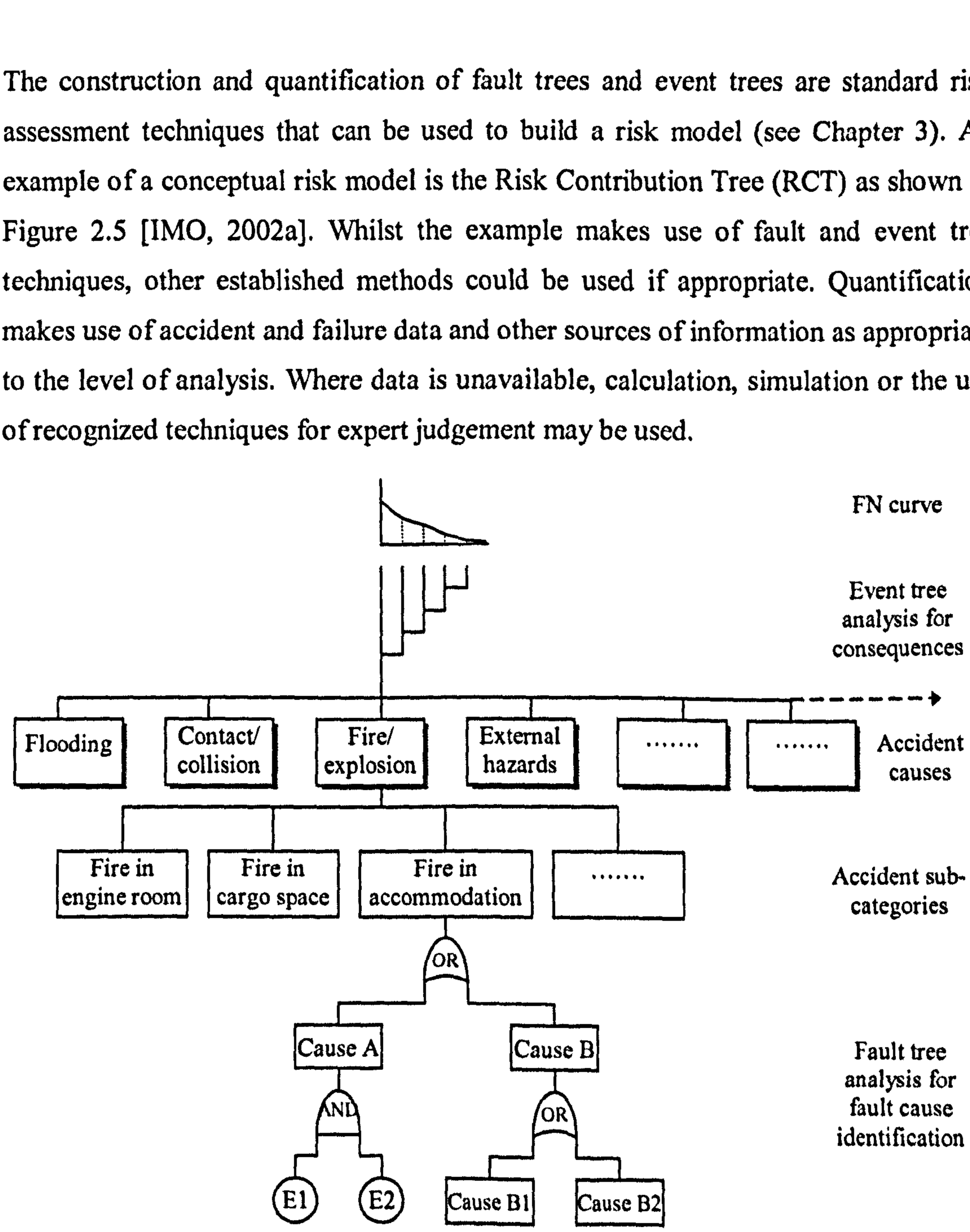


Figure 2.5 Example of a risk contribution tree

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

2.3.1.3 FSA step 3 – Risk control options

The purpose of step 3 is to propose effective and practical risk control options (RCOs) consisting of the following four principal stages [Bråfelt.& Larsson 2000]:

1. Focusing on risk areas needing control.
2. Identifying potential risk control measures (RCMs).
3. Evaluating the effectiveness of the RCMs in reducing risk by re-evaluating step 2.
4. Grouping RCMs into practical regulatory options.

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

The purpose of focusing significant risks is to screen the output of step 2 so that the effort is focused on the areas most needing risk control. The main aspects to making this assessment are to review [Wang, Labrie & Ruxton, 1993]:

1. Risk levels, by considering frequency of occurrence together with the severity of outcomes. Accidents with an unacceptable risk level become the primary focus.
2. Probability, by identifying the risk areas that have the highest probability of occurrence. These should be addressed irrespective of the severity of the outcome.
3. Severity, by identifying the risk areas that contribute to highest severity outcomes. These are be addressed irrespective of their probability.
4. Confidence, by identifying areas where the risk model has considerable uncertainty either in risk, severity or probability. These uncertain areas should be addressed.

Structured review techniques are typically used to identify new RCMs for risks that are not sufficiently controlled by existing measures. These techniques may encourage

the development of appropriate measures and include risk attributes and causal chains. Risk attributes relate to how a measure might control a risk, and how causal chains relate to where, in the "initiating event to fatality" sequence, risk control can be introduced. RCMs (and subsequently RCOs) have a range of attributes. The prime purpose of assigning attributes is to facilitate a structured thought process to understand how an RCM works, how it is applied and how it would operate. Attributes can also be considered to provide guidance on the different types of risk control that could be applied. Many risks will be the result of complex chains of events and a diversity of causes. For such risks the identification of RCMs can be assisted by developing causal chains which might be expressed as follows [IMO, 2002]:

causal factors → failure → circumstances → accident → consequences

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

1. Reducing the frequency of failures through better design, procedures, organizational policies, training, etc.
2. Mitigating the effect of failures, in order to prevent accidents.
3. Examine the circumstances in which failures may occur.
4. Mitigating the consequences of accidents.

RCMs are to be evaluated regarding their risk reduction effectiveness by using step 2 including consideration of any potential side effects of the introduction of the RCM. The purpose of this stage is to group RCMs into a limited number of well thought out practical regulatory options. There is a range of possible approaches to grouping individual measures into options. The following two approaches, related to likelihood and escalation, can be considered:

1. Generic approach which provides risk control by controlling the likelihood of initiation of accidents and may be effective in preventing several different accident sequences.
2 Distributed approach which provides control of escalation of accidents, together with the possibility of influencing the later stages of escalation of other, perhaps unrelated, accidents. In generating the RCOs, the interested entities (also named as

stakeholders), which may be affected by the combinations of measures proposed, should be identified.

The output from step 3 consists of:

1. A range of RCOs which are assessed for their effectiveness in reducing risk.
2. A list of interested entities affected by the identified RCOs.

2.3.1.4 FSA step 4 - Cost benefit assessment

The purpose of step 4 is to identify and compare benefits and costs associated with the implementation of each RCO identified and defined in step 3. A cost benefit assessment may consist of the following stages [Mathiesen, 1997]:

1. Consider the risks assessed in step 2, in terms of both frequency and consequence, in order to define the base case in terms of risk levels of the situation under consideration.
2. Arrange the RCOs, defined in step 3, in a way to facilitate understanding of the costs and benefits resulting from the adoption of an RCO.
3. Estimate the pertinent costs and benefits for all RCOs.
4. Estimate and compare the cost effectiveness of each option, in terms of the cost per unit risk reduction by dividing the net cost by the risk reduction achieved as a result of implementing the option.
5. Rank the RCOs from a cost-benefit perspective in order to facilitate the decision-making recommendations in step 5 (e.g. to screen those which are not cost effective or impractical).

Costs are be expressed in terms of life cycle costs and may include initial, operating, training, inspection, certification, decommission costs, etc. Benefits may include reductions in fatalities, injuries, casualties, environmental damage and clean-up, indemnity of third party liabilities, etc. and an increase in the average life of ships [Wang, Yang & Sen, 1995]. The evaluation of the above costs and benefits can be carried out by using various methods and techniques. Such a process should be conducted for the overall situation and then for those interested entities which are most influenced by the problem in question. In general, an interested entity can be

defined as the person, organization, company, Coastal State, Flag State, etc. who are directly or indirectly affected by an accident or by the cost effectiveness of the newly proposed RCO. Different interested entities with similar interests can be grouped together for the purpose of applying the FSA methodology and identifying decision-making recommendations.

The output from step 4 consists of:

1. Costs and benefits for each RCO identified in step 3 from an overview perspective.
2. Costs and benefits for those interested entities which are the most influenced by the problem in question.
3. Cost effectiveness expressed in terms of suitable indices.

2.3.1.5 FSA step 5 – Recommendations for decision making

The purpose of step 5 is to define recommendations which should be presented to the relevant decision makers in an auditable and traceable manner. The recommendations would be based upon the comparison and ranking of all hazards and their underlying causes; the comparison and ranking of risk control options as a function of associated costs and benefits [Yang & Singh, 1994] should follow the identification of those risk control options which maintain risk levels below the ALARP level.

Recommendations are to be presented in a form that can be understood by all parties irrespective of their experience in the application of risk and cost benefit assessment and related techniques [Delgado, Herrera, & Martinez, 1998]. Those submitting the results of an FSA process must provide timely and open access to relevant supporting documents and a reasonable opportunity for, and a mechanism to, incorporate comments.

The output from step 5 consists of:

1 An objective comparison of alternative options, based on the potential reduction of risks and cost effectiveness, in areas where legislation or rules should be reviewed or developed.
2. Feedback information to review the results generated in the previous steps.

2.4 Current status of FSA

The FSA methodology has been developed by a joint Working Group of the IMO's Maritime Safety and Environmental Protection Committees, based upon research undertaken in the UK [IMO, 1996], [IMO, 1997]. The two committees approved guidelines setting out the details of the method during 1997. Although many of the elements of the approach described above are well established in other contexts, their application to the shipping industry, and in an overview or generic way, is relatively new and unproven. Trial applications are presently being undertaken, with the intention of reporting the results and experience gained to the IMO [IMO, 1998].

Consideration is also being given, by a Correspondence Group of IMO members, to the development of suitable mechanisms and procedures by which the FSA process can be applied by the IMO committees in their future decision making. FSA is intended to be applied at an overview level (for example to all the hazards affecting a particular ship type), with a view to identifying and prioritising the principal risks and regulatory options. FSA results will part a summary of the key risks relevant to the scope of the study, and information regarding the relative costs and benefits of the regulatory options for addressing those risks. The conclusions of an FSA study should therefore facilitate a proactive approach by the IMO, by providing a justifiable basis for making decisions about the need for, and content of, maritime regulations [IMO, 1997]. It is not however the purpose of FSA to take account of the details of specific ships, or their arrangements, operations, etc, nor is the process designed to address the risks facing a particular owner or ship. As with all risk assessments, the results obtained are dependent in part upon data (eg historical incident and accident information), and also upon judgement in interpreting that data and anticipating industry trends, the impact of changes in technology, the potential for future accidents, etc. The results of an FSA study are therefore dependent upon not only the availability of relevant data, but also suitably qualified and experienced people to undertake such judgements [IMO, 1999].

The safety case approach was introduced to the UK offshore industry by the UK Health & Safety Executive (HSE) [HSE, 1998]. For offshore activities a Safety case has to be produced for submission to the HSE. This safety case regime is primarily a UK offshore approach.

The primary objective of a safety case approach is to ensure an adequate level of safety for a particular ship, based upon the management and control of the risks associated with that ship [Stansfeld, 1994]. A central feature of a safety case is that the ship-owner takes responsibility for assessing the risks associated with his ship, and for documenting how his safety management system limits those risks to an acceptable level. The document containing details of the risk assessment and the safety management system is called a safety case. The safety case approach constitutes a demonstration, to the vessel's owner, and to his employees, customers and society at large, that risks arising from the operation of the ship are adequately understood and controlled. In some industries, for example the UK offshore oil & gas industry, the safety case regime is mandatory, i.e. operations cannot legally be commenced until a safety case approach has been compiled by the owner and submitted to the official regulator for scrutiny and approval [HSE, 2002]. However, it is beginning to be recognised by responsible owners in the shipping industry that a safety case approach can be adopted voluntarily. Thus, in addition to complying with existing prescriptive regulatory requirements, an owner may choose voluntarily to compile a safety case and introduce a safety management system, for example to protect his business interests or reputation, or where he wants to achieve a higher level of safety than is implied by the regulations. It should be noted that although described above in the context of a vessel's owner, a safety case approach can, where appropriate, be compiled and maintained by a vessel's operator [HSC, 2004].

A safety case approach will include a comprehensive description of the ship itself, and of its operation and the environment within which it operates. The risk assessment will be undertaken using a number of established techniques, such as FMEA [IMCA, 2002] (Failure Mode and Effects Analysis) and HAZOP [Kletz, 1974] (Hazard and Operability study) studies for hazard identification, and fault and event tree analyses [Villemeur, 1992] for the determination of risk. Risks will be quantified to the extent it is appropriate to do so. Risk criteria will be set, relevant to the vessel and its operational context, and usually in accordance with the ALARP principle [Kumamoto, & Henley, 1979]. Likewise, the safety management system will be developed from established good management principles, and will be an integral part of the company's overall management strategy. The safety management system will include elements firstly of setting policy, secondly of organising, planning and

implementing actions to fulfil that policy, and finally of monitoring review and feedback to assess performance against the policy [MOD, 1996]. Typically, for a complex engineering system, a design safety case approach would initially be compiled. This would subsequently be developed and expanded into an operational safety case as the vessel enters service. Thereafter, the safety case approach would normally be subject to regular review, with updating as necessary, to take account of changing conditions, ownership, activities, modifications, etc. A safety case approach will usually make reference to extensive back-up information recording details of the ship and its operation, the risk assessments, risk criteria, etc. It is essential that the safety case approach is developed with the involvement of staff who have close familiarity with the system, its operation, company practice, procedures, etc. This approach also ensures ownership of, and commitment to, the safety targets and philosophy contained within the safety case. However, in compiling a safety case, an owner will often need to seek specialist assistance, particularly in respect of the quantified assessment of risks.

The effectiveness of the safety management system is usually monitored and verified by means of regular audits, and compliance with the requirements of the safety case checked by means of inspections.

The safety case approach is well established in industries other than shipping, most notably in the offshore oil and gas sector. However, the approach can, in principle, be applied to ships, and in recent years there has been discussion of this possibility. There are at present no known requirements by maritime regulators to impose a safety case regime on ship owners. All known current examples of the application of the safety case approach for ships fall into the voluntary category, in that the organisations involved have decided to develop safety cases without being required to do so by any regulatory authority. Most notably, the UK Ministry of Defence introduced a safety case regime for each of its new ships with effect from 1996 [HSE, 1998]. In the merchant shipping sector, a few companies are known to have adopted the safety case approach. One of them is BP Tankers which, has adopted the safety case in view of their newly-built crude oil tankers for the Alaskan oil trade [BP, 2004].

The safety case approach is intended to be applied primarily to a large engineering system like a ship [Wang & Ruxton, 1998]. It provides a comprehensive and detailed

evaluation of all the risks to which that ship is exposed, together with an explicit statement of the safety management system that the owner has established for controlling and reducing those risks to an acceptable level. The safety case approach document therefore provides the reference source, not only for checking the completeness and validity of the owner's risk assessment, but also as the basis for auditing the owner's management system and operations, and for inspecting the vessel, with the object of verifying compliance with the provisions of the case. The principal limitation of a safety case regime is that it presumes a high degree of responsibility on the part of the vessel's owner to be accountable for the risks created by his vessel and its operation. Therefore, exclusive reliance upon a safety case regime as a mechanism for ship safety regulation would only be practical within a framework where the regulator has both the competence to assess the veracity of the safety case, and also the authority to exercise effective sanctions in the event of being dissatisfied with the case itself or the owner's compliance with its provisions. A further limitation on the widespread introduction of the safety case approach for shipping is the burden of work required to undertake the complex analyses and compile extensive documentation for each and every vessel.

Public safety awareness and the related distribution of responsibilities to local authorities has increased the need for tools to evaluate the total safety in the port environment. The maritime (nautical) operations determine an essential part of this safety. Traditionally expert opinion more recently completed with simulation studies, or fast-time simulations, help to evaluate the different design or existing port lay-outs and operational measures within a given environment and a given traffic distribution. This is still a viable option for the basic assessment of the feasibility of a design on the operational level but fails to predict the total levels of risk and consequences of measures once the total traffic distribution needs to be evaluated [HSE, 1988]. Over the last two decades additional quantitative safety management assessment tools have been developed which take into account the total vessel traffic image and its related risks in the whole physical port environment and which are capable of evaluating the consequences of measures on a strategic level. More recent developments in the Netherlands and the UK (Port Marine Safety Code) [DETR, 2000] suggest the application of FSA to ports as a panacea to all strategic safety issues, a promise which eventually can come true if due consideration is given to the small details. Which type

of study will be performed depends on the main question that has to be answered. A rough subdivision of safety studies is presented in Table 2.2.

		Safety Studies		
Study Parameters	**Generic Vessel**	Daily operations	Human failure	Technical failure
	Port	Traffic		Lay-out
	Environment	Wind	Current	Waves
	Organisation	On shore		On ship
	Policy level	Classification level		

Table 2.2 Application of FSA in various safety studies

The application of FSA methodology in port safety assessment is increasing and appropriately recognised as a valuable tool to identify the risk determining factors and to put these factors within the right framework of the total port system. However, the quantification of the actual risk level and the consequences of measures still require considerable input from analysed accident databases and more detailed models. The usage of FSA will result in improved risk assessment models, based on more physical relationships in which the impact of regulatory aspects is modelled. Because the outcome of the risk assessment model is directly used in the decision process as to whether a RCO is effective or not, it is very important to improve this model where possible.

The European Maritime Pilot's Association (EMPA) has suggested that operational procedures and working instructions should be entirely based on and be in line with FSA [EMPA, 2006]. The management of the Pilot Organisations should benefit from a better understanding of the technical risks being taken by the Pilot Organisation by using the Formal Risk and Formal Safety Assessment methodology. The FSA methodology will define a logical and systematically structured approach, for decision-making based on qualitative and quantitative Risk and Safety Assessment. Using the FSA methodology should enable the Pilot organisation to define in advance the problems needing to be addressed, together with any relevant deadline condition or constrains. For the trial ports (Rotterdam, River Elbe and Antwerp) EMPA submitted a detailed trial application to demonstrate the practicability and usefulness

of FSA for operational pilotage. FSA is based on reliable incidents containing hazardous and damage occurrence data.

The trial application methodology covered [EMPA, 2006]:

- Prioritising areas and/or parts of harbours and fairways.
- Classifying ship and cargo types.
- Identifying hazards by defining failure modes e.g. grounding, drifting, fire, explosions.
- Defining the causes of failures e.g. engine failure, steering failure, on-board navigational equipment failure, human failure.
- Geographic area or region including meteorological, hydrological and hydrographic data.
- Assessing risks, including the frequency of occurrence (likelihood) and the consequence or impact.
- Defining risk control options.
- Cost/Benefit Assessment (CBA) or alternative risk management options to reduce likelihood and impact.

Another case that FSA is being utilised is through a project developed by Det Norske Veritas (DNV). One of the work packages is aimed at developing risk or probabilistic models of particular relevance to ship design. The subprojects relate to fast and accurate flooding prediction in case of damage, probabilistic assessment of structural strength (Structural Reliability Analysis models), probabilistic intact stability, prediction of collision and grounding, and fire and explosion. This work links to and extends ongoing trends in design and regulatory development. For example, DNV has recently completed the HARDER project, which provided the basis for the new Probabilistic Damage Stability Regulations at IMO; the next step is to include the time aspect (flooding prediction), and intact stability [DNV, 2006]. Gradually, tools will be introduced that can be used directly in design and explicitly minimise risks. This work package will address regulatory aspects, involving such issues as risk evaluation criteria, approval process of risk-based designs, requirements on documentation and qualification of personnel when it comes to assessing the reliability of engineering systems. As a basis for the risk aspects, FSA studies are being carried out for cruise vessels, LPG carriers and container ships.

Looking back a few years in 2001, International Association of Classification Societies (IACS) submitted a proposal to the Maritime Safety Committee (MCA) concerning the fore-end watertight integrity of bulk-carriers [IMO, 2001a]. The whole study was supported by minor statistical data which gave analysts problems in terms of decision making recommendations as far as the integrity of the vessels' structure is concerned. Low percentage of data existed specially in terms of double skinned bulk-carriers. Even though the different bulk-carrier sizes were separated in different categories there was lack of data for the smaller handy-size carriers and even less as far as the newest larger vessels were concerned. Even though the study produced certain recommendations as far as the strengthening of forward structure is concerned, it lacked the interdependence analysis between the different sizes of vessels, so that it could be able to recommend a common utility plane of solutions.

The above studies were developed at the fundamental levels of risk assessment. There is much concern though as it can be clearly seen, in terms of handling data being vague or uncertain. Interdependence of components is another issue which traditional techniques cannot handle efficiently in order to produce rational results and recommendations. The methods chosen to conduct risk estimation have gaps that require advanced models producing rational solutions in terms of engineering reliability and safety.

2.5 Statistical data treatment

Every risk or uncertainty modelling has to be supplied with reliable failure and repair data input, which will enable the quantification process to be achieved. A vast amount of reliable maritime database is available to serve this purpose. When no data for a component failure mode can be obtained, it may be possible to express the failure in terms of fundamental and quantifiable parameters and to analyse it using limit state reliability analysis, although there is uncertainty about the relevant distributions [Sii & Wang, 2003].

Casualty includes any accidental grounding, or any occurrence involving a vessel which results in damage related to the vessel, its apparel, gear, cargo, or injury or loss of life of any person; and includes among other things, collisions, strandings, groundings, founderings, heavy weather damage, fires, explosions, failure of gear and

equipment and any other damage which might affect or impair the seaworthiness of the vessel [IMO, 2002]. The obtained data is usually treated from its raw form depending on its intended use within the analysis structure. In some cases, such as with accident or initiating events, available data may be need to be treated and supplied in terms of frequency per ship/installation operating year. The best way to assign a frequency to an event is to research industry databases and locate good historical frequency data that relates to the event being analysed. Before applying historical frequency data, a thoughtful analysis of the data should be performed to determine its applicability to the event being evaluated [Mishra, 1992]. The analyst needs to consider the source of the data, the statistical quality of the data (reporting accuracy, size of data set, etc.) and the relevance of the data to the event being analysed. Also, the data may best be utilised for safety assessment by converting a failure or a repair rate into a corresponding probability value.

2.5.1 Failure databases

The following are some of the available sources that may be useful for obtaining failure and repair data to carry out quantitative safety analysis.

- FARADIP.THREE [Smith, 1992]: This database is a summary of many useful databases and shows, for each component, the range of failure values. The failure data of various components such as alarms, mechanical items and instruments is included in this database.
- US Military Handbook 217: This data source is produced by the Rome Air Development Center under contract to the US Department of Defence and is an electronic failure data bank.
- OREDA-Offshore Reliability Data [DNV, 2002]: It is a collection of offshore failure rate and failure mode data with an emphasis on safety-related equipment. It covers a great range of components and equipment.
- Reliability Technology [Green, & Bourne, 1972]: This book contains failure rate data obtained mostly from US and UK atomic energy sources.
- Lloyds Data Bank [LR, 1982]: It mainly covers the failure data in the shipping industries.

- Others: The reliability data of the various electronic and non-electronic components may also be obtained from various published papers and books [Smith, 1985].

It is also useful to record and utilise data from near misses and errors. Furthermore, in an effort to ensure that safety assessment carried out in an as efficient as possible way, novel techniques should integrate expert judgement with the obtained data in a formal manner as it will be demonstrated in the following chapters of the thesis.

2.6 Concluding remarks

The adoption of FSA by the IMO, together with other recommendations, has introduced a new dimension to the way that safety is considered within the shipping community, and it is rapidly gaining international acceptance as a solution, enabling the application of risk based techniques to international shipping. As progress continues, it will represent a fundamental cultural change from the present reactive approach to one that is proactive and soundly based on an evaluation of risk. Although at an early stage and despite considerable confusion in some quarters, FSA offers the challenge of working in an industry that will make greater use of risk-based approaches. FSA differs from the safety case approach recommended in that it aims to support the rule making process at a generic level and to provide a logical methodology to establish rules, which may well be predominantly prescriptive. The approach will encourage inter-disciplinary approaches to safety and should produce more effective rules, which address the problems identified in a holistic manner rather than in an ad hoc way. It will also allow for the aggravating human element to be incorporated into its process. It is necessary to establish an acceptable risk evaluation criteria based on cost effectiveness. It should however be noted that the acceptable cost would be a function of and depend on the level of risk. There is still plenty of space for improvement on FSA within the maritime field.

CHAPTER 3: REVIEW OF ANALYTICAL TECHNIQUES

3.1 Introduction

In order to be able to associate the content of "risk" with both engineering systems and organisational procedures there are three main concepts that we must introduce. The first is the concept of risk. Risk is defined as the product of the likelihood of occurrence of a hazardous event by its respective consequences. The second and third concepts needed introducing are reliability analysis and safety analysis. Reliability analysis of an item involves studying its characteristics expressed by the probability that it will perform a required function, under given conditions, for a pre-set period of time [Villemuer, 1992]. If such an analysis is extended even further into accommodating the study of the consequences of the failures, in terms of possible damage to property, to the environment and to personnel, the study is thereafter referred to as safety analysis which can be either quantitative or qualitative or a combination of them.

Safety can be defined as the ability of an item, equipment, or system not to cause injuries to people, or material damage or other unacceptable consequences during its use [Villemuer, 1992]. For the sake of simplicity when we refer to an engineering system, organisational processes as a meaning will also be included. The assessment of risk associated with an engineering system can be summarised in the following three questions:

1. What can go wrong?
2. What are the effects and consequences?
3. How often will they occur?

Safety analysis pays particular attention to the following two aspects:

- Safety when the item operates correctly: This aspect deals with the accident prevention, where a large number of regulations already exist to deal with this.

- Safety when the item or a part of it has failed: This aspect deals with the technical safety of the item, which can be investigated by simply using the same tools as those for reliability.

Safety analysis examines techniques, which can be applied to items in order to reach a safe state in case of failure [Wang, 1995]. On the other hand reliability assurance examines techniques in order to minimize the total number of failures. However, techniques designed in order to increase the safety state of an item can cause reduction in an item's or a system's reliability [Birolini, 1993]. For example, trying to ensure the clarity of drinking water within a fresh water network on board a vessel, we tend to add more components such as filters thus reducing the overall system's reliability. Safety is the ability of a system or process which does not cause, under given conditions, critical or catastrophic consequences [Villemuer, 1992]. If examined in a holistic way the three concepts of risk, safety and reliability operated as sums included partially one inside the other. Therefore, extending reliability in terms of hazards and consequences caused by the failure of the item to perform according to its manufacturer's standards, we get safety analysis, which in turn if analysed against all possible internal or external factors influencing the system that the component in question is part of, we get risk analysis.

The answers given from questions 1, 2, 3 concerning risk analysis, will provide adequate information about the safety of the system under investigation. Such information is interesting, mainly for statistical reasons, but is of no practical use unless there is a method(s) for controlling and managing the risk levels of the specified hazards and bringing them down to tolerable levels. Hence, for a safety assessment to be complete, the topic of how we can measure risk and thus reduce it should be addressed.

When analysts examine modern engineering systems such as vessels or offshore platforms, it is extremely difficult to treat the system as one entity due to the increased complexity that its sub-systems impose [Wang & Ruxton, 1998]. It is easier, and more efficient, to identify the various sub-systems and further break them down to their components. This will enable analysts to deal with one smaller system at a time, and as

soon as all of them are assessed, the sub-assessments will be combined to give a clear and overall risk picture of the initial system. A well-established pattern of hazard identification and risk assessment techniques has been introduced within the last few years in the marine industry [Mannan, 2005]. The analyst must choose wisely according to the nature and depth of analysis that he would like to go into [Hauge, 2001]. Choosing the proper techniques can also enable the analyst to identify a greater range of hazards that would have been omitted otherwise. There is a variety of techniques available to the analyst ranging from inductive to deductive and qualitative to quantitative.

Uncertainty in risk analysis is a major limiting factor when trying to assess the reliability and hence the safety of a marine engineering system [Wang, 2001]. Cases that include uncertainty require techniques that can handle it in an effective and efficient way in order to produce rational results. These techniques assist the analyst in understanding how the system would have behaved when an unwanted scenario takes place. Further explanations will be given through the test cases of the chapters to follow. It is appropriate at this point to go through a review of the major risk estimation and assessment techniques currently used in the marine industry for the assessment of reliability and safety of systems and processes. These techniques are able to cover aspects of the overall risk estimation model [Sen *et al.*, 1993]. Through a critical review, it is possible to identify their key points and address any gaps that can be covered by the novel proposed methodologies within the next chapters.

Safety analysis can generally be divided into two broad categories: the quantitative and the qualitative analysis methods. Depending on the safety data available to the analyst/decision maker, either a quantitative or a qualitative safety analysis can be carried out to study the risk of a system in terms of probability of occurrence for each hazard and its possible consequences [Aldwinckle & Pomeroy, 1983].

3.2 Qualitative safety analysis

Qualitative safety analysis is used to identify possible hazards and take proper precautions that will reduce the likelihood of occurrence and the level of consequences produced by those hazards in a linguistic manner. Generally this technique aims to generate a list of potential failures that affect the system examined. Since this method does not require quantitative failure data as an input to the analysis, it relies heavily on engineering judgement and past experience.

A commonly employed method in qualitative safety analysis is the use of the risk matrix [Halebsky, 1989], [Tummala & Leung, 1995]. The two parameters considered are the likelihood of occurrence of the failure event and the severity of the consequences of the failure event. Upon identifying all the hazards within the system considered, each hazard is evaluated in terms of these two parameters. Qualitative methods require from the analyst to assign linguistic variables in order to describe accurately both the likelihood as well as the severity of occurrence. Variables like catastrophic, critical, marginal and negligible are used to describe the respective severity of the consequences caused. The above mentioned linguistic variables can be classified in a number of categories according to the area examined. Table 3.1 shows four categories and their respective severity consequences, hierarchically, in terms of property, personnel, environment and company's reputation.

Table 3.1 Hazard consequence classification

Category	Description	Property	Personnel	Environment	Reputation
I	Catastrophic	System loss	Death	Ecosystem damage	Media crisis
II	Critical	Major system damage	Severe injury/illness	Major localised damage	Extensive referral on TV, radio, newspapers
III	Marginal	Minor system damage	Minor injury/illness	Minor localised damage	Minor referral on TV, radio or newspapers

IV	Negligible	Insignificant system damage	Insignificant injury/illness	Insignificant localised damage	Insignificant referral on radio, TV or newspapers

Similarly Table 3.2 gives 4 linguistic variables chosen to describe the frequency of occurrence and/or the occurrence probability. Variables like frequent, probable, occasional and remote, can be used by the analyst to describe the time period that the undesirable event takes place. An additional quantitative column exists next to the qualitative one in order to give a brief indication of the time intervals that each variable represents [Military Standards, 1993].

Table 3.2 Hazard probabilities and levels

Level	Description	Qualitative Description	Quantitative Description
A	Frequent	Likely to occur several times during the lifetime of the system	The probability of occurrence is greater than 10^{-1}
B	Probable	Likely to occur a few times during the lifetime of the system	The probability of occurrence is between 10^{-1} and 10^{-2}
C	Occasional	Likely to happen once in the lifetime of the system	The probability of occurrence is between 10^{-3} and 10^{-2}
D	Remote	Unlikely but possible to occur less than one time during the lifetime of the system	The probability of occurrence is between 10^{-6} and 10^{-3}

Based on Tables 3.1 and 3.2 the analyst is called to assess hazards and suggest appropriate control measures based on the frequency of occurrence and the severity of consequences of each hazard. Critical evaluation is of utmost importance, thus experience plays a very important role in decision making when it comes to qualitative techniques. Tables 3.1 and 3.2 are combined in such a way as to form a risk matrix, presented in Table 3.3 [Halebsky, 1989]. The risk matrix in its simple form as presented in Table 3.3 can assist the analyst to prioritise the hazards ranging from those that require immediate control measures, up to the hazards that require control measures only on a need to perform in a safe manner. The risk matrix takes the frequency of occurrence or the

occurrence probability of an identified hazard versus the severity of consequences that the particular hazard would have if it occurred, and the square in the matrix that the two variables meet is the base for deciding the magnitude of the control measures which need to be taken.

Table 3.3 The risk matrix

Description	Frequent A	Probable B	Occasional C	Remote D
Catastrophic	A-1	A-2	A-3	A-4
Critical	B-1	B-2	B-3	B-4
Marginal	C-1	C-2	C-3	C-4
Negligible	D-1	D-2	D-3	D-4

- The red areas A-1, A-2, A-3, B-1, B-2, B-3 and C-1 require immediate action and control measures need to be taken. The control measures must be turned towards the initial design stage or re-evaluation of the process in question in order to control or eliminate the hazards identified to an acceptable safety level.
- The yellow areas A-4, B-3 and C-2 have particular importance, and actions should be taken against the control of the consequences and hazard probabilities in an operational or maintenance level.
- The green areas can be separated in two categories. The first is the one consisting of areas B-4 and C-3. This category's control measures should be exercised only if cost benefit analysis performed is acceptable.
- For areas C-4, D-1, D-2, D-3 and D-4 control measures and further actions are required only on a need to perform safely.

Further development of the risk matrix on engineering systems and port operations, can be seen in Table 3.4 where the analyst can make decisions based on multiple simultaneous consequence categories. In Table 3.4, it can be seen that after defining the values for the occurrence frequency, several linguistic values have been chosen for different hazard related categories. Consulting with industrial experts four main hazard categories have been identified. Property, personnel, environment and company's reputation are of crucial importance when trying to assess the overall imposed risk during the operation, installation or maintenance of an engineering system or an imposed organisational process. Examining the four hazard categories separately the following are obtained:

1. Property: Any minor of major property damage, results in loss of operation due to down time, along with any costs that may be incurred for repairs or replacement.
2. Personnel: Human injuries, no matter how minor or severe may be, can always end up in delays in operation of the engineering system in question.
3. Environment: Beyond the ethics of protecting the environment any damage imposed to it can end up in many years of ecosystem recovery if not treated properly.
4. Reputation: Media and the image of a company projected by them can lift or extinguish a company from its business area. Media crisis can cause much more damage than any of the above three mentioned factors if not treated properly.

Table 3.4 Combined risk matrix

						Likely to happen	Several times during lifetime	Likely to happen once	Unlikely but possible during
						The probability of occurrence is greater than 10^{-1}	The probability of occurrence is between 10^{-1} and 10^{-2}	The probability of occurrence is between 10^{-3} and 10^{-2}	The probability of occurrence is between 10^{-6} and 10^{-3}
Property	**Personnel**	**Environment**	**Reputation**	**Category**	**Description**	**Frequent A**	**Probable B**	**Occasional C**	**Remote D**
System loss	Death	Ecosystem damage	Media crisis	I	*Catastrophic*	A-1	A-2	A-3	A-4
Major system damage	Severe injury/illness	Major localised damage	Extensive referral tv, radio, newspapers	II	*Critical*	B-1	B-2	B-3	B-4
Minor system damage	Minor injury/illness	Minor localised damage	Minor referral on tv, radio, newspapers	III	*Marginal*	C-1	C-2	C-3	C-4
Insignificant system damage	Insignificant injury/illness	Insignificant localised damage	Insignificant referral on radio, newspapers	IV	*Negligible*	D-1	D-2	D-3	D-4

The risk matrix is probably the most commonly used method when qualitative assessment needs to be utilised. Its main aim is the estimation of the risk imposed by the occurrence of each hazard identified. It can handle uncertainty giving rational results based on expert judgements and past experience or limited statistical data. It can handle different simultaneous consequence categories but lacks the ability to handle multiple criteria and express interdependencies between systems and components at different levels. For example it can be appropriately used for qualitative assessment if it had to deal with just a single row of consequences but it lacks the ability to deal with different consequence cells for each consequence column. It can be utilised at either a preliminary design level or prior to more in-depth reliability/safety analysis of an engineering system. It usually follows a failure mode and effects analysis, which will be analysed in section 3.4.3 of this chapter.

3.3 Quantitative safety analysis

Quantitative risk analysis utilises what is known and assumed about the numerical failure characteristics of each individual component to build a mathematical model that is associated with some or all of the following information [Aldwinckle & Pomeroy, 1983]:

- Failure rates.
- Repair rates.
- Mission time.
- System logic.
- Maintenance schedules.
- Human error.
- System layout.

Quantitative analysis like qualitative analysis requires information concerning the occurrence probability or frequency of occurrence of a hazard and their respective severity of consequences; only this time the linguistic variables used in qualitative analysis need to be quantified. Quantitative risk analysis must include [Aldwinckle & Pomeroy, 1983]:

- The occurrence probability of each system failure event: A system failure, considered to be the main event, results from simultaneous occurrence of the basic events associated with each of the minimal cut sets leading to this system failure. The occurrence probability of a system failing may be calculated on the basis of the identified cut sets and failure probability data of the associated basic events.

- The magnitude of its possible consequences: The possible consequences of a system's failures can be quantified in terms of possible loss of lives/human injuries, property damage, ecosystem damage and the reputation of the managing company which was affected by the consequences of the failure event.

Consistency checking is required to validate the results produced from quantitative analysis. The following studies are always useful for obtaining reliable results:

- Sensitivity analysis.
- Comparison with prior analysis if possible (if possible it should be stated in the case that no prior statistical data exist).
- Model checking.

3.4 Methods for Safety and Reliability Assessment

The reliability analysis usually takes place at the end of the design process right after the layout of the system has been determined. The role of the analysis is to verify if the reliability of the system satisfies the demanded reliability standards. However, if it is performed at the end of the design process it becomes too costly, as usually there is not enough time available to introduce major changes in the system if required. Therefore, the results of the analysis have little influence on the system's design. The reliability analysis would have a major influence on the design, if it were to be applied during the conceptual design. This would result in a more reliable and less expensive system. A system that is reliable in concept, is less expensive than a system that is not reliable in concept, but was improved at a later phase of the design or manufacturing process [Dodson & Nolan, 1999].

A number of well-established safety and reliability analytical methods are available to aid assessments of a risk-based nature. The appropriate technique(s) that can be applied to carry out assessment tasks would depend on the clarified hazards, their available data and the stage reached in the analysis up to that point.

3.4.1 Preliminary hazard analysis

Preliminary hazard analysis (PHA) was introduced in 1966 after the Department of Defence of the United States of America requested safety studies to be performed at all

stages of product development. The Department of Defence issued guidelines that came into force in 1963 [Military Standards, 1963]. PHA is performed to identify areas of the system, which will have an effect on safety by evaluating the major hazards associated with the system. It provides an initial assessment of the identified hazards. PHA typically involves:

1. Determine hazards that might exist and possible consequence effects.
2. Determine a clear set of guidelines and objectives to be used during a design.
3. Create plans to deal with critical hazards.
4. Assign responsibilities for hazard control (management and technical).
5. Allocate time and resources to deal with hazards.

Brainstorming techniques are used during which, the design or operation of the system is discussed on the basis of the experience of the people involved in the brainstorming activity. Checklists are commonly used to assist identifying hazards [DOD, 2000].

The results of the PHA are often presented in tabular form, which would typically include information such as but not limited to [Henley & Kumamoto, 1992], [Smith, 1992], [Villemuer, 1992]:

1. A brief description of the system and its domain.
2. A brief description of any sub-systems identified at this phase and the boundaries between them.
3. A list of identified hazards applicable to the system, including a description and any possible available references.
4. A list of identified accidents applicable to the system including a description, references and a description of the associated hazards and accident sequences.
5. The accident risk classification.
6. Preliminary probability targets for each accident.
7. Preliminary predicted probabilities for each accident sequence.
8. Preliminary probability targets for each hazard.

9. A description of the system functions and safety features.
10. A description of human error which could create or contribute to accidents.

The advantages of using the PHA method include:

1. It identifies the potential for major hazards at a very early stage of project development.
2. It provides basis for design and maintenance decisions.
3. It helps to ensure system to system and system to environment compatibility.
4. It facilitates the basic framework for a full hazard analysis later.

The disadvantage of PHA is that it is not comprehensive and must be followed by a full HAZard and OPerability (HAZOP) study. HAZOP will be analysed further down within this chapter.

3.4.2 What-if approach

What-if analysis uses a creative team, brainstorming "what if" questioning approach to the examination of a system in order to identify potential hazards and their consequences [CCPS, 1992]. Hazards are identified, existing safeguards noted, and qualitative severity and likelihood ratings are assigned to aid the risk management decision making process. Questions that begin with what-if are formulated by engineering personnel, experienced in the process or operation preferably in advance. There are several advantages and disadvantages in using the what-if approach [Groumpos & Merkuryev, 2002].

The advantages include:

1. A team of relevant experts extends knowledge and creativity pool.
2. Easy to use.
3. Ability to focus on a specific element (i.e. human error or environmental issues).

4. Ability to address issues like minor changes of system parameters. This is also called sensitivity analysis as it describes how sensitive a system is in minor parametric alterations.

The disadvantages include:

1. The quality of the what-if analysis is dependent on knowledge, thoroughness and experience of a team.
2. Loose structure that can let hazards slip through.
3. It does not directly address operability problems.

3.4.3 Failure mode, effects and criticality analysis

Failure mode effects analysis (FMEA) [SAE, 1967] is a technique which itemises in the form of an inventory all failure modes of each piece of equipment and their effect on the system. The emphasis is on hardware failure. A risk analyst applies this technique, when he/she wants to answer the question "what can go wrong with this system?"

A failure mode is the number of different ways a piece of equipment or operation can fail [Kumamoto, 1992], [Villemeur, 1992]. Some examples are shown in Table 3.5.

Table 3.5 Examples of failure modes

System	Failure modes
Belt conveyor system	Belt snaps Roller bearing fails Roller seizes Conveyor collapses
Actuated valve in fluid pipeline	Fails to open Fails to close Internal leakage External leakage
Pressure control system	Fails high Fails low Degraded Erratic

FMEA identifies single failure modes that play a significant part in an accident or loss event. The analysis is not efficient for identifying combinations of equipment failures that lead to accidents. Human errors are not usually considered specifically in FMEA, even though the effects of mal-operation are usually included in an equipment failure mode.

3.4.3.1 Significant failure modes

The significant failure modes for components are listed as follows:

- Failure to open/close/start/stop or continue operation.
- Spurious failure.
- Degradation.
- Erratic behaviour.
- Scheduled service/replacement.
- External/ internal leakage.

Most components would fall in one of the above categories

3.4.3.2 FMEA Methodology

FMEA methodology involves completing an FMEA table by systematically examining every piece of equipment and recording all failure modes that may be possible. For each failure mode, immediately effected and expected events are recorded. Table 3.6 shows a typical FMEA table along with a described example of the role of relief valves within a vessel's steering gear system.

Table 3.6 FMEA table

Component	Function	Failure mode	Failure cause	Effect on the system	Detection means	Operation actions	Comments
Relief Valve	Relief valves are used to protect the piping system from oil overpressure. If the pressure inside the piping system is increased above the expected it may cause damage to the pipes and flanges.	Valve stuck open Valve stuck close Valve is leaking	Mechanical failure Human error Erosion	Incorrect operation may cause damage to other components of the system Loss of oil due to leakage	Regular checks of the valve from the engine room personnel to monitor valve's good operation	Remove the faulty valve and replace it if maintenance of the valve is impossible	Low possibility of failure because the relief valves are strictly inspected from surveyors during the steering gear's operation

Sometimes it is useful to extend an FMEA to include criticality ranking (Failure Mode, Effects and Criticality Analysis - FMECA). Here each failure mode would be ranked according to a chosen scheme. FMEA is a qualitative technique and measures of significance are qualitatively assessed, as shown in Table 3.1.

Criticality analysis allows a qualitative or a quantitative ranking of the criticality of the failure modes of items, as a function of the severity classification and occurrence likelihood. As long as the probability of occurrence of each failure mode of an item can be obtained from a reliable source, the criticality number of the item under a particular severity class may be quantitatively calculated as:

$$C = \sum_{i=1}^{N} E_i L_i t \qquad [3.1]$$

E_i = Failure consequence probability of failure mode i.

L_i = Likelihood of occurrence of failure mode i.

N = The number of the failure modes of the item, which fall under a particular severity classification.

t = Duration of applicable mission phase.

Once the criticality numbers of the item under all severity classes have been obtained, a criticality matrix can be constructed to provide a means for criticality comparison. Such

a matrix displays the distribution of criticality of the failure modes of the item and provides a tool for assigning priority for corrective action. Criticality analysis can be performed at different system/sub-system levels and the information produced at low levels may be used for criticality analysis at a higher level [Wang et al., 1995].

An FMECA is an inductive process that involves the compilation of reliability data as well as the consequences imposed on the system if any of the individual items parting it fail. It can be integrated into the hazard identification phase of the safety and reliability assessment process [Wang et al., 1995]. To maximise its usefulness as a decision making tool, it should be initiated at the earliest stage of design, and then updated and expanded to lower levels as the design progresses. In the maritime industry Det Noske Veritas (DNV) and the American Bureau of Shipping (ABS) adopted the requirement for FMEA/FMECA in the mid 1970s and early 1980s [Coggin, 2001].

The completed FMEA or FMECA is a systematic tabulation of the effects of equipment failure within a process or system [Kumamoto, 1992]. Equipment failures with an unacceptable criticality ranking should be re-examined to verify the failure modes and their effects, and to reduce or eliminate them where needed [Villemeur, 1992].

The FMEA methodology consists of the following step [Pentti & Atte, 2002]:

1. Define the complete functional boundaries of the system to be analysed. This is done by marking up a set of drawings and annotating them to show their functional limits and dependencies.
2. Define the level of detail. It is necessary to decide whether the study will be conducted at component level, or at sub-component level. For example, if a centrifugal pump is one component in the system, a component level analysis might include the failure modes of the pump (stopped, racing, low output, cavitating, seal leakage, etc.). A sub-component level analysis will have to look at each of the elements that make up the pump (casing, impeller, shaft, seal, drive motor, etc).

3. Very often, sub-component level of detail is not required, unless there is a specific need based on the type of application, e.g. nuclear or aerospace industry. As a compromise, major sub-components may be included.
4. FMEA data sheet. The main elements of a data sheet are shown in Table 3.6. The sheet typically includes the following:

- Header information describing the system being studied, drawing references, list of team members, date and location of study, etc.
- Component identified. This would include a functional identifier, (e.g. boiler feed-water pump), an identification tag that can be tied to a drawing, and reference to the system or subsystem of which the component is a part.
- Failure mode. This should be concise and realistic. A failure frequency may be included, based on the information in Table 3.2.
- Effect on system. This requires examination of the failure mode from a multidisciplinary perspective by the team. This mainly depends on the expertise of the team, and available documentation, and is the most critical aspect of the study.
- A severity ranking may be included, based on the way the failure mode affects the system, using Table 3.1 as a guide.
- Method of failure detection. For high severity (critical or higher) consequences, it is necessary to provide some form of failure detection. The method may detect incipient failures before they become critical. If no detection exists, the team may develop one and include it in the study recommendations. The detection method could be procedural, e.g. regular inspection and testing.
- System and operator response. The response may include the following [Wang, 1995]:

➢ Ability of the automatic controls to absorb the effects of failure, if the design includes this capability.
➢ Ability of the operator to respond to the failure in time. This should be realistic and not too optimistic.
➢ Resolutions on any additional hardware, or changes to procedures required.

The following documents are required as a minimum, for the FMEA/FMECA study:

- Project design basis.
- Engineering line diagrams (these are also referred to as piping and instrumentation diagrams or P&IDs) in the process industries.
- Electrical line diagram.
- System description.
- Instrument logic or ladder diagrams.
- Instrument loop diagrams.

Some other additional important documents are:

- Training manuals.
- System operating procedures.
- Manufacturer's manuals for equipment.

3.5 Advantages and limitations of FMEA

The major advantages of FMEA are the ease of construction at component level and quick identification of critical failures in a properly conducted study. It is useful for machinery and material handling systems compared to other techniques. Furthermore, for systems with predominantly linear interactions, FMEA provides the simplest way of identifying and correcting potential failures that would have an adverse effect on system performance. FMEA also provides valuable information on the failure modes, which could be used in more sophisticated techniques such as fault tree analysis for quantification of system failure frequency [Wang et al, 1995].

There are a number of limitations in the range of applicability of the FMEA technique such as:

- It addresses only one component at a time, and may not reveal the complex and hidden interactions in the subsystem and between subsystems in the system.
- It does not provide sufficient detail for quantification of system consequences.

It should be noted that FMEA and FMECA are useful when used in conjunction with three other hazard analysis tools. These are Hazard and Operability Study (HAZOP), Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) where contributing equipment failure leads to a stated hazard. These techniques will de described in the following pages.

3.6 HAZOP

HAZOP study, is a systematic examination of the design or operation of an installation, as represented by layout and engineering diagrams with all control, instrumentation and sequence of operations shown, all design documents and operations manuals [Kletz, 1974]. Deviations from all design values of key parameters are studied, using guidewords to control the examination evaluation. Examples of such guidewords are found in Table 3.7.

Table 3.7 Examples of HAZOP guidewords with associated examples

Guideword	Example
No	No flow, no signal
Less	Less flow, less cooling
More	Excess temperature, excess pressure
Opposite	Cooling instead of heating
Also	Water as well as lubricating oil
Other	Heating instead of pumping
Early	Opening the drain valve too soon
Late	Opening the drain valve too late
Part of	Part of Incomplete drainage

In the chemical process plants, the design is given in a piping diagram. In the manufacturing context the operation is represented as an engineering diagram. This diagram is a schematic representation of the material flow with all operational controls and protection devices shown on each item of equipment. HAZOP study is undertaken by a group of senior representatives from design, project and operating personnel, using a comprehensive checklist of guidewords or questions about possible deviations from normal operations

3.6.1 Cases to be applied

The study is generally undertaken before the construction of new equipment, or before making major modifications to existing systems, in order to facilitate the recognition of a large number of hazards or potential operating problems which can be avoided by redesign or adoption of suitable operating procedures [Henley & Kumamoto, 1992]. The earlier a potential problem is found, the less expensive it is to rectify the problem, and the more likely it is that the solution will in fact be implemented. It can be said that it is a more advanced FMEA.

This structured simulation of the operations and deviations serves as an excellent means of communication between design and operating staff, and forms a useful base for writing operating procedures [Kletz, 1974]. While the technique appears to be time consuming at the design stage, costs are normally recovered rapidly by smooth and prompt commissioning and avoidance of further modifications during commissioning and subsequent operation.

The FMEA/HAZOP study could form the basis of a statutory approval for new systems or significant modifications to existing systems, where the organisation seeking approval provides all necessary data and evaluation to the relevant authorities for consideration [Hendershot et al., 1998]. It may also be possible for a member of the approval authority to participate in the HAZOP team.

For existing operations, the study could be undertaken to identify possible hazards that are not obvious, to minimise business interruption risks and to improve operability on the whole by making appropriate changes to equipment, control systems, protection systems and to operating/maintenance procedures [HSE, 2002].

3.6.2 Process to be followed

The team formally reviews each part on the engineering diagram using a series of questions to consider what could happen to the process, equipment and personnel in an abnormal situation and how that situation could arise. The team looks for every deviation of operational parameters in an open ended way, making the assumption that a problem can only arise when there is a deviation from the design or operating intentions, e.g. no movement or reverse movement when there should be a forward movement.

The guidewords are applied to each parameter for that line or equipment item/ group. The typical parameters in a fluid system handling facility are flow, level, pressure, temperature and composition. In the case of materials handling, the parameters are speed, load, direction, impact, orientation, temperature, packaging, access, etc.

It is essential to make the guidewords as specific as possible and appropriate to the type of process or operation studied, in order to make the HAZOP technique most effective [Henley & Kumamoto, 1992].

3.7 Fault tree analysis

Fault Tree Analysis (FTA) is a widely used tool for the systematic analysis of combinations of events that can lead to an incident [Veseley et al., 2002]. A fault tree is a

logical diagram showing the different ways that a system can fail in terms of a defined final failure event.

A simplified fault tree for a liquefied petroleum gas (LPG) related fire event is shown in Figure 3.1. The tree depicts the causes of failure by working backwards from the 'top-event', identifying all contributors to the event. The tree structure is created by tracing back the top-event to possible causes (failure modes or basic events), which may be component failures, human errors or any other events that can lead to the final incident.

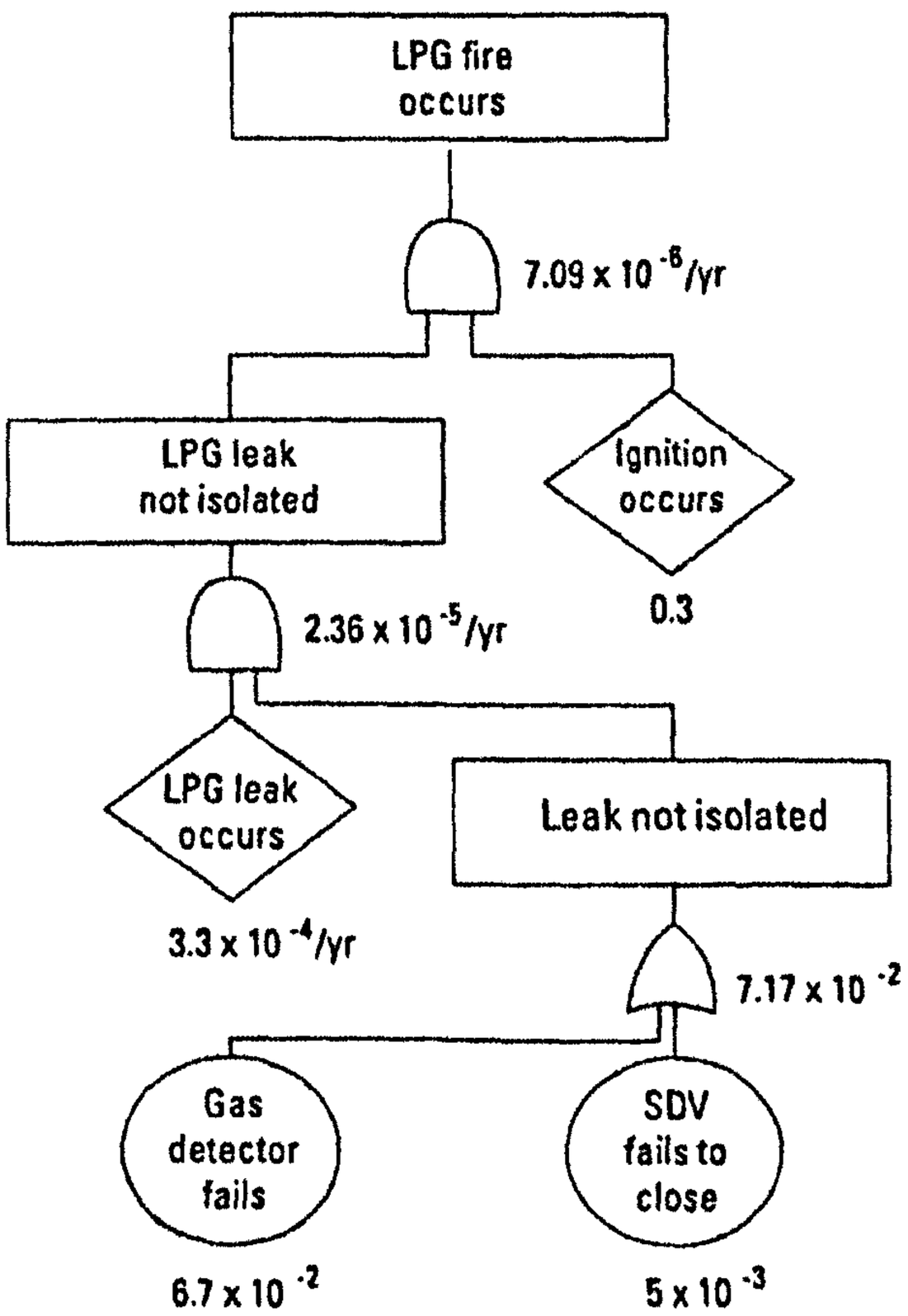


Figure 3.1 FTA of LPG fire

There is a standard nomenclature for FTA. The most commonly used symbols and their definitions are listed in Table 3.8 [Kumamoto & Ernest, 1996].

EXCLUDED
UNDER
INSTRUCTION
FROM
UNIVERSITY

Table 3.8 Most commonly used symbols for FTA

In general, the failure of an item, equipment or the development of an undesirable situation (e.g. high pressure level in tank) will create a 'demand' on the protection system

to operate, e.g. level switch to close feed valve. The undesirable top event occurs when there is a demand and the protection system fails.

A demand on the protection system to be brought into operation is generally expressed as a frequency (e.g. number of times/year). The chance that the 'protection system would be in a failed state' when the demand occurs is expressed as a probability.

For instance, presence of gas in an LPG installation is a demand on the gas detector (protection system) to shut off the isolation valves. If the detection fails when called upon to act, or the isolation valve fails to close, then there is the chance of a fire or gas explosion, if the leak finds an ignition source (see Figure 3.1).

In order to calculate the frequency of the top event, failure rate frequencies and/or probabilities of failure are applied to each of the basic events. There are several basic rules for deriving results from within fault trees and there is a logic technique called Boolean algebra that reduces the size of a fault tree to minimise its complexity and produce the minimum possible combination of basic events that lead to the occurrence of the top event. These minimum combination are called minimum cut-sets [Henley & Kumamoto, 1992], [Villemeur, 1992].

3.7.1 Fault tree construction

A good summary of fault tree construction is provided by Lees [Lees, 1996], and is described as follows:

"The construction of a fault tree appears a relatively simple exercise, but it is not always as straightforward as it seems and there are a number of traps that should be avoided" [Lees, 1996]. Prior to construction of the fault tree, it is necessary to properly define and understand the function of the system in question. Both the system itself and its boundaries need to be clearly defined [Fussell, 1973]. Information on the system is generally available in the form of functional diagrams such as piping and instrument

diagrams along with more detailed instrumentation and electrical diagrams. There will also be other information required on the equipment and its operation as well as for the working environment. The quality of the final tree depends crucially on a good understanding of the system, and time spent on this stage is well repaid. It is emphasised by Fussell [Fussel, 1973], that "the system boundary conditions should not be confused with the physical boundaries of the system". The system boundary conditions define the situation for which the fault tree is to be constructed.

An important system boundary condition is the top event. The initial system configuration constitutes additional boundary conditions. This configuration should represent the system in the failed-free state. Where a component has more than one operational states, an initial condition needs to be specified for that component. Furthermore, there may be fault events declared to exist and other fault events not to be considered, these being termed by Fussell the "existing system boundary conditions" and the "not-allowed system boundary conditions" [Fussel, 1973], respectively. The principal elements in fault trees are the top event, primary/basic events, intermediate events, and the "AND" and "OR" gates.

Some points worth taking into consideration when constructing a fault tree are:

- If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.
- All inputs to a particular gate should be completely defined before further analysis of any of them is undertaken.
- Gate inputs should be properly defined fault events, and gates should not be directly connected to other gates.

Each event in the tree, whether it is a top, intermediate or basic event, should be carefully defined. Failure to observe a proper discipline in the definition of events can lead to confusion and an incorrect tree. The identifiers assigned to events are also important. If a single event is given two identifiers, the fault tree itself may be correct, although slightly

confusing, but in the minimum cut sets the event will appear as two separate events, which is incorrect.

For a process system, the top event will normally be a failure mode of the equipment. The immediate causes will be the failure mechanisms for that particular failure. These in turn constitute the failure modes of the contributing subsystems, and so on. The procedure followed in constructing the fault tree needs to ensure that the tree is consistent. Two types of consistency may be distinguished: series consistency within one branch and parallel consistency between two or more branches. Account needs also to be taken of events, which are certain to occur, and those, which are impossible. The development of a fault tree is a creative process. It involves identification of failure effects, modes and mechanisms [Vesely et al, 2002] Although it is often regarded primarily as a means of quantifying hazardous events, which it is, the fault tree is of equal importance as a means of hazard identification. It follows also that fault trees created by different analysts will tend to differ. The differences may be due to style, judgement and/or omissions and errors.

It is generally desirable that a fault tree has a well-defined structure. In many cases such a structure arises naturally. It is common to create a 'demand tree', which shows the propagation of the faults in the absence of protective systems, and then to add branches, representing protection by instrumentation and by the process operator, which are connected by AND gates [Villemeur, 1992].

3.7.2 Dependence

A fundamental assumption in fault tree analysis is that the events considered are independent, unless stated otherwise. Formally, the events are assumed to be statistically independent. In practice, there are many types of situations where events are not completely independent. In fault tree this problem was originally known as 'common mode failure', then as 'common cause failure' and now more usually as 'dependent failure' [Villemeur A., 1992].

After consultation, in the form of a structured interview, with several industrial experts (see Appendix II), the following examples of dependency chosen are as follows:

- A single component sharing a control function and a trip function. This design is generally to be avoided, but some older engineering systems don't separate these two. An example is a control valve being used as a shutdown valve as well.
- The failure of a piece of equipment or a component giving rise to more than one demand. An example is the fully pressurised cargo system on board an LPG vessel, causing both high pressure and low temperature conditions calling upon the protection system to operate.
- Supply from a common utility such as electric power or instrument air for pneumatically actuated instruments.
- Common degrading factors for several protection systems, such as vibration, corrosion, dust, humidity etc.
- A fire or explosion disabling a number of pieces of equipment simultaneously.

The problem is particularly acute in systems, such as LPG containment and gas free systems, where a very high degree of reliability is sought. The method of achieving this is through the use of protective systems incorporating a high degree of redundancy. On paper, the assessed reliabilities of such systems are very high. But there has been a nagging worry that this protection may be defeated by the phenomenon of dependent failure, which may take many and subtle forms [Lees 1996]

Again, following the structured interview method, and after consultation of the same industry's experts (see Appendix II), the following situations, which can cause dependent failure, include:

- A common utility.
- A common defect in manufacture.
- A common defect in application.
- A common exposure to a degrading factor.
- An external influence.

- A hazardous event.
- Inappropriate operation.
- Inappropriate maintenance.

Not all-dependent failures involve independent equipment. Another significant type of dependent failure is the overload, which can occur when one piece of equipment fails and throws a higher load on another piece of operating equipment.

Failures caused by domino effects, and escalation faults generally, may also be regarded as dependent failures. Dependent failure, then, is a crucial problem in high reliability systems.

Two examples are given below:

- A cable tray carries a coaxial cable, carrying signals between field instruments and the control room. A single cable can carry several signals. Should the cable fail due to a fire, impact, electrical fault, power failure etc., and then all the protection systems to which the cable had carried signals would be disabled at the same time.
- In an LPG cargo tank, the safety system contains three independent oxygen analysers, high oxygen alarm/trip based on a two-out-of-three failure voting system. However, if all analysers draw a process gas sample from a single sampling point, a blockage of the sampling nozzle would disable all the analyser protection function simultaneously.

Once the dependence potential has been identified, there are two ways of representing it in the tree [Vesely, 2002]:

- Continue to enter each fault separately as it occurs in the tree, but ensuring that each such entry is assigned the same identifier, so that the minimum cut sets are determined correctly.
- Enter the effect as a single fault under an AND gate higher up the tree.

A further measure, which may be taken to identify dependent failure, is to examine the minimum cut sets for common susceptibilities or common locations. In the first approach the minimum cut sets are obtained using the laws of Boolean algebra.

In such situations, when a fault tree construction includes separate blocks for each demand/protection failure combination, the same block may appear in more than one branch; or alternatively, the same mode may appear in more than one block. The initial fault tree has to be 'reduced' to ensure that such duplications would not distort the top event frequency. This 'reduction' is achieved with the aid of Boolean algebra. Just as normal algebra adds or multiplies quantities, which have a numerical value using normal rules of arithmetic, Boolean Algebra operates on 'logical' quantities [Wang et al, 2001].

The laws for simplifying sets and obtaining the minimum cut sets leading to the top event in a fault tree are based on the basic logic gates of AND, OR and NOT being used in differing combinations. Suppose " · " stands for "AND" and " + " stands for "OR", and suppose that " $\bar{A}$ " and " $\bar{B}$ " represent the events of "not A" and "not B" respectively, then the typical Boolean algebra rules are described as in Table 3.10.

Table 3.9 Boolean algebra rules

Name of the rule	AND form	OR form
Identity law	$A \cdot 1 = A$	$A + 0 = A$
Null (or dominance) law	$A \cdot 0 = 0$	$A + 1 = 1$
Idempotent law	$A \cdot A = A$	$A + A = A$
Inverse law	$A \cdot \bar{A} = 0$	$A + \bar{A} = 1$
Commutative law	$A \cdot B = B \cdot A$	$A + B = B + A$
Associative law	$(A \cdot B) \cdot C = A \cdot (B \cdot C)$	$(A + B) + C = A + (B + C)$
Distributive law	$A + (B \cdot C) = (A + B) \cdot (A$	$A \cdot (B + C) = A \cdot B + A \cdot$

	+ C)	C
Absorption	$A \cdot (A + B) = A$	$A + A \cdot B = A$
De Morgan's law	$\overline{A \cdot B} = \bar{A} + \bar{B}$	$\overline{A + B} = \bar{A} \cdot \bar{B}$
Double Complement law	$\bar{\bar{A}} = A$	

Owing to such simplification rules, the occurrence probability of a top event can be obtained from the associated minimum cut sets [Bozzano & Villafiorita, 2003].

3.7.3 Examples of FTA

The following example is used to demonstrate the procedure required to build and assess a fault tree. It can be considered as a tutorial in the construction of fault trees for those not being familiar with this process.

An LPG mix system takes two chemicals C1 and C2 at a set ratio and reacts them to form a product P. The feed flows are independently controlled by two control valves. Should either control valve fail, the reaction ratio would be upset, resulting in an automatic shutdown. The automatic shutdown is achieved by a high C1/C2 ratio trip, shutting down the C1 feed. It is critical to shutdown reactant C1 as it is highly flammable. There is no independent shutdown valve on the C1 feed line, and the control valve is also used as the shutdown valve (dependence).

The fault tree is given in Figure 3.2,

where:

A = C1 feed control valve fails to high

B = C2 feed control valve fails to low

C = C1/C2 ratio high trip relay failure

T = flameable C1 vented to atmosphere (top event).

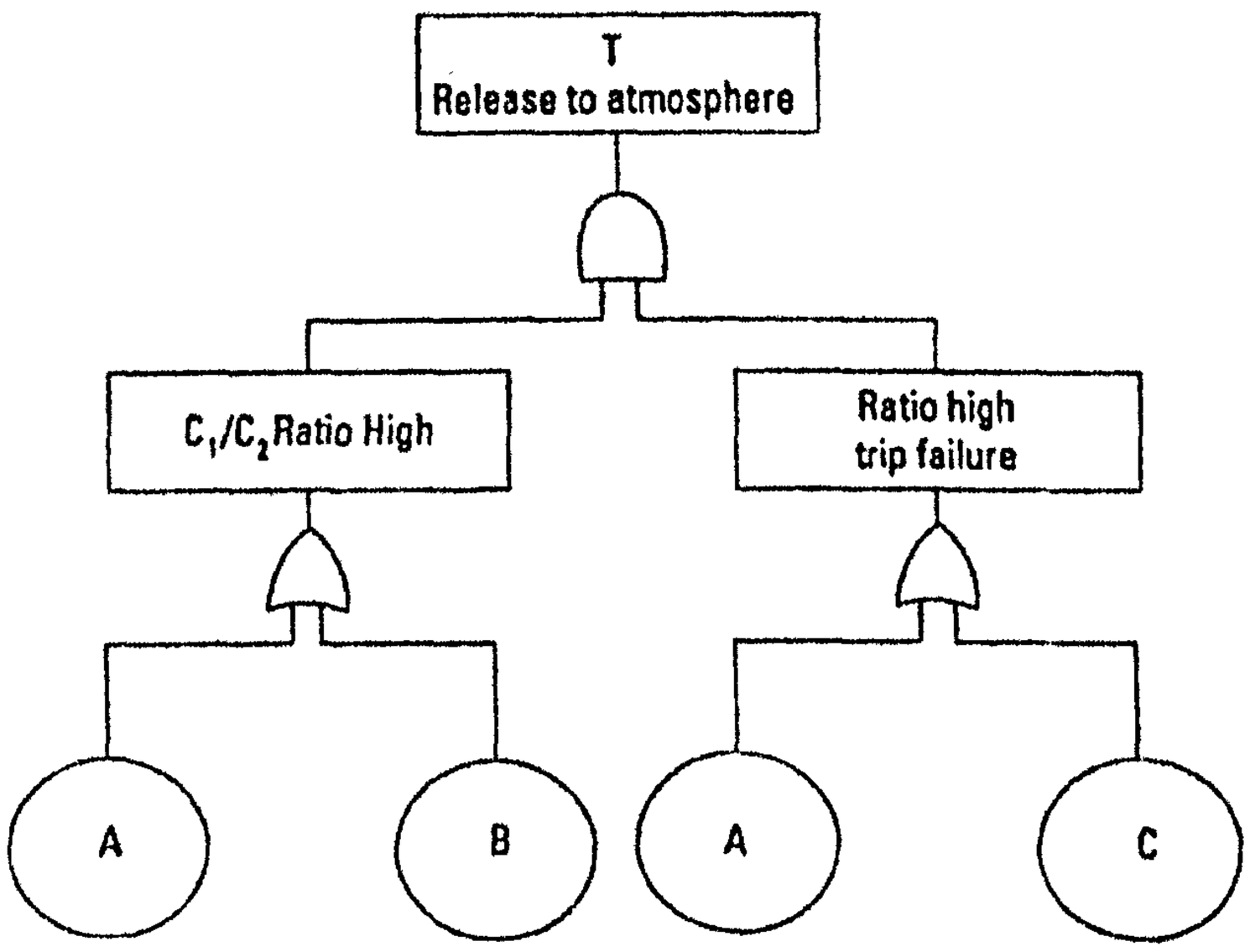


Figure 3.2 Unreduced fault tree for LPG mixer

The base event A appears twice entering an AND gate in the fault tree (C1 control valve fails to high). Therefore, this fault tree needs to be reduced. The fault tree can be represented by the following algebraic expression:

$T = (A + B)\ (A + C)$

$T = A\ A + A\ B + A\ C + B\ C$

Applying the Boolean reduction rules of Table 3.10,

$$T = A+B\ C$$

The reduced tree is shown in Figure 3.3.

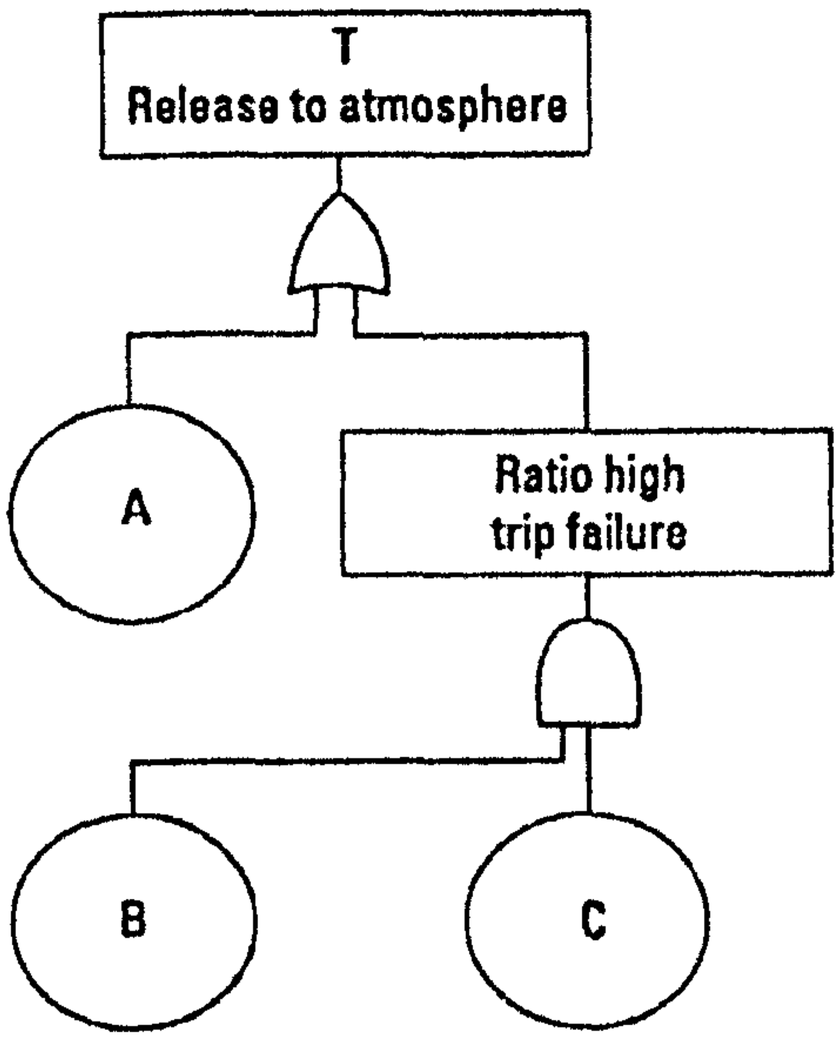


Figure 3.3 Boolean reduced fault tree for LPG mixer

The minimum cut sets are:

A

BC

In the second approach, since it is known that A causes the dependence, it can be directly linked to the top gate. This is possible in simple systems but can mislead in complex systems for which the first approach is more suitable.

FTA can be used in both reliability and safety assessment. The principles of FTA in both of these assessments are the same although in reliability assessment it is usually used for measuring system performance while in risk assessment it is used for investigating undesirable events with increased severity of consequences [Wang et al, 1993]. It can be carried out in the risk estimation phase of the safety and reliability assessment process to identify the minimal cut sets associated with major brake-downs (top events) and to

assess the occurrence probability of each top event in order to assist in design decision making and hazard identification process. FTA's major disadvantage is the lack of handling data in cases of uncertainty and vagueness. It can only produce quantitative results if quantitative information is readily available from statistical data or failure databases. Another major drawback of the method is the lack of producing results based on interdependences of components within a system. Methods like fuzzy sets and Bayesian approach are more suited in cases with high complexity level and data under uncertainty.

3.8 Event tree analysis (ETA)

In the case of standby systems and in particular, safety and mission-oriented systems, the Event Tree Analysis (ETA) is used to identify the various possible outcomes of the system following a given initiating event which is generally an unsatisfactory operating event or situation. In the case of continuously operated systems, these events can occur (i.e. components can fail) in any arbitrary order. In the ETA, the components can be considered in any order since they do not operate chronologically with respect to each other. ETA provides a systematic and logical approach to identify consequences and to assess the probability of occurrence of each possible resulting sequence caused by the initiating failure event [Henley & Kumamoto, 1992], [Villemuer, 1992].

Event trees are primarily safety oriented by nature, being particularly suitable for the analysis of systems where time is a significant factor, for example, when manual intervention can avoid further development of an incident if applied within a specified time, such as a secondary cooling water system in a heat exchanger. Working forward in time from the failure event, the operation of each safety means or contingency plan is considered. When these fail to achieve the desired result, the consequence is established and the frequency is determined [Henley & Kumamoto, 1992], [Villemeur, 1992], [Birolini, 1993].

Figure 3.4 shows an event tree analysis concerning a main engine lubricating oil pump that failed in its operation. A series of risk control measures are examined sequentially and all the possible ending scenarios are calculated based on their respective consequences. Multiplying the probabilities that correspond to any path from the initiation of the failure event to the end of any consequence, the path will give us the probability of occurrence of that particular scenario.

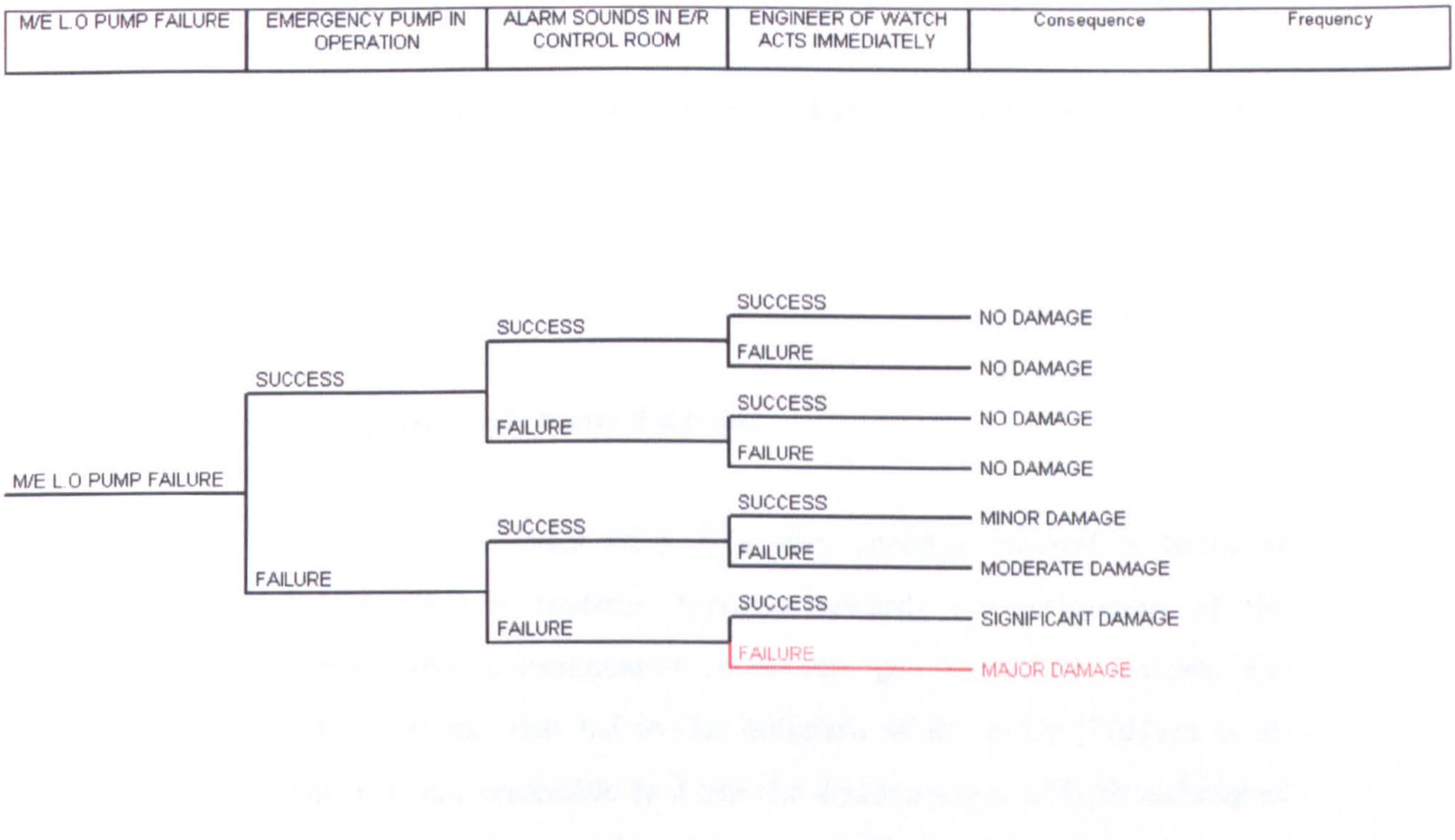
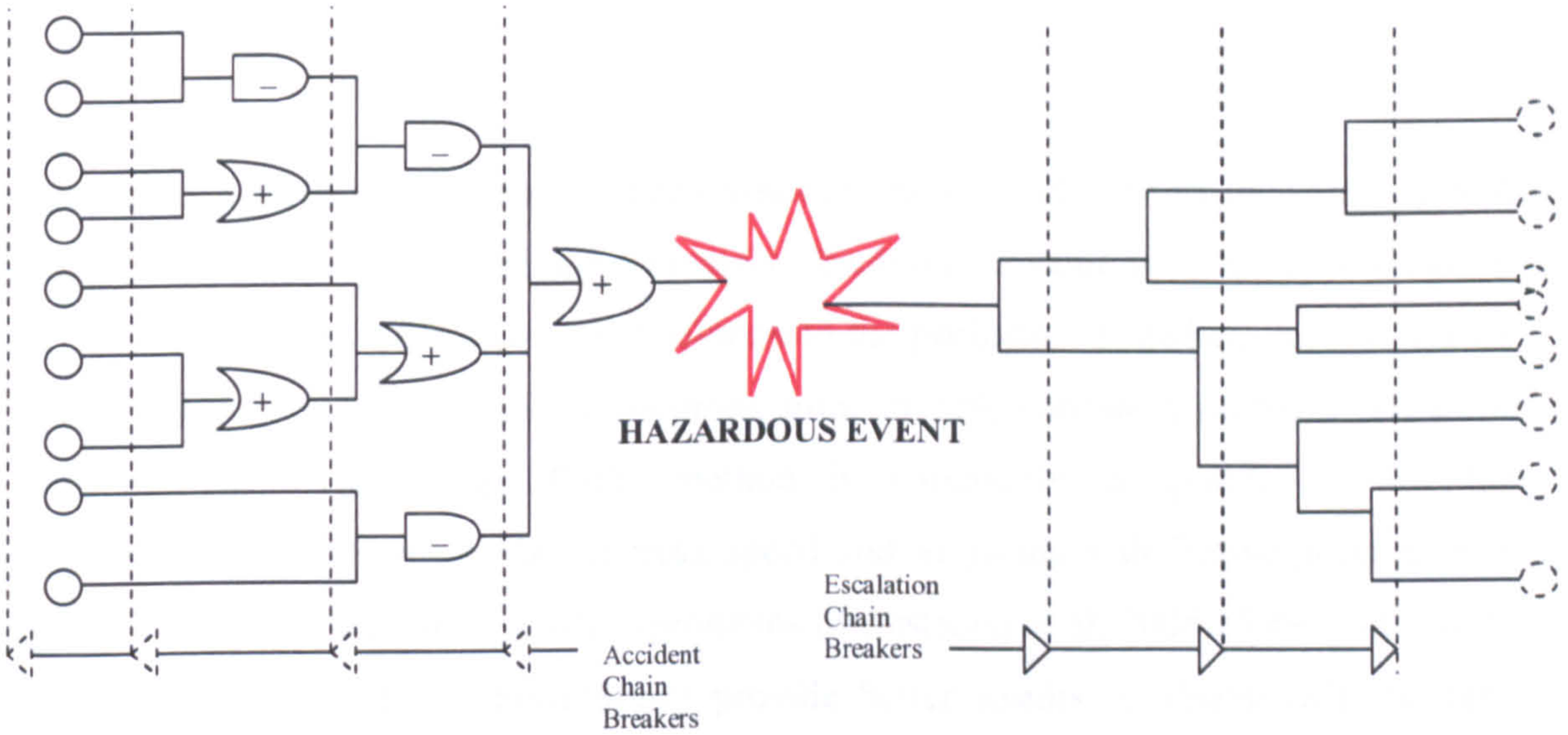


Figure 3.4 Event tree analysis of a main engine lubricating oil pump failing

3.9 Cause consequence analysis

Cause consequence analysis (CCA) is nothing more than a combined FTA with ETA. This results in an upgraded ETA as it compiles the information gathered from the FTA and propagates it to the ETA. Figure 3.5 gives a schematic representation of the combination of the two techniques. This analytical diagram method was developed in the 1970s at RISØ National Laboratories in Denmark [Nielsen, 1977] to specifically aid in



the reliability and risk analysis of nuclear power plants in Scandinavian countries [Villemeur, 1992].

Figure 3.5 Cause consequence schematic diagram

Starting from a main hazardous event CCA is a very versatile method in terms of operation [IMO, 2002a]. It can continue forward towards the estimation of the probabilities of its respective consequences or it can go backwards towards the identification of the basic events that led to the initiation of the event [Nielsen et al, 1977]. In general terms it is not preferable as it has the disadvantages of both techniques combined and for simple situations it provides the analyst with additional work.

3.10 Simulation analysis

Simulation analysis is any method imitating the behaviour of an actual system under reliability and safety assessment. For example, Monte Carlo simulation [Cortazar & Schwartz, 1998] is a simulation method that uses statistical trials in calculating multiple scenarios (i.e., evaluating substantive hypotheses) of the risk-based analytical model by repeatedly sampling values from the probability distributions for the uncertain variables to get an approximate solution to a problem. There is a random process where some parameters of the process are equal to the required quantities of the problem. Since these

parameters are not known exactly, many assumptions are made so that the parameters of the process can be determined approximately. Each time a value is randomly selected, it forms one possible scenario and one solution to the problem. Together, these scenarios give a range of possible solutions/outcomes, some of which are more probable and some less probable. The Monte Carlo method is commonly acceptable due to the approximation of its results but it lacks speed and in giving a definitive point as best likely solution to the risk estimation problems [Armstrong et al, 2005]. First and second order reliability methods (Form/Sorm) provide better results in almost half the time Monte Carlo requires and along with this a most likely failure point among a locus of possible solutions. Further analysis of a modified version of Form/Sorm methods will be presented in Chapter 6 of this thesis.

3.11 Subjective reasoning analysis

In cases where there is unavailability of data, analysts are required to produce a model based on subjective judgments. These mathematical models can give rational results but cannot accommodate cases where in-depth analysis is required. Linguistic variables are used while trying to give a qualitative measurement to quantities. For example, when a description is required to explain the transition between different levels of the same quantity e.g. if a cargo is examined the transition from medium to heavy cannot be a single point on a graph. Realistically, the weight would gradually increase towards the heavy condition. Subjective reasoning could be combined with FMEA and the risk matrix, in an attempt to give a more thorough description to the model examined.

Problems like that are better tackled using fuzzy set theory which will be analysed in a more extensive way in this thesis in Chapter 4 of this thesis.

3.12 Outline of the techniques developed to deal with uncertainty

The techniques examined in the previous sections of this chapter are commonly used within the marine industry framework for risk and estimation assessment. All of them

though show significant difficulty in tackling interdependence between the components of an engineering system, or dealing with vagueness and uncertainty conditions. There are certain techniques developed like Bayesian networks (BNs), fuzzy-logic (FL) and evidential reasoning (ER), which have proved efficient and effective in dealing with vague and uncertain conditions in cases where traditional techniques face problems. These techniques will be further discussed, analysed and applied through a number of test cases within the chapters of the thesis.

3.12.1 Bayesian networks

BNs are part of a class of probabilistic models with strong connections to graph theory. Initially their main usage was to back up logical statements based on deterministic production rules. The immediate advantage is that each variable may have more values than the traditional true and false and not all relations have to be deterministic.

Influence diagrams, which further extend the notion of BNs by including decision nodes and utility nodes, have been used in human reliability assessment [Humphreys, 1995] and decision-making on explosion protection offshore [Bolsover & Wheeler, 1999]. A good reference work for the computational method underlying the implementation of them is included in Hugin software as described [Jensen, 1993]. Hugin software enables a powerful risk assessment solution that is easy to use, flexible, and appropriate for use on marine and offshore applications. Other renowned program packages for BN building and influencing include MSBNx [Kadie et al, 2001], created at Microsoft Research, and Netica [Netica, 2002], the commercial program developed by Norsys Software Corp.

3.12.2 Fuzzy logic

Fuzzy logic systems are knowledge/rule-based systems constructed from human knowledge in the form of fuzzy IF-THEN rules [Wang, 1997]. The rules output an IF-THEN statement in which some words are characterised by continuous membership functions [Zadeh, 1965]. For example, the following is a fuzzy IF-THEN rule:

IF the likelihood of a hazard is frequent AND severity of occurrence is catastrophic, THEN risk level is high. The linguistic variables frequent, catastrophic and high are characterised by the membership functions. The starting point of constructing a fuzzy logic system (FLS) is to obtain a collection of fuzzy IF-THEN rules from human experts or based on the domain knowledge. As a fuzzy system is constructed from a collection of fuzzy IF-THEN rules, the next step is to combine these rules into a single system. Different fuzzy systems use different principles for this combination. An important contribution of fuzzy system theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping thus being able to tackle uncertainty and vagueness when it appears during the reliability and safety assessment of engineering systems and processes. Its main advantages are:

- It provides a tool for directly working with the linguistic variables when assessing risks. Thus, fuzzy theory enables analysts to evaluate risks in a neutral manner.
- Vague, qualitative or imprecise data as well as quantitative data can be used in the assessment and can be dealt in a consistent manner.
- It is capable of providing a flexible framework for combining the elements of criticality, probability of occurrence, severity and reliability.

3.12.3 Evidential reasoning

Problems within the field of engineering involve both quantitative and qualitative data which, in the majority of times may contain some form of uncertainty or lack of evidence. Multiple attribute decision making requires a certain background as set by [Belton & Stewart, 2002], [Huang & Yoon, 1981], [Saaty, 1988]. The continuous development in technical complexity of engineering systems has led into the extensive use of safety methods that can appropriately provide a safety assurance as far as the operation and practice of these systems are concerned. It has not been, up until the last couple of decades that appropriate research has commenced in the area of evidential

reasoning. It started initially as an extension to research made within the artificial intelligence area by [Buffardi, 1998], [Yager, 1987] and [Zimmermann, 1990]. The upcoming results from the research followed, came from examples [Yang & Singh, 1994] and [Yang, 2001]. An approach based on a model evaluation analysis as well as on the theory of evidence was introduced by [Shafer, 1976]. Within the last few years there are examples of usage of an evidential reasoning (ER) approach within different engineering areas like ship design, marine system analysis and synthesis [Wang et al., 1995], [Wang, 1997], [Wang & Yang, 2001], and in areas outside engineering, such as organizational assessment [Yang et al., 2001].

The safety of a large engineering system, such as a sea going vessel, is affected by a great number of factors associated with its design, manufacturing, installation, commissioning, operation and maintenance [Wang, 2001]. This means that in many cases there are always some parameters that are imprecisely or inaccurately known, resulting in a non-complete mathematical model of the system. Evidential reasoning can tackle multi-criteria decision making models under uncertainty conditions.

3.13 Conclusion

In this chapter, typical safety analysis methods were outlined in terms of their requirements, advantages and limitations. Some of these techniques have been successfully used in the industry and still continue to be used. However, the application of these conventional techniques to complex engineering systems and processes is not as straightforward as it may seem at the beginning. Certain modifications or introduction of novel techniques are needed to enhance the application of such methods. These modifications include the ability of the analysis methods to handle data that is associated with a high degree of uncertainty and the integration of expert opinion in a formal manner, where there is no bias of opinion. The following chapters examine, analyse and test the applicability of such novel methods.

CHAPTER 4. A MULTI-CRITERIA DECISION MAKING METHODOLOGY ASSISTING A VESSEL SELECTION PROCESS

4.1 Introduction

Marine engineering systems, like cargo handling machinery, are affected by a great number of factors associated with their design, manufacturing, installation, commissioning, operation and maintenance. This means that in many cases there are always some parameters that are imprecisely or inaccurately known resulting in non-complete mathematical models of the system.

In cases like this, when experts try to assess the safety of a system they encounter the following problems [Wang & Yang, 2001]:

A) Different types of assessments (numbers, linguistic terms, and/or stochastic values) depending on the characteristics of the decision criteria.

B) Imprecise assessments due to insufficient data, shortcomings in expertise, small time intervals for evaluation or inability of the expert to provide a fully detailed assessment.

C) Proper and robust aggregation of subjective and objective assessments made on multiple decision criteria.

It is due to the problems identified in A, B and C that decision-making process is based on subjective opinions [Wang, 1997]. This occurs due to inaccurately known data, or parameters with a high level of uncertainty that cannot be handled properly with methods based on conventional mathematics. Such problems were often omitted even though their role within the engineering system was of high importance.

Probabilistic decision theory can handle uncertain parameters in the aspect of randomness. Probabilistic Risk Analysis (PRA) methods, like fault tree analysis (FTA) can be used to assess system safety and the information produced can be utilised in building a multi-objective model for decision-making purposes. On the

other hand however, it is insufficient in tackling uncertainties in terms of fuzziness or vagueness and incompleteness. If fuzziness, such as the intersection point between different temperature levels, vagueness such as unreliable subjective descriptions due to lack of expertise or incompleteness such as lack of statistical data is actually the case, multiple criteria decision-making (MCDM) techniques can be employed to process the constructed model in order to produce efficient design and operational solutions [Yang, 2001]. In many cases, due to lack of evidence, individuals find easier to provide subjective judgments using verbal grades. However, it is necessary to establish the fact that these grades will mean the same thing to more than one person, as seen in chapter 3. Therefore, descriptors like very good, good, average, poor or even very likely, likely, impossible, are all terms used by safety engineers and decision makers and have the same meaning to all of them. It is true that the descriptors provided before are fuzzy and non-probabilistic, and hence non-probabilistic methods like fuzzy sets modelling may be more appropriate to analyze the safety of an engineering system containing incomplete information.

In complex marine engineering systems the problems encountered are of a dual nature. They contain both quantitative and qualitative assessments. What would seem an obvious thing to do is either to convert the qualitative assessments to quantitative forms by assigning a quantitative value to each qualitative assessment or to transform the quantitative assessments to qualitative forms by using the already defined descriptors (assessment grades). Multiple attribute decision-making requires a certain background as set by Belton & Stewart [Belton & Stewart, 2002], Huang & Yoon [Huang & Yoon, 1981] and Saaty [Saaty, 1988]. It has not been up until the last couple of decades that research has commenced in the area of evidential reasoning. It started initially as an extension to the research made within the artificial intelligence area by Buffardi and Zimmermann [Buffardi, 1998] [Yager, 1987] [Zimmermann, 1990]. The upcoming results from the research that followed, came from examples given by Yang & Singh [Yang & Singh, 1994], [Yang, 2001]. An evidential reasoning approach is based both on a model evaluation analysis and on the theory of evidence as presented by Shafer [Shafer, 1976]. Within the last few years there have been examples of application of the evidential reasoning (ER) approach within the marine engineering areas like ship design [Sen & Yang, 1995], as well as in the marine system analysis and synthesis [Wang et. al., 1995] [Wang, 1997] [Wang & Yang,

2001], and in areas outside engineering, like organizational self assessment as it will be seen in Chapter 7 of this thesis.

It is common sense that every decision a safety engineer makes contains, to some extent, uncertainty and risk. The aim of this chapter is to indicate a proper course of action in such cases where criteria under uncertainties exist. The original ER approach is revisited in section 4.2 along with the rest of the techniques used to form this chapter. Section 4.3 contains the properties of the proposed ER approach and section 4.4 a vessel selection assessment carried out to demonstrate the properties of section 4.3. This chapter is concluded in section 4.5 with the discussion of results.

4.2 Theory background

4.2.1 Dempster-Shafer theory and evidential reasoning approach

Evidential reasoning is a process of drawing plausible conclusions from uncertain or incomplete information. The theory of evidence was first introduced by Dempster in 1967 and it was further developed by his student Shafer in 1976. Therefore it is common to encounter ER as the Dempster-Shafer theory (D-S theory) [Shafer, 1976].

The D-S theory is essentially based on probability theory, yet it is more flexible in a manner that it allows probability judgments to capture the inaccurate nature of the examined factor. This results in degrees of likelihood being measured by probability intervals, as opposed to point probabilities in the Bayesian approach. The D-S theory uses a number between 0 and 1 to set the degree of belief for a proposition, which could be parted from multiple grades (i.e excellent, good, average, bad). For example the function of a newly developed automated loading/unloading arm for Liquefied Petroleum Gas (LPG) vessels can be evaluated as 80% excellent, 60% good, 20% average. Such an example clearly indicates that the evaluation can be assigned to more than one grade according to the supporting evidence and the subjective experience of the safety engineer. Another advantage of this method is the fact that the grades of belief do not have to sum up to 1. In the example provided before the evaluation could have been 60% good and 20% average. The unassigned belief, the remaining 20%, could be the result of uncertain data, lack of information or evidence or even insufficient expertise.

When dealing with a decision-making problem, safety engineers are asked to use their knowledge in terms of preference and evaluation to make the best possible decision. The ER approach developed by [Yang & Singh, 1994] was made specifically for problems incorporating both qualitative and quantitative criteria under uncertainties. The strongest point of ER is its ability to deal with incomplete, uncertain and vague as well as complete and precise data. It is also useful as it enables the experts involved in a decision-making problem to reach their decisions either in a subjective or a quantitative way. This inherently means that judgments can be made in terms of verbal descriptors rather than specific numbers as was clearly presented at the example above.

4.2.2 Utilization of the ER approach

The ER approach operates in a frame that employs a belief structure to represent an assessment as a distribution. Four evaluation grades are assumed as follows:

$H = \{H_1, H_2, H_3, H_4\}$ = {Slightly preferred, Moderately preferred, Preferred, Greatly Preferred}

Using the four evaluation grades, the assessment of an attribute A_1 on an option O_1, denoted by $S(A_1(O_1))= \{(\beta_{1,1},H_1), (\beta_{2,1},H_2), (\beta_{3,1},H_3), (\beta_{4,1},H_4)\}$, where $1 \geq \beta_{n,1} \geq 0$ with $n = 1,\ldots,4$, denotes the degree of belief that the attribute A_1 is assessed to the evaluation grade H_n. $\sum_{n=1}^{4} \beta_{n,1} > 1$ cannot exist. $\sum_{n=1}^{4} \beta_{n,1} = 1$ is considered to be a complete distributed assessment of $S(A_1(O_1))$ and $\sum_{n=1}^{4} \beta_{n,1} < 1$ is considered to be an incomplete assessment of $S(A_1(O_1))$. Within the ER approach the last two conditions can both be accommodated [Yang, 2001]. Within ER approach it is common to have a problem with M attributes A_i, K options O_j and N evaluation grades H_n, with $i = 1,\ldots,M$ and $j = 1,\ldots,K$ and $n = 1,\ldots,N$. It must be noted that it is possible that each attribute can have its own set of evaluation grades that may be different from those of other attributes [Yang, 2000].

Based on the evidence combination rule provided from D-S theory, the ER approach uses an evidential reasoning algorithm to aggregate belief degrees [Yang & Sing, 1994] [Yang & Sen, 1994] [Yang, 2001].

Assume that ω_i is the relative weight of the attribute A_i and it is set that $1 \geq \omega_i \geq 0$ and $\sum_{i=1}^{L} \omega_i = 1$, where L is the total number of attributes in the same group for aggregation. To further analyze the discussion and without loss of generality the combination of three assessments will be presented below. Two of them are complete ($S(A_2(O_1))$ and $S(A_3(O_1))$) and only one is incomplete ($S(A_3(O_1))$) due to uncertain or lack of data, or even shortage in expertise from the decision maker's side. Assume that the second assessment is given by $S(A_2(O_1)) = \{(\beta_{1,2},H_1), (\beta_{2,2},H_2), (\beta_{3,2},H_3), (\beta_{4,2},H_4)\}$, and the third assessment is given respectively by $S(A_3(O_1)) = \{(\beta_{1,3},H_1), (\beta_{2,3},H_2), (\beta_{3,3},H_3), (\beta_{4,3},H_4)\}$. The problem is to aggregate all three assessments in $S(A_1(O_1)) \oplus S(A_2(O_1)) \oplus S(A_3(O_1))$ in order to achieve rational decision making results and obtain a clear picture of the problem addressed.

In order to combine 3 assessments it is required to combine initially the first two and the combined result is then used to aggregate it with the third assessment. The same principle would apply if the decision maker would have to deal with more assessments that need to be combined.

Firstly, take $S(A_1(O_1)) \oplus S(A_2(O_1))$ for example. Let

$$m_{n,1} = \omega_1 \beta_{n,1} \text{ (n=1,...,4) and } m_{H,1} = 1 - \omega_1 \sum_{n=1}^{4} \beta_{n,1} = 1 - \omega_1$$

$$m_{n,2} = \omega_2 \beta_{n,2} \text{ (n=1,...,4) and } m_{H,2} = 1 - \omega_2 \sum_{n=1}^{4} \beta_{n,2} = 1 - \omega_2$$

where each $m_{n,j}$ (j=1,2) is denoted as basic probability mass and each $m_{H,j}$ is the remaining belief unassigned to H_j (j=1,2,3,4). The ER algorithm is used to aggregate the basic probability masses to generate combined probability masses denoted by m_n with (n=1,...,4) and m_H using the following equations:

$m_n = k(m_{n,1}m_{n,2} + m_{n,1}m_{H,2} + m_{H,1}m_{n,2})$, (with n=1,...,4)

$m_H = k(m_{H,1}m_{H,2})$ with

$$k = \left(1 - \sum_{n=1}^{4}\sum_{t=1}^{4} m_{t,1}m_{n,2}\right)^{-1} \text{ with } (n \neq t)$$

The combined probability masses will now be aggregated with the third assessment following the same general principle. What should be done now is to aggregate $S(A_{1,2}(O_1)) \oplus S(A_3(O_1))$ where $S(A_{1,2}(O_1)) = S(A_1(O_1)) \oplus S(A_2(O_1))$.

Let for example $S(A_{1,2}(O_1) = \{(H_1,0.5), (H_2,0.4), (H_3,0.1), (H_4,0)\}$, and $S(A_3(O_1)) = \{(H_1,0.1), (H_2,0.3), (H_3,0.4), (H_4,0)\}$. Let also $S(A_{1,2}(O_1))$ be twice as important as $S(A_3(O_1))$. Since $\sum_{i=1}^{L}\omega_i = 1$ then it is obvious that $\omega_{1,2} = 0.67$ and $\omega_3 = 0.33$. The sum of the attributes in the third assessment does not add up to 1 due to lack of data, or uncertainty in data or even due to shortage of expertise from the decision maker's side. Therefore the normalized $S(A_{1,2}(O_1))$ and $S(A_3(O_1))$ will become:

$S(A_{1,2}(O_1) = \{(H_1,0.5x0.67), (H_2,0.4x0.67), (H_3,0.1x0.67), (H_4,0)\}$

$S(A_3(O_1)) = \{(H_1,0.1x0.33), (H_2,0.3x0.33), (H_3,0.4x0.33), (H_4,0)\}$

Similarly with the equations stated above:

$m_{n,1,2} = \omega_{1,2}\beta_{n,1,2}$ (n=1,…,4) and $m_{II,1,2} = 1 - \omega_{1,2}\sum_{n=1}^{4}\beta_{n,1,2} = 1 - 0.67*1 = 0.33$

$m_{n,3} = \omega_3\beta_{n,3}$ (n=1,…,4) and $m_{II,3} = 1 - \omega_3\sum_{n=1}^{4}\beta_{n,3} = 1 - 0.33*0.8 = 0.736$

$$k = \left(\sum_{n=1}^{4}\sum_{t=1}^{4} m_{t,1,2}m_{n,3}\right) \text{ with } (n \neq t) \Rightarrow k = 0.13$$

$m_{1,1,2,3} = (1\text{-}k)^{-1}$ x $(m_{1,1,2}$ x 067 x $m_{1,3}$ x 0.33 + $m_{1,1,2}$ x 067 x $m_{II,3}$ + $m_{1,3}$ x 0.33 x $m_{II,1,2}) = 0.3$

$\Rightarrow m_{1,1,2,3} = 0.3$

Similarly for the rest

$m_{2,1,2,3} = 0.295$

$m_{3,1,2,3} = 0.116$

$m_{4,1,2,3} = 0$

Therefore the unassigned belief in the combined assessment is:

$m_{H,1,2,3} = 1 - 0.3 - 0.295 - 0.116 = 0.289$

This results in the final set of the combined $S(A_{1,2}(O_1)) \oplus S(A_3(O_1))$ being

$S(A_{1,2,3}(O_1)) = \{(H_1,\beta_{1,1,2,3}), (H_2,\beta_{2,1,2,3}), (H_3,\beta_{3,1,2,3}), (H_4,\beta_{4,1,2,3})\}$

$\beta_{1,1,2,3} = m_{1,1,2,3} / (1 - m_{H,1,2,3}) = 0.42$

Similarly:

$\beta_{2,1,2,3} = 0.415$

$\beta_{3,1,2,3} = 0.163$

$\beta_{4,1,2,3} = 0$

Finally $S(A_{1,2,3}(O_1))$ can be obtained as follows:

$S(A_{1,2,3}(O_1)) = \{(H_1,0.42), (H_2, 0.415), (H_3, 0.163), (H_4, 0)\}$. It can be seen that from the combination of the assessments the unassigned belief has been dramatically reduced to just 0.002. It is therefore a great advantage of the ER approach to deduct decision results even if the data used is vague, incomplete or imprecise.

4.2.3 Decision tables and decision trees

A simple but effective way of aiding the decision making process is the decision tables and decision trees. These two formats can be interchangeable once a decision situation has been established in any of the two forms. In real life problems, the decision maker does not always know the true nature of the problem, but is aware of the states that exists. Due to applicability reasons in this chapter only decision trees will be dealt with, as they are much easier to use rather than decision tables. A decision table gives an illustration of a system along with all the sub-components involved enabling the safety engineer or the decision maker to "see" the relation of all

condition applicable. It also provides the flexibility to add any new data found during the process of decision-making [Sen & Yang, 1995]. This of course means that not only addition but any kind of modification can be instantly made to the decision tree according to the updated information on the case.

4.2.4 Fuzzy set theory

Zadeh in 1965 described the properties of fuzzy sets as a class of objects with a continuum of grades of membership in the interval [0,1] in order to deal with fuzzy and uncertain data that is typically represented by linguistic, rather than numeric variables. Each linguistic variable in fuzzy set theory (FST) is assigned a membership that is defined by the user. This means that each object x in a fuzzy set X is assigned a grade of membership by a membership function usually denoted by $\mu(x)$ whose values range from 0 to 1. This is not to be confused with the quantity of a probability density function f(x), as the integral of f(x) must sum to 1, whereas in $\mu(x)$ there is no such restriction.

FST has been successfully applied for a wide range of single and multiple criteria decision-making problems. Yager in 1981 proposed a fuzzy logic based methodology for making qualitative multicriteria decisions. He also applied a fuzzy multicriteria decision making algorithm for personnel selection process and finally in 1994 he proposed a multicriteria decision making approach in selecting the most suitable tool for a specific manufacturing application like fixture design. The concepts of fuzzy values managed to capture the characteristics of the data of different materials specified in the engineering handbooks which were multidimensional and qualitative. In 1998 Pan et. al. developed and used fuzzy goal programming for purchasing dredgers under uncertainty. In 2001 Sii et. al. applied a fuzzy logic based approach to qualitative safety modelling for marine systems.

Zadeh's words give a summary of the usefulness of fuzzy approaches by saying: "a fundamental contribution of fuzzy logic is a methodology for computing with words which mimics human reasoning" [Zadeh, 1965].

4.3 Operations with fuzzy sets

Let X be a set i.e, X= $\{x_1, x_2,\ldots, x_n\}$. The fuzzy subset of X is defined by a function from X into {0,1}; that is the membership function. The membership function for each subset of X is noted by X = $\{ \mu_1/x_1, \mu_2/x_2,\ldots, \mu_n/x_n\}$, the notation of μ_i/x_i will refer to the fuzzy subset whose membership value at x_i is μ_i. Assume that A and B are fuzzy subsets of X. Suppose the membership values for the subsets A and B are denoted by μ_A and μ_B respectively. The basic fuzzy operations such as union, intersection, complement, Cartesian product and composition of fuzzy sets are listed as follows:

(a) Union of A and B:

$\mu_{AUB} = \max(\mu_A, \mu_B)$; The union of A and B produces fuzzy set C with membership values that are the maximum of the component values.

(b) Intersection of A and B:

$\mu_{A\cap B} = \min(\mu_A, \mu_B)$. The intersection of A and B produces fuzzy set C with membership values that are the minimum of the component values.

(c) Complementation of A:

$\mu_A = 1 - (\mu_A)$. The membership values of the complementary set A are just 1 – the corresponding membership values of A.

(d) Cartesian product of A and B:

$\mu_{AxB} = (\mu^{ij}_{AxB})$ where $\mu^{ij}_{AxB} = \min(\mu^{i}_{A}, \mu^{j}_{B})$

(e) Composition: Given the membership functions for the fuzzy subset A and for the Cartesian product of the subsets A and B, the membership function for B can be obtained as follows using the composition rule of inference:

$\mu_B = \mu_{AoAxB} = (\mu^{j}_{B})_{1xn}$; where $\mu^{j}_{B} = \max(\min(\mu^{1}_{A}, \mu^{1j}_{AxB}),\ldots,\min(\mu^{n}_{A}, \mu^{nj}_{AxB}))$, j=1,2,…,n. For reasons of simplicity the subsequent fuzzy subset descriptions will drop the index following the division symbol and merely use ordered list of membership values to characterize the fuzzy subset. Therefore, the fuzzy set X will become, X = $\{ \mu_1, \mu_2,\ldots, \mu_n\}$.

4.4 An novel evidential reasoning approach in marine operations and its application to a vessel selection process

Decision problems are better visualized through the application of a decision tree as discussed in section 4.2.3. In the first level, the main concern of the problem is discussed. In the second level, there are several criteria, each of which has a different contribution to measuring and helping getting to the overall destination. Then it is common that many of the second level criteria could be broken further down to sub-criteria in order to be able to facilitate the assessment as completely as possible. The de-composition of these criteria reaches a point that the decision maker is happy that he has adequate information to start the decision process. Once the sub-division of criteria is complete, the decision maker will evaluate each alternative based on the lowest level criteria. The results will be transformed from the lowest level criteria to their respective upper levels and eventually towards the main goal. This is achieved through the application of the ER approach, which could be described as a hierarchical evaluation into which all criteria are aggregated into the top goal of the problem.

A safety assessment framework incorporating ER approach within port operations is presented in this section. The proposed framework consists of the following steps:

1. *Define the problem and set the assessment grades for main goal:* The first step is to describe the specific decision related problem in detail, either using quantitative or qualitative terms.

2. *Set the criteria levels and their respective grades:* After the initial goal is set, the second level criteria are defined, along with any sub-level criteria below them, up until the decision maker is happy with the structure of the problem defined.

3. *Evaluate each alternative based on the sub-sequent level criteria:* In order to find out how well an alternative performs across all criteria, the lowest level criteria assessment needs to be first transformed to their relevant upper levels and ultimately, to the top-level goal.

4. *Use the ER algorithm:* In order to make the transformation from lower level to upper level criteria, the information is fed into a multi criteria decision making software developed for analysis of multilevel decision problems. The software which will assist in the decision making process is called Intelligent Decision System via Evidential Reasoning "IDS" [Yang and Xu, 2001]. It is a windows based tool, which can be used to built up a model, define alternatives and criteria and perform the assessment for the decision maker.

5. *Rank alternatives, results and discussion:* As soon as the aggregated values are derived for each of the vessels in question the ranking takes place according to the higher value in terms of preference.

6. *Decision making:* Based on the combination of the steps above, the decision maker can now come to a certain conclusion concerning the decision problem that the analyst is dealing with. The results from IDS as well as the criteria and alternatives selected will be the prime factors that will set the boundaries for further discussion.

This procedure will be illustrated through an example described in the next section. The requirements for a verification experiment are essential to identify and assess the validity of the results obtained. The contribution of industrial expert's judgment in the form of a structured interview (see Appendix III, section A), within the example presented was invaluable as they added to the credibility and soundness of the results obtained. However, a verification experiment is to be made by presenting the results to independent experts in the area of assessing a vessel's quality.

4.5 A decision making based example: application of a novel evidential reasoning approach to a vessel selection process

The example is chosen to demonstrate the usage of a novel evidential reasoning approach which can be used as a significant tool in assisting the marine industry in cases often met like the selection process of a vessel for a particular transfer of cargo. The example illustrates how evidential reasoning can be used to assess multiple criteria containing both qualitative and quantitative data including uncertainties in information.

Within marine industry's boundaries, the selection of a proper vessel for the transfer of a liquid oil cargo is a process consisting of 3 different stages. The first stage is the request or the invitation for a particular cargo by either a refinery with stand alone discharge facilities or by an independent customer who will transfer the cargo delivered by other means away from the initial storage tanks. Then it is the stage of the broker trying to find a list of proper vessels that match the criteria set by the charterer. Finally, there is the stage of the vessel selection among the ones pre-selected by the broker.

Looking at port safety during cargo handling operations there are two main factors involved in this process. Initially it is the vessel that should fulfil certain characteristics and secondly it is the port of loading or discharge of cargo. This test case aims at selecting a suitable vessel and satisfying the requirements it needs to meet in order to approach a port on the west coast of the United States. When a request is made from the charterers to the brokers, concerning a particular cargo and a port of destination, the broker is searching, looking for the most suitable vessel in the market that fulfils the criteria. It is true that in the first instance, several vessels will match the criteria. Nevertheless this is not always the case. A vessel's dimensions and cargo capacity are not just the only factors affecting the decision process. Selecting the best vessel is a complex decision making process for the marine industry. It requires a number of criteria to be simultaneously measured and evaluated. Due to the nature of the criteria, sometimes they conflict with each other leading to one criterion being increased at the expense of another.

4.5.1 Step 1: Define the problem

The case examined is a decision making process, in selecting an appropriate oil tanker with capacity of 80,000 tonnes to deliver a cargo of oil to a pre-specified port of call chosen by the charterers. Therefore the main or top goal of this decision making process is to select the most appropriate vessel based on the information required from the charterers side, the brokers' side and the port's specifications. For simplicity reasons and without loss of generality it is assumed that there is just one decision maker in this case, the author of this thesis, who should initially define the assessment grades for the evaluation of the vessel based on the results of the structured interviews

(see Appendix III, section A). The following assessment grades have been chosen for this case: very bad, bad, average, good, very good and excellent. The next step is the definition of assessment grades for the second level criteria involved in the decision making process. What is more, all the sub-sequent levels of criteria should also be analysed up until the decision maker is completely satisfied with the overall assessment. It is of common sense that not all criteria will have the same assessment grades. It depends on the nature of the criteria and the preferences (proper wording) of the decision maker. Figure 4.1 illustrates the criteria used for the assessment along with their sub-level attributes. There are five sub-levels of assessment criteria within this example case. The criteria chosen are some of the most significant taken under consideration from the decision maker's side.

Explaining analytically the criteria it is worth mentioning a few details for each one:

- Integrity: This criterion is concerned with the condition of the vessel both as far as structural and mechanical conditions are concerned. It examines the thickness of the bottom plating, side shell, cargo tanks as well as brackets and frames around the hull, along with the reliability data gathered for the main and auxiliary engines. Cargo handling equipment is also investigated. Finally the actual age of the vessel is of great importance as the conditions of both mechanical and structural components are directly related to age.

- Pollution Prevention: In order for a vessel to be able to sail it must fulfil certain requirements as far as pollution control is concerned. Structural characteristics like double bottoms and double side skins are useful as they prevent a great percentage of possible leakages of cargo, from being spilt into sea. Finally, the emission values for both NOx and COx are important in order to get in specific ports. The port of call is based at the west USA, where the permitted emission levels are low and pollution regulations are extremely strict.

- Vessel's Running Costs: During the operation of the vessel there are certain factors like fuel (by saying fuel we include factors like diesel, lubricating oil, cylinder oil), stores consumption and crew salary that need to be investigated. A

vessel that has the capability to be run with less crew members is more desirable in terms of daily expenditure during time at sea.

- Restrictions on Vessel: These are imposed by geographical factors mainly. Since the vessel will sail from Europe to west USA through the Panama Canal it should have limitations as far as the draft and breadth is concerned in order to fit into the locks.

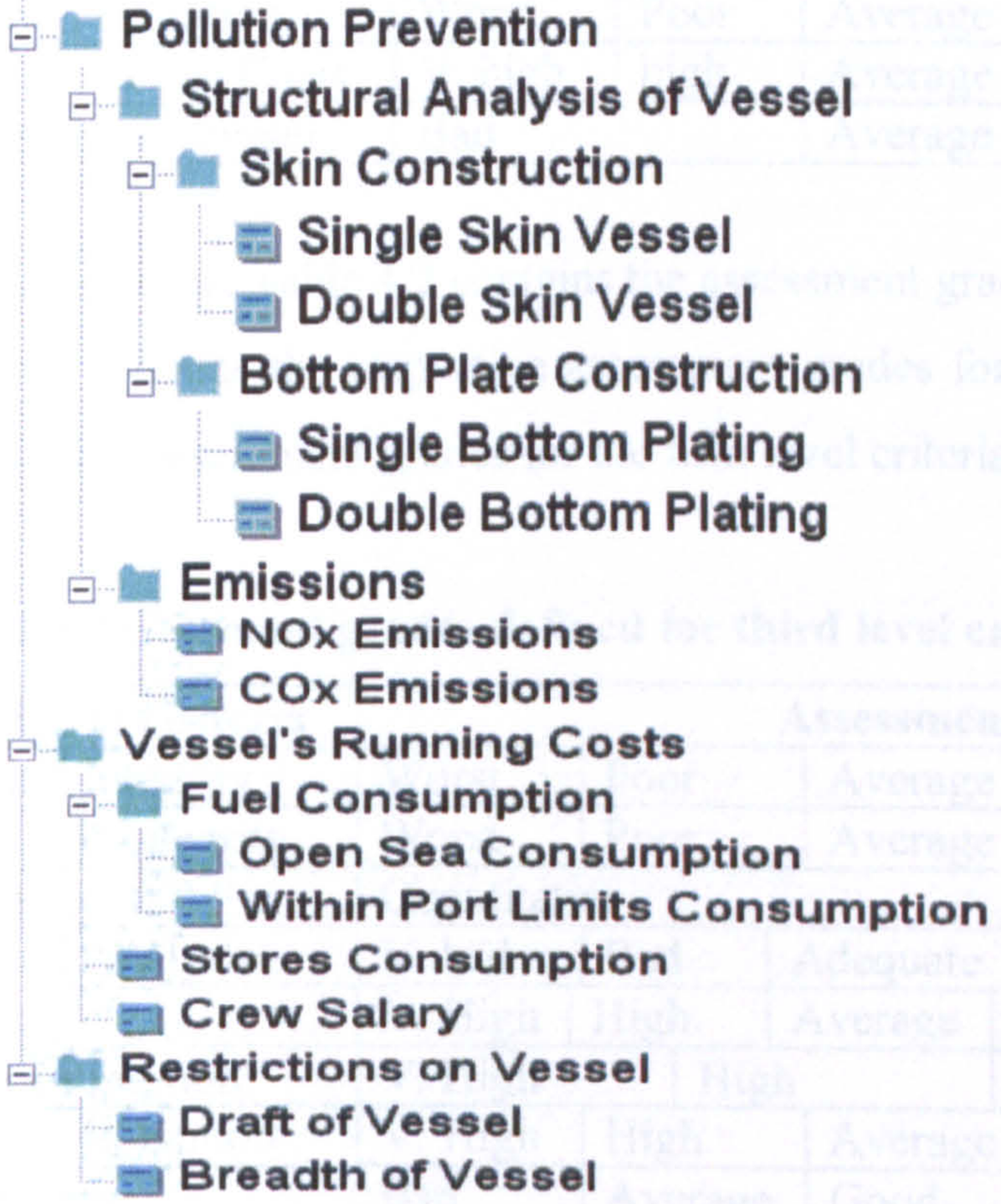


Figure 4.1. Main goal and sub-criteria levels

4.5.2 Step 2: Set the criteria levels and their respective assessment grades

Table 4.1 contains the main criteria used to assess each vessel at the second level. Each criterion is being characterized by a set of assessment grades under which each vessel is assessed accordingly. Similarly, for the second, third, fourth and fifth sub-level of criteria similar assessment grades are defined. Assessment grades are not the same in each criterion as each condition can be better assessed into grades based on the personal intuition and personal preferences of the decision maker. In the case that a criterion can be evaluated in a quantitative manner, then no assessment grades are needed. The decision maker will be able to assign upper and lower limits within the criterion or, in other cases just an arithmetic value will be substantial to complete the evaluation of the criterion. For example, the age of the vessel is assessed into grades with the aid of a maximum and a minimum arithmetic limit of years.

Table 4.1 Assessment grades defined for second level criteria

Main criteria	**Assessment Grades**					
Integrity	V. bad	bad	Average	Good	V. good	
Pollution Prevention	Worst	Poor	Average	Good	V. good	Excellent
Vessel's Running Costs	V. high	high	Average	Low	V. low	Minimum
Restrictions on Vessel	Bad		Average		Good	

In the same sense, Table 4.2 contains the assessment grades for the third level criteria, Table 4.3 contains the respective assessment grades for the fourth level criteria and Table 4.4 the assessment grades for the fifth level criteria.

Table 4.2 Assessment grades defined for third level criteria

Third Level Criteria	**Assessment Grades**				
Structural Integrity	Worst	Poor	Average	Good	Best
Mechanical Integrity	Worst	Poor	Average	Good	Best
Age (in years)	Quantitative				
Structural Analysis	V. bad	Bad	Adequate	Good	V. Good
Emissions	V. High	High	Average	Low	V. Low	Min.
Fuel Consumption	V. High	High	Average	Low		
Stores Consumption	V. High	High	Average	Low	V. Low	
Crew Salary	Bad	Average	Good	High	V. High	
Draft of Vessel	Quantitative					
Breadth of Vessel	Quantitative					

Table 4.3 Assessment grades defined for fourth level criteria

Fourth Level Criteria	Assessment Grades					
Bottom Shell Plate Thick.	V. Thin	Thin	Average	Thick	V. Thick	
Side Shell Plate Thickness	V. Thin	Thin	Average	Thick	V. Thick	
Main Engine Reliability	V. Bad	Bad	Average	V. Good	Excellent	
Aux. Engine Reliability	V. Bad	Bad	Average	V. Good	Excellent	
Cargo Handling Equip.	Poor	Average	Good	V. Good		
Skin Construction	V. Weak	Weak	Average	Strong	V. Strong	
Bottom Plate Construction	V. Weak	Weak	Average	Strong	V. Strong	
NOx Emissions	V. High	High	Low	V. Low		
Cox Emissions	V. High	High	Low	V. Low		
Open Sea Consumption	V. High	High	Average	Low	V. Low	Min.
Within Port Limits Cons.	V. High	High	Average	Low	V. Low	Min.

Table 4.4 Assessment grades defined for fifth level criteria

Fifth Level Criteria	Assessment Grades						
Loading Pumps, Valves	Malfunction	Very Unreliable	Unreliable	Average	Reliable	Very Reliable	Fully Operational
Discharge Pumps, Valves	Malfunction	Very Unreliable	Unreliable	Average	Reliable	Very Reliable	Fully Operational
Single Skin Vessel	V. Weak	Weak	Good	Strong	V. Strong		
Double Skin Vessel	V. Weak	Weak	Good	Strong	V. Strong		
Single Bottom Plating	V. Thin	Thin	Adequate	Thick	V. Thick		
Double Bottom Plating	V. Thin	Thin	Adequate	Thick	V. Thick		

4.5.3 Step 3: Evaluate each alternative based on the sub-sequent level criteria

Some of the criteria presented are of quantitative nature. In order to proceed to upper level transformation they are required to be converted using a method named utility theory. Take for example the sub-criterion "age in years" under the age group of criteria. Age as an upper level criterion is defined by five assessment grades (very bad, bad, average, good, excellent). "Age in years" is defined within numbers 3 and 15, with 3 being an excellent case scenario and 15 the worst-case scenario. In order to make the transformation the interval between 3 and 15 needs to be divided into certain intervals, adequate enough to match the assessment grades of the upper level.

Table 4.5. Transforming a quantitative sub criterion to the associated upper level qualitative criterion

Age	Very bad	Bad	Average	Good	Excellent
Age in years	15	12	9	6	3
Assessment grades	0.0	0.25	0.5	0.75	1

According to the information given in Table 4.5, Vessel 3 is said to have an "age in years" of 14. This value is 33.3% very bad and 66.6% bad, since it is in-between the values of 12 and 15. When a vessel is evaluated on "age", for example, sub-criteria such as structural and mechanical integrity along with their respective sub-criteria are additionally taken into consideration. All sub-attributes are assessed using subjective judgments. Due to the fact that a different number of grades are used for the upper level criterion and the sub criteria, the decision maker needs to establish basic rules concerning the sub level criteria and their association to the upper level criteria.

4.5.3.1 Rule based information transformation technique

The creation of unique evaluation grades is used in order to facilitate raw data collection. The grades defined will need to be transformed for assessment of a general attribute. The transformation takes place with the aid of the decision maker's expertise and knowledge. These transformations are called rules. Both qualitative and quantitative data can be easily transformed in this manner.

4.5.3.2 Qualitative data transformation technique

In assessment, different words may be used to describe equivalent standards. Such equivalence can be established using equivalence rules. For instance a "very unreliable" loading pump/valve, means that the quality of the pump/valve is "poor" as far as the operation is concerned. Then an evaluation grade "very unreliable" in loading pumps/valves assessment is said to be equivalent to a grade "worst" in quality assessment which characterises the mechanical integrity of each vessel. Similarly, if "unreliable" is equivalent to "poor", "normal" to "average", "reliable" to "good" and "very reliable" to "excellent", then it can be said that the set of grades {very unreliable, unreliable, normal, reliable, very reliable} in loading pump/valve assessment is equivalent to the set {worst, poor, average, good, excellent} which

defines the mechanical integrity of each vessel. Suppose each grade $H_{n,i}$ of a basic set H^i means a grade H_n of a general set H or more analytically,

$H = \{H_n, n=1,\ldots, N\}$.

$H^i = \{H_{n,i}, n = 1,\ldots, N_i\}$.

$H_{n,i}$ means H_n, with $n = 1,\ldots, N$.

Then with $N = N_i$ the basic set H^i is said to be equivalent to the general set H. Suppose H^i is equivalent to H and $N = N_i$. Then a general assessment would be: $S(e_i) = \{(H_n,\beta_{n,i}), n = 1,\ldots, N\}$ is said to be equivalent to a basic assessment $S^i(e_i) = \{(H_{n,i},\gamma_{n,i}), n = 1,\ldots,N_i\}$ if and only if $\beta_{n,i} = \gamma_{n,i}$, $n =1,\ldots,N$.

In general, it may not always be the case that $N = N_i$. It is also common that $H_{n,i}$ in H^i may not exactly mean any single grade in H but a number of grades in H to certain degrees. For instance a "very weak" double bottom plate might mean that the quality of the plate is between "worst" and "poor" in structural integrity. Generally, if a grade $H_{n,i}$ in H^i means a grade H_l in H to a degree of $a_{l,n}$ ($l = 1,\ldots, N$) with $0 \leq a_{l,n} \leq 1$ and $\sum_{l=1}^{N} a_{l,n} = 1$, then it can be said that $H_{n,i}$ is equivalent to $\{(H_l, a_{l,n}), l = 1,\ldots, N\}$.Taking this last equation as granted, a basic assessment $S^i(e_i)$ is said to be equivalent to an upper level more general assessment $S(e_i)$ if and only if $\beta_{l,i} = \sum_{n=1}^{N_i} a_{l,n}\gamma_{n,i}$ with $l = 1,\ldots,N$. The implementation of the transformation process is done through the development of matrix equations [Yang, 1999]. IDS software has this algorithm of transformation between different levels of assessment built in for the ease of the decision maker to speed up the decision-making process.

4.5.3.3 Quantitative data transformation technique

A quantitative basic attribute can be assessed using numerical values. In this case, equivalence rules also need to be extracted from the decision maker to transform a

value to an equivalent expectation so that the quantitative attribute can be aggregated in conjunction with other qualitative attributes. To carry out such a transformation, it is fundamental for the decision maker to provide rules relating each evaluation grade to a particular value. For instance, the actual numerical age of a vessel "3" may mean that the quality of the vessel is "excellent" as far as an overall condition of the vessel is concerned. In other words, the age of "3" years is equivalent to "excellent" overall condition. Similarly, age values like 6, 9, 12 and 15 years old may mean that a general overall condition of a vessel is "good", "average", "bad", "very bad" respectively. In general, suppose a value $h_{n,i}$ for an attribute e_i is judged to be equivalent to a grade H_n with $h_{n,I}$ meaning H_n ($n = 1,\ldots, N$). Without loss of generality suppose e_i is the "age" attribute, with $h_{n-1,I,}$ a smaller value being preferred more than $h_{n,I,}$ a larger value. Let $h_{N,i}$ be the largest feasible value and $h_{I,i}$ the smallest. Then a value h_j on e_j may be represented using the following equivalent expectation:

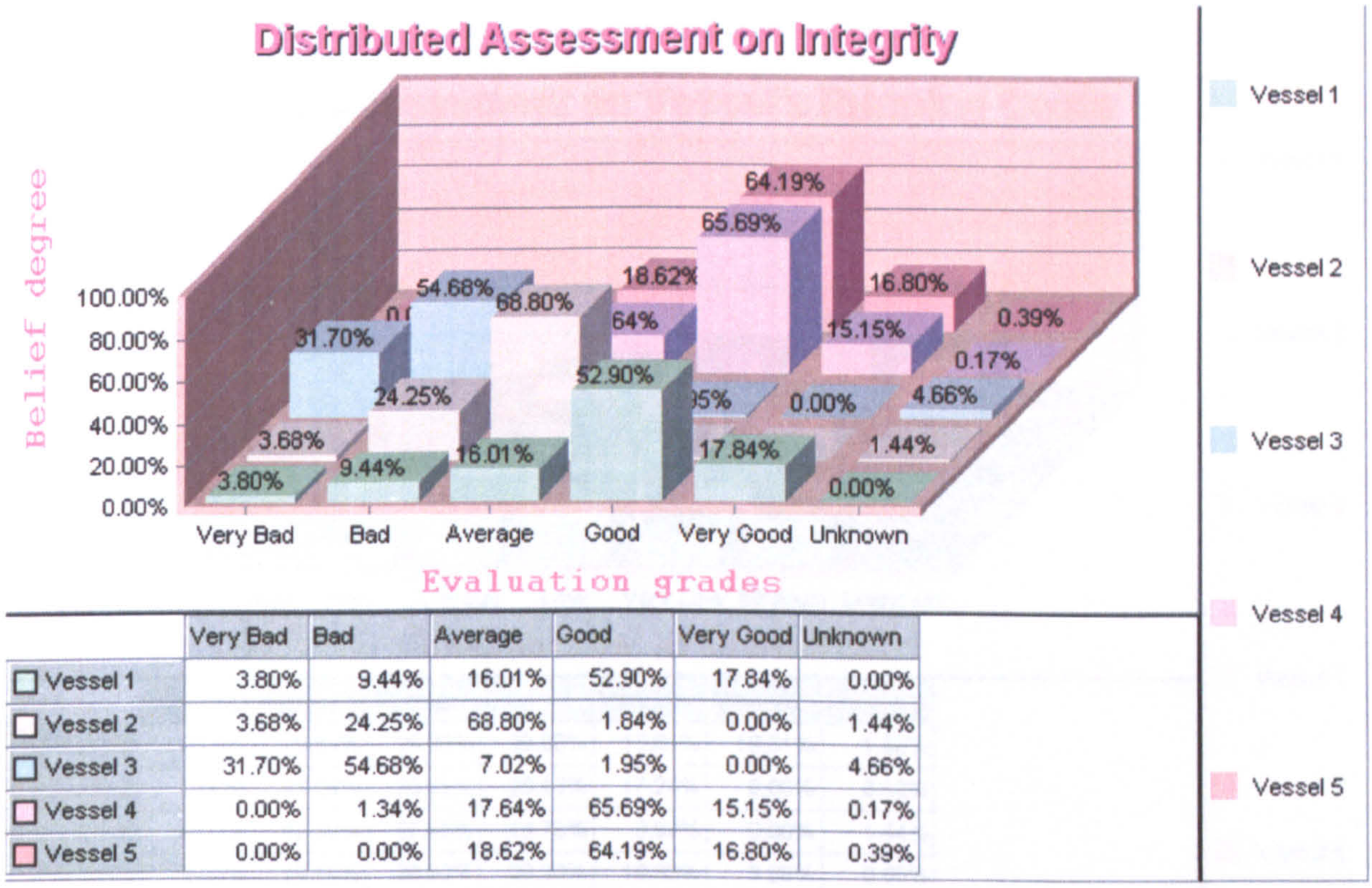
$S^i(h_j)= \{h_{n,i},\gamma_{n,j}), n =1,\ldots, N\}$ where $\gamma_{n,j} = (h_{n,i} - h_j) / (h_{n,i} - h_{n-1,i})$, $\gamma_{n-1,j} = \gamma_{n,j} - 1$ if $h_{n,i} \geq h_j \geq h_{n-1,i}$ [Yang, 1999].

As in the qualitative transformation, the development of matrix equations was necessary to characterise the transformation process. It is worth mentioning that when the term "equivalent transformation" is used in this chapter it means that the underlying utility of an original assessment is equal to that of its transformed assessment. This means that the completeness or incompleteness should be retained after the transformation between different utility planes takes place.

4.5.4 Step 4: Use the ER algorithm

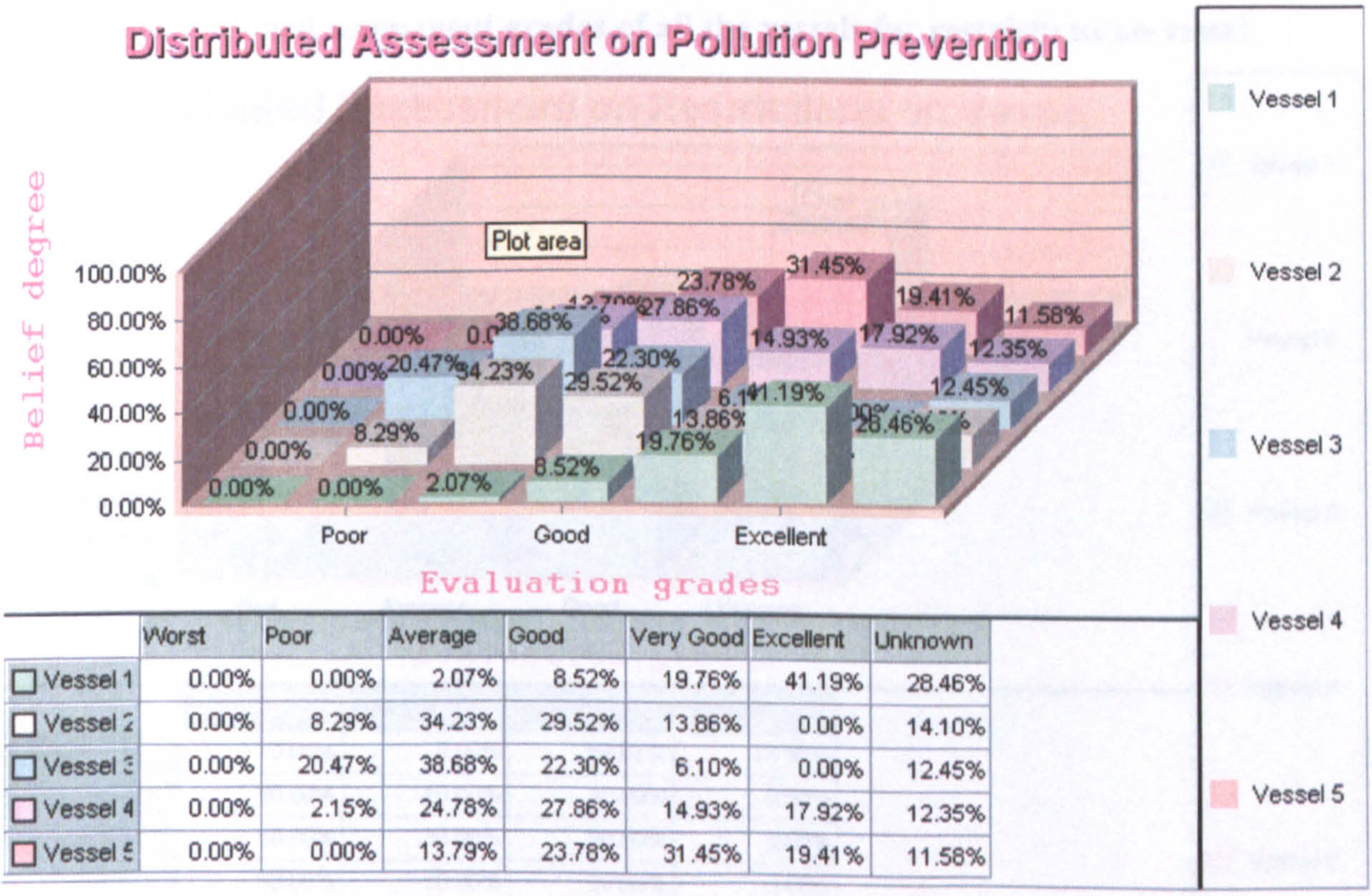
The assessment values given by the decision-maker are used within the IDS software and the aggregated results are extracted for the main criteria level (second level) and presented in Tables 4.6, 4.7, 4.8 and 4.9. The values within the cells indicate the degree of belief assigned to each assessment grade respectively. Tables 4.6, 4.7, 4.8 and 4.9 are also of outmost importance as an external observer can see the strong and week points of each one of the vessels selected in respect with the associated criteria. All values were derived from the IDS software.

Table 4.6 Combined assessment grades of all the vessels for integrity



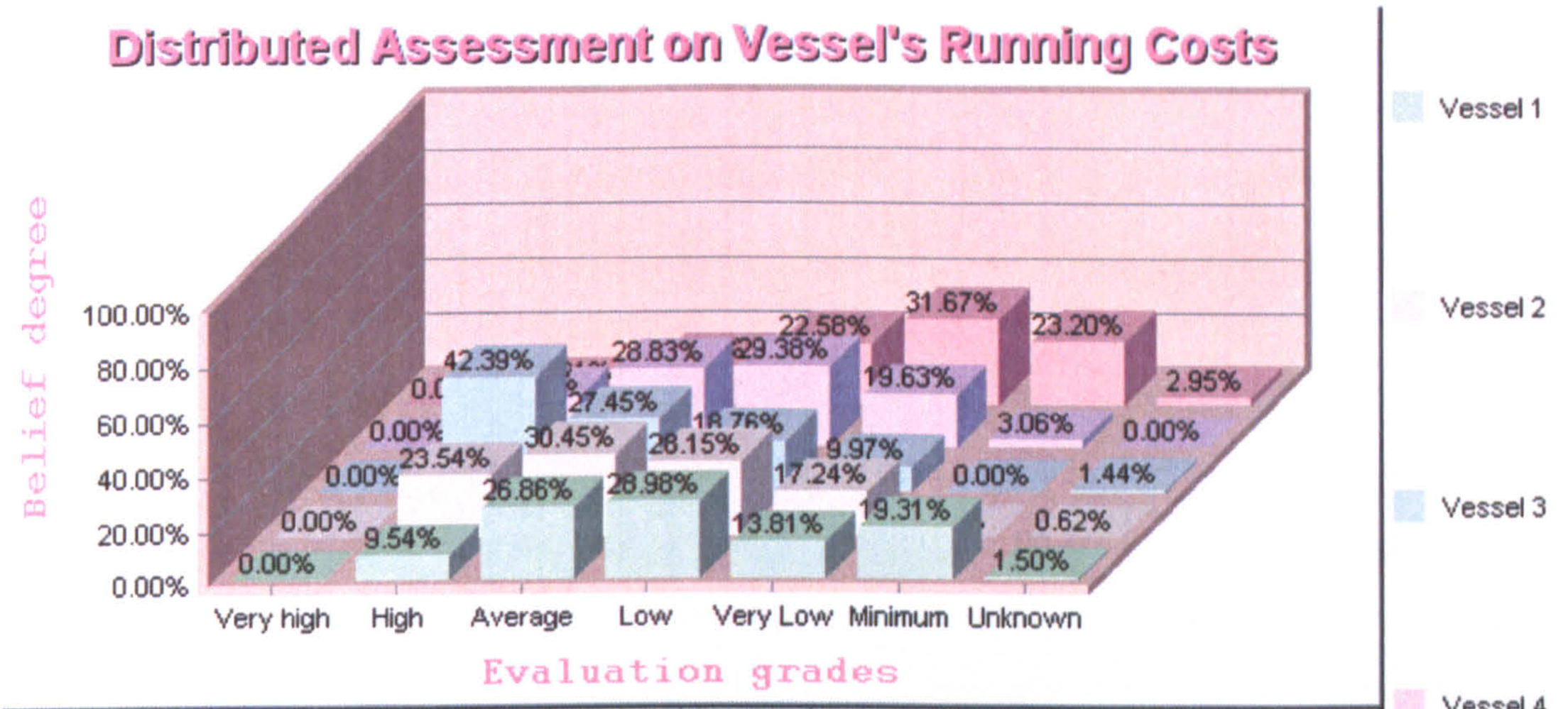
	Very Bad	Bad	Average	Good	Very Good	Unknown
Vessel 1	3.80%	9.44%	16.01%	52.90%	17.84%	0.00%
Vessel 2	3.68%	24.25%	68.80%	1.84%	0.00%	1.44%
Vessel 3	31.70%	54.68%	7.02%	1.95%	0.00%	4.66%
Vessel 4	0.00%	1.34%	17.64%	65.69%	15.15%	0.17%
Vessel 5	0.00%	0.00%	18.62%	64.19%	16.80%	0.39%

Table 4.7 Combined assessment grades of all the vessels for pollution prevention



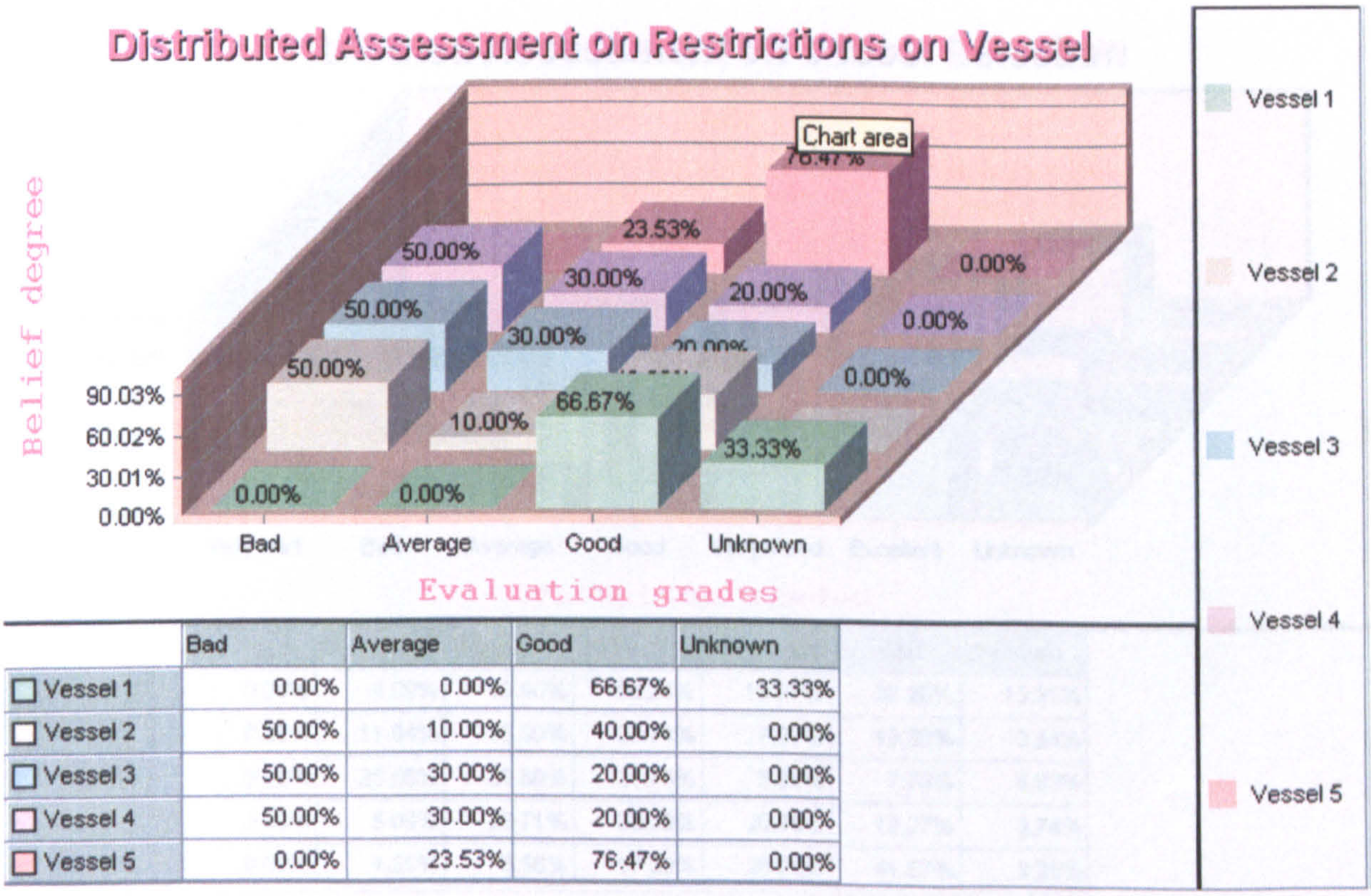
	Worst	Poor	Average	Good	Very Good	Excellent	Unknown
Vessel 1	0.00%	0.00%	2.07%	8.52%	19.76%	41.19%	28.46%
Vessel 2	0.00%	8.29%	34.23%	29.52%	13.86%	0.00%	14.10%
Vessel 3	0.00%	20.47%	38.68%	22.30%	6.10%	0.00%	12.45%
Vessel 4	0.00%	2.15%	24.78%	27.86%	14.93%	17.92%	12.35%
Vessel 5	0.00%	0.00%	13.79%	23.78%	31.45%	19.41%	11.58%

Table 4.8 Combined assessment grades of all the vessels for vessel's running costs



	Very high	High	Average	Low	Very Low	Minimum	Unknown
Vessel 1	0.00%	9.54%	26.86%	28.98%	13.81%	19.31%	1.50%
Vessel 2	0.00%	23.54%	30.45%	28.15%	17.24%	0.00%	0.62%
Vessel 3	0.00%	42.39%	27.45%	18.76%	9.97%	0.00%	1.44%
Vessel 4	0.00%	19.10%	28.83%	29.38%	19.63%	3.06%	0.00%
Vessel 5	0.00%	5.81%	13.79%	22.58%	31.67%	23.20%	2.95%

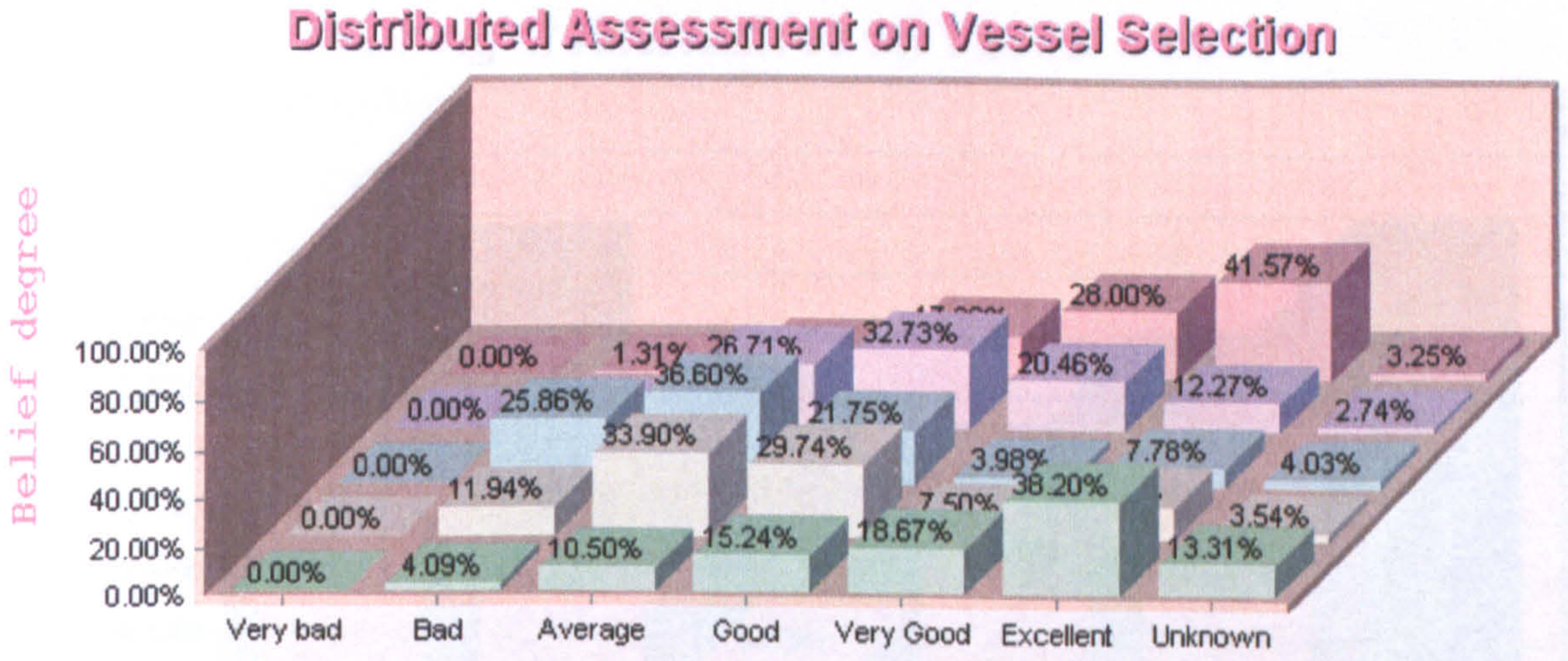
Table 4.9 Combined assessment grades of all the vessels for restrictions on vessel



	Bad	Average	Good	Unknown
Vessel 1	0.00%	0.00%	66.67%	33.33%
Vessel 2	50.00%	10.00%	40.00%	0.00%
Vessel 3	50.00%	30.00%	20.00%	0.00%
Vessel 4	50.00%	30.00%	20.00%	0.00%
Vessel 5	0.00%	23.53%	76.47%	0.00%

The assessments in Tables 4.6, 4.7, 4.8 and 4.9 need to be propagated to the top level. In doing this, the IDS software produces the results shown in Table 4.10. The numbers under each grade indicate the aggregated assessments (or degrees of belief) of the decision maker.

Table 4.10 The overall assessment of the vessels selected



	Very bad	Bad	Average	Good	Very Good	Excellent	Unknown
Vessel 1	0.00%	4.09%	10.50%	15.24%	18.67%	38.20%	13.31%
Vessel 2	0.00%	11.94%	33.90%	29.74%	7.50%	13.38%	3.54%
Vessel 3	0.00%	25.86%	36.60%	21.75%	3.98%	7.78%	4.03%
Vessel 4	0.00%	5.09%	26.71%	32.73%	20.46%	12.27%	2.74%
Vessel 5	0.00%	1.31%	8.56%	17.32%	28.00%	41.57%	3.25%

4.5.5 Step 5: Alternatives ranking, results and discussion

The best way to rank the vessels following Table 4.10 would be through their respective utility values generated by quantifying the assessment grades at the top level. This is due to the fact that there are close similarities in the values indicated in Table 4.10. IDS uses the concept of a utility interval to characterize the unassigned degree of belief (or unknown percentage). The ER algorithm produces a utility interval enclosed by the two extreme cases where the unassigned belief goes either to the least preferred grade (minimum utility) or goes to the most preferred grade (maximum utility).

A graphical representation of utility intervals is illustrated in Figure 4.2. The vessels are ranked based on the average utility but sometimes this can lead to mistaken results. In order to be able to say that one vessel is better than another, the preferred vessel's minimum utility must be equal or greater than the compared vessel's maximum utility. Therefore it is up to the decision maker to choose the boundaries of comparison. In Figure 4.2 the minimum utility value is represented by red colour, the average utility value by green colour and the maximum utility value by blue colour.

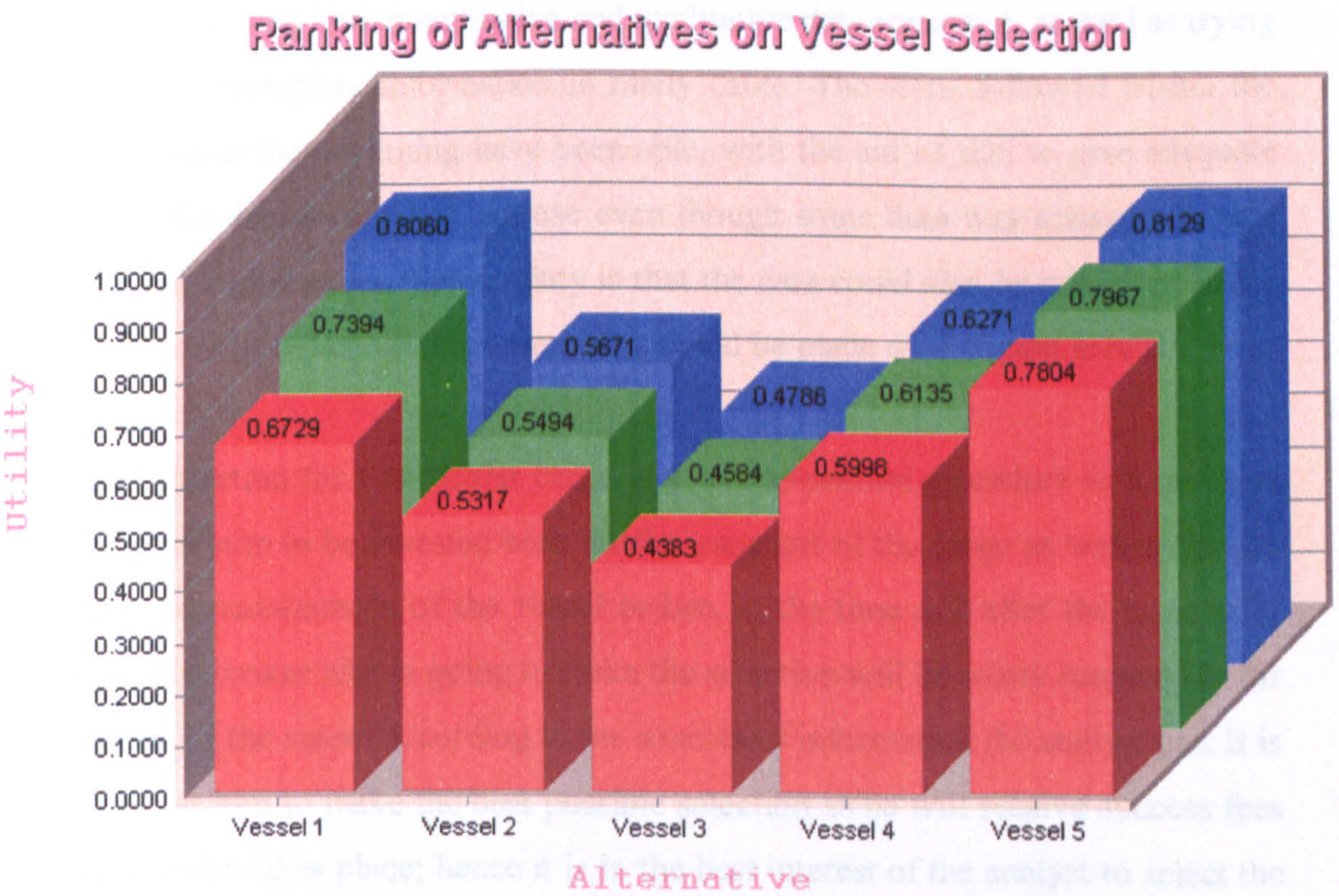


Figure 4.2 Ranking of vessel's utility values

In this example the comparison of minimum and maximum utility values will be used. Maximum and minimum utilities are given by IDS (see Appendix III section D).

Hence, from Figure 4.2, having found maximum and minimum utilities the average utility is calculated and used to rank the vessels within the selection process. The final ranking of vessels is as follows:

Vessel 5 is more preferred than Vessel 1, which is more preferred than Vessel 4, which is more preferred than Vessel 2, which in turn is more preferred than Vessel 3.

4.5.6 Step 6: *Conclusion*

In the example examined, an ER approach was used in order to tackle the problem of the vessel selection incorporating both qualitative and quantitative information. The information provided by the brokers in this instance, contained a small percentage of uncertainty in terms of the data provided, as seen in each of the main criteria, due to the factors influencing the proper gathering of data like incomplete report on the specified vessel by the independent surveyor that checked it. Nevertheless the problem of assessing both quantitative and qualitative data remained, as well as trying to cope with incomplete information in many cases. The steps followed within the framework set at the beginning have been able, with the aid of IDS to give adequate results that the decision maker can use even though some data was missing. A very important aid in this case of uncertainty is that the data could also be presented in the form of degrees of belief, so that assessment could be made on different levels.

The vessel selection for a particular cargo is a very important procedure as it involves a large capital sum to be invested both for the transport of the cargo as well as for the operation and maintenance of the vessel before, at the time and after the transfer of the cargo. The broker who is going to make the selection will be solely responsible for the selection of the vessel according to the sources of information the analyst has. It is imperative for him to make the best possible selection as he will receive success fees after the transfer takes place; hence it is in the best interest of the analyst to select the best possible vessel.

IDS software aids in cases of decision making as it enables the decision maker to have both tabular and graphical data at hand to make any necessary comparisons. The combination of the usage of IDS along with the case of a vessel selection can prove to be extremely useful as vessel selections are common in a weekly basis within the marine industry. It can provide the appropriate foundation which can be adjusted to any type of vessel with minor modifications and eventually provide a better comparison tool. The results produced from IDS match to a great extend the initial descriptions and assessment data used for each one the vessels in question, thus validating the ranking procedure.

CHAPTER 5: MARINE SAFETY ASSESSMENT AND BAYESIAN NETWORKS

5.1 Introduction

Bayesian networks (BNs) are a class of probabilistic models with strong connections to graph theory. Initially their main usage was to back up logical statements based on deterministic production rules. The immediate advantage is that each variable may have more values (also named states) than the traditional true and false and not all relations have to be deterministic.

BNs have already been extensively used in areas away from the marine industry such as artificial intelligence. Additionally, Microsoft uses BNs in order to operate the troubleshooting section of Windows [Microsoft, 2003]. The need for increased safety levels is more than obvious throughout the last 10 years. Engineering systems are becoming increasingly advanced and complex, creating the need for appropriate data and reliability logging.

Most marine engineering systems utilise the aid of sensors in different points of operation in order to record operational and reliability figures. The databases created using the readings taken from the sensors are invaluable because if they are combined with appropriate risk estimation methods, they can reduce the probability of hazards and failures within an engineering system. As systems are more complex, the engineers are required to analyse them as accurately as possible [Wang et al, 1996]. Conventional risk estimation techniques like fault tree analysis and event tree analysis use the conventional work / fail states to describe the function of an engineering system. This is not adequate, as a component or even the system itself can be governed by a number of states exceeding work and fail. This requires the use of a method, which can provide credible results in such a manner, which will make them easily presentable as well as being able to update the model built with new data without having to re-build it from the beginning. BNs can provide this tool to accommodate such a need [Frühwirth, 1993]. They are flexible enough to be combined with other risk estimation techniques, and at the same time being able to deal with both quantitative and qualitative data, and allow an easy data update, consistent throughout the whole model.

5.2 Background theory/definitions.

A BN consists of a set of nodes and a set of directed arcs. Each node represents a probability value and each arc indicates the dependence between the probabilities. In probabilistic reasoning, random variables (abbreviated, r.v) are used to represent events and/or objects in the world. By making various combinations to these r.v, any state can be modelled [Jensen, 1993]. Thus, this will involve computing joint probabilities of the given r.v. Unfortunately, the task is nearly impossible without additional information concerning relationships between the r.v. In the worst case scenario, the probabilities of every node combination should be readily available, which eventually would be very hard to calculate.

On the other hand, consider the chain rule as follows:

P(A1, A2, A3, A4, A5) = P(A1 | A2, A3, A4, A5) P(A2 | A3, A4, A5) P(A3 | A4, A5) P(A4 | A5) P(A5).

Bayesian networks take this process further by making the important observation that certain r.v. pairs may become uncorrelated once information concerning other r.v. is known [Pearl, 1988]. More precisely, the following independence condition may be applied:

P(A | C1, ..., Cn, U) = P(A | C1, ..., Cn) for some collection of r.v U. This can be interpreted as saying that A is determined by C1, ..., Cn regardless of U.

Combined with the chain rule, these conditional independencies allow us to replace the terms in the chain rule with the smaller conditionals. Thus, instead of explicitly keeping the joint probabilities, all we need are smaller conditional probability tables, which can then be used to compute the joint probabilities.

5.3 Inference

There are two types of computations performed with Bayesian Networks: belief updating and belief revision [Pearl, 1988]. Belief updating concerns the computation of probabilities over random variables, while belief revision concerns finding the maximally probable global assignment. Model update is performed in accordance with observations using Bayes rules [Bayes, 1989]. For random variables X1 and X2, Bayes rules state:

$$P(X1 \mid X2) = P(X2 \mid X1)\, P(X1) / (\sum_{all\_i} P(X2 \mid X1 = x_i)\, P(X1 = x_i)) \qquad [5.1]$$

Assume X2 is observed to be in state x_j. Applying [5.1] to each state of X1 the probability distribution $P(X1 \mid X2 = x_j)$ is computed as follows:

$$P(X1 \mid X2 = x_j) = P(X2 = x_j \mid X1)\, P(X1) / (\sum_{all\_i} P(X2 = x_j \mid X1 = x_i)\, P(X1 = x_i)) \qquad [5.2]$$

Computations like [5.1] and [5.2] can be performed for larger networks and the model allows exploitation of the way to answer queries and to investigate different scenarios. Belief revision can be used for modelling explanatory/diagnostic tasks. Basically, some evidence or observations are given, and the task is to come up with a set of hypotheses that together constitute the most satisfactory explanation/interpretation of the evidence at hand. This process has also been considered abductive reasoning in one form or another [Hobbs et al, 1988], [Shanahan, 1989], [Peng & Regia, 1990], [Santos, 1994] and [Charniak et al, 1994].

Although performing belief revision and updating (even approximating methods) have been shown to be quite hard [Dagum & Luby, 1993] special network topologies contain certain algorithms that perform well, such as junction trees [Pearl, 1988]. Various approaches to reasoning with Bayesian Networks include stochastic simulation, integer programming, and message passing. In this chapter focus will therefore be exclusively on algorithms based on junction trees.

5.4 Decision and junction trees

5.4.1 Decision trees and decision problems

Any case which requires choices to be made among alternative courses of action with uncertain consequences is described as a decision problem, whose structure is determined by three basic elements [Jensen, 1993]:

1. A set $\{a_i, i \in I\}$ of available actions, one of which is to be selected.
2. For each action a_i, a set $\{E_j, j \in J\}$ of uncertain events describing the uncertain outcomes of taking action a_i.
3. Corresponding to each set $\{E_j, j \in J\}$, a set of consequences $\{c_j, j \in J\}$.

Suppose action a_i is chosen; then one and only one of the uncertain events E_j, $j \in J$, occurs and leads to the corresponding consequence c_j, $j \in J$. In such cases, the decision problem can be represented schematically by means of a decision tree as seen in Figure 5.1.

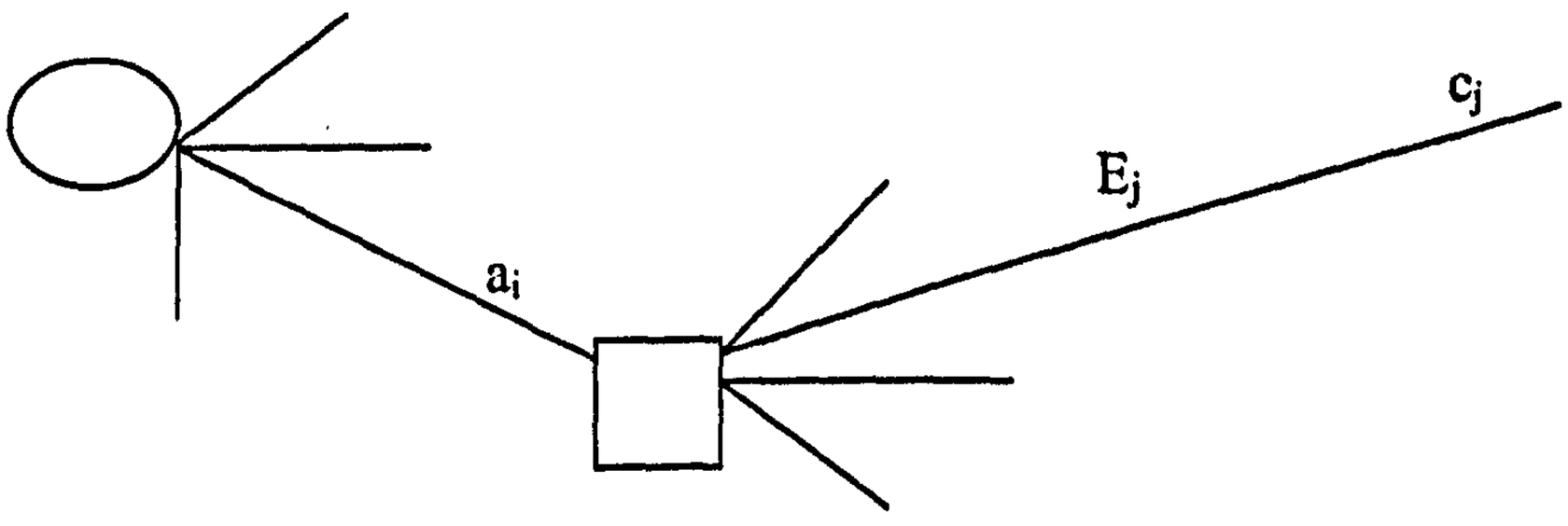


Figure 5.1 Decision tree

The circle represents a decision node, where the choice of an action is required. The square represents an uncertainty node where the outcome is beyond our control. Following the choice of an action and occurrence of a particular event the branch leads to the corresponding consequence. It becomes clear from the decision tree representation that identification of any a_i, $i \in I$, can be done using the combination of $\{E_j, j \in J\}$ and $\{c_j, j \in J\}$. This means that choosing a_i as an optimised solution for the uncertain scenario labelled by the pairs (E_j, c_j), $j \in J$, it is possible to write $a_i = \{c_j \mid E_j, j \in J\}$.

5.4.2 Junction trees

Extending the decision tree into more complex situations, the junction tree is born [Jensen & Dittmer, 1994]. It is a graphical representation of the model dealt with. The nodes of the junction tree are called cliques as each consists of a set of variables from the original network (decision tree). When there are loops in the BN, local propagation will not work, because of double counting evidence. In fact, local propagation is correct if and only if the graph is triangulated, i.e., there are no cordless cycles containing a number of nodes (more than 4). Intuitively, triangulation connects together those nodes that feature in a common term when summing out. The order of summing terms out is equivalent to the elimination order used to triangulate the graph. Finding an order that minimises the sum of the clique size (which determines the computational complexity) is not particularly hard. The maximal cliques in the triangulated graph are the clusters, which can be joined together to form a junction tree. This has the property that if x is a member of junction tree nodes i and j, then x must be a member of every node on the path between i and j. This property (called the junction tree property) ensures that local propagation of information leads to global consistency. The triangulation procedure is only defined for undirected graphs. It is not sufficient to simply ignore the direction of the arcs in the original BN, since directed and undirected graphs have different independence properties [Jensen & Dittmer, 1994]. In particular, parents who share a common child might not be independent in a directed graph but will be independent in an undirected graph unless the parents are connected (otherwise, the child would separate the parents). Hence we must first "moralize" the BN, i.e., connect together "unmarried" (non-connected) parents who share a common child, and then drop the directionality on the arcs. After moralization, it is possible to proceed with triangulation as before. Once we have the (undirected) junction tree structure, we can either root it, thus converting it into a tree-structured BN, define the cliques for the new cluster nodes, and apply Pearl's junction tree algorithm [Pearl, 1988], or we can leave it as an undirected tree, define potential functions for the new cluster nodes, and apply a local message algorithm specifically designed for undirected graphs. The latter approach is what is usually meant when people talk of the junction tree algorithm. The undirected formulation is slightly simpler because it is symmetric. The methodology used to construct a junction tree is based on the algorithm created by Lauritzen and Spiegelhalter [Lauritzen & Spiegelhalter, 1988] and is described as follows:

The moralisation step connects all variables in the set $pa(x_i) \cup x_i$, where pa is the parent variables of x_i.

1. Deletion. Delete the directions on all arcs.
2. Triangulation. The cliques are identified by successive elimination of the variables as follows; a variable may be eliminated if all neighbours are mutually connected. The eliminated variable and its neighbours then form a clique. If the neighbours are not mutually connected, fill-in links are added to the graph to obtain full connectivity of the variables in the clique. If at any point a clique is formed so that it consists of a subset of an existing clique, it should be deleted. When all variables are eliminated, all cliques are identified. The undirected graph consisting of all the initial variables and all the links is called a triangulated graph.
3. The cliques are connected so that the junction tree property is obtained.

In order for a junction tree (JT) to be valid it should follow the JT property [Lauritzen & Spiegelhalter, 1988]. This states that all cliques on the path between two cliques A1 and A2 for example must contain the intersecting set of variables A1 $\cap$ A2. This set S = A1 $\cap$ A2 is called the separator set. An example is shown at Figure 5.2 (a),(b),(c),(d) of how a JT is formed

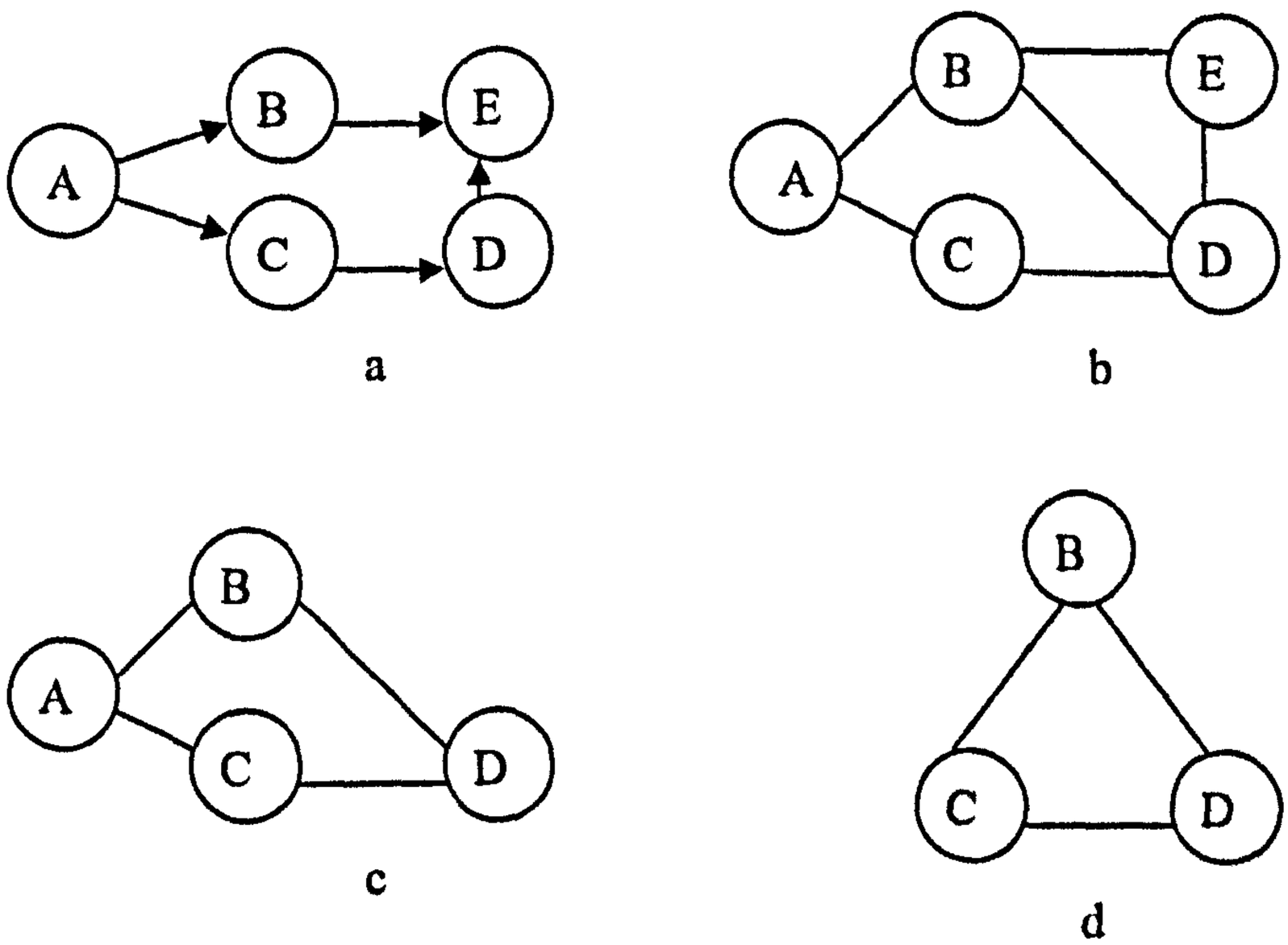


Figure 5.2 Formation of junction tree

In Figure 5.2 (a) The initial decision tree has taken the proper form of a BN.

In Figure 5.2 (b) The arcs are deleted and parent variables (B and D leading to E) are connected.

In Figure 5.2 (c) The elimination process begins by deleting the variable which has common parent variables. Hence E is eliminated. E belongs to the clique of {BDE} and the remaining graph appears as shown above.

In Figure 5.2 (d) Variable A is chosen to be eliminated, thus forming the clique consisting of {A,B,C}, and the remaining variables form the last clique of {B,C,D}. Equally to A, any other variable could have been eliminated, as long as the junction tree property is maintained.

The cliques formed were {A,B,C}, {B,D,E}, {B,C,D}. The next step is to arrange them in such a way that the JT property is maintained. This means that a common separator set should exist in between the first and the last clique. Taking the first combination sequence of {A,B,C}, {B,D,E} and {B,C,D} there is {A,B,C}$\cap$ {B,C,D} = {B,C} which is not contained in the intermediate clique. Similarly, {B,C,D} $\cap$ {B,D,E}= {B.D} which is not included in the intermediate set. Looking at {B,D,E}$\cap${A,B,C} = {B} which is included in the intermediate clique. This means that the last tree satisfies the JT property.

5.5 Marginalisation

From the updated joint table the marginal distributions of each individual variable may be found by summation over all other variables. This is known as sum-marginalisation [Vellido, & Lisboa, 2001]:

$P(x_i) = \sum_{x_i \in U} P(U)$, where P(U) is the joint probability table derived by the product of all clique tables divided by the product of all separator tables. These are created by the insertion of probability tables to the cliques and their respective separators tables as soon as the junction tree is constructed.

Sum-marginalisation has the property that the order in which the individual variables are marginalized out does not change the result. The same operation may be performed when a finding has been inserted.

It is seen that all marginal probability distributions conditional on the given evidence may be obtained from the updated joint distribution. In a similar manner, a finding may be inserted in a clique table. Similarly, any variable or set of variables may be marginalised out.

5.6 Message passing

For large networks, Bayes' simple rule becomes unruly, therefore it is necessary to use a message-passing algorithm. The sum-product algorithm is a general form of the forward-backward algorithm [Kschischang, 2000]. It attempts to compute various marginal functions associated with the global function in a factor graph. Once one or more nodes have been observed to be of some value, messages are passed inward from an arbitrary set of nodes at the edge of a graph. When they reach an edge, their direction is reversed, and when they reach their origin, they are absorbed.

The first messages are passed from some set of single connected function nodes to the variable nodes that they depend upon. No computation is necessary in this step because the messages are simple identity messages that specify the knowledge stored in the function that creates them. The variable nodes then pass the same identity message along to the next function node that they are connected to. These steps are marked 1 and 2 respectively in Figure 5.3.

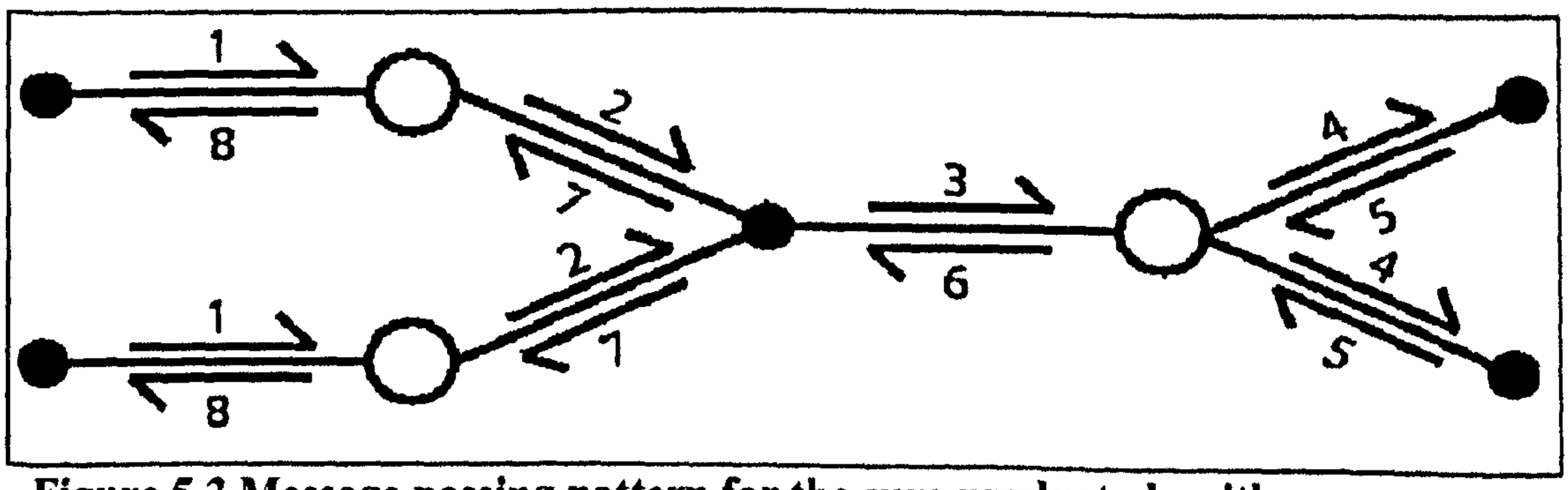


Figure 5.3 Message passing pattern for the sum-product algorithm

Assuming that a finding f (f is a form of a likelihood vector taking values between 0 and 1), is to be inserted into a clique A, the value of f is computed, then multiplied by P(U). The message towards clique B is computed by marginalising out all other variables than those of the separator. The updated separator table remains the same no matter if the message was sent from 1 to 2 or from 2 to 1. Each message is received according to that same argument. The sum of these computations becomes the message to the next variable, marked 3 in Figure 5.3. Step 4 is the same as step 2. In step 5, the functions at the periphery of the graph reverse the flow of messages, performing the same marginalisation as in step 3. Steps 6, 7, and 8 follow the same procedure, in the reverse path.

5.7 Max-propagation

Max-propagation is an alternative type of propagation by which, given evidence on one or more variables, the most probable configuration of the rest of variables in the network can be identified. A configuration is a set consisting of exactly one state from each variable. Max-propagation thus identifies the configuration which best explains the observed evidence. It can be compared to a minimum cut-set obtained from a fault tree.

The configuration of maximum probability may be identified by a procedure based on message passing in the junction tree [D'Ambrosio, 1999]. Instead of the message type described above, max-messages are computed by replacing summation with maximisation. This creates a message, which is composed by the maximum probability of each state along a certain path. Exactly as before, the message needs to be collected and distributed along the nodes of the BN.

5.8 Finding the M most likely configurations

Once the most probable configuration of variables (M_1) has been identified by the method of max-propagation, the second most probable configuration (M_2) can be found by a procedure, which again is based on insertion of evidence and subsequent max-propagation. The key is that the second most likely configuration will differ from the most likely in at least one of the variables. First an ordering of the number of

variables in the network is formed. The procedure is to insert evidence and perform max-propagations N (N=1, 2, 3,..., N) times. All propagations should defer for at least one variable between them. The algorithm created by Nilsson [Nilsson, 1998], is considered to be the most effective in this type of calculation but it was not yet incorporated into the Hugin software [Hugin expert, 2003].

5.9 D-separation

Pearl, Geiger and Verma, computer scientists at UCLA working on the problem of storing and processing uncertain information efficiently in artificially intelligent agents, solved this mathematical problem in the mid 1980s [Pearl, 1996], [Geiger & Heckerman, 1995], [Verma, 1993]. Pearl and his colleagues realized that uncertain information could be stored much more efficiently by taking advantage of conditional independence, and they used directed acyclic graphs (graphs with no loops from a variable back to itself) to encode probabilities and the conditional independence relations among them. D-separation was the algorithm they invented to compute all the conditional independence relations entailed by their graphs [Pearl, 1988]. Spirtes, Glymour and Scheines, working on the problem of causal inference at the Philosopy Department at Carnegie Mellon University in the late 1980s and early 1990s, connected the artificial intelligence work of Pearl and his colleagues to the problem of testing and discovering causal structure in behavioural sciences [Spirtes et. al, 1993]. Eventually, Pearl and his colleagues proved many more interesting results about graphical models, what they entail, and algorithms to discover them. In 1994, Spirtes proved that d-separation correctly computes the conditional independence relations entailed by cyclic directed graphs interpreted as linear statistical models [Spirtes, 1994], and in the same year Richardson [1994] developed an efficient procedure to determine when two linear models, cyclic or not, are d-separation equivalent. In 1996, Pearl proved that d-separation correctly encodes the independencies entailed by directed graphs with or without cycles in a special class of discrete causal models [Pearl, 1996]. Also in 1996, Spirtes et. al, proved that d-separation works for linear statistical models with correlated errors. Therefore, it should be obvious that d-separation is a central idea in the theory of graphical causal models.

The "d" in d-separation and d-connection stands for dependence. Thus if two variables are d-separated relative to a set of variables Z in a directed graph, then they

are independently conditional on Z in all probability distributions such a graph can represent. Roughly, two variables X and Y are independent conditional on Z if knowledge about X gives you no extra information about Y once you have knowledge of Z. In other words, once Z is known, X adds nothing to what is known about Y.

A path is active if it carries information, or dependence. Two variables X and Y might be connected by lots of paths in a graph, where all, some, or none of the paths are active. X and Y are d-connected, however, if there is any active path between them. Let's examine on what makes a path active or inactive. A path is active when every vertex on the path is active. Paths, and vertices on these paths, are active or inactive relative to a set of other vertices Z. First let's examine when things are active or inactive relative to an empty Z. To make matters concrete, consider all of the possible undirected paths between a pair of variables A and B that go through a third variable C.

1)	A	-->	C	-->	B
2)	A	<--	C	<--	B
3)	A	<--	C	-->	B
4)	A	-->	C	<--	B

The first is a directed path from A to B through C, the second a directed path from B to A through C, and the third a pair of directed paths from C to A and from C to B. If these paths are interpreted causally, in the first case A is an indirect cause of B, in the second B is an indirect cause of A, and in the third C is a common cause of A and B. All three of these causal situations give rise to association, or dependence, between A and B, and all three of these undirected paths are active in the theory of d-separation. If the fourth case is interpreted causally, then A and B have a common effect in C, but no causal connection between them. In the theory of d-separation, the fourth path is inactive. Thus, when the conditioning set is empty, only paths that correspond to causal connection are active. A path is active in the theory of d-separation just in case all the vertices on the path are active. Since C is the only vertex on all four paths between A and B, it must be active in the first three paths and inactive in the fourth. In the first three, C is a non-collider on the path, and in the fourth C is a collider. When the conditioning set is empty, non-colliders are active. Non-colliders transmit information (dependence). When the conditioning set is empty, colliders are inactive.

Colliders do not transmit information (dependence). Now consider what happens when the conditioning set is not empty. When a vertex is in the conditioning set, its status can be either active or inactive. Consider the four paths above again, but now let's consider the question of whether the variables A and B are d-separated by C.

1)	A	-->	C	-->	B
2)	A	<--	C	<--	B
3)	A	<--	C	-->	B
4)	A	-->	C	<--	B

In the first three paths, C is active when the conditioning set was empty, so now C is inactive on these paths. To fix intuitions, it is necessary to interpret the paths causally. In the first case the path from A to B is blocked by conditioning on the intermediary C, similarly in case 2, and in case 3 there is conditioning on a common cause, which make the effects independent.

In the fourth case, C is a collider and thus inactive when the conditioning set is empty. This can also be made intuitive by considering what happens when looking at the relationship between two independent causes after conditioning on a common effect. Consider the following example, in which there are two independent causes of a car refusing to start: having no gas and having a dead battery.

dead battery --> **car won't start** <-- no gas

The fact that the battery is charged means nothing about whether there is gas, but the statement that the battery is charged after the car won't start means that the gas tank must be empty. Therefore, independent causes are made dependent by conditioning on a common effect, which in the directed graph representing the causal structure is the same as conditioning on a collider. David Papineau [Papineau, 1985] was the first to understand this case, but never looked at the general connection between directed graphs interpreted causally and conditional independence.

5.10 Proposed methodology

The system described, an LPG reliquefaction plant, imposes a high risk factor as there are a number of components involved which, if not operated properly, can result in probable destruction of property, injuries or even fatalities. A safety framework incorporating the BN approach within the plant operation is presented in this section. The proposed framework consists of the following steps:

Step 1: Analyse the engineering system and make the logical determinations between the factors (components) involved in each BN. Assign appropriate nodes and directional arcs to model the operation of the network.

Step 2: The constructed BN is further developed into a junction tree. The junction tree follows a certain order of construction:

- Moralisation. The moralisation step connects all variables in the set $pa(x_i) \bigcup x_i$ for all i, with $pa(x_i)$ being the set of parent variables of the variable x_i.

- Deletion. The direction of all arcs is deleted from the BN.

- Triangulation. The cliques are identified by successive elimination of the variables in the following way. A variable may be eliminated if all its neighbours are mutually connected. The eliminated variable and its neighbours then form a clique. If the neighbours are not mutually connected, fill-in links are added to the graph to obtain full connectivity of the variables in the clique. If at any point a clique is formed so that it consists of a subset of an existing clique, it is superfluous and should be deleted. The undirected graph consisting of all the initial variables and all the links (both original and fill-ins) is called a triangulated graph. The formed cliques are then connected in order to form the junction tree.

Step 3: Before insertion of evidence (failure rates/probabilities of failure), the separator table needs to be found between two adjacent cliques containing the common information for both of the cliques. For example, for cliques Y and Z, this is done by performing a sum-marginalisation of the separator set $S = Y \bigcap Z$ so that the

separator table $t_s = P(S)$ contains the common information about Y and Z as seen in the theory section.

Step 4: Once the junction tree has been established as well as the sum-marginalisation of the separator tables, the assignment of states and probability tables/evidence (containing the failure rates/probabilities of failure from the failure databases) may commence with the aid of Hugin software [Hugin expert, 2003]. Each clique is dealt separately. The principles of message passing between two nodes within a BN are applied in this step. It is assumed that failures follow an exponential distribution within a preset time t=1,000,000 working hours. The value of t was selected as 1,000,000 hours in order to match the criteria established by well known failure databases such as the OREDA database published by DNV which uses the same period of time for estimation of the component's failure probabilities.

Step 5: Having the evidence (failure rates/probabilities of failures) on one or more variables, the most probable configuration of the rest of variables in the network can be identified. A configuration is a set consisting of exactly one state from each variable. Max-propagation is used to identify the configuration which best explains the observed evidence inserted in a BN's junction tree. The most probable configuration can be seen as a cut-set obtained from a fault tree analysis.

Step 6: Discussion of results obtained from Hugin software, and means of reducing risk to as low as reasonably practicable levels.

Step 7: Conclusion. Having obtained the results from the software as well as having the reliquefaction plant modelled by BN an overview of the process will be given stressing the advantages of using a technique such as Bayesian Networks for risk assessment.

Hugin software will be used for the computation of steps 4, 5 and 6. An analytical explanation of each step and how it is related to the test case given in the next section. Hugin software will produce the results concerning the most probable configurations of components within the reliquefaction plant.

5.11 Test case: Risk assessment of an LPG reliquefaction plant through the application of Bayesian Networks

5.11.1 The reliquefaction plant; functions and operation

Butane and propane, liquefied petroleum gases (LPG) cargoes were carried initially under pressure into tanks tested for 50 psi, from 1941 to 1959. In 1960, the manager of Shell company's French fleet realised that if the cargo was cooled, its density increased and more cargo could be carried in the same ship. Additionally, if this lower temperature could be reliably maintained at all times, the lower design pressure would permit a reduction in tank scantlings with appropriate savings in tank weight and cost. The efficiency of cargo handling has been increased over the years reaching today with the fully refrigerated LPG vessels capacities between 20,000 and 80,000 m^3.

With the exception of fully pressurized gas carriers, means must be provided to control cargo vapour pressure in the cargo tanks both during loading and passage. In the case of LPG and chemical gas tankers some form of reliquefaction plant is fitted. This plant is specifically designed to perform the following essential function [ISGOT, 2001]:

- To cool down the cargo tanks and associated piping before loading.
- To reliquefy the cargo vapours generated by flash evaporation, liquid displacement and boil-off during loading and return it to the cargo tanks.
- To keep the cargo at a temperature and pressure within the design limits of the cargo system during transport.

This test case is intended to demonstrate the application of Bayesian Networks to assess the probability of hazards imposed by the operation of a reliquefaction plant. Failures to the plant can result in loss of cargo, damage to property, injuries and even fatalities.

There are three main types of reliquefaction plants operating today [ISGOT, 2006], [LPG/C Melina, 1980]:

- The direct system:

Boil-off vapours from the cargo tank are drawn off by the compressor and compressed. The compression process increases the pressure and the temperature of the vapour allowing it to be condensed against seawater in the condenser. In the cargo condenser the gas is cooled and liquefied at a temperature of 5 to 10°C above the seawater temperature. The condensed liquid is then flashed back to the tank via a float-controlled expansion valve (Joule-Thompson valve). This cycle is suitable where pressures are relatively high as in the carriage of semi-refrigerated products (high boiling point cargoes).

- The indirect system.

Indirect cooling is used for cargoes, which cannot be compressed for chemical reasons. The boil-off passes from the tank under its own pressure to a condenser for better efficiency. The common refrigerants are hydrogen, helium and propane. The refrigerant from the cargo condenser is compressed and then condensed against seawater. The condensed liquid is returned to the bottom of the cargo tank by gravity. If the evaporator is arranged below the dome, a pump has to be installed for cargo liquid return.

- The cascade system.

This is the system that will be analysed with the aid of Bayesian Networks. A cascade system is a reliquefaction plant where the compressed cargo vapour is condensed by evaporation of a liquid refrigerant gas such as R22. The heat from the cargo evaporates the R22, which is compressed, condensed in a seawater-cooled condenser, and cooled by passage through an expansion valve. Today, this system is the most common cooling process for large fully refrigerated LPG ships. The main advantage of the cascade system of reliquefaction is that the same refrigerant is used for all cargoes, which means that a plant can be designed with the temperature of the seawater coolant as the only variable, and since the maximum temperature of the seawater likely to be encountered in service can be easily ascertained, it is not too difficult to design a plant capable of working within these conditions.

The maximum temperature of the cooling water for the plant is usually around 35°C, and it is very unlikely that warmer cooling water will be met in service. The cycle is also more efficient (better cooling effect), as the R22 (type of refrigerant) temperature in the cargo condenser can be below 0°C. Additionally, for more advanced types of ships which carry products whose critical temperatures are below that of seawater (like methane –162°C for example [Wikipedia, 2006]), the cascade or even double cascade system is the only method available.

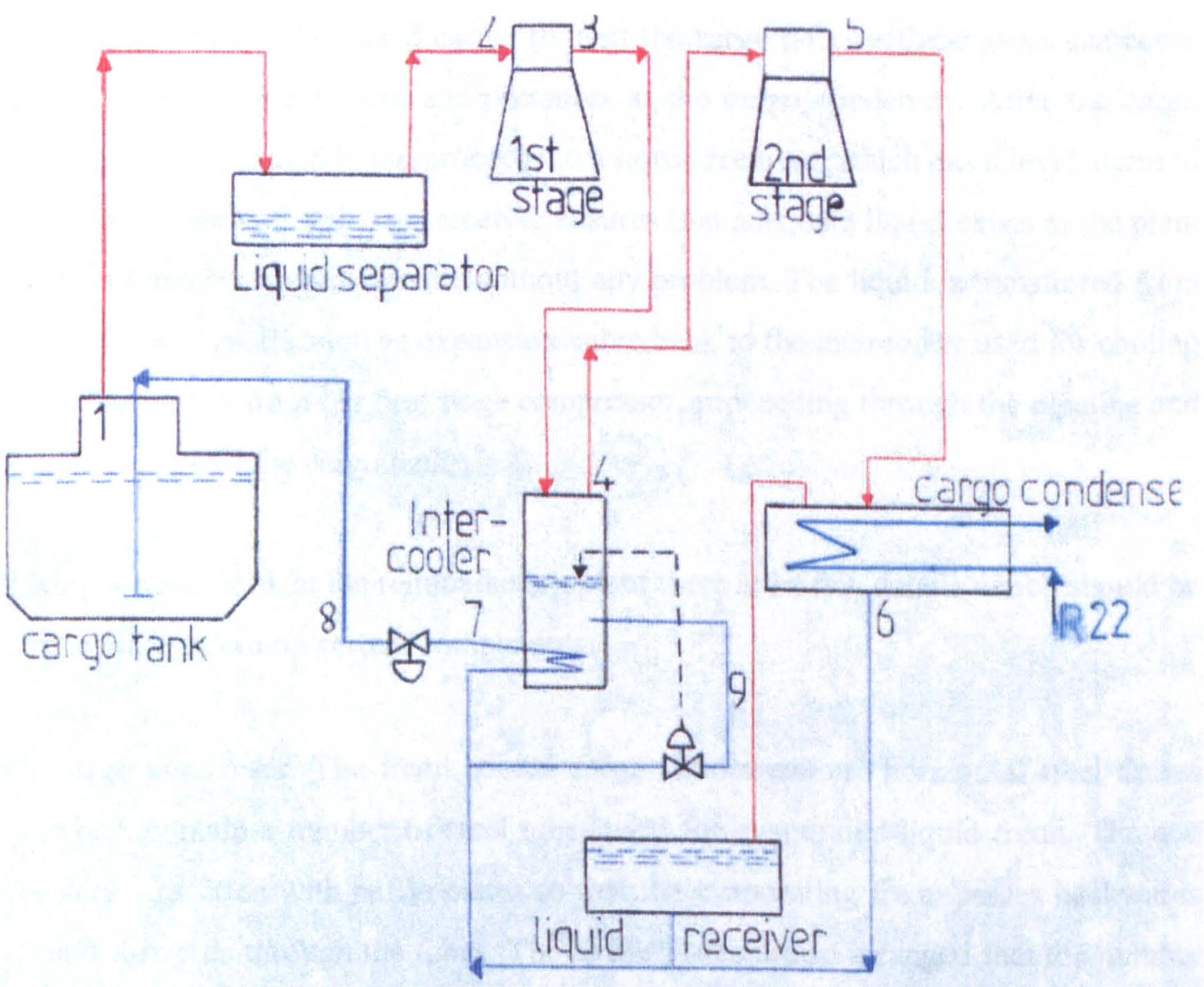


Figure 5.4 LPG reliquefaction plant

Examining Figure 5.4, the cargo carried in the LPG cargo tank is propane. Boil-off creates propane vapour, which is transferred out of the cargo tank by means of a suction pump. The vapour follows the vapour line and passes through a liquid separator, which is used to gather the liquid droplets contained within the vapour. This gathering takes place due to the fact that only vapour should be inserted into the compressor. As soon as all liquid is left in the separator, the remaining vapour is inserted to the first stage compressor. A filter is situated just before the suction of the compressor to collect any impurities in the vapour. The compressor has liquid high-

level alarms in case liquid is passed through the plant, which will be damaging to the compressor. The vapour leaving the first stage low-pressure compressor is passed from an intercooler for further cooling. The intercooler uses the condensed liquid at the end of the cycle as a refrigerating mean to the vapour. As soon as the temperature is brought down, the cooled-down vapour goes into a second stage high-pressure compressor. The vapour is then directed into a cargo condenser, which uses an external refrigerating network based on freon R22. Just above the condenser an uncondensed vapour-gathering chamber is situated. It is used to hold gases like nitrogen, which has been used earlier to inert the cargo tank, as these gases can cause extremely high temperatures and pressures at the cargo condenser. After the cargo condenser the saturated liquid proceeds to a liquid receiver, which has a level alarm to maintain a constant level. This receiver ensures that adequate liquid exists in the plant so that all machinery will operate without any problem. The liquid is transferred from the liquid receiver through an expansion valve back to the intercooler used for cooling down the vapour from the first stage compressor, proceeding through the pipeline and sprayed back into the cargo tank.

Taking a closer look at the reliquefaction plant there are a few details which should be mentioned concerning certain components:

- Cargo condenser: The freon cooled cargo condensers are horizontal steel drums which contain a number of steel tubes used for evaporated liquid freon. The end plates are fitted with baffle plates so that the evaporating freon passes backwards and forwards through the tubes. The baffle plates are so arranged that the number of tubes through which the freon passes is a geometric progression. That is, through three tubes in the first pass, nine on the return, twenty-seven in the third, eighty-one in the fourth and so on, so that the freon is being continuously expanded. The admission of liquid freon is controlled by a thermostatically controlled expansion valve located immediately outside the condenser.

- Cargo liquid receiver: The condensed liquid from the cargo condenser is collected in the liquid receiver. The level in the receiver operates a float valve governing the main valve in the liquid outlet pipeline. A hand operated by-pass valve is also fitted.

- Cargo intercooler: In the two-stage compressor, the discharge temperature of the first stage is so high that if the hot vapour was fed directly to the suction of the second stage, the high pressure discharge temperature would be excessive and the compressor would stop itself on the high pressure / high temperature cut-out. Therefore the temperature of the low-pressure discharge is reduced by spraying in the liquid from the condenser, which quickly evaporates and so cools the vapour before it passes to the second stage. The liquid injection is controlled by a float, which, via a controller, operates a valve permitting sufficient liquid to enter the inter-stage cooler to maintain a low level of liquid. If the level of the liquid rise, a float switch will stop the compressor to prevent liquid entering the suction. The high-pressure suction draws vapour from the top of the inter-stage cooler. A liquid droplet trap is placed between the inter-stage cooler and the compressor high-pressure suction to remove and liquid droplets. Any liquid collected in the trap, will be drained back into the inter-stage cooler. When the compressor stops, the drop in lubricating oil pressure operates a controller, which closes a valve and shuts off the liquid injected into the inter-stage cooler.

5.11.2 Analysis of steps incorporated in the methodology

Step 1: The reliquefaction system is analysed and appropriate BN(s) are constructed. The purpose of this step is to give a graphical representation using BNs, of the operation of the reliquefaction system and the way that its components influence one another. After the initial position of nodes and arcs Figure 5.5 is derived.

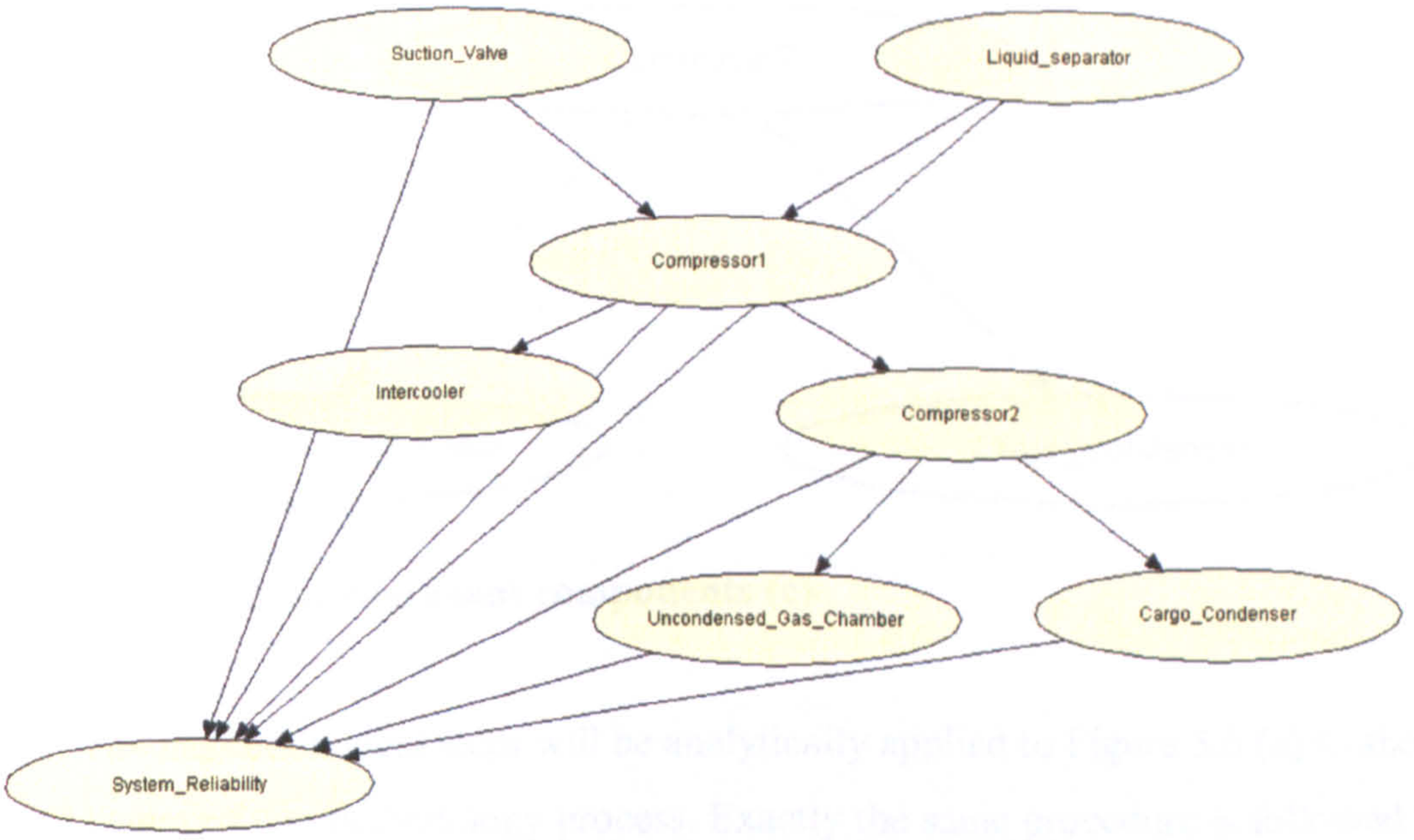


Figure 5.5 Bayesian representation of the reliquefaction system components

For simplicity of calculations, Figure 5.5 presented, will be broken down to three smaller BNs as shown in Figure 5.6 (a), (b), (c).

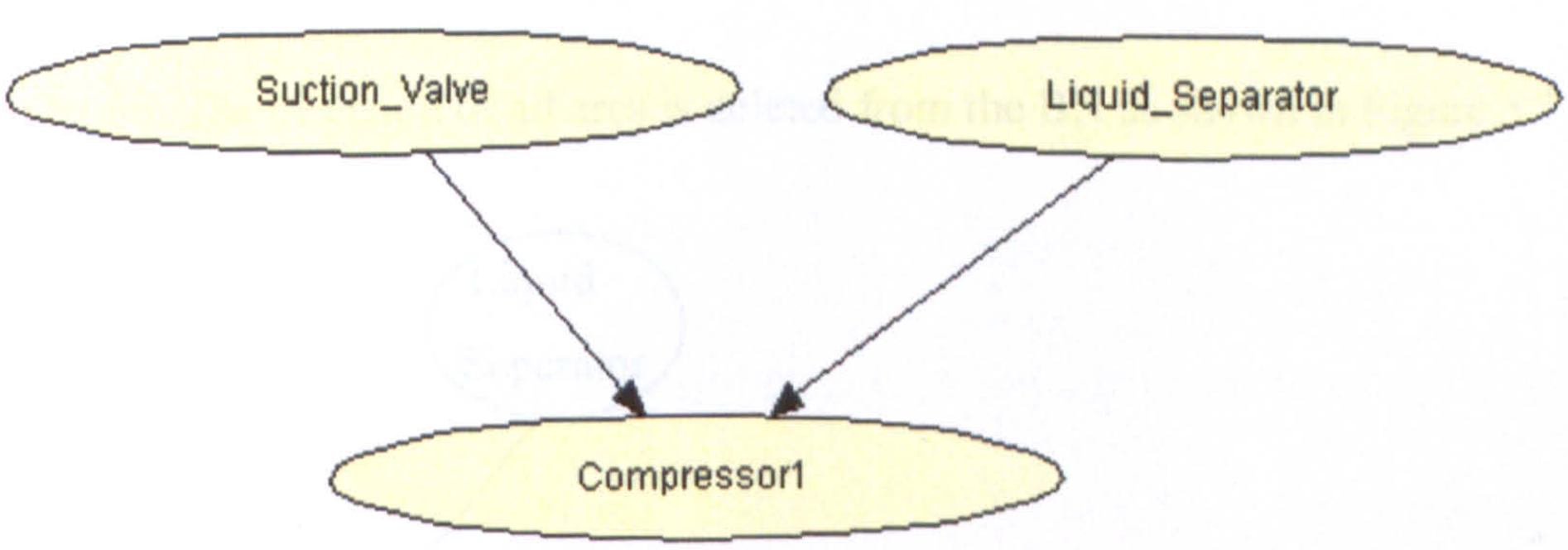


Figure 5.6 Reliquefaction plant components (a)

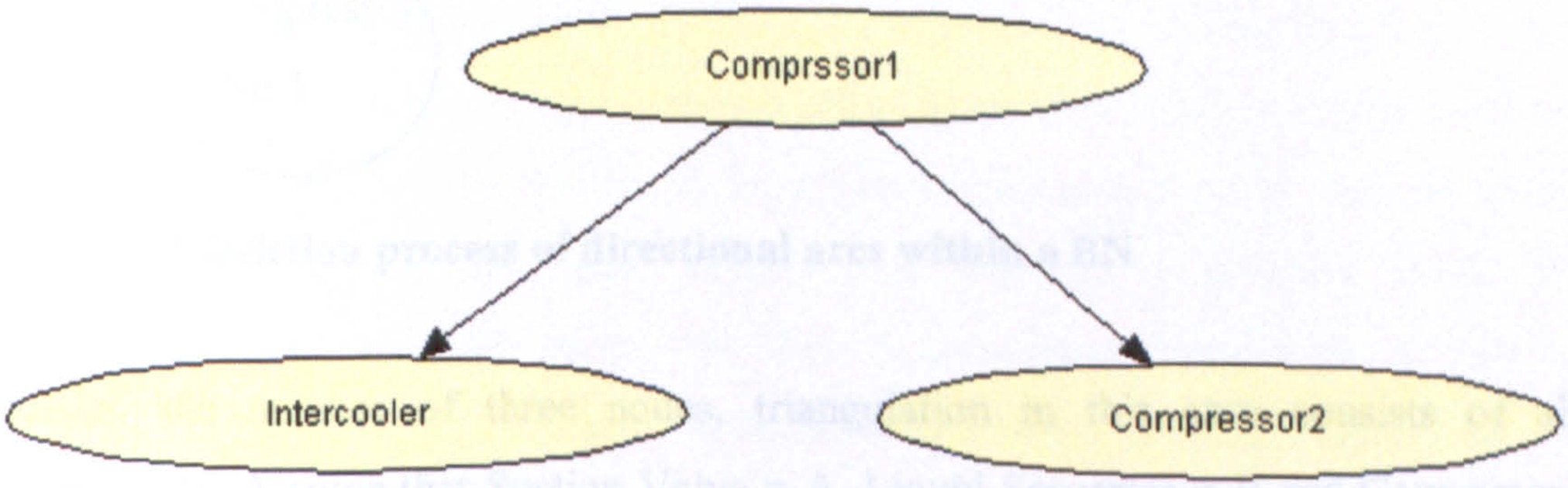


Figure 5.6 Reliquefaction plant components (b)

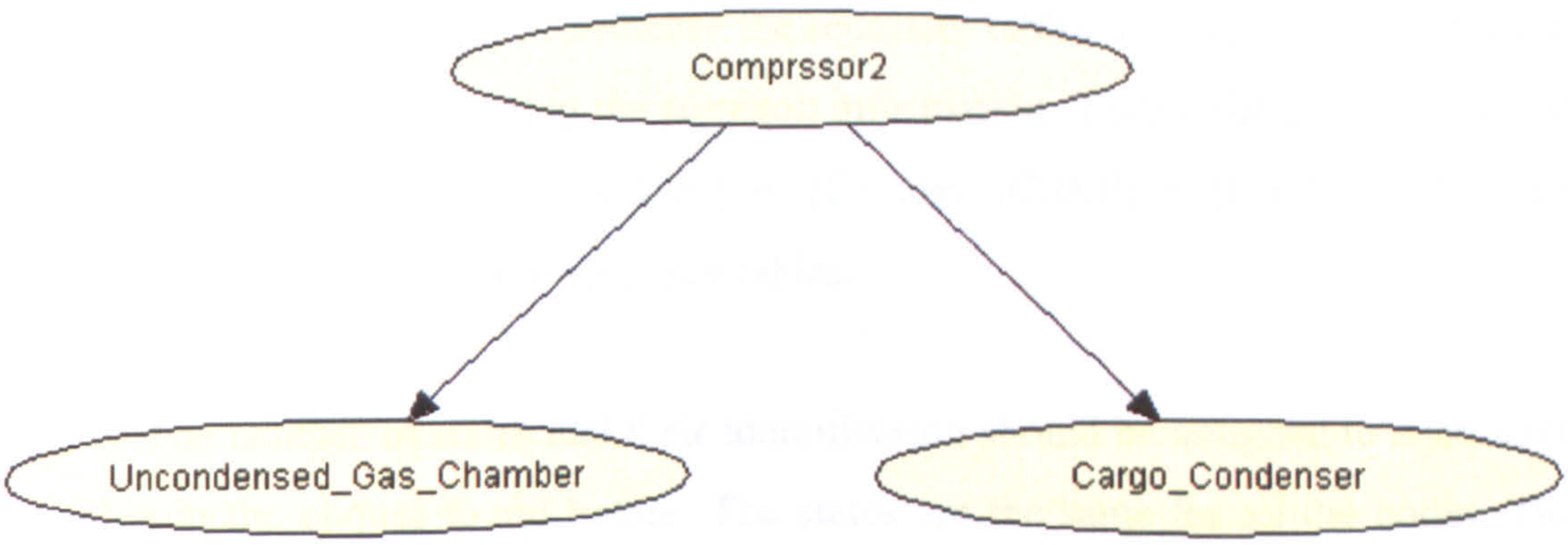


Figure 5.6 Reliquefaction plant components (c)

Step 2: The methodological steps will be analytically applied to Figure 5.6 (a) to show the full extent of the methodology process. Exactly the same procedure is followed to derive results from Figures 5.6 (b) and 5.6 (c). The constructed BN in Figure 5.6 (a) should be transformed into a junction tree. This is achieved as follows:

Moralisation: Since there are only 3 nodes included in this example no moralization is required.

Deletion: The direction of all arcs is deleted from the BN as shown in Figure 5.7.

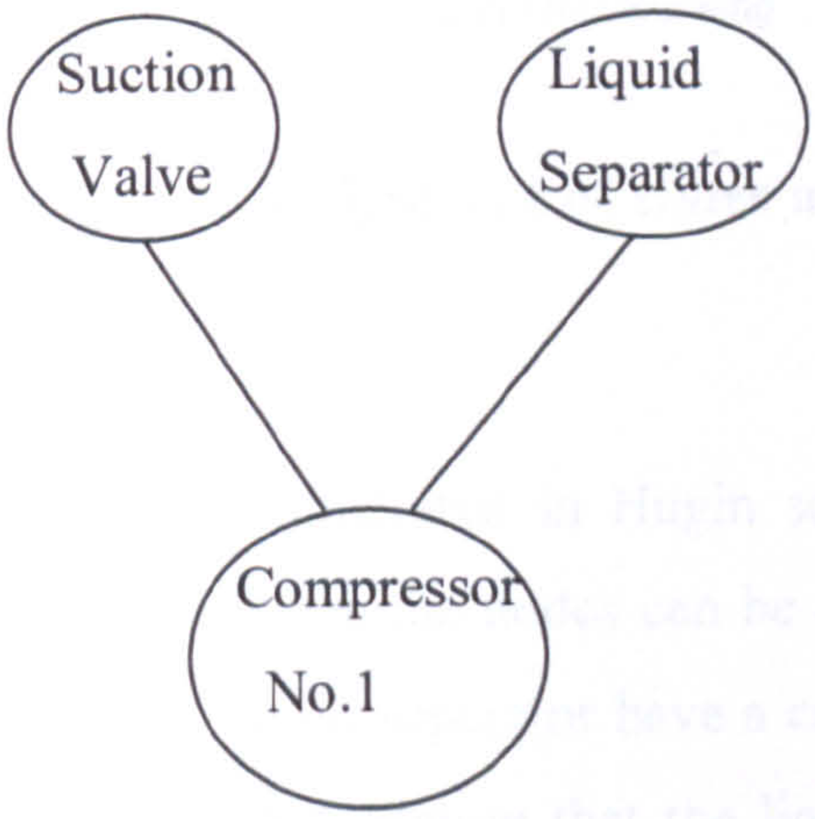


Figure 5.7 Deletion process of directional arcs within a BN

Due to the number of three nodes, triangulation in this case consists of all components. Assume that Suction Valve = A, Liquid Separator = B and Compressor No.1 = C. Therefore the clique formed is {A,B,C}. Similarly for Figures 5.6 (b) and Figure 5.6 (c) the cliques formed are {C,D,E}and {E,F,G} with D = Intercooler, E = Compressor No.2, F = Uncondensed gas chamber and G = Cargo Condenser.

Step 3: Before the insertion of evidence the separator tables need to be found between two adjacent cliques containing the common information. Taking the above identified cliques by pairs {A,B,C} ∩ {C,D,E} = {C} and {C,D,E}∩ {E,F,G} = {E} are obtained. {C} and {E} are the separator tables.

Step 4: The number of states and their identification should be assigned to each node included in the cliques found before. The states are the same for all the nodes. The assignment of two states, Operating and Not Operating governs all components of the BNs in this test case. Insertion of failure probabilities is required at this stage. The information used is taken from the OREDA handbook [OREDA DNV, 2002], as well as from expert's judgements with field experience (marine engineers, academics). Figure 5.8 refers to clique {A,B,C}

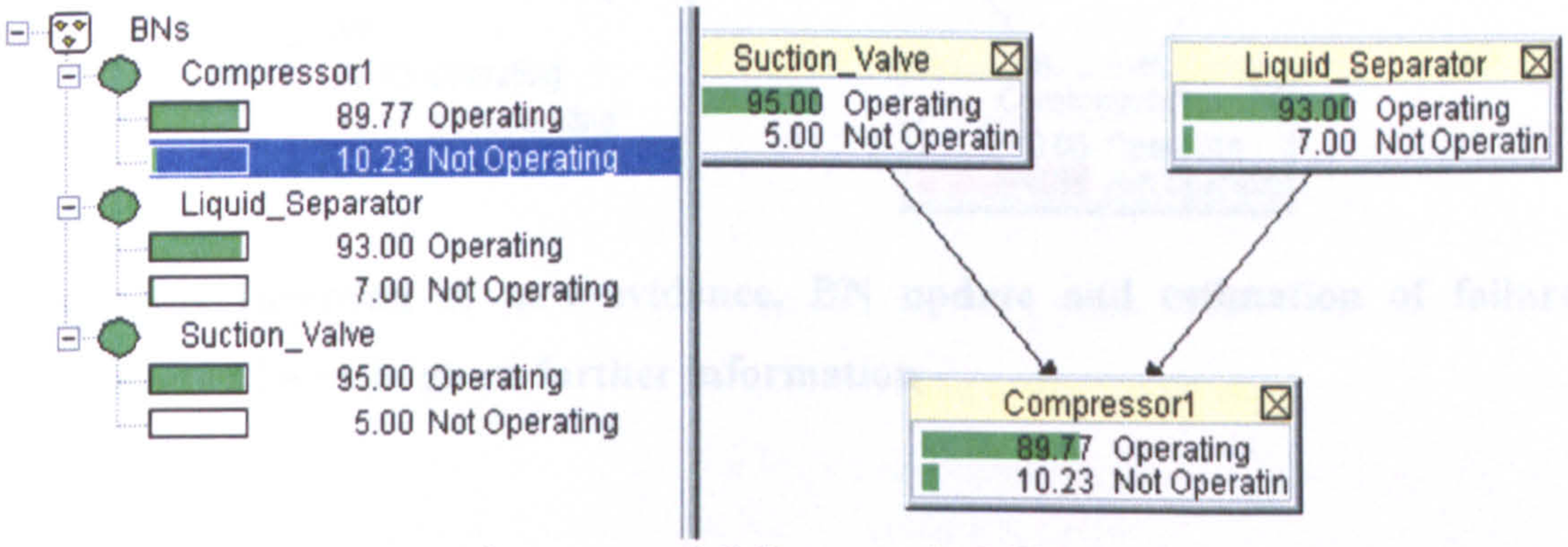


Figure 5.8 Assignment of states and failure probabilities to the nodes within the BN

Figure 5.8, illustrated in Hugin software, falls into the area of d-separation. The relation between the nodes can be qualitatively expressed by stating that the suction valve and liquid separator have a common effect towards the proper operation of the 1st compressor. Stating that the liquid separator is operating properly has no actual meaning. Stating that the liquid separator is functioning properly while the compressor is not operating means that there is something wrong with the suction valve from the cargo tank. Therefore, independent causes are made dependent by conditioning on a common effect.

The information provided in Figure 5.8 can be utilised in a different way as to determine elements as requested by the decision maker/safety engineer. If compressor 1 is in the state of non-operation, what is the probability of the liquid separator being

in the same state? All that is needed is to set the compressor in the 100% non-operating status and propagate the new piece of evidence throughout the network, (using the message passing technique) thus updating all nodes with the new information inserted. As can be seen from Figure 5.9, the insertion of new evidence was successful and the probability of the liquid separator being into the non-operating state is estimated to be 0.5862.

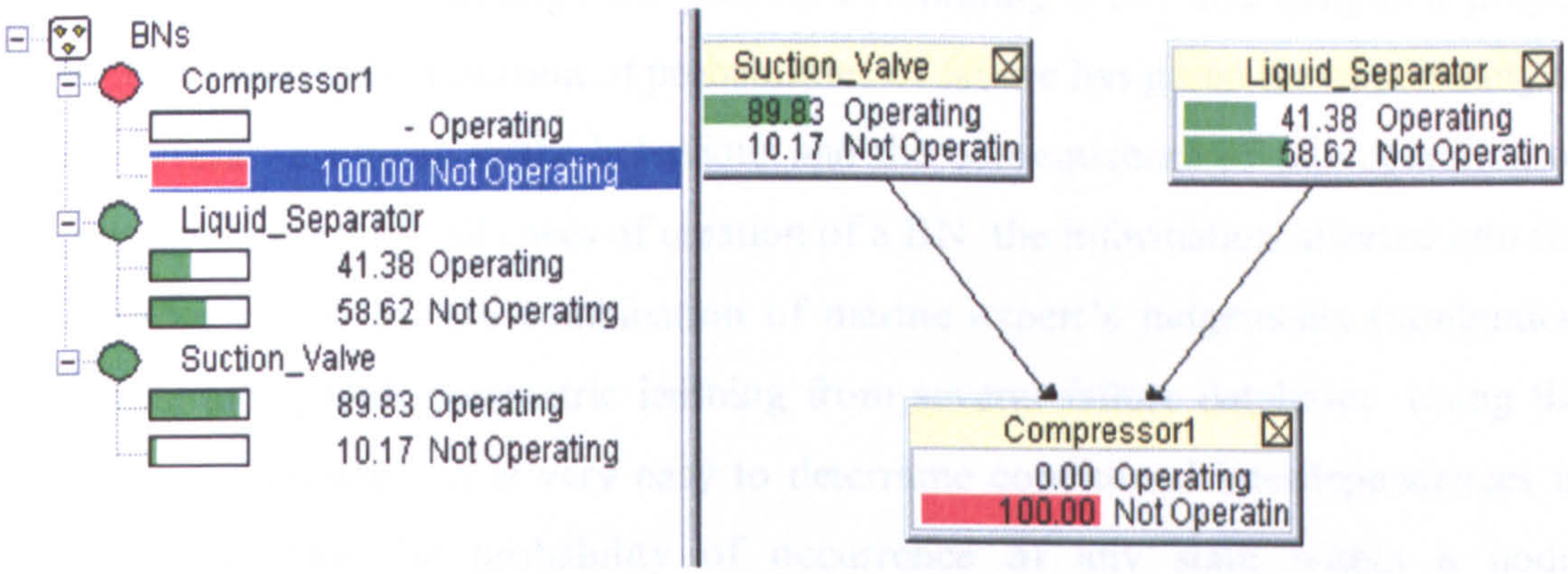


Figure 5.9 Insertion of new evidence, BN update and estimation of failure probability of a node given further information

Step 5: As can be seen from Figure 5.9 if a 100% non-operation state exists for compressor 1, it has to be the result of one of the states from each node. At first glance, it seems that if the liquid separator is in the non-operating state and the suction valve at the operating state the compressor will be at the non-operating state. This is not always the case as from time to time values may differ. It is therefore necessary to estimate what is the most probable set of configuration of the states that leads to the failure of the compressor's operation. Using the principle of max-propagation as stated in the theory section the most likely combination of states is revealed leading to the failure of the compressor. Figure 5.10 illustrates the most likely combination of states by assigning them with a value of 100.00.

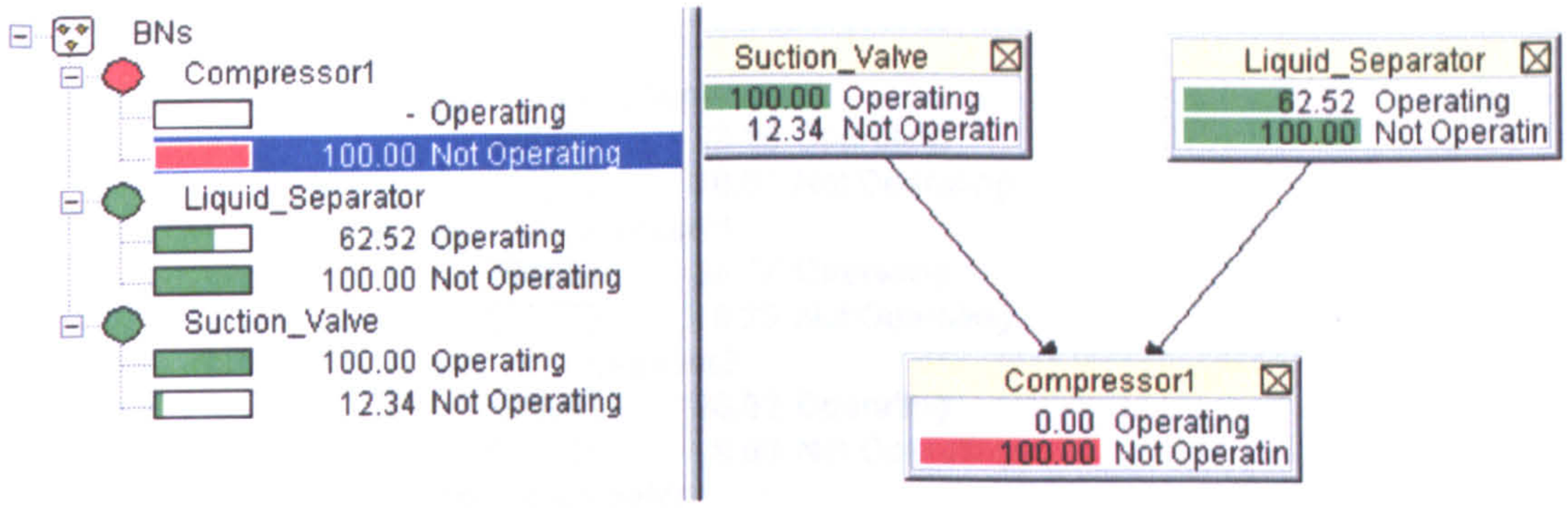


Figure 5.10 Most likely combination of states leading to failure of compressor

Step 6/7: Having gone through the process of building a BN and assigning proper states to the nodes, the insertion of probabilities of failure has given the opportunity to derive several results as to the behaviour and the consequences of non-operation of the system elements. In all cases of creation of a BN, the information inserted into the child nodes comes from a combination of marine expert's judgements (academics, engineers) along with parametric learning from several failure databases. Using the aid of Hugin software, it is very easy to determine conditional interdependences in order to calculate the probability of occurrence of any state within a node. Additionally, by being able to derive the most likely combination of states, the decision maker/safety engineer will be able to determine the areas in which further analysis should take place in order to improve either operating or design factors through reducing the probabilities of occurrence of certain states reduced. Having seen the analysis concerning a small set of nodes, the process can be expanded to accommodate larger engineering systems. Knowledge of interdependence and the way one component is affecting the other is crucial as it will allow the decision maker / safety engineer to produce the proper estimations as far as the operating states are concerned.

Examining the fully constructed BN in Figure 5.5, the information concerning each node is fed into Hugin software. Figure 5.11 illustrates the assignment of states and failure probabilities to the nodes within the BN used to describe the system reliability during the operation of a reliquefaction system operating on board an LPG vessel.

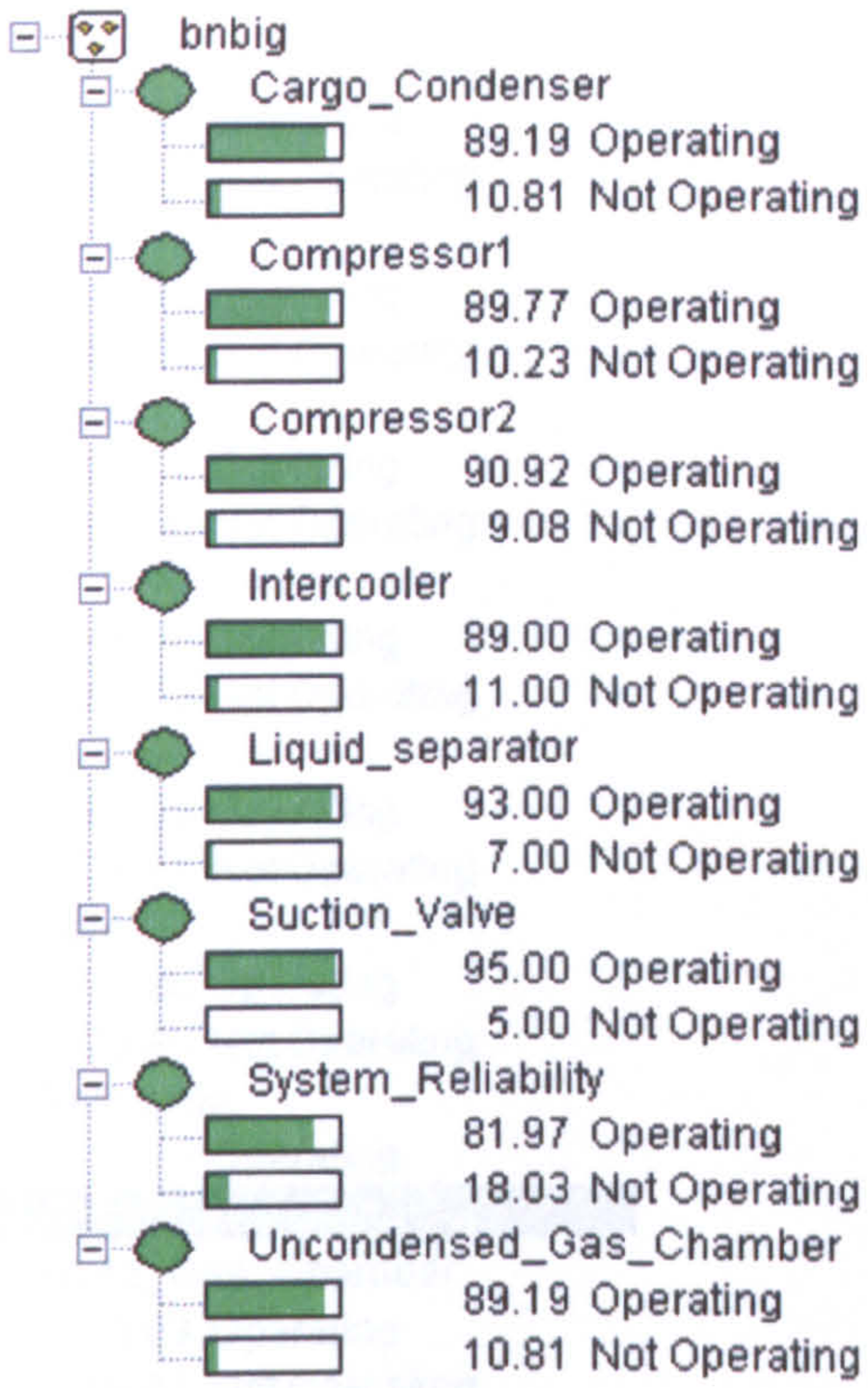


Figure 5.11 Assignment of states and failure probabilities to the nodes within the BN

In a similar manner as before, any node can be given a 100% value to any state in order to see how the rest of the states change as the BN is updated by the insertion of new information. Figure 5.12 illustrates the condition that the system reliability is at a non-operating state, meaning total fault during the functioning of the plant. Figure 5.12 also gives the update values in all node states. Again in this case the advantage of a BN at the update and propagation stage of information is clear. In the same sense, any node of the system could be isolated in order to see how this change would affect the rest of the system. In this way, the experts can either suggest operational changes or, when funds are available, try to redesign the system by making it as failure-proof as possible.

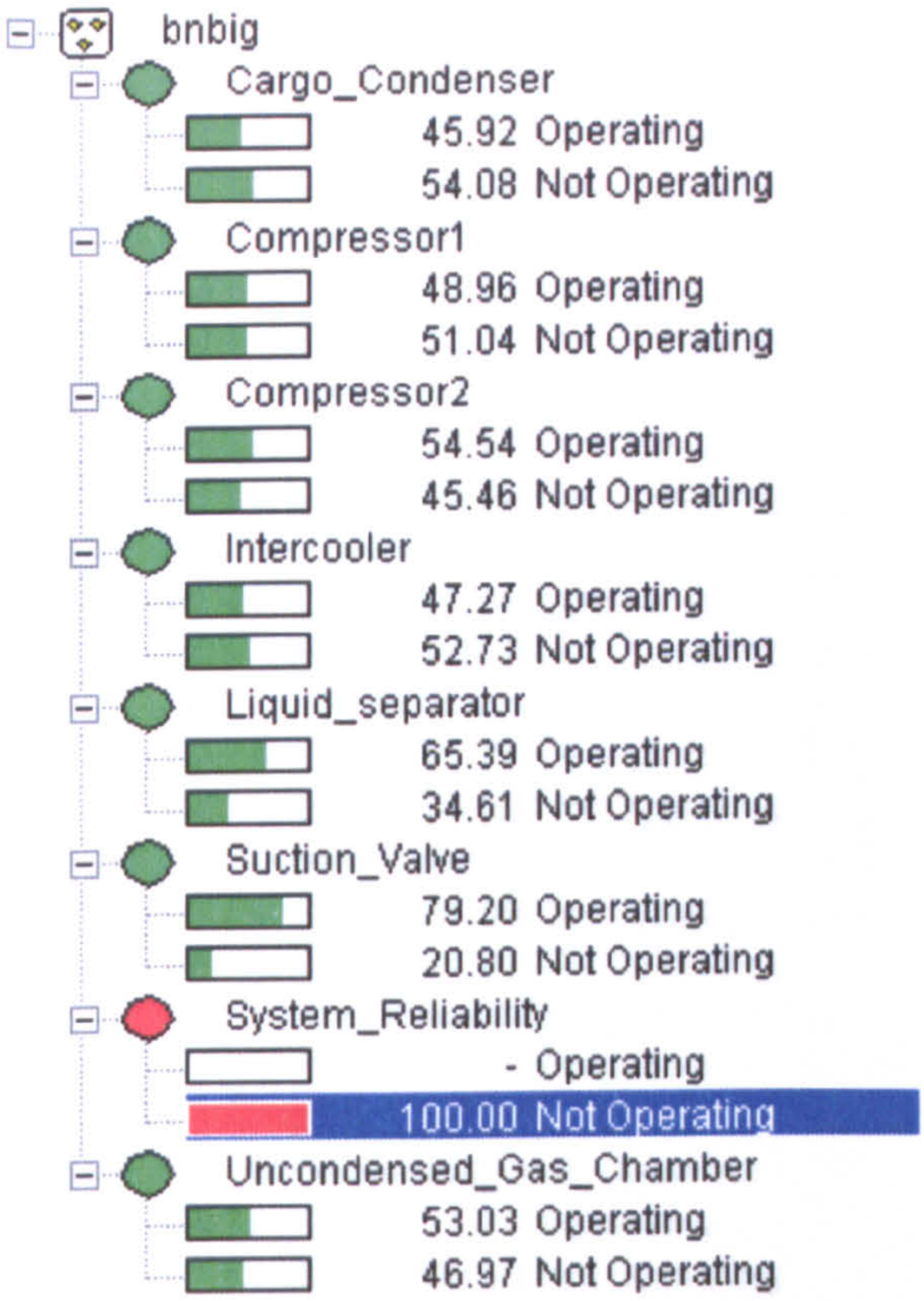


Figure 5.12 Insertion of new evidence, BN update and estimation of failure probability of a node given further information

The last part of the BN analysis requires the identification of the combination of each particular state, which will lead to the isolated state selected. Using Figure 5.13, it is seen that the node in question is the system reliability. As it can be seen in order for a system to be in a completing non-operative state, it does not mean that all nodes (system components) have to be in a non-operating state. The combination of a few vital components can prohibit the system from operating properly. The calculations were made using Hugin software. The state in red represents the isolated condition, which is caused by the combination of the rest of the states within the BN. The states included within the most likely combination are given a designation of 100%. This is not considered to be a number, as the total percentage of the two states will exceed 100%. This is considered to be a symbol given by the software's developers to designate which state is included in the combination.

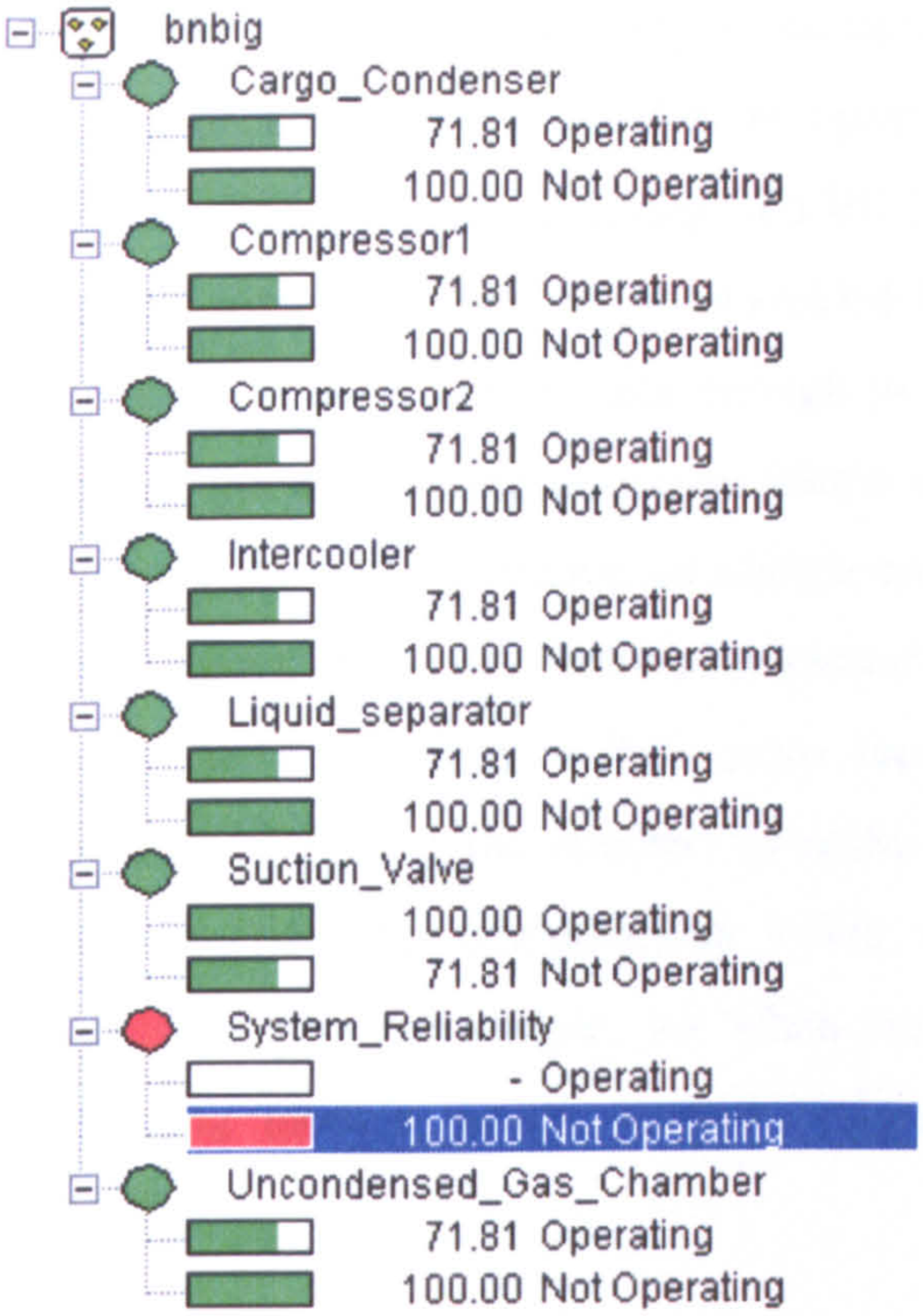


Figure 5.13 Most likely combination of states leading to failure of compressor

5.12 Conclusion

Bayesian networks have proven to be an excellent tool concerning the analysis of system reliability, enabling answering questions concerning either the operation or reliability of the system in an efficient, fast and easy to understand way. The initial problem is the formulation of appropriate junction trees, but as soon as this is determined, the process is easy to follow in order to derive adequate results. It can certainly be expanded for more analytic use within the marine industry specifically when it comes to calculating the reliability and safety of an engineering system. Following the proposed methodological steps, insertion of new evidence, update and re-compilation of the model constructed are performed easily. A BN has the main advantage over other commonly used techniques for risk estimation (fault tree, event tree) that apart from the graphical representation of the problem and its results, the decision maker / safety engineer can insert any specific state to each variable so that the analyst can describe the system in question with greater accuracy. Techniques like BN, fault tree analysis and event tree analysis, can either be used as stand-alone risk estimation methods or can be combined to derive more accurate results. They can

complement each other according to the nature of the problem. For example an event tree can be converted into a BN to increase the states within each consequence produced. An additional advantage of a BN is the ability to combine several influence diagrams, something that cannot be tackled by conventional risk estimation methods. What is more, BNs are flexible enough to tackle qualitative and quantitative data. Based on the engineering evolution which sets an increasing number of sensors for monitoring purposes at almost all marine engineering systems, BNs will have a vast range of data that can be combined to produce interdependence reliability estimations. This on the other hand is their main limitation. The complexity of calculations becomes harder when the numbers of nodes start to increase. Therefore it would not be recommended for computations within very large and combined networks. The elements of BNs are simple, yet when combined they can form a wide range of engineering models, as the majority of operation and reliability aspects can be captured.

PAGE NUMBERING AS ORIGINAL

CHAPTER 6. A MODIFIED VERSION OF THE VARIABLES TRANSFORMATION IN FORM/SORM METHOD FOR ESTIMATION OF THE MOST LIKELY FAILURE POINT

6.1 Introduction

The Form/Sorm method has initially been proposed by Hasofer and Lind [Hasofer & Lind, 1974] for normal vectors X and was extended later to arbitrary distributions by Rackwitz and Fiessler [Rackwitz & Fiessler, 1978]. Its main computational task is the calculation of the location of the most likely failure point (or β-point) by a suitable search algorithm. The distribution function of X must be differentiable. Usually, the probability estimate is sufficiently accurate for most practical purposes. What is more, for applications within the field of toxic hazards, it is proposed as a means for performing sensitivity analyses, possibly in parallel with a risk calculation carried out by conventional methods.

In this chapter, the basis of the method is outlined, the theory and factors influencing the calculations are analysed and a test case examining the risk arising from the operation of a port cargo handling crane is presented. Calculations use, as a consequence model, commercial software for the prediction of failure points. The use of a proposed screening procedure utilising the sensitivity formulas that the method provides, in order to identify the most significant uncertainties, is demonstrated.

The identification of a single set of input values containing sufficient information to summarise (at least approximately) the entire risk analysis is considered to be an important feature of the method and is proposed as the basis of a means for assessing the validity of the consequence model.

6.2 The Form/Sorm Method

6.2.1 Background theory

Assume that a calculation of a quantity Q is being estimated by means of a mathematical model, which may range in complexity from a simple expression to complicated reliability software. The model requires a number of input quantities, which may be subdivided into two groups. The first contains inputs, whose values are either readily available or, are known within an uncertainty, small enough not to influence the final results. This group of inputs will be characterised as constants in this chapter. The second group, which is of particular interest in this chapter, contains quantities whose values are uncertain. Each of these latter quantities should be represented not by a single value x_i but by a random variable Xi with an appropriate probability distribution [Lin & Kiureghian, 1986]. These uncertain input quantities are characterised as basic variables. It should be noted that each of these basic variables mentioned, needs to be represented by a single value X_i each time a simulation of the model is run.

Hence, the calculation performed by the model can be represented as:

$$Q = Q(X) = Q(X_1, X_2, \ldots\ldots, X_N) \qquad [6.1]$$

where X is the vector of the N basic variables and the constants in the calculation have been included implicitly in equation [6.1].

Let a safety margin of:

$$M = Q_{lim} - Q \qquad [6.2]$$

where, Q_{lim} is the maximum acceptable value of the quantity Q, and the condition

$$Q(x) < Q_{lim} \qquad [6.3]$$

defines states that are in the "pass" region (R_P). The condition

$$Q(x) > Q_{lim} \qquad [6.4]$$

defines states that are in the "fail" region (R_F). Finally, the equality

$$Q(x) = Q_{lim} \qquad [6.5]$$

defines an N – 1 dimensional surface which marks the division between the two regions and which is known as the failure region boundary or failure surface; x was used instead of X as we do not want to define a vector but a distribution.

Assume that a best-estimate calculation of Q is made, and that $Q < Q_{lim}$. A number of factors need to be addressed within a safety case in order to perform all the necessary reliability calculations.

i) The most likely combination of states which can cause Q or Q(X) (since Q=Q(X)) to exceed Q_{lim}.

ii) The probability P_F that Q will actually exceed Q_{lim} given the uncertainties within the calculations.

iii) The degree of sensitivity that the failure probability has according to each variable.

Form/Sorm method can provide solutions for factors i, ii and iii as mentioned above.

6.2.2 Location of the most-likely failure point

The most likely failure point (MLFP) method works on a different principle from commonly used failure estimation methods like the Monte Carlo simulation. Referring to Figure 6.1, it is assumed a case of LPG cargo been released to the atmosphere from a safety relief valve. Assume that Dd contour in the diagram denotes the limit after which, the atmosphere contains gas in such a percentage that can be easily ignited. The means of the distributions in the process of calculating the percentage of gas in the atmosphere are located at point O, which in the case presented is within the pass region [Scott, 1992]. O is considered to be the best estimate point (BEP). The further

point O lies away from the contour, the smaller the probability that the quantity Q(X) will exceed Q_{lim} as stated before.

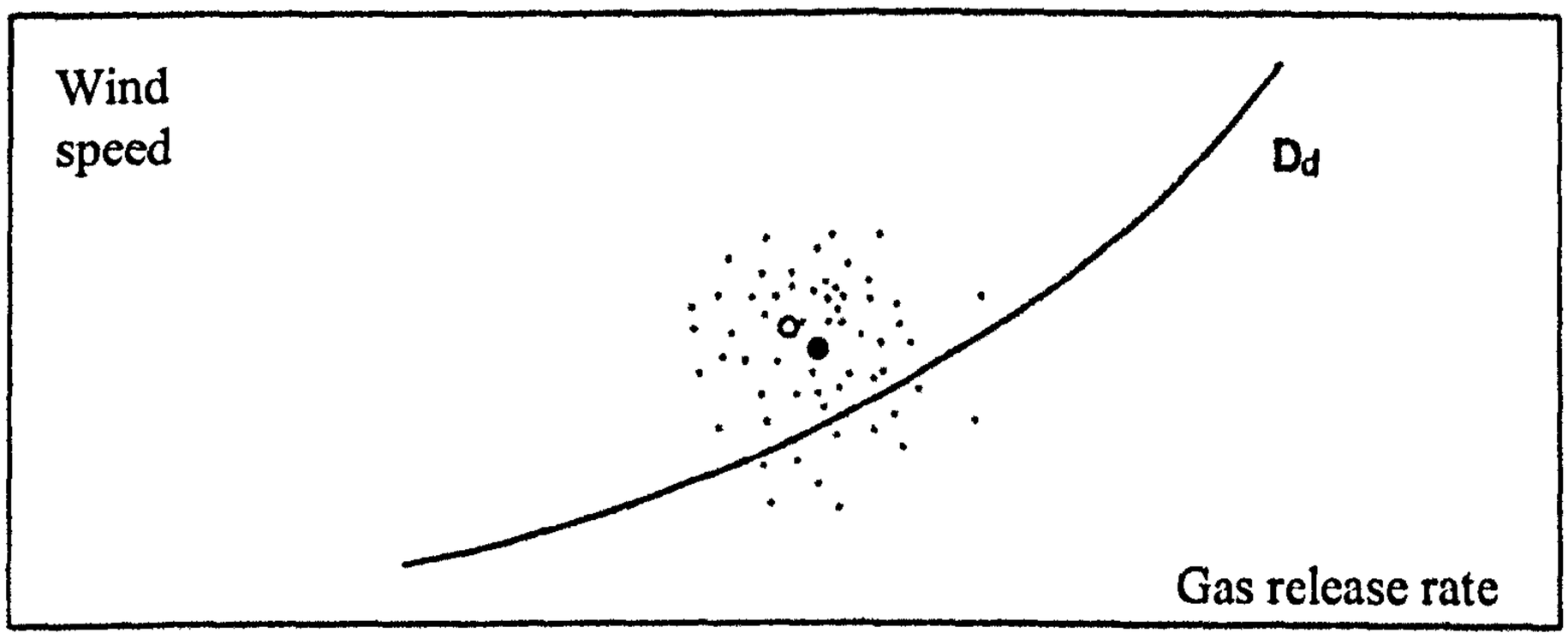


Figure 6.1 Contour based on the Monte Carlo simulation

The principle of the MLFP method is firstly to define a standardised coordinate system in which this distance can be expressed, and then calculate the distance by finding the point of closest approach of the contour to O as seen in Figure 6.2. Finally, to estimate P_f by performing an analytic integration over a region which, approximates the failure region [Evans et al, 1993]. P_f is the failure probability predicted by the calculation. In order to achieve that, it is required to transform the set of variables used in the problem addressed in such a format that can be readily usable to give results. The most common case is that the initial set of variables, noted N, is going to be parted from variables being both correlated and non-normally distributed. In order for this set to be usable in risk estimation, it is required to be transformed into another set of N' independent and normally or log-normally distributed variables which can be used on a standardised co-ordinate system.

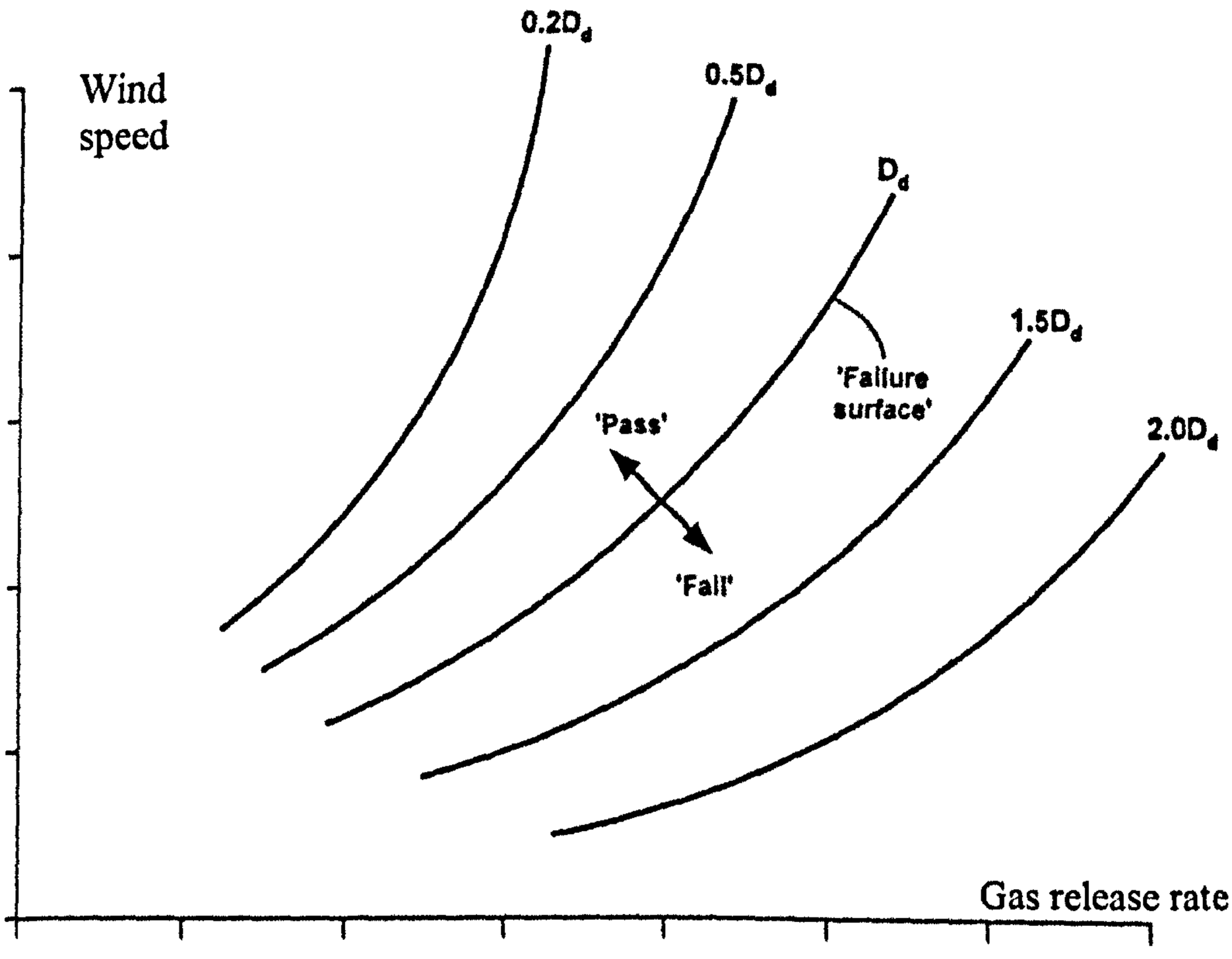


Figure 6.2 Contours passing from the fail and pass regions, for estimation of BEP

The transformation to the standard coordinate system is achieved using the following method. Assume that an input quantity x to the consequence model is uncertain. This uncertainty is represented by a continuous probability distribution $p_x(x)$ or alternatively, by the cumulative probability distribution (the integral of $p_x(x)$) $P_x(x)$. The value of x is converted to the value of an alternative variable u_x by means of the following equation:

$$\Phi(u_x)=P_x(x) \qquad [6.6]$$

where $\Phi(u) = 0.5(1+\text{erf}(u/\sqrt{2})$ [Mitchell, 1996] is the cumulative standard normal distribution; that is the cumulative distribution corresponding to the normal (i.e Gaussian) density distribution ϕ for a variable of mean 0.0 and standard deviation 1.0.

erf is the error function for each element of x, and it is noted as $erf = \frac{2}{\sqrt{\pi}} \times \int_0^x e^{-t^2} dt$.

Therefore, $\phi(u) = \frac{e^{-\frac{u^2}{2}}}{\sqrt{2\pi}}$ [6.7]

Each variable u_x has a standard normal distribution and is referred to as the standard normal variable corresponding to x. The best estimate values for uncertain variables are taken to be those by the medians of the probability distributions. In this chapter, the combined distribution is a function of the distance from the BEP and the circles shown in Figure 6.3 represented by contours of constant probability density . The point of closest approach therefore also possesses the maximum probability density (in the transformed system) and it is known as the most likely failure point (MLFP).

Assuming that the distance (essentially the combined number of standard deviations)

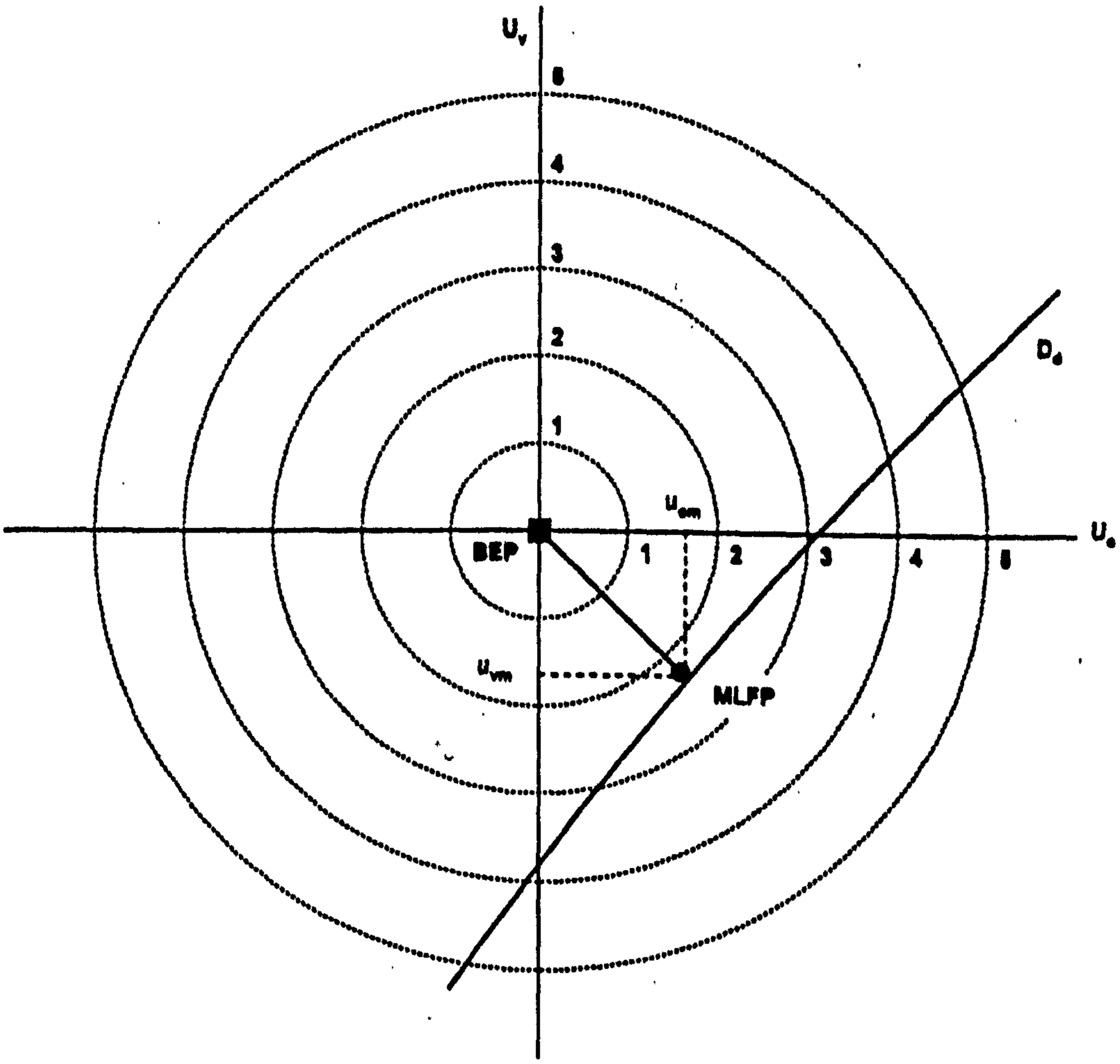


Figure 6.3 Representation of the MLFP from the BEP at the centre of axis

from the BEP to the MLFP is β, then the integral of the probability density over the region beyond the failure surface in Figure 6.3, relative to the position of BEP, can be estimated as P_I using the following equation:

$$P_I = \Phi(-\beta) \qquad [6.8]$$

The above equation applies to any number of uncertain variables.

6.2.3 Estimation of the failure probability integral

The failure probability P_f is calculated as the integral of the joint probability distribution over the entire failure region (R_F) [Kendal et al, 1994]. Therefore:

$$P_F = \int_{R_F} \phi_u(u)(du) \qquad [6.9]$$

where $\phi_u(u)$ is the joint probability density function for the random variables u and R_F is the failure region. Since the u values are all uncorrelated, $\phi_u(u)$ becomes:

$$\phi_u(u) = \prod_{i=1}^{N} \phi_{u_i}(u_i) \qquad [6.10]$$

where $\phi_{u_i}(u_i)$ is the standard normal probability density function

$$\phi(u) = \frac{e^{\frac{u^2}{2}}}{\sqrt{2\pi}}$$

The integral in Equation [6.9] usually cannot be evaluated as it stands since the shape of the failure region boundary (failure surface) is unknown and, even if it were known exactly, the required calculation would be too complicated to perform. The Form and Sorm methods allow this integral to be evaluated approximately by representing the shape of the failure surface in the vicinity of the MLFP.

6.3 The Form approximation

The first order reliability method (Form) approximates the failure surface as the tangent line, plane or hyper plane (depending respectively upon whether N is 2, 3 or >

3) at the MLFP. The Form approximation to P_f is then easy to evaluate. Since the joint probability density distribution in u-space is rotationally symmetric about the origin, it is possible to transform the co-ordinate system by rotating about the origin to produce new axes ($z_1,\ldots,z_N$) such that z_N passes through the MLFP (the orientation of $z_1,\ldots z_{N-1}$ relative to z_N is not relevant here). In this case the Equations [6.9] and [6.10] become [Mitchell, 1996]:

$$P_f = \int_{-\infty}^{\infty}\ldots\int_{-\infty}^{\infty}\int_{\beta}^{\infty}\prod_{i=1}^{N}\phi(z_1)dz_1\ldots dz_N \qquad [6.11]$$

where β is the distance from the origin to the MLFP.

The subscript 1 on P_f denotes the first-order approximation. Since it is possible to separate the variables, each integral can be carried out separately. The integrals from $-\infty$ to $+\infty$ are all equal to 1.0 having as a result the following:

$$P_{f1} = \int_{\beta}^{\infty}\phi(z_N)dz_N \qquad [6.12]$$

$$= \Phi(-\beta) \qquad [6.13]$$

where Φ is the cumulative lognormal distribution ($\Phi(y) = \frac{1}{2}\,[\,1 + \mathrm{erf}(y\sqrt{2})]$. Expression [6.13] is the first order approximation to Equation [6.9].

In order to obtain a better estimation of the value of P_f the Sorm approximation is used by just adding a number of extra evaluations of Q.

6.4 The Sorm approximation

The basis of the second-order reliability method (Sorm) will not be discussed in detail in the chapter. However, calculations using the commercial structural reliability package Sysrel [Strurel. 2000], gave adequate Sorm estimates of P_f. The Sorm approximation uses information about the curvatures of the failure surface at the MLFP, which are approximated as parabolic, paraboloidal or hyper-paraboloidal, depending on the number of uncertain variables, to derive an improved estimate of P_f. The Sorm failure probability P_{f2} may be evaluated exactly by means of an analytical

integral [Bjerager, 1990] as follows:

$$P_{f2} = \Phi(-\beta)\prod_{i=1}^{N-1}(1+\psi(-\beta)k_i)^{-\frac{1}{2}} \qquad [6.14]$$

where k_i are the surface curvatures referred to above, and $\psi=\frac{\phi}{\Phi}$.

The N-dimensional integral [6.11] with the failure region boundary described by Equation [6.14] can be reduced to an integral over a single variable, and can thereby be evaluated by numerical methods.

6.5 First-order importance and sensitivity measures

The Form/Sorm method, in addition to providing estimates of P_f, produces useful additional information concerning the sensitivity of the results to variations in the input quantities, allowing the user to judge which variables of the analysis are of most importance.

6.5.1 Sensitivity of the quantity of interest to variations in the basic variables

The constrained minimisation calculation referred above, produces values given by the equation $\nabla Q = [\partial Q/\partial u_1, \partial Q/\partial u_2, \ldots, \partial Q/\partial u_N]$ at various points in its search including the initial (e.g. median or mean value) point and the most-likely failure point. The sensitivity of Q to small changes in each x_i at these points may therefore be calculated as:

$$\frac{\partial Q}{\partial x_i} = \frac{\partial Q}{\partial u_1}\cdot\frac{\partial u_i}{\partial x_i} \qquad [6.15]$$

and since it is stated at the beginning that $\Phi(u_i) = P_i(x_i)$ [6.15]:

$$\frac{\partial u_i}{\partial x_i} = \frac{p_i(x_i)}{\phi(u_i)} \qquad [6.16]$$

where $p_i(x_i) = \frac{\partial P_i}{\partial x_i}$ represents the probability density function appropriate to the ith-variable evaluated at x_i and $\phi(u_i) = \frac{\partial \Phi}{\partial u_i}$ is the standard normal density function evaluated at u_i. Therefore by combining the above two mentioned equations:

$$\frac{\partial Q}{\partial x_i} = \frac{p_i(x_i)}{\phi(u_i)} \cdot \left(\frac{\partial Q}{\partial u_i}\right) \qquad [6.17]$$

These rates of change represent the quantities estimated in traditional sensitivity analyses.

6.5.2 Importance of contribution of each variable to the failure probability

In addition to the type of sensitivity information discussed previously, it is clearly of interest to determine which variables have the most influence on P_f, which means, for which variables it would be better to reduce the uncertainty as much as possible [Scott, 1992], [Kendall et al, 1994]. The most immediate results of this are the relative sizes of the values of u_i at the MLFP since these represent the numbers of standard deviations, and hence the probability density for each variable

The most immediate piece of information arises from the co-ordinates of the MLFP. Since β largely determines the failure probability and since,

$$\beta^2 = \sum_{i=1}^{N} u_{im}^2 \qquad [6.18]$$

where, u_{im} with i=1...N are the co-ordinates of the MLFP as mentioned further above, then the fractional contribution I_i of the ith uncertain variable can be expressed as:

$$I_i = \left(\frac{u_{im}}{\beta}\right)^2 \qquad [6.19]$$

and it may be seen that the values of I_i sum to 1.

The values of I_i or $\sqrt{I_i}$, if the value is assumed to be normally distributed, are directly related to the sensitivity of P_{fl} to changes in the parameters of the probability distributions (i.e. μ or σ) for each variable [Evans et al, 1993]. The values of I_i provide a guide as to the relative importance of the variables in terms of their effect on determining the failure probability.

6.6 Effect of replacing an uncertain variable by a constant

When performing an uncertainty analysis, one of the most useful pieces of information is a measure of the effect of replacing an uncertain variable by a constant, thereby allowing the unimportant variables to be filtered out and so reducing the dimension N of the failure region [Lin & Kiureghian, 1986].

When a variable x_i is replaced by its mean value μ_i, then the change of $\Delta\beta$ in the distance from the origin to the MLFP is given by:

$$\Delta\beta = \beta[(1 - I_i)^{-1/2} - 1] \qquad [6.20]$$

If I_i is small, it can also be stated as:

$$\Delta\beta = \frac{\beta I_i}{2} \qquad [6.21]$$

and hence,

$$\Delta P_{fi} = \frac{\phi(\beta)\beta I_i}{2} \qquad [6.22]$$

All variables whose combined effect upon β (or P_{fl}) is less than some threshold value can be omitted.

6.7 Points in Form/Sorm worth reviewing

It is appropriate here to review the ways in which the importance and sensitivity formulas described in the previous sections may be used and, particularly, to emphasise some of their limitations.

Firstly, it is anticipated that the analyst will, in addition to deciding if the failure probability is acceptable, wish to ascertain which variables are the most important in determining the failure probability. When this has been decided, it is further assumed that he/she will require some indication of the expected benefit (in terms of reduction in P_f) as a result of a reduction in the standard deviations of particular variables. This information can then be used for further analysis, if necessary. Probability distributions assigned to the uncertain variables might represent different circumstances, for example [Kaimal & Finnigan , 1994], [Madsen et al, 1986]:

1. The variable represents a well-defined physical quantity, whose exact value is not known (e.g. the tensile strength of the material from which an LPG tank is constructed).

2. The variable represents a fitted parameter, whose value appropriate to the circumstances being analysed is uncertain (e.g. the wind speed and direction).

3. The quantity is genuinely variable with time, so that the value at the time of occurrence of the incident being analysed is not predictable (e.g. the quantity of hydrocarbon in gaseous form present in a tank).

Although the circumstances represented by the distribution do not affect the calculation or the interpretation of the results, they may influence the choice of variables for which a reduction in standard deviation is to be attempted. It is worth mentioning that the derived sensitivities apply to the first-order approximation for the failure probability. The term "most likely failure point", can be misleading in some cases. When the best-estimate point (BEP) lies in the pass region, then the MLFP does indeed represent the most likely combination of input quantities giving rise to failure. However, if the BEP is in the fail region, then the MLFP becomes the most likely combination of input quantities giving rise to a pass. The MLFP should be interpreted as the point on the boundary between the pass and fail regions (failure surface) with the highest probability.

6.8 Background of variable transformation theory using the conventional Rosenblatt method

Form/Sorm method and in extension MLFP estimation, require that the N uncertain input variables should be transformed into N' variables that are (a) independent and (b) normally, or log-normally distributed as it will be presented in the test case. The requirement (b) is straightforward for any variable, provided that the input variables are independent between them. The possibility of a general means for deriving a set of N independent normally or log-normally distributed random variables in order to represent a joint probability distribution $F(x_1, x_2,..., x_N)$ of N interdependent variables may be seen from the following general expressions from probability theory. If A and B represent 2 events and P(A) is the probability of A occurring and, $P(B \cap A)$ is the probability of A and B occurring together, then the probability of B occurring, given A has occurred [P(B/A)] is given by the following expression in the set theory [Rosenblatt, 1952]:

$$P(B/A) = P(B \cap A)/P(A) \qquad [6.23]$$

$$P(B \cap A) = P(B/A)P(A) \qquad [6.24]$$

If events A and B are independent, then Equation [6.24] becomes,

$$P(B \cap A) = P(B)P(A) \qquad [6.25]$$

In the case of N events $E_1 \ldots E_N$, Equation [6.24] can be generalised to

$$P(E_1 \cap E_2 \cap \ldots E_N) = P(E_N / E_1 \cap E_2 \cap \ldots E_{N-1}) \times P(E_{N-1} / E_1 \cap E_2 \cap \ldots E_{N-2}) \times \ldots \times P(E_2 / E_1) \times P(E_1) \qquad [6.26]$$

Let E_i be the event that the random variable X_i takes on a value less than or equal to the value x_i for i= 1...N. The probability $P(E_1 \cap E_2 \cap \ldots E_N)$ is then conventionally written as $F(x_1,x_2,\ldots,x_N)$ where F is the joint cumulative probability distribution for

random variables $X_1 \ldots X_N$. In this case, Equation [6.26] becomes:

$$F(x_1,x_2,\ldots,x_N) = F(x_N/(X_1=x_1) \cap (X_2=x_2) \cap \ldots \cap (X_{N-1}=x_{N-1}) \times$$
$$F(x_{N-1}/(X_{N-1}=x_{N-1}) \cap (X_2=x_2) \cap \ldots \cap (X_{N-2}=x_{N-2}) \times \ldots \times$$
$$F(x_2 / (X_1=x_1)) \times F(x_1) \qquad [6.27]$$

where $F(x_1)$ is the cumulative probability distribution for X_1, i.e.

$$F(x_1) = \int_{-\infty}^{X_N} \int_{-\infty}^{\infty} \ldots \int_{-\infty}^{\infty} f(x_1, x_2, \ldots, x_N) dx_1 dx_2 \ldots dx_N \qquad [6.28]$$

In general $F(x_i/(X_1=x_1) \cap (X_2=x_2) \cap \ldots \cap (X_{i-1}=x_{i-1}))$ is the cumulative probability distribution for random variable X_i.

Equation [6.27] represents the joint probability distribution $F(x_1,x_2,\ldots,x_N)$ as the product of N separate terms. If each term in the product is considered as representing the probability distribution of a single random variable U_i then, by using Equation [6.25] which can be generalised as well to N terms, these variables must be independent. Therefore it is defined that:

$$\Phi(u_1) = F(x_1)$$
$$\Phi(u_2) = F(x_2/(X_1=x_1))$$
$$\ldots\ldots$$
$$\Phi(u_N) = F(x_N / (X_1=x_1) \cap (X_2=x_2) \cap \ldots \cap (X_{N-1}=x_{N-1})) \qquad [6.29]$$

where, Φ is the cumulative normal distribution, and variables u_i, with i = 1...N, are independent and lognormally distributed, as required, and the product of $\Phi(u_1)$ $\Phi(u_2) \ldots \Phi(u_N)$ is equal to the original joint probability distribution as in Equation [6.27]. Therefore, given a vector of values of the original variables $(x_1,x_2 \ldots x_N)$ these values can in principle be transformed into values of the independent normally distributed variables u_i by means of the following sequence [Rosenblatt, 1952]:

$$u_1 = \Phi^{-1}[F(x_1)]$$

$u_2 = \Phi^{-1}[F(x_2) / (X_1=x_1))$

.....

$u_N = \Phi^{-1}[F(x_N) / (X_1=x_1) \cap (X_2=x_2) \cap ... \cap (X_{N-1}=x_{N-1})]$

The method that Rosenblatt proposed, and which is briefly described above is the one traditionally used for cases of variable transformation from one set to a proper one used within the failure probability calculations. What follows below is a different method of variable transformation applied to both normal and lognormal distributed variables, called the Nataf transformation. It is shown in the test case that according to the problem addressed a better failure probability estimation can be derived using the Nataf method [Nataf, 1962].

6.9 Modified variable transformation method: The Nataf method for correlated variables

The property of correlation is a special case of that of interdependence and implies a linear relationship between pairs of random variables as it is will be shown further down. For the case of two random variables X_1 and X_2, the covariance between them is given by [Lin & Kiureghian, 1986]:

$$Cov(X_1,X_2) = E(X_1X_2) - E(X_1)E(X_2) \qquad [6.30]$$

where E represents the expectation value, which itself is defined as:

$$E(X) = \int_{-\infty}^{\infty} xf(x)dx \qquad [6.31]$$

for a single variable, and

$$E(X_1X_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x_1x_2 f(x_1,x_2)dx_1dx_2 \qquad [6.32]$$

for the product of variables X_1,X_2.

The correlation coefficient for random variables X_1 and X_2, symbolised as ρ is defined as:

$$\rho = \frac{Cov(X_1, X_2)}{\sigma_1 \sigma_2} \qquad [6.33]$$

where σ_1 and σ_2 are the standard deviations of X_1 and X_2. With the definition given in Equation [6.33], the value of correlation coefficient is limited to $-1 \leq \rho \leq 1$.

Although it is common to view ρ as a measure of the interdependence of random variables X1 and X_2, it is nevertheless the case that strongly interdependent variables may have $\rho = 0$. An example of this would be a joint distribution which is constant over a unit circle, i.e. [Scott, 1992]:

$$f(x_1,x_2) = 1/\pi \text{ for } x_1^2 + x_2^2 \leq 1 \Rightarrow \rho = 0$$

Evaluation of ρ for this distribution yields a value of 0, and yet X_1 and X_2 are interdependent, since the range of one depends upon the value of the other. Conversely though, random variables, which are independent, always have a correlation coefficient of zero. For variables whose joint distributions are not precisely known, or for cases where the joint distribution is to be approximated, it may be convenient not to specify the entire joint distribution $f(x_1,x_2)$ but only [Kendal et al, 1994]:

(1) The marginal distribution $f(x_1)$ of X_1.

(2) The marginal distribution $f(x_2)$ of X_2.

(3) The degree of correlation ρ between them.

This gives the opportunity to estimate apart from the effect of the uncertainty in the input values used, the effect of any possible correlation between them. This can only be done using the Nataf transformation.

6.9.1 The Nataf Method

The principle of the Nataf transformation (see also Equation [6.32]) is to construct a pre-specified form of joint probability distribution $f(x_1,x_2)$, which preserves the marginal distribution of each variable and the correlation between them, according to the following formula [Nataf, 1962]:

$$f(x_1,x_2) = \frac{f(x_1)f(x_2)}{\phi(z_1)\phi(z_2)}\phi(z_1,z_2,r) \qquad [6.34]$$

where, $\phi(z_1,z_2,r)$ is the bivariate standard normal probability density distribution, with correlation coefficient r, where $-1 \leq r \leq 1$, and the quantities $f(x_1)$ and $f(x_2)$ are normally distributed. The relationship between r and the quantity ρ, defined in the previous section, is explained as follows. The bivariate standard normal probability density distribution has the explicit form of [Nataf, 1962]:

$$\phi(z_1,z_2,r)=\frac{1}{2\pi c^2}e^{\left[-\frac{1}{2c^2}(z_1^2-2rz_1z_2+z_2^2)\right]} \qquad [6.35]$$

where, $c^2 = 1 - r^2$ [6.36]

Equation [6.34] is related to the variable transformation procedure described in the MLFP section, where a basic variable x is transformed into a new variable u by having a standard normal distribution. In the case of Equation [6.34] though, the new variables noted z_1 and z_2 are still correlated with correlation coefficient r. However, because of the definition of the joint normal distribution (for two or more variables), it is possible to transform variables z_1 and z_2 to u_1 and u_2, which have standard normal distributions and are independent, so completing the transformation from x_1, x_2 to u_1 and u_2. Considering only two variables, the transformation is as follows:

$u_1 = az_1 + bz_2$ [6.37]

$u_2 = bz_2 + az_2$ [6.38]

where,

$$a = \left(\frac{1+c}{2c^2}\right)^{\frac{1}{2}} \qquad [6.39]$$

and

$$b = \left(\frac{1-c}{2c^2}\right)^{\frac{1}{2}} \qquad [6.40]$$

Assume a quantity $y_i=(x_i-\mu_I)/\sigma_i$. ρ is estimated by:

$$\rho = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} y_1 y_2 \phi(z_1, z_2, r) dz_1 dz_2 \qquad [6.41]$$

There are therefore, three possible approaches to the problem of deriving r from the specified value ρ.

(1) Solve equation [L] numerically.

(2) Use the formulas given by [Liu, et. all, 1986].

(3) Use the approximation presented here that $r = \rho$.

The latter approach is acceptable because,

- If ρ is being used as the varied parameter in a sensitivity survey, it is equally permissible to specify r as the varied parameter, rather than ρ.
- Again from [Liu, et. All. 1986], it is indicated that r and ρ do not differ significantly in most cases.

As soon as the above process completes and the joint probability distributions are derived the failure probability integral over the failure region is estimated as well as the MLFP, and the Form and Sorm approximations. The example presented is indicative of the difference between the results that the two methods used, Rosenblatt and Nataf produce and eventually show that the Nataf transformation is a better way to transform the basic input variables. In both cases, the same reliability software Sysrel [Strurel, 2000] was used.

6.10 Test case and comparison of transformation results

For a new automatic container crane.,there are two different braking conditions to be provided for normal operations and emergency conditions. All brakes should be capable of rapidly stopping the crane plus the working load from maximum full load speed without the aid of regenerative braking. One of the main braking systems of the crane is the long travel braking system. It should be able to arrest the crane from full speed. The crane's ability to stop is greatly affected by the braking system's ability to prevent skidding. In crane locations where prevailing winds can cause problems, arrangements are provided to tackle this situation. These are:

- "Drop in" type storm pin.
- Hydraulic or gravity operated rail claws or clamps.
- Hydraulic or gravity operated wedge type skid brakes.
- Cam brakes.

Given a case where a crane is in operational condition, the crane's anemometer has been set to bring the crane into stop at a wind speed of 20 mph. The crane is equipped with hydraulic operated wedge type skid brakes. Strong winds start blowing at a speed of 25 mph. The emergency stopping condition of the crane is activated. At that time the crane was at maximum full load speed carrying a 40 TEU container. A number of parameters governed by uncertainty are involved in the complete description of the test case (see Table 6.1) and should be included in the calculations required to estimate the probability of failure of the cargo crane brakes.

6.10.1 Define quantity Q

A few relatively simple mathematical equations are used to model the quantity Q which is the stoppage of the container at full operating speed during heavy winds condition. Assume that the quantity Q described in the first section of this chapter is represented by:

$$Q = \left(\prod_{i=1}^{N} X_i \right)^{\frac{1}{N}} \text{ with the failure surface defined by the condition} \qquad [6.42]$$

$$Q = 1.0 \qquad [6.43]$$

This function has been chosen to represent a simple way of using the modified Form/Sorm method. The analysis that will be performed contains a number of X_i variables which are either normally or log-normally, distributed. From Equations [6.1] to [6.5] it is seen that in our case the MLFP is going to be at position $x_1 = x_2 = x_3 = \ldots = x_N = 1.0$ [Mitchell, 1996].

6.10.2 Set the variables

The probability distribution for 6 of the variables X_i was each selected to be log-normal, although normal variables would also fit the conditions. In this case the quantity $Y=\ln X$ is normally distributed with mean m and standard deviation s.
The standard normal variables u_i are therefore defined as:

$$u = \frac{Y_i - m}{s} \qquad [6.44]$$

With this assumption, the expression for the failure probability takes a particularly simple form. Taking logs of Equations [6.42] and [6.43], the failure surface can be expressed by the following condition:

$\sum_{i=1}^{N} y_i = 0$ or by using Equation [6.44] it becomes:

$$\sum_{i=1}^{N} u_i = -\frac{Nm}{s}$$

which is the equation of a hyper-plane in u-space. The Form approximation for this problem will therefore be exact, with the failure probability being calculated as $\Phi(-\beta)$, as mentioned at the MLFP section, where β is the closest approach of the hyper-plane to the origin. Because of the symmetry that values present, the point of closest approach to the BEP will have $u_1=u_2=\ldots=u_N$ so,

$$\sum_{i=1}^{N} u_i = Nu_c$$

where,

$u_c = -m/s$

and hence

$$\beta = -\frac{N^{\frac{1}{2}}m}{s}$$

The test case was performed for values of N being 2,5,10. As it is obvious, normal and log-normal distributions were used in this example. Since each variable is different and a number of parameters influence their effect on the total system, each variable will have a mean and a standard deviation. Table 6.1 gives an overview of the variables used, along with their respective distributions and Table 6.2 gives the values of their means, standard deviations and medians for each distribution.

Table 6.1 List of uncertain variables along with their respective distributions

Variables presenting uncertainty	Distribution type
Wind speed	Normal (1)
Rain severity	Lognormal (2)
Frost conditions	Normal (3)
Wind stability/vibrations of crane	Lognormal (4)
Level of lubrication of steel wires	Lognormal (5)

Grip level of rail clamps	Normal (6)
Level of cleanliness of crane rails	Lognormal (7)
Level of lubrication of hoist ropes	Lognormal (8)
Failure of wind arrestors	Lognormal (9)
Failure of seals at limit switches	Normal (10)

The quantities m and s above related to μ and σ by the use of the following expressions [Madsen et al, 1986], [Kaimal & Finnigan, 1994], [Panofsky & Dutton, 1984]:

$$m = \ln\left[\frac{\mu^2}{(\mu^2+\sigma^2)^{\frac{1}{2}}}\right]$$

and

$$s = \left[\ln\left(\frac{\mu^2+\sigma^2}{\mu^2}\right)\right]^{\frac{1}{2}}$$

The median value of X, x_{med}, is given by

$$x_{med} = \frac{\mu^2}{(\mu^2+\sigma^2)^{\frac{1}{2}}}$$

Therefore the values of m, s, and x_{med} are given at Table 6.2.

Table 6.2. Values of m, s, x_{med} for normal and lognormal distributions

Distribution	μ	σ	m	s	x_{med}
(1)	10	5	2.191013317	0.472381	8.944
(2)	5	2	1.53522791	0.385253	4.642
(3)	3	1	1.045932031	0.324593	2.846
(4)	0.5	0.5	-1.039720771	0.832555	0.353
(5)	2	0.2	0.688172015	0.099751	1.990
(6)	2	0.4	0.673536824	0.198042	1.961
(7)	1	0.5	-0.111571776	0.472381	0.894

(8)	3	1	1.045932031	0.324593	2.846
(9)	1	1	-0.34657359	0.832555	0.707
(10)	6	4	1.607897079	0.606403	4.992

The results from the calculations are given to the Tables 6.3 and 6.4. Column 1 of each table gives the value of N and columns 2 and 3 respectively the following quantities:

n_g = number of evaluations of ∇Q (vector quantity of Q).

n_a = number of additional evaluations of Q (general quantity calculated by the consequence model) performed in order to locate the MLFP.

In most cases ∇Q is calculated numerically, requiring n_g evaluations of Q. The total number of evaluations of Q is given in column 4 of Tables 6.3 and 6.4. In order to reduce the effect of particularly favourable or unfavourable initial points, each case was repeated 5 times with different random number set for each run. The entries showing the numbers of ∇Q and Q evaluations are therefore averages of 5 separate runs, rounded to the nearest whole number. The results shown at Tables 6.5 and 6.6 indicate that the Form method can be very promising if appropriate variable transformation is used. The last two columns of Tables 6.3 and 6.4 compare the Form result for the MLFP with that for the analytic expression for β. The two sets of values are seen to agree to 2 or 3 significant figures. Furthermore, Table 6.5 illustrates the difference of using Rosenblatt and Nataf variable transformation techniques within the same software. The results, P_{fl} in Rosenblatt and Nataf, are presented against the results (P_f) for the same case deducted by using Monte Carlo method, which will be used as a reference and comparison point for the final discussion. Table 6.6 indicates the number of model runs required for running the Form method and the Monte Carlo respectively.

Table 6.3 Normal distribution, form calculations

N	n_g	n_a	Eval. Q	Φ	Form
2	6	22	34	3.870×10^{-2}	3.868×10^{-2}
5	7	28	63	2.618×10^{-3}	2.613×10^{-2}
10	7	26	98	3.928×10^{-5}	3.918×10^{-5}

Table 6.4 Lognormal distribution, form calculations

N	n_g	n_a	Eval. Q	Φ	Form
2	5	21	30	2.780×10^{-1}	2.799×10^{-1}
5	7	27	61	1.760×10^{-1}	1.759×10^{-1}
10	7	27	97	9.402×10^{-2}	9.397×10^{-2}

Table 6.5 Comparison of failure probabilities

Transformation	Nataf				Rosenblatt				Monte
Method	FORM				FORM				Carlo
N	n_g	n_a	Q	Pf_1	n_g	n_a	Q	Pf_1	Pf
2	3	17	23	2.780×10^{-1}	9	14	32	2.788×10^{-1}	2.780×10^{-1}
5	6	22	52	1.759×10^{-1}	4	6	26	1.756×10^{-1}	1.760×10^{-1}
10	7	29	99	9.400×10^{-2}	6	8	68	9.402×10^{-2}	9.402×10^{-2}

The results deducted in Table 6.5, are compared with the results estimated by the Monte Carlo simulation. Finally, Table 6.6 demonstrates the speed of estimation of results of each one of the distributions selected, by comparing the number of model evaluations for each case.

Table 6.6 Comparison of model evaluations required by Form and Monte Carlo methods

Number of evaluations			
Distribution	N	FORM	Monte Carlo
Log-normal (a)	2	34	258
	5	63	3820

	10	98	$2.5x10^5$
Log-normal (b)	2 5 10	30 61 97	36 57 106

6.11 Discussion of results and conclusions

This chapter was developed to indicate the usability of Form/Sorm method and to present a different technique for tackling with uncertainty and vagueness in cases that fuzzy variables need to be taken under consideration for the calculation of failure probabilities. Its strong points are the transformation of the basic uncertain variables chosen to a common utility plane and an estimation of the most likely failure point among them.

The functionality of the variable transformation methods was tested by application on a simple port cargo handling crane system. The results derived were presented in comparison between both Rosenblatt and Nataf transformations and were also put against the results of Monte Carlo simulation which is considered a benchmarking method. This comparison was made in order to test the efficiency, reliability as well as accuracy of the technique. Failure probability estimates were obtained for ten model evaluations for $N \leq 10$ where N is the number of uncertain variables represented. The results indicate that their approximation using Nataf transformation is closer to the values deducted from the Monte Carlo simulation. It is worth mentioning at this point that for a decision maker who prefers to calculate P_f using Monte Carlo, an initial Form/Sorm search for the MLFP provides a suitable result for subsequent optimisation of the Monte Carlo calculations by means of importance sampling. It is advisable that further investigation would take place into examining the Form/Sorm

method using the Nataf variable transformation by applying it into more complicated systems. The main advantage of Form/Sorm against the Monte Carlo is the lesser duration of time it takes to complete the probability estimates. In addition, as presented in the test case, for P_f of 10^{-2} or less Form/Sorm can offer a better alternative to Monte Carlo simulation method when a fast first calculation of probability estimates is required. The graphical representation of the MLFP as it can be seen from Figure 6.3 can assist in a quick ranking of uncertain variables in order of importance according to their distance from the BEP and the contour of the pass/fail region, creating a useful by-product of Form/Sorm method.

Summing the above points, it is concluded that the Form/Sorm method using the Nataf variable transformation technique is sufficiently robust and efficient enough to be considered for use on a routine basis for the assessment of confidence in calculated safety margins.

CHAPTER 7: ORGANISATIONAL SELF-ASSESSMENT PERFORMANCE IN TERMS OF SAFETY MATURITY USING THE EVIDENTIAL REASONING APPROACH

7.1 Introduction

Public concern about the safety of large and complex marine engineering systems has increased nowadays more than ever before. Many major corporations are either hiring or developing specific departments dealing with safety issues. This dictates a course of action towards increase in performance, specifically if the company is dealing with safety related matters. Unavoidably, this generates the question of how a company can be determined as better compared with one providing the same services or even how it would measure the extend to which it has further increased or decreased its performance throughout a fixed time interval. Comparison and self-assessment are the two key factors dealt with in this chapter.

The methodology proposed in this chapter assigns five linguistic variables to describe the maturity self-assessment standards. Sharp et al., presented a list of eleven characteristics in his paper [Sharp et al., 2002] trying to assess the organizational maturity in terms of design for safety of offshore applications concerned. These characteristics were identified and itemised in three main groups, representing formal safety implementation and a longer-term investment in safety. As soon as the levels of maturity were established, the levels of design for safety were set. The latter levels produced the eleven elements of safety, which were assigned a value from one to four in order to assess the performance and organisational maturity of any company. This model though, fails to give an accurate image of the status of the company's operation. The lack of criteria, the lack of using linguistic variables and the lack of stages of comparison set it as an incomplete model. Moore and Bea [Moore & Bea, 1995] on the other hand tried to give a set of five categories under which classification of safety factors addressing organisational self-assessment is concerned. They established a model based solely on graphical representations, giving only a minor weight to the analysis of the factors leading to the problem by assigning them all with the same three linguistic variables. This of course compromises the validity of

the method, as an independent assessor or a decision maker may try to express each of the criteria influencing the comparison process by using a set of linguistic variables matching the specific criterion. The advantage of the method proposed by Moore and Bea, compared to Sharp's method was that it indicated the interdependence between the factors involved in the test case, even if that occurs at a preliminary surface level. Mannarelli in his paper [Mannarelli et al., 1996] described a method under which a model is developed to compare maturity and error, in high and low risk organisations according to human error reliability in other operational or design stages.

In order to help managers and other executive members diagnose the root cause of organisational problems and challenges, by giving guidance towards a proper management of change, this chapter presents a distinctive approach incorporating evidential reasoning. This enables a fast and reliable self-assessment and comparison with other companies in the same field. The purpose of the methodology proposed is to identify and underline the factors producing ineffective outcomes. In the same sense the method can be used to examine the factors affecting an organisation's ability to meet critical organisational challenges such as sudden changes in governmental regulations, major shifts in customer expectations or even new competitive threats. Then decisions are made based on the organisation's capacities and prospects for planned change.

The organisations that will incorporate the concept and the approach presented here into their own decision-making will need to look for the sources and challenges that need to be dealt with and act upon them. After deciding which changes to implement, they need to obtain periodic feedback on the implementation processes and outcomes. They will need to use this feedback for their benefit in order to see what further changes are required, along with certain adaptation to several influencing factors. As it will be seen from this chapter, several levels of criteria appear within the decision making process. They are broken down to extend the analysis as much as possible.. This method can create a connection between theory and practice, by opening a broad spectrum of organisational theory and research but at the same time responding directly to the distinctive conditions shaping organisational operations and change options.

Weisbord's six-box model [Weisbord, 1976] is a straightforward and easy to use method to model the main criteria before the application of ER takes place. The six-box model aims at preparing the ground for the creation of the criteria seen in Section 7.3. In presenting it, Weisbord tried to gather years of consulting experience and provide users with six key factors any problem may generate. The model's ease of comprehension and its potential use in management development made it a widely spread cited material in organisation's development texts [French & Bell, 1995], as well as being recommended as the diagnostic model of choice when diagnosis is done under time constraints or when organisational participants do not have any prior knowledge of open system concepts [Burke, 1982]. The starting point of the model is the identification of those organisational outputs with which both the external customers and the internal producers are dissatisfied. Identification of these outputs leads the participants towards the sources that cause the dissatisfaction from both sides. Internal producers are the key players during decision making within an organisation, and if they are not satisfied, organisational ineffectiveness exists and needs to be dealt with.

General managers and human resources (HR) specialists often question whether their organisation is developing the HR programmes and practices that are most critical to the success of a project. One way to answer this question is through benchmarking [Glanz & Dailey, 1992]. This technique involves measurement of a key HR practice, followed by a comparison between practices in the focal organisation and the best practices of other organisations in order to target several areas for further improvement. In very large multinational organisations, practices from other units within the same organisation can be used as internal benchmarks. Benchmarking had its origins in investigations performed by an independent firm concerning another company's practice code in functional areas, such as production or distribution, in which the second firm has an outstanding reputation [Tucker et. al, 1987]. Benchmarking can help HR managers decide which current practices should be encouraged and which new practices initiated. HR practitioners can also use benchmarking to help justify investments in particular HR practices. As soon as the six-box model is built and combined with ER, the organisation's managers will be in a position to know if their performance can be used as a benchmark for others within the same field.

7.2 Background theory of evidential reasoning (ER)

The background information on ER was given analytically in Chapter 4, in sections 4.2.1, 4.2.2 and 4.2.3. What will be seen in the next sections is the development of a methodology based on ER approach and existing organisational methods.

7.3 Methodology of the organisational self-assessment and comparison model

This model has been developed in order to ensure the quality of service of the organisation which, will meet both the appropriate target set as well as the time constraints imposed, up until the completion of the project.

There are four factors, which should be taken into consideration in order to achieve the required results. The factors in sequential order are:

1) Gathering of data in order to obtain a comprehensive overview of operations. The focus of data should be on the core problems and challenges that need to be met.
2) Use of theoretical frames to organise core problems and challenges and to link them into the organisational features.
3) Development of a model that captures the nature of the ineffective outcomes.
4) Feedback gained from the model and the relevant acquired data.

The organisation at the beginning will need to form an initial model, which contains the elements that will be explored for the safety project in question. Then it needs to present the problems or the challenges, which should be tackled at the diagnostic level (2^{nd} level criteria as it will be seen further down). The organisation will seek to clarify the nature of these problems and develop a preliminary view of organisational strengths and weaknesses. During these stages, the organisation will also try to judge the likelihood that members will co-operate with data-gathering activities, the prospects for involving external participants in the diagnosis and the organisation's receptiveness to feedback. The level of feedback achieved, and the way it implements changes within the organisation is described by the linguistic variables characterising the maturity levels (top level criterion).

7.4 A modified ER approach methodology in organisational self-assessment

A generic comparison framework is proposed through the following steps to assist in the application of the methods discussed in the theory section of this chapter. The main aim is to present a credible means of comparison, which at the same time could be used as a self-assessment tool, if required, to measure performance and set the benchmarking levels within similar companies. The following steps describe the process followed in order to reach adequate results.

Step 1. Create and adjust a six-box model based on leadership. Create an itemised list of main factors influencing each one of the six boxes.

The six-box model shown in Figure 7.1 exists to contain the possible causes of dissatisfaction with organisational products or services. Each box represents a cluster of frequently occurring organisational problems. It is essential to analyse the content of the boxes before proceeding to the proposed methodology as they will be used along with the principles of evidential reasoning.

- Helpful mechanisms. Refers to internal procedures for coordination, control, communication and information management that are intended to help employees in their work roles.
- Relationships. Refers to both within and among organisational units, including conflict resolution arrangements.
- Leadership. Appears as the common point for the remaining five boxes because Weisbord [Weisbord, 1976] assumes "that leaders and their choices, including those concerning the organisation's mission and strategy play a very important role within the organisational effectiveness. Leaders are defined as the key decision makers".
- Structures. Refers to the division of work between several teams or individuals operating within the safety-oriented company.
- Strategy. Extends the vision of the leaders in such a way as to be clear to the rest of the involved teams.
- Rewards. Refers to the proper distribution of rewards after the completion of a project or after a successful self-assessment.

EXCLUDED
UNDER
INSTRUCTION
FROM
UNIVERSITY

Leaving aside the simplicity of this model, when it is ready to be incorporated with the ER regime a few weaknesses are to be addressed. Its major weakness is the lack of a firm theoretical foundation. Weisbord did not provide clear guidelines as to which would be the best way to combine the boxes and particularly how to explain the "gap" between two boxes. Therefore, the model is deceptively simple [Burke, 1994]. To apply it either as a self-assessment tool or as an initial form of a comparison tool, analysts need to work out a complex combination of "gaps" between the boxes.

Figure 7.1 The six-box graphical model [Weisbord, 1976]

Figure 7.1 is analysed to its components so that the itemised list of criteria can be properly assigned. The list of factors is derived as described before under the guidance of expert judgements. Examining the diagram it is obvious that the leadership of the company is responsible for the majority of actions and it is the main factor that will affect the overall performance of the company. Therefore, the top goal (i.e. organisational maturity) will be assigned to the leadership box.

Table 7.1 shows the list of the remaining boxes along with the factors assigned to them in each case. These factors will form part of the second level (main criteria) criteria in the methodology towards the decision-making model.

Table 7.1 List of remaining boxes and main criteria factors assigned to them

Strategy	Safety strategy and planning processes
Structures	Safety data, information and safety knowledge
Rewards	Measurement and benchmarking
Helpful mechanisms	Innovation and research
Relationships	Management and human resources (HR)

A preliminary mathematical model can be constructed on the basis of Bayesian theory. Dependence and independence exists between all 6 boxes as illustrated in Figure 7.1. The preliminary model can be considered as proposed below:

Suppose each of the boxes is considered as a random quantity X_1, $X_2 \ldots X_n$, and also suppose that a predictive model is assumed which specifies that for all n, the joint density function can be written as $p(X_1, X_2, \ldots, X_n) = \prod_{i=1}^{n} p(Xi)$ so that Xi are independent quantities. It then follows straightforwardly that for any $1 \leq m \leq n$, $p(X_{m+1},\ldots,X_n|X_1,\ldots,X_m) = p(X_{m+1},\ldots,X_n)$. This model will produce an initial arithmetical value for each set of $X_1,\ldots,X_n$, which will defer according to the company examined. Additionally, the assignment of linguistic variables can strengthen the model as a credible comparison or self-assessment tool, as further uncertainties can be covered through the assignment of linguistic variables. ER and Intelligent Decision System (IDS) [Yang & Xu, 2001] will address this problem.

Step 2. As soon as the factors are itemised, the top goal assessment grades are set to the common box influencing all others (usually the leadership or management). All assessment grades ranging from the top goal to the last sub criteria level have been chosen by the author of this thesis, after consultation with industrial experts in the form of a structured interview (see Appendix IV).

The assessment grades are assigned to the top goal criterion, expressed through the leadership box. Table 7.2 shows the assessment grades selected.

Table 7.2 Assessment grades defined for organisational maturity

Top goal	**Assessment Grades**				
Maturity level	Initial class performance	Repeatable class performance	Defined class performance	Managed class performance	Optimised class performance

Starting from the best result a company can achieve and ending with the worst, the five levels are proposed as follows:

- Optimised. The organisation has strongly integrated a constant improvement process at its operation. It is the best in its class and the results are used as benchmarking for other.
- Managed. The organisation has a fairly good improvement process. It produces good results, lays down the requirements and tries to meet them through feedback.
- Defined. Systematic process based approach. The organisation has a fixed processes path and tries to adopt the early stages of the improvement trends.
- Repeatable. The organisation tries to do what has already been done without being able to define the actual process to achieve it.
- Initial. When all the above characteristics stop to exist the organisation is struggling to deal with the problem faced.

Consultants and researchers draw a very wide range of definitions and measures of organisational effectiveness. To contribute to successful diagnosis, the effectiveness criteria in use should be appropriately chosen to describe as extensively as possible all the aspects of the organisation in question. The number of criteria reflects the problem's multidimensional nature [Denison & Mishra, 1995]. In order to reach the stage of assigning values to these linguistic variables another set of criteria (2^{nd} level criteria) needs to be proposed as seen in Step 3.

Step 3. The main factors (second level criteria) associated with the rest of the boxes that have already been itemised in Step 1 are given their respective assessment grades.

Following a process similar to Step 2 the assignment of assessment grades is given to the main criteria used for comparison. Table 7.3 shows the proposed respective assessment grades along with a separate analysis for each one of them.

Table 7.3 Assessment grades defined for second level criteria

Main criteria	Assessment Grades				
Safety Data, Information and Knowledge	Very little	Little	Average	Enough	More than enough
Innovation & Research	Very basic	Basic	Normal	Advanced	Excellent
Management and H.R	Very bad	Bad	Average	Good	Very good
Measurement and Benchmarking	Very bad	Bad	Average	Good	Very good
Safety Strategy and Planning Processes	Reactive approach		Stable approach		Pro-active approach

- Safety data, information and knowledge. This is mainly the research that will be done from the organisation's side in order to assess the usage of safety-related historical data that can relate to the particular case examined.
- Innovation and Research. This depends on the effort put in from the company itself. More advanced companies will have their own R&D departments to tackle complex projects assigned to them. Another option would be to hire an external research source like a university to assist with unknown projects.
- Management and human resources. This is probably one of the most important factors of the 2nd level criteria as the assignment of appropriate personnel is taking place along with a clearly defined hierarchy structure as to the way that encountered problems are to be solved.
- Safety strategy and planning processes. The ability of planning ahead and creating different safety scenarios is shown with this criterion. The innovation of the team dealing with a problem is expressed through the safety strategy and the planning process of the company.

Step 4. Sub-criteria are assigned according to the nature of the main factors respectively.

Second level criteria are further extended to 3rd level criteria. It is always within either the decision maker's or the independent assessor's power to analyse all criteria up to a

point where he/she feels comfortable that all aspects have been thoroughly examined. 3rd level criteria are further extended as proposed in Tables 7.4 and 7.5. Analysis of a representative two levels of criteria along with their respective assessment grades can be found in Appendix IV section B.

Table 7.4 Assessment grades defined for third level criteria

3rd level criteria	Assessment Grades				
Organisational Updates	Not very often		Often		Regular
Educational Background and Further Training	Very poor background	Poor background	Average background	Good background	Very good background
Supply Management	Very bad	Bad	Average	Good	Very good
Design Management	Very bad	Bad	Average	Good	Very good
Application of Technical Standards	Very loose	Loose	Normal	Strict	Very strict
Self-Assessment Tools	Very few	A few	Average	Enough	More than enough
Port Security Measures	Very loose	Loose	Normal	Strict	Very strict
Independent Comparison Sources	Not very often		Often		Regular

Table 7.5 Assessment grades defined for fourth level criteria

4th level criteria	Assessment Grades				
Technical Chapters	Very few	A few	Average	Enough	More than enough
Literature Review and Research of new Tech.	Never	A little	Normal	A lot	Continuous
Number of Employees from Higher Education	None	A few	Average	A lot	Whole staff
Level of Funding for Employee Training	Very low	Low	Normal	High	Very high
Comparison of Income between 2 Sequential Years.	Lower		Same		Higher
Customer Satisfaction Forms and Reviews	Very bad	Bad	Normal	Good	Very good
Increased Security Personnel	Very low	Low	Normal	High	Very high
Regular Content Control	Never	A little	Normal	A lot	Continuous
Increased CCTV Throughout Terminal	Never	A little	Normal	A lot	Continuous

Step 5. In order to find out how well an alternative performs across all criteria, the lowest level criteria assessment needs to be first transformed to their relevant upper

levels and ultimately, to the top-level goal. The analytical description of the ER algorithm is given in Chapter 4 within the sub sections of 4.5.

Step 6. In order to make the transformation from lower level to upper level criteria, it is required to feed the information into multi-criteria decision-making software developed for analysis of multilevel decision problems. The software which will assist us in the decision making process is called Intelligent Decision System via Evidential Reasoning "IDS" [Yang & Xu, 2001]. It is a windows based tool, which can be used to built up a model, define alternatives and criteria and perform the assessment for the decision maker.

Step 7. As soon as the aggregated values are derived for each of the companies compared, the ranking takes place according to the overall performance degrees.

Step 8. Based on the combination of the steps above, the proposed methodology will give the assessor the ability to come to certain conclusions concerning the comparison problem that he is dealing with. The criteria and alternatives selected will be the prime factors that will set the boundaries for further discussion.

This methodology will be illustrated through a test case described in the next section. The requirements for a verification experiment are essential to identify and assess the validity of the results obtained. The contribution of expert engineers and academics within the test case presented was invaluable as they add to the credibility and soundness of the results obtained. Weighting factors can also be assigned. For simplicity of calculations it is assumed that all factors have the same weighting factor as far as the final assessment is concerned.

7.5 Test case

An independent source is required to assess the organizational maturity overall performance of four similar organizations Company1, Company2, Company3, and Company4. All of the four companies compared, deal with safety-oriented projects. A short description on the profile of each of these 4 companies is given in Appendix IV in section C. The aim of the test case is to show how the methodology steps can be

utilised in a way that produces credible comparability results concerning the overall performance of each one of the companies. This means the identification of the company with the highest overall score, but at the same time being able to assess the four companies in relation to any of the main criteria identified. For example, company C1 may have a higher overall score than C2 does, but when it comes to comparing a specific main criterion C2 may have a higher score than C1 does for this particular criterion.

Figure 7.2 illustrates a graphical representation of the main goal along with all levels of main and sub-criteria.

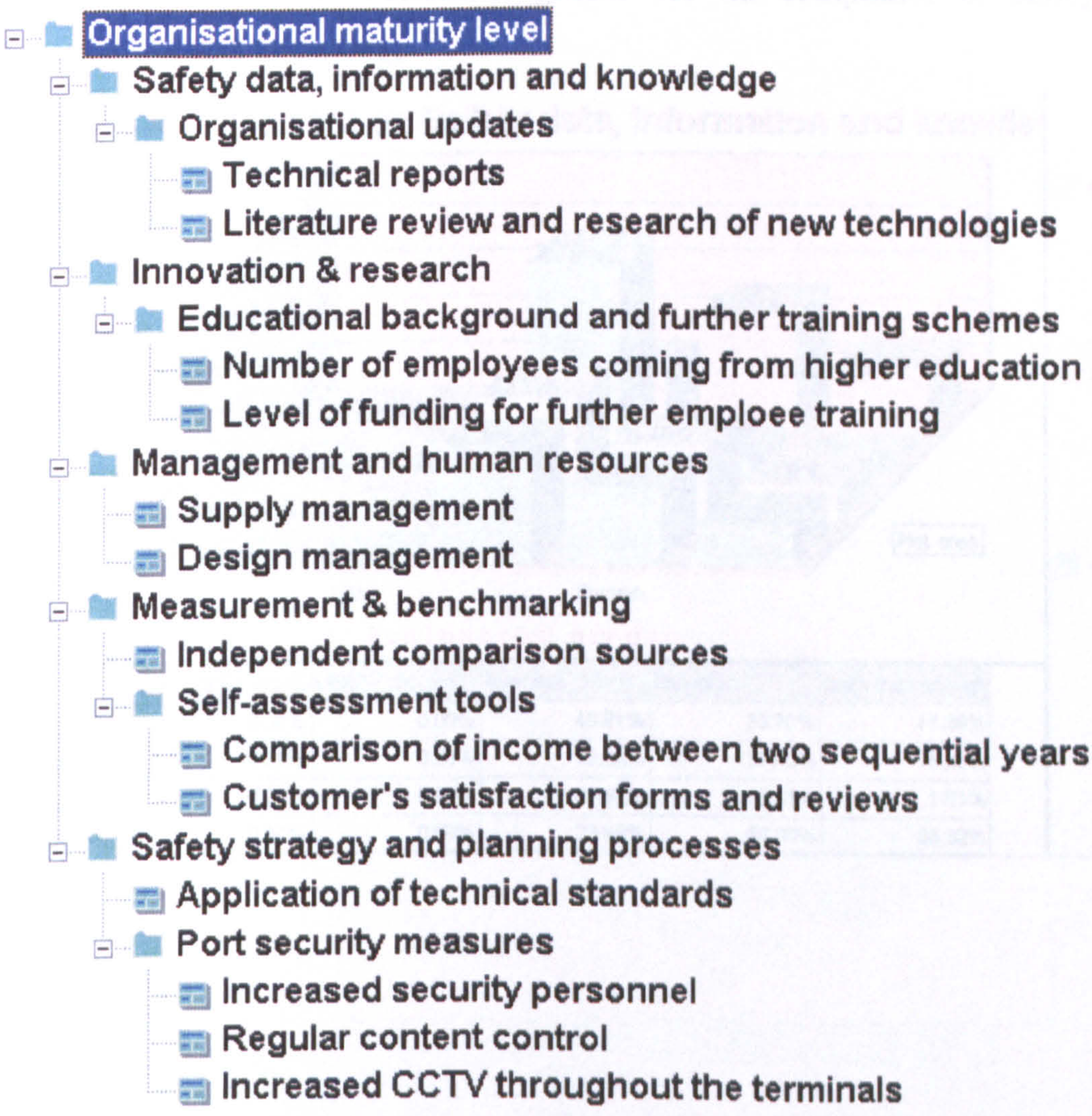
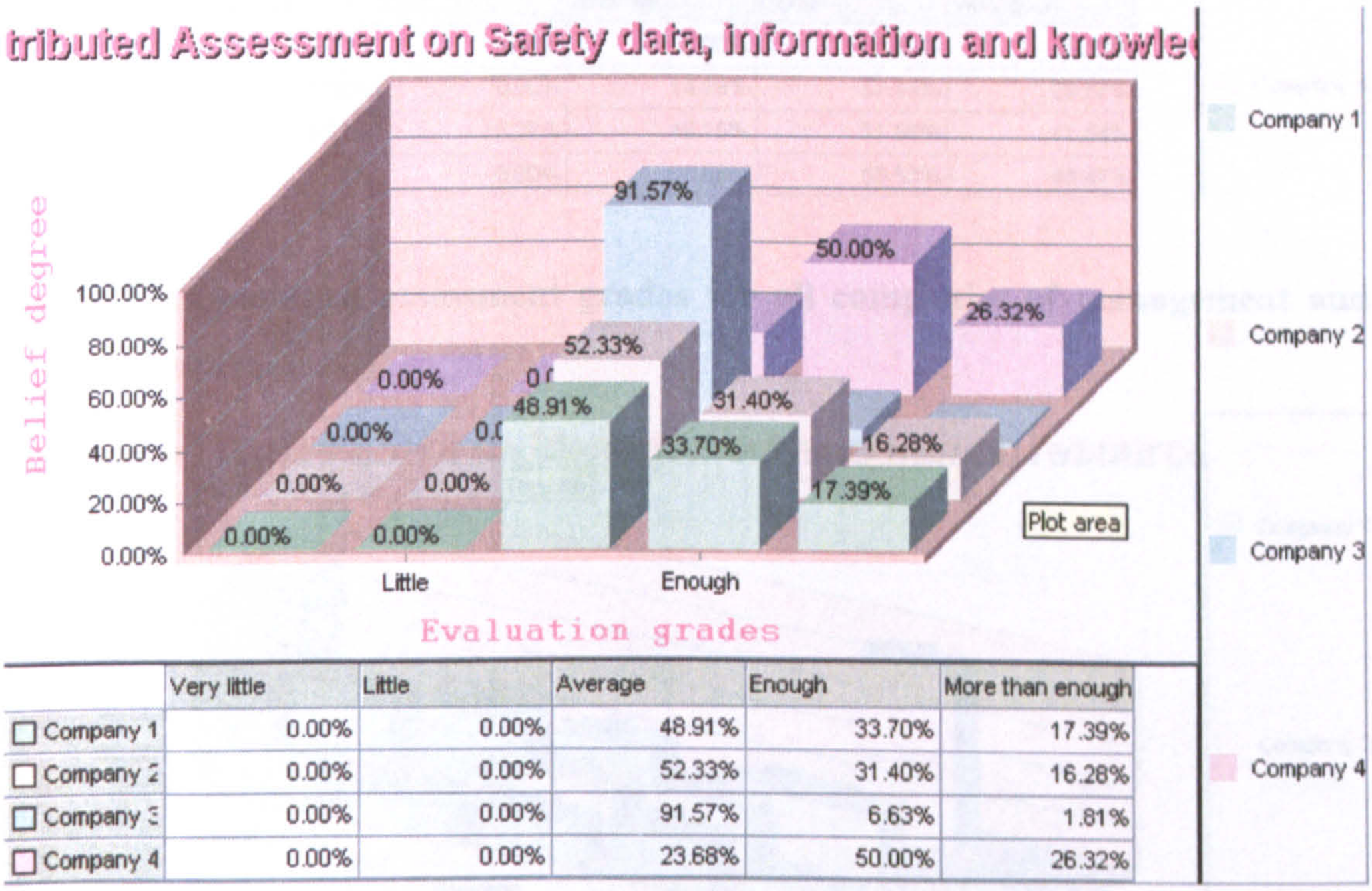


Figure 7.2 Hierarchy of main and sub-criteria

7.5.1 The ER assessment tables

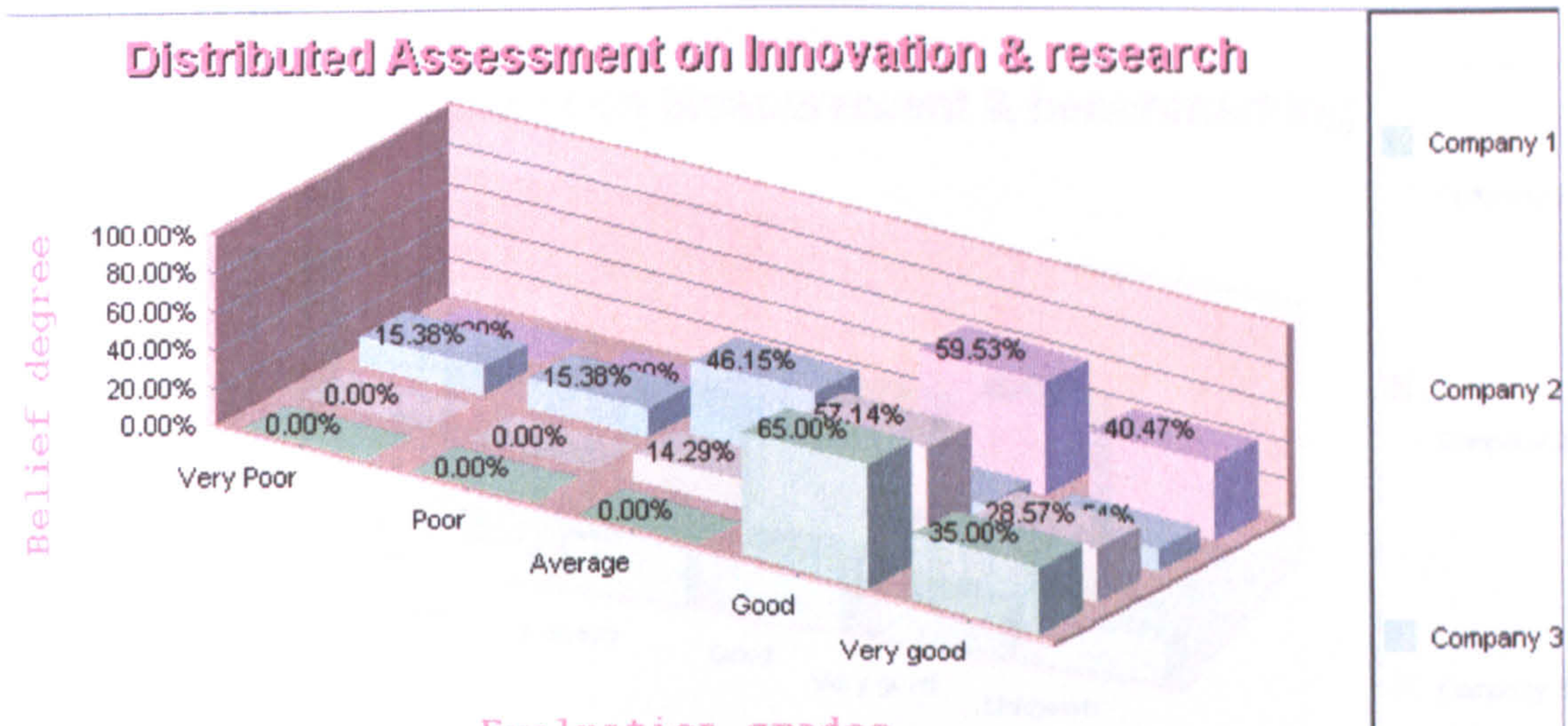
The assessment values given by the author, who is the decision maker in this case, are used within IDS software and the aggregated results are extracted for the main criteria level (second level) and presented in Tables 7.6, 7.7, 7.8, 7.9 and 7.10. The numbers within the cells indicate the degree of belief assigned to each assessment grade respectively. Tables 7.6 to 7.10 are also of outmost importance as an external observer can see the strong and weak points of each one of the companies selected in respect with the associated criteria. All values were derived from the IDS software.

Table 7.6 Combined assessment grades for all companies of safety data, information and knowledge



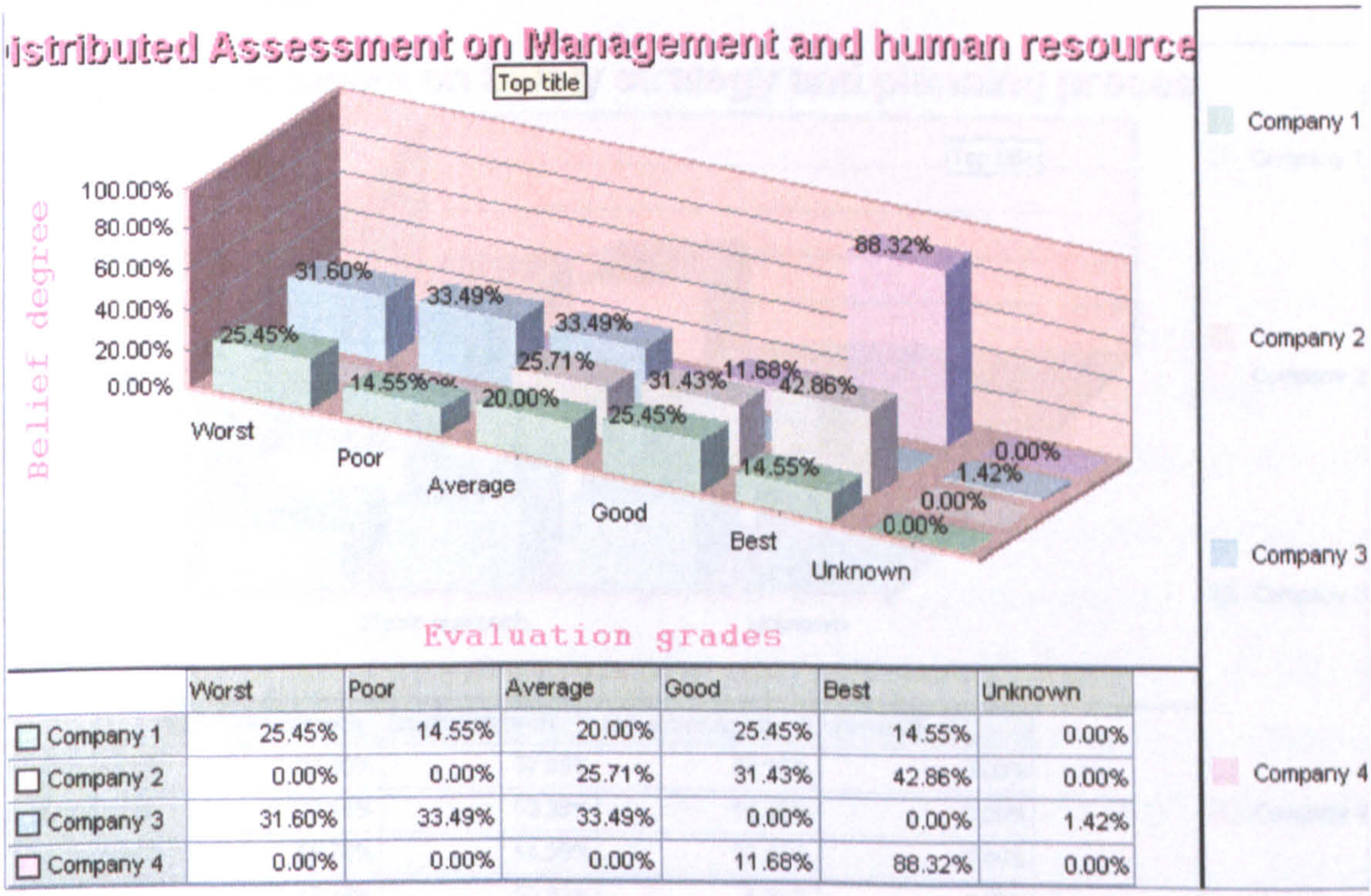
	Very little	Little	Average	Enough	More than enough
Company 1	0.00%	0.00%	48.91%	33.70%	17.39%
Company 2	0.00%	0.00%	52.33%	31.40%	16.28%
Company 3	0.00%	0.00%	91.57%	6.63%	1.81%
Company 4	0.00%	0.00%	23.68%	50.00%	26.32%

Table 7.7 Combined assessment grades for all companies of innovation & research



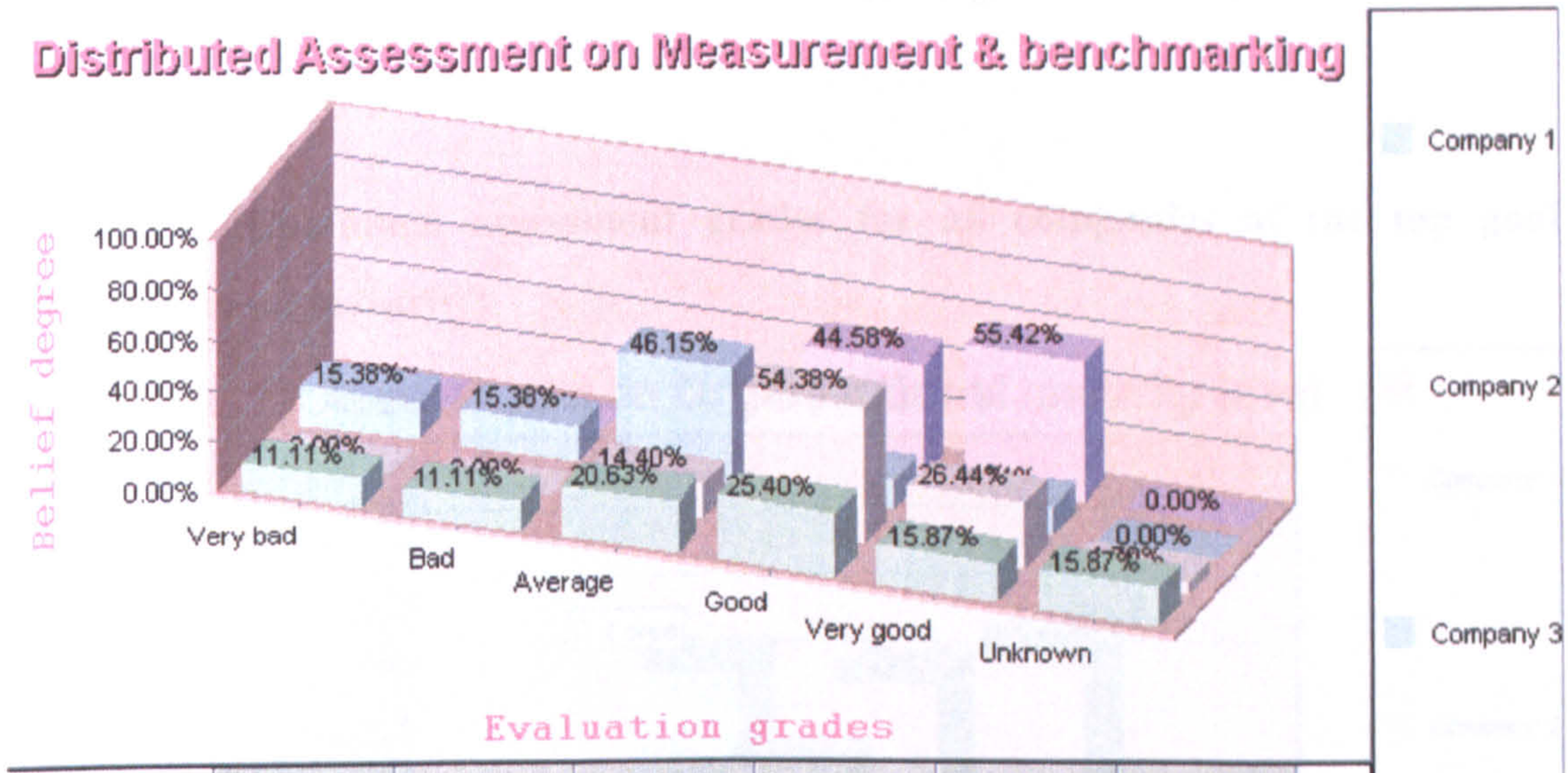
	Very Poor	Poor	Average	Good	Very good
Company 1	0.00%	0.00%	0.00%	65.00%	35.00%
Company 2	0.00%	0.00%	14.29%	57.14%	28.57%
Company 3	15.38%	15.38%	46.15%	11.54%	11.54%
Company 4	0.00%	0.00%	0.00%	59.53%	40.47%

Table 7.8 Combined assessment grades for all companies of management and human resources



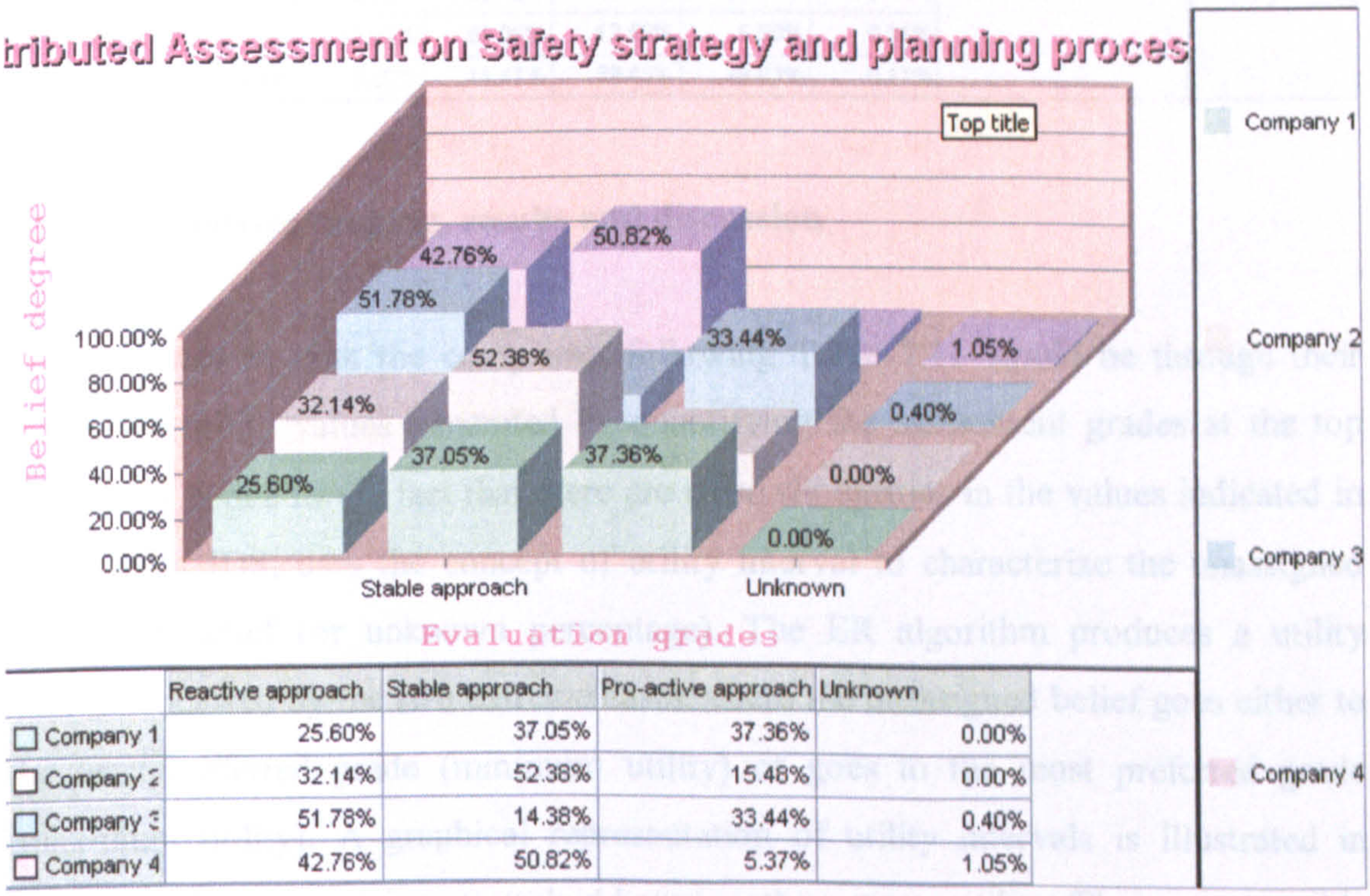
	Worst	Poor	Average	Good	Best	Unknown
Company 1	25.45%	14.55%	20.00%	25.45%	14.55%	0.00%
Company 2	0.00%	0.00%	25.71%	31.43%	42.86%	0.00%
Company 3	31.60%	33.49%	33.49%	0.00%	0.00%	1.42%
Company 4	0.00%	0.00%	0.00%	11.68%	88.32%	0.00%

Table 7.9 Combined assessment grades for all companies of measurement & benchmarking



	Very bad	Bad	Average	Good	Very good	Unknown
Company 1	11.11%	11.11%	20.63%	25.40%	15.87%	15.87%
Company 2	0.00%	0.00%	14.40%	54.38%	26.44%	4.79%
Company 3	15.38%	15.38%	46.15%	11.54%	11.54%	0.00%
Company 4	0.00%	0.00%	0.00%	44.58%	55.42%	0.00%

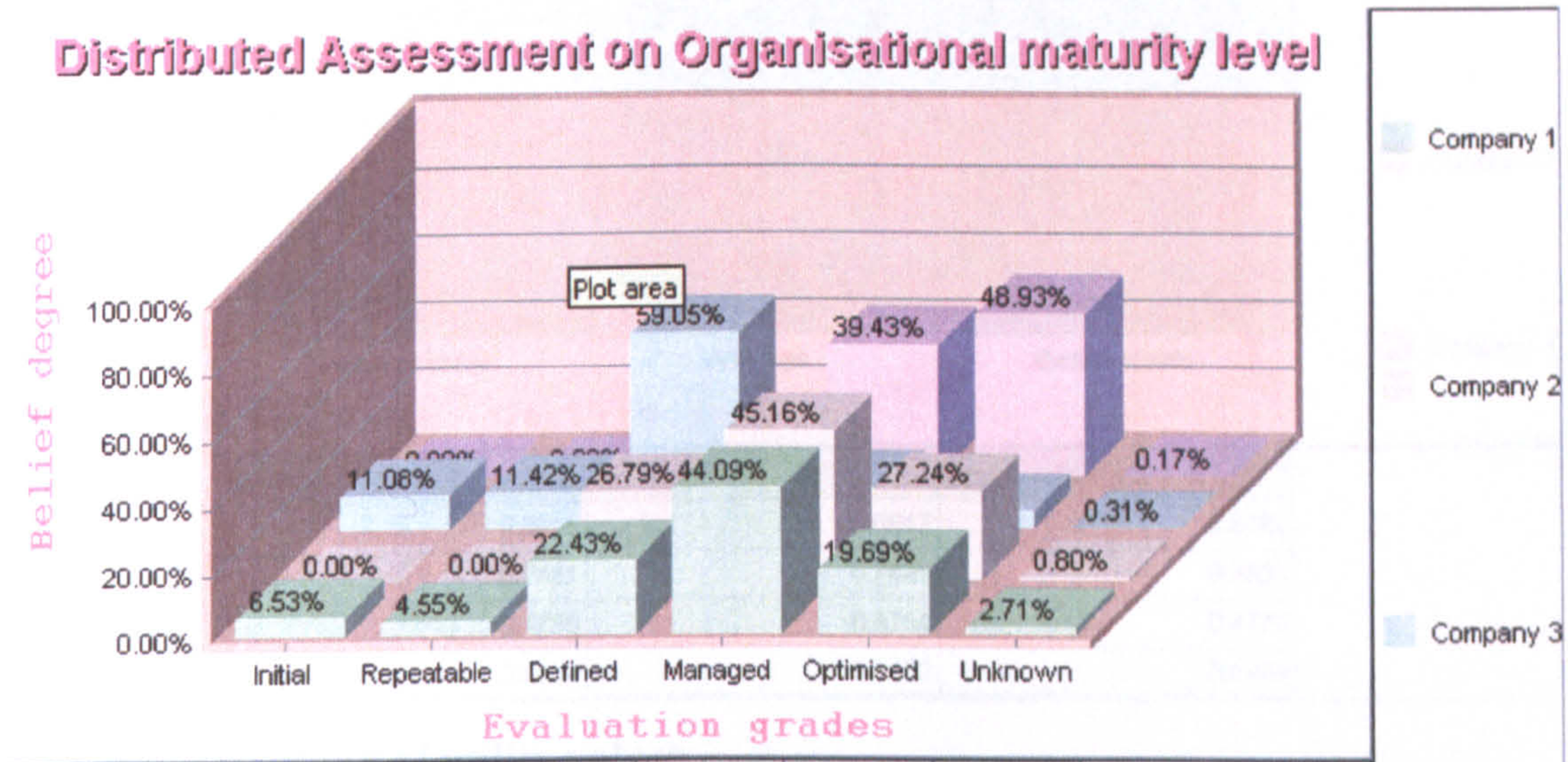
Table 7.10 Combined assessment grades for all companies of safety strategy and planning processes



	Reactive approach	Stable approach	Pro-active approach	Unknown
Company 1	25.60%	37.05%	37.36%	0.00%
Company 2	32.14%	52.38%	15.48%	0.00%
Company 3	51.78%	14.38%	33.44%	0.40%
Company 4	42.76%	50.82%	5.37%	1.05%

The assessments in Tables 7.6 to 7.10 need to be propagated to the top level. In doing this, the IDS software produces the results shown in Table 7.11. The numbers under each grade indicate the aggregated assessments (or degrees of belief) of the decision maker.

Table 7.11 Combined assessment grades for all companies of the top goal (organisational maturity)

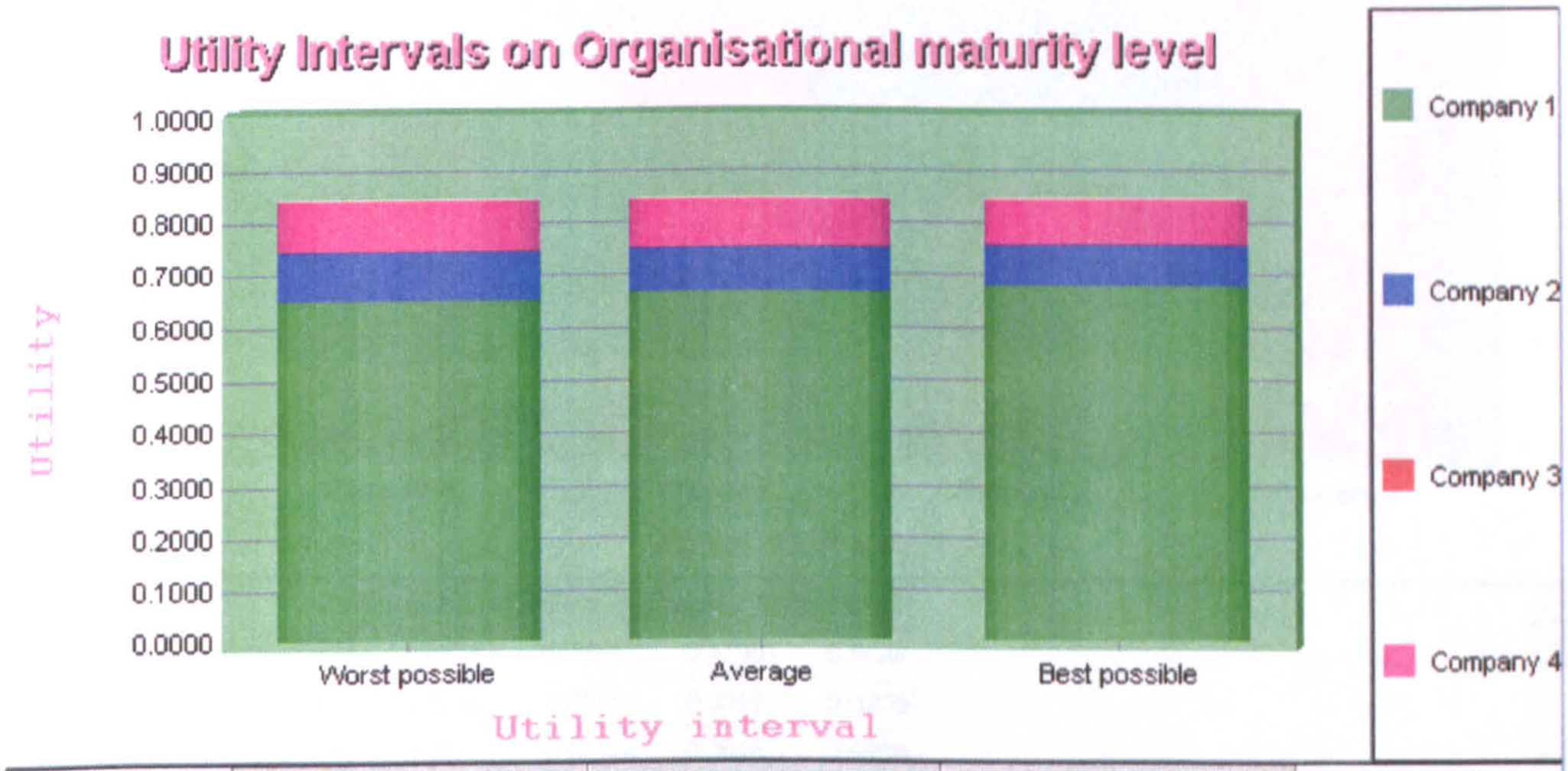


	Initial	Repeatable	Defined	Managed	Optimised	Unknown
Company 1	6.53%	4.55%	22.43%	44.09%	19.69%	2.71%
Company 2	0.00%	0.00%	26.79%	45.16%	27.24%	0.80%
Company 3	11.08%	11.42%	59.05%	12.56%	5.59%	0.31%
Company 4	0.00%	0.00%	11.47%	39.43%	48.93%	0.17%

7.5.2 Alternatives ranking, results and discussion

The best way to rank the companies following Table 7.11 would be through their respective utility values generated by quantifying the assessment grades at the top level. This is due to the fact that there are close similarities in the values indicated in Table 7.11. IDS, uses the concept of utility interval to characterize the unassigned degree of belief (or unknown percentage). The ER algorithm produces a utility interval enclosed by the two extreme cases where the unassigned belief goes either to the least preferred grade (minimum utility) or goes to the most preferred grade (maximum utility). A graphical representation of utility intervals is illustrated in Figure 7.3. The companies are ranked based on the average utility. The worst possible

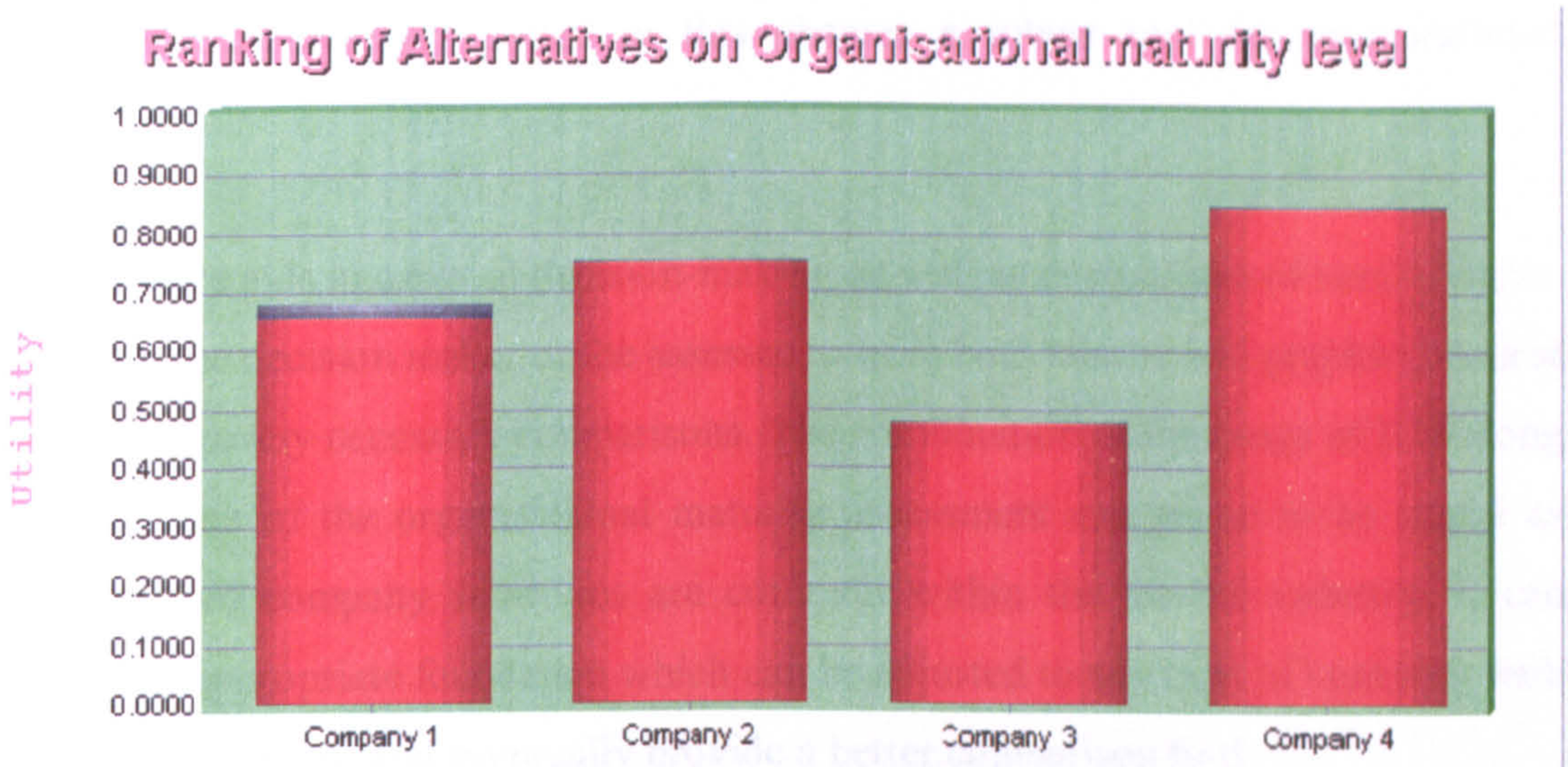
utility value is represented by green colour, an average utility value is represented by blue colour and the best possible utility value is represented by magenta colour.



	Worst possible	Average	Best possible
Company 1	0.6511	0.6647	0.6782
Company 2	0.7451	0.7491	0.7531
Company 3	0.4739	0.4754	0.4770
Company 4	0.8424	0.8432	0.8441

Figure 7.3 Ranking of utility values

Having found maximum and minimum utilities the average utility is calculated and used to rank the maturity level within the selection process. The final ranking of companies is as shown in Figure 7.4:



	Company 1	Company 2	Company 3	Company 4
Minimum score	0.6511	0.7451	0.4739	0.8424
Average minus minimum	0.0135	0.0040	0.0015	0.0009
Maximum minus average	0.0135	0.0040	0.0015	0.0009

Figure 7.4 Graphical ranking of companies compared

Company 4 is more preferred than company 2, which is more preferred than company 1, which is more preferred than company 3 in terms of overall organisational maturity.

7.6 Conclusion

In the example examined, an ER approach was used in order to tackle the problem of comparing different companies in terms of organisational maturity incorporating both qualitative and quantitative information. The problem of assessing both quantitative and qualitative data remains to cope with incomplete information in many cases. The steps followed within the methodology set at the beginning have been able, with the aid of IDS, to give adequate results that the decision maker can use even though some data was missing. A very important advantage in this case is that data could also be presented in the form of degrees of belief, so that assessment could be made at different levels. The results produced from this test case are validated against the current status of the 4 companies that have been assessed. The final ranking of the 4 companies matches closely their actual current status thus proving the proposed

combined methodology applied in this chapter a robust tool for organisational comparison.

IDS software aids in cases of decision-making as well as comparison of similar items. It enables the decision maker or the assessor to have both tabular and graphical data at hand to make any necessary comparisons. The combination of the usage of IDS along with the case of the organisational maturity assessment can prove to be useful as safety related company selections are common within the marine industry. It can provide an appropriate foundation which can be adjusted to any type of company with minor modifications and eventually provide a better comparison tool.

CHAPTER 8: CONCLUSION

8.1 Review

The research in this thesis was motivated by the requirement to tackle uncertainty and human element problem issues in the marine and offshore industry. As such, several powerful and efficient tools and techniques were employed in the development of integrative risk-based analytical models for maritime application domains. The development phases for the models had to be supplied with data and uncertainties were handled via inference processing that are based on sound theorems, rules or logic. The proposed methodologies were also enabled via resourceful maritime case studies in order to demonstrate their practicality. This falls into place with the overall aim of this thesis.

Before the scene of this thesis was set, background research revealed that safety in the marine industry was previously a case of being reactive in terms of responses after the occurrence of a major accident. A change in this culture would enable proactive approaches to be applied, and as such, near misses and incident occurrences would be taken under consideration. Formal safety assessment (FSA) is the main framework required reviewing in the marine industry in opposition to the safety case required for offshore installations. On the basis of FSA concepts, a proposed framework for the risk-based assessment settings of this research has been developed in a generic sense to be effectively applicable to all ship types, offshore installations, their systems/subsystems and the maritime environment. The framework incorporates risk analysis for which data was obtained from industrial databases and/or by expert judgement. A review of the fundamental FSA principles was presented. Established methodologies concerning safety and reliability analytical tools were reviewed in their application to generate domain models.

Multi-criteria decision making synthesis based on ER is utilised as a selection tool when dealing with an organisational vessel selection process. All the mentioned proposed models have their respective test case to demonstrate their applicability within a marine engineering and organisational regime. Bayesian network (BN) was adopted as the modelling tool that deals with the random/inherent uncertainties and

also enables a powerful marine decision-support solution. In this thesis it is called to deal with cargo handling engineering systems such as an LPG's reliquefaction plant. First and Second order reliability methods (Form/Sorm) using a specific variable transformation methodology for variables that are ruled by uncertainty or vagueness, present a Cartesian coordinate system where the most likely failure point can be calculated when searching an overall failure probability. Organisational self assessment is an upraising issue within the marine industry specially when it comes to safety related assessment. When dealing with complex engineering systems, it is required both from the public view and from the organisation handling the system that safety standards are met and hopefully exceeded. Organisational self assessment in terms of safety maturity has been an issue evidential reasoning (ER) and the six box model are called to assess. The proposed combination of these two techniques provides a tool able to create a risk modelling plane making the ranking of companies working in the same area viable even if some comparison data is governed by uncertainty or vagueness.

Following the review of the research conducted within this thesis, it can be confirmed that not only has the work followed a logical sequence, but that most importantly, the aim and objectives of this thesis have been successfully achieved. Collectively, each one of the developed tools for the risk-based analytical modelling can be integrated into the proposed framework given by the FSA approach.

8.2 Principal statements

The undertaken research has resulted in the following principal statements:

- Where it is difficult to describe the basic failure events of a system using probabilistic risk analysis methods, subjective reasoning analysis has been more appropriate to assess the safety of the system. Also, the information from one technique/tool, such as a risk contribution tree (RCT), can be used to process the information produced using another technique/tool, such as a BN. Therefore, the use of well-established safety and reliability analytical techniques (e.g., event tree and fault tree) and/or the developed risk-based analytical tools (e.g., fuzzy logic and Bayesian network) in an integrated

manner may make safety assessment comparatively efficient and convenient since safety information and the advantages of each method may be more efficiently explored.

- The current FSA is an appropriate proactive approach for ensuring improved maritime safety and environmental protection, though the overriding problem on the handling of uncertainty and the human element issue is still not well embraced in such risk-based practice. Maritime industry today chooses to adopt aspects of established FSA techniques like FTA, ETA and RCT. This is despite the fact that it can integrate the application of newly developed (e.g., BN and ER) risk analysis methods in a transparent and justifiable manner. However, choosing only the established techniques it falls short of the unrivalled handling for the different types of uncertainties presented in each study.
- Results from the BN risk-based analytical modelling that were undertaken for an LPG's reliquefaction plant indicate that BNs are promising techniques for maritime risk analysis. These BNs can also be expanded to form influence diagrams, which permit rapid development of a practical decision model.
- The ER approach when combined with the six-box model proposed by Weisbord can form through a multi-criteria decision making framework a powerful ranking tool addressing the organisational issues of safety maturity self assessment. Because of the flexibility that the six box model presents it can leave space to decision makers to expand to further areas at an organisational and management level.

8.3 General limitations

The developed risk-based analytical models provide useful integrative tools for a proactive maritime world but have limitations owing to the complex nature of marine engineering systems and organisational processes. Some of the imposed limitations include the following:

- Conditional probabilities are more difficult to obtain, especially if the probability is conditioned on several states. Many of such probabilities

required to quantify a BN cannot be derived from databases and scientific literature. Therefore, they may need to be taken from domain experts, based on their knowledge and experience.

- No industrial data could be found for situations of maritime near misses and errors and neither has any such subjective judgement been made available by the maritime industry for qualitative risk-based reasoning to be enabled. This is due to the lack of validation of subjective opinions against approved models. All the case study data used in this study, are those from accident database and/or the opinion of experts.
- While the FSA is intended to address safety and environmental aspects, the scope of this study was confined mainly to engineering and organisational systems and processes .

These limitations did not alter the validity of the conclusions and generalisations of the conducted research. Nonetheless, tackling these limitations should enable the advancement of the integrative risk-based modelling to safety-critical maritime systems.

8.4 Proposed future work

Based on the principal statements and the general limitations there are areas concerning the risk based analytical modelling where further analysis needs to be undertaken. Further or future work could be undertaken in the following areas:

- Sensitivity analysis in BNs is broadly concerned with understanding the relationship between local network parameters and global conclusions drawn based on the network. A key aspect of sensitivity analysis is the number of considered parameters. The simplest case involves one parameter at a time, i.e., A single parameter can only be allowed to change in the network to ensure a query constraint. Single parameter changes are easy to visualise and compute, but they are only a subset of possible parameter changes. Thus, a recommendation of great interest is that of changing multiple parameters in the network simultaneously to ensure the query constraint.

- The combined risk matrix presented in Chapter 3 can form the basis of categorisation of all the processes taking place on board a vessel. An easy to follow guide can be formed to give an initial qualitative assessment of processes according to the case examined which then can be fed into a multiple criteria decision making synthesis based on evidential reasoning to choose to deduct quantitative assessments of those processes.
- The developed risk based methodologies can be used to tackle issues of environmental safety. Coast guards and classification societies have started paying great attention to bilge and sludge systems on board vessels. Risk modelling can be applied to those two networks separately along with their respective machinery in order to ensure that the probability of the system failing and its respective consequences remain low enough. This is so that any kind of pollution through either the 3-way discharge valve or any other wrongly connected bilge or sludge line can be avoided.
- Further expansion of the combined ER and six box model can be utilised to assess the severity of consequences in terms of company reputation that an incident may cause. Possible combination with risk modelling techniques like fuzzy logic (FL) or Petri nets can be of usage specially at the duality level of cause and consequence.

8.5 Concluding remarks

In total, this research has been successful in meeting its aim of generating proactive risk-based analytical models that implement novel techniques within a maritime safety framework via its set objectives. Whilst the FSA has provided an elegant route to the application of the well-established safety and reliability analytical techniques for conducting risk analysis, the risk-based analytical modelling of BN, ER and Form/Sorm has been developed to provide powerful tools for uncertainty treatment.

REFERENCES

Aldwinckle, D. S. & Pomeroy, R.V. (1983) "A Rational Assessment of Ship Safety and Reliability." Transactions of Royal Institution of Naval Architects (RINA), Vol.125, pp 269-288.

Armstrong, M., Bailey, W. & Couët, B. (2005) "The Option Value of Acquiring Information in an Oilfield Production Enhancement Project." Journal of Applied Corporate Finance, Vol.17, pp 99.

Barker, C.F & Campbell, C.B. (2001) "Risk management in total system ship design." Journal of Naval Engineers, Vol.112, pp 355-365.

Barker, A. (1990) Engineering quality by design. ASQC Quality Press. New York.

Bayes, T. (1989) "An essay towards solving a problem in the doctrine of chances." Biometrika, Vol.8, pp 293-315.

Belton, V. & Stewart, T.J. (2002) Multiple criteria decision analysis: an integrated approach. Norwell, MA. Kluwer.

Birolini, A. (1993) Quality and reliability of technical systems. Hardcover. Germany.

Bjerager, P. (1990) "On computational methods for structural reliability analysis." Structural Safety, Vol.9, pp 79-96.

BP Global (2004) High Seas Safety. Reports and Publications.
Available from www.bp.com
[Accessed: 2nd September 2006]

Bråfelt, O. & Larsson, T. J. (2000) "Risk Control in the Shipping Industry: Relevant Applications for the Prevention of Accidents." Special Issue of the Safety Science Monitor, Vol.4, Issue 1, Article 3.

Bolsover, A.J. & Wheeler, M. (1999) Decision-Making to Treat an Explosion Hazard. Proceedings of the 8th Annual Conference on Safety on Offshore Installations. ERA Technology. London.UK.

Bozzano, M. & Villafiorita, A. (2003) "Integrating Fault Tree Analysis with Event Ordering Information." Proceedings of ESREL 2003. Maastricht. The Netherlands, pp 247-254.

Bufardi, A. (1998) "On the construction of fuzzy preference structures." Multi-Criteria Decision Analysis, Vol.7, pp 57-88.

Burke, W.W. (1982) Organization development. Little Brown. Boston.

Burke, W.W. (1994) Diagnostic models for organizational development. Howard & Associates. New York.

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

Charniak, E. Shimony, T. & Solomon, E. (1994) "Cost-based abduction and MAP explanation." Artificial Intelligence, Vol.66, pp 345-374.

Coggin, R. (2001) FMEA Annual Trials and Experience of the Ocean Intervention. Dynamic Positioning Conference. Houston. USA.

Conan, G. d'Ozouville, L. & Marchand, M. (1978) Amoco Cadiz - preliminary observations of the oil spill impact on the marine environment. One day session, Amoco Cadiz, Brest, France, 7 June 1978. Le Centre National pour l'Exploitation des Oceans. Paris. France.

Cortazar, G. & Schwartz, E.S. (1998) "Monte Carlo Evaluation Model of an Undeveloped Oil Field." Journal of Energy Finance & Development, Vol. 3, pp 73-84.

D'Ambrosio, B. (1999) "Inference in Bayesian Networks." Artificial Intelligence Magazine, Vol.20,pp 21-36.

Dagum, P. & Luby, M. (1993) "Approximating probabilistic inference in Bayesian belief networks is np-hard." Artificial Intelligence, Vol.60, pp 141-153.

Delgado, M. Herrera, F. E. & Martinez, L. (1998) "Combining Numerical and Linguistic Information in Group Decision Making." Journal of Information Sciences, Vol.107, pp 177-194.

Denison, D. & Mishra, A. (1995) "Towards a theory of organizational culture and effectiveness." Journal of Organizational Science. Vol.6, pp 204-223.

DETR (2000) Port Marine Safety Code. Department for Transport. London.

DNV Home (2006) Innovative and Risk-Based Ship Design. Classification News, No. 2.
Available from www.dnv.com
[Accessed: 18th August 2006]

DOE (1990) The Public Enquiry into the Piper Alpha Disaster (Cullen Report). Department of Energy (DOE), HMSO. London. UK.

EMPA (2006) "How Port Directive Fiasco Made History." European Maritime Pilot's Association Journal. Vol.42, pp 1-5.

EPA (1996) "Proposed Guidelines for Ecological Risk Assessment." US Environmental Protection Agency (EPA) Notice, Federal Register, FRL-5605-9, Vol.61, pp 47551-47631.

Evans, M. Hastings, N. & Peacock, B. (1993) Statistical distributions. Wiley & Sons. New York. USA.

French, W. & Bell, C. (1995) Organization development. 5th ed. Englewood cliffs. Prentice Hall. New Jersey.

Frey, G. Brendan, J. (1998) Graphical models for machine learning and digital communication. The MIT Press.

Frühwirth-Schnatter, S. (1993) "On Fuzzy Bayesian Inference."Fuzzy Sets and Systems, Vol. 60, pp 41-58.

Fussel, J.B. (1973) Synthetic Tree Model - Formal Methodology for Fault Tree Construction. ANCR-1098. Spring Field. USA.

Galt, J.A. Lehr, W.J. & Payton, D.L. (1991) "Fate and transport of the Exxon Valdez oil spill." Journal of Environmental Science & Technology. Vol. 25, pp 202-209.

Geiger, D. & Heckerman, D. (1995) "A characterization of the dirichlet distribution with application to learning bayesian networks." Proceedings of the Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann, pp 196-207. San Francisco. California.

Glanz, E.F. & Dailey L.K. (1992) Benchmarking and human resource management. Garden City. New York.

Green, A.E. & Bourne, A.J. (1972) Reliability Technology. John Wiley & Sons. New York. USA.

Groumpos, P.P. & Merkuryev, Y. (2002) "A Methodology of Discrete-Event Simulation of Manufacturing Systems: An Overview." Studies in Informatics and Control,Vol.11, pp 53-60.

Guedes, C.G. & Teixeira, A.P. (2001) "Risk assessment in maritime transportation." Reliability Engineering and System Safety. Vol.74, pp 299-309.

Halebsky, M. (1989) "System Safety Engineering as Applied to Ship Design." Journal of Marine Technology, Vol.26, pp 245-251.

Hasofer, A.M. & Lind, N.C. (1974) "An exact and invariant first order reliability format." Journal of Mechanical Engineering, Vol.100, pp 111-121.

Hauge, H.J. (2001) A Survey of Software Safety. NTNU Technical Report. Norwegian University of Science and Technology (NTNU). Norway.

Henley, E. J. & Kumamoto, H. (1981) Reliability Engineering and Risk Assessment. Prentice Hall. Englewood Cliffs. New Jersey. USA.

Hendershot, D.C. Post, R.L. Valerio, P.F. Vinson, J.W. Lorenzo, D.K. & Walker, D.A. (1998) Putting the "OP" Back in "HAZOP." MAINTECH South '98 Conference and Exhibition. Houston. USA.

Hobbs, J. Stickel, M. Martin, P. & Edwards, D. (1988) "Interpretation as abduction." Proceedings of the 26th Annual Meeting of the Association for Computational Linguistics. Association for Computational Linguistics, pp 95-103. Menlo Park. California.

House of Lords (1992) Safety aspects of ship design technology. Select Committee on Science and Technology. 2nd report. London.

HSC (2004) Consultative Document 198: Proposals to Replace the Offshore Installations (Safety Case) Regulations 1992.

HSE (2003) Transport Fatal Accidents and FN-Curves: 1967-2001. Research Report 073. HSE Books.

HSE (2002) Marine Risk Assessment. Offshore Technology Report 2001/063. Prepared by Det Norske Veritas (DNV). HSE Books.

HSE (2001) Reducing Risks, Protecting People. HSE's Decision-Making Process. HSE Books.

HSE (1998) A guide to the Offshore Installations (Safety Case) Regulations 1992. 2nd Edition. HSE Books.

HSE (1988) Docks Regulations 1988. Approved Code of Practice with Regulations and Guidance. HSE Books.

Huang, C.L. & Yoon, K. (1981) Multiple attribute decision making methods and applications: a state of the art survey. Springer-Verlang. New York.

Hugin (© 1995-2003) Hugin expert light A/S. Denmark.

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

IMCA (2002) Guidelines on Failure Modes and Effects Analyses (FMEAs), International. Marine Contractors Association (IMCA). London. UK.

IMO (2004) Formal Safety Assessment Risk Evaluation, Submitted by the International Association of Classification Societies (IACS). MSC 78/19/2.

IMO (2002) Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process. MSC Circ.1023/MEPC Circ.392.

IMO (2002a) International Collaborative FSA Study on Bulk Carriers - Step 2 of FSA (Risk Analysis) WP 11. Develop Risk Contribution Tree Components, MSC 75/INF.22. Submitted by France to IMO.

IMO (2001) Focus on IMO: A Summary of IMO Conventions. London. UK.

IMO (2001a), Formal Safety Assessment of Bulk Carriers Fore-end Watertight Integrity. Submitted by IACS to IMO. MSC 74/5/4.

IMO (1999) Resolution of the 1997 SOLAS Conference Relating to Bulk Carrier Safety. Series ID: IMO-160E.London.

IMO (1998) Formal Safety Assessment Experience Gained from the Trial Application Undertaken by the United Kingdom. Submitted by the United Kingdom to IMO Maritime Safety Committee. MSC 69/INF.

IMO (1997) Interim Guidelines for the Application of Formal Safety Assessment (FSA) to the IMO Rule-making Process. MSC/Circ.829 and MEPC/Circ.335.

IMO (1996) Formal Safety Assessment. MSC 66/INF.8. Submitted by the United Kingdom to IMO Maritime Safety Committee. London.

ISGOT (2006) International Safety Guide for Oil Tankers and Terminals. 5th Edition. Witherbys Publishing.

Jensen, F.V. & Dittmer, S.L. (1994) "From Influence Diagrams to Junction Trees." Proceedings of the 10th Conference on Uncertainty in Artificial Intelligence. Morgan Kaufmann. San Francisco. USA, pp 367-373.

Jensen, F.V. (1993) Introduction to Bayesian Networks: HUGIN. Aalborg University Press. Denmark.

Kadie, C.M., Hovel, D. & Horvitz, E. (2001) MSBNx: A Component-Centric Toolkit for Modeling and Inference with Bayesian Networks. Microsoft Research Technical Report MSR-TR-2001-67. Microsoft Corporation. Redmond. USA.

Kaimal, J.C. & Finnigan, J.J. (1994) Atmospheric boundary layer flows. Oxford University Press. New York. USA.

Kendal, M.G. Stuart, A. & Keith, J. (1994) The advanced theory of statistics. Vol.1. Distribution Theory. Oxford University Press. New York. USA.

Kletz, T. A. (1974) HAZOP and HAZAN - Notes on the Identification and Assessment of Hazards. Institute of Chemical Engineers. Rugby. UK.

Kschischang, F. (2000) "Factor graphs and the sum-product algorithm." IEEE Transactions on Information Theory, Vol.47, pp 498-519.

Kumamoto, H. & Ernest, J. (1996) Probabilistic risk assessment and management for engineers and scientists. 2nd Edition. John Wiley & Sons. New York.

Lauritzen, S.L. & Spiegelhalter, D.J. (1988) "Local computations with probabilities on graphical structures and their application to expert systems." Journal of the Royal Statistical Society, Vol.50, pp 157-224.

Lin, P.L. & Kiureghian, A. (1986) "Multivariate distribution models with prescribed marginals and covariances." Probabilistic Engineering Mathematics, Vol.1, pp 105-112.

Liu, P.L. & Kiureghian, A. (1991) Optimisation algorithms for structural reliability." Journal of Structural safety, Vol.9, pp 161-177.

LPG/C Melina (1980) Liquefied Petroleum Gas/Carrier Melina. Cargo Plant Operating Manual. Provided by Interunity Management Corporation. Athens. Greece.

LR (1982) Pump System Reliability Data. Lloyds Register (LR). London. UK.

Madsen, H.O. Krenk, S. & Lind, N.C (1986) Methods of structural safety. Prentice Hall. Englewood Cliffs. New Jersey. USA.

Mannan, S. (2005) Lees' Loss Prevention in the Process Industries. 3rd Edition. Butterworth Heinemann Ltd.

Mannareli, T. Roberts K.H. & Bea, R.G. (1996) "Learning how organizations mitigate risk." Journal of Contingencies and Crisis Management, Vol.4, pp 83-92.

Mathiesen, T. C. (1997) Cost Benefit Analysis of Existing Bulk Carriers, DNV Paper Series No 97-P008.

Meek, C. (1995) "Strong completeness and faithfulness in bayesian networks," Proceedings of the Conference on Uncertainty in Artificial Intelligence, Morgan Kaufmann. San Francisco, California, pp 411-418.

Microsoft Corporation (2003) Help and Support Centre Networks. Available from: www.microsoft.com

[Accessed : 10th September, 2006]

Misra, K. B. (1992) Reliability Analysis and Prediction. Elsevier Science Publishers. Oxford. UK

Mitchell, B. (1996) Comparative assessment of advanced techniques for the evaluation of confidence levels in calculated safety margins. HSE Books. London. UK.

MOD (1996) Safety Management Requirements for Defence Systems. Defence Standard 00-56. Ministry of Defence (MOD), Issue 2. Glasgow. UK

Moore, W.H. & Bea, R.G. (1995) "Management of Human and Organizational Error in Operational Reliability of Marine Structures." Final Joint Industry Project Report. Report No. HOE-93-1. University of California. Berkeley. California.

MSA (1993) Formal Safety Assessment, MSC66/14, Submitted by the United Kingdom to IMO Maritime Safety Committee, London.

MSA (1996) Formal Safety Assessment, MSC66/14, Submitted by the United Kingdom to IMO Maritime Safety Committee.

Nataf, E. (1962) Determination of confidence levels in probability distributions. Academy of Sciences. Paris.

Netica (2002) Netica-J Reference Manual - Version 2.21. Java Version of Netica API. Norsys Software Corporation. Norway.

Nielsen D.S. Platz, O. & Kongs, H.E (1977) Reliability Analysis of Proposed Instrument Air System. RISØ-M-1903. RISØ National Laboratories. Denmark.

Nilsson, D. (1998) "An efficient algorithm for finding the M most probable configurations in probabilistic expert systems." Journal of Statistics and Computing." Vol.8, pp 159-173.

NOAA (1978) The Amoco Cadiz oil spill: A preliminary scientific report. A National Oceanic and Atmospheric Administration and Environmental Protection Agency special report. Washington DC. USA.

OREDA (2002) Offshore Reliability Data Handbook. 4th Edition. Det Norske Veritas. Norway.

Pan, H. & McMichael, D. (1998) Fuzzy Causal Probabilistic Networks - A New Ideal and Practical Inference Engine. Proceedings of IAIAF'97. 1st International Conference on Multisource-Multisensor Information Fusion. Las Vegas. USA.

Panofsky, H.A. & Dutton, J.A. (1984) Atmospheric turbulence. Wiley & Sons. New York. USA.

Peachey, J. (1995) Formal Safety Assessment Seminar. Overview of the 5 Steps of FSA. International Maritime Organisation MSA. Section 1, Paper 2.

Pearl, J. (1988) Probabilistic reasoning in intelligent systems: Networks of plausible inference, Morgan Kaufman, San Mateo, California.

Peng Y. & Reggia, J.A. (1990) Abductive inference models for diagnostic problem-solving. Springer-Verlag. New York.

Pentti, H. & Atte, H. (2002) Failure Mode and Effects Analysis of Software-Based Automation Systems. VTT Industrial Systems. Helsinki. Finland.

Rackwitz, R. & Fiessler, B. (1978) Structural reliability under combined random load sequences. Computational and Structures, Vol.9, pp 489-494.

Rice, S.D. Spies, R.B. Wolfe, D.A. & Wright, B.A. (1996) Proceedings of the Exxon Valdez oil spill symposium. American Fisheries Society. Bethesda. Maryland. USA.

Riding, J. F. (1997) "Formal Safety Assessment (FSA): Putting Risk into Marine Regulations." Transactions of the IMarE, Vol.109, pp 185-192.

Rosenblatt, M. (1952) "Remarks on multivariate transformation." Mathematics and Statistics, Vol.23, pp 470-472.

Saaty, T.L. (1988) The analytic hierarchy process. University of Pittsburgh. Pittsburgh. USA.

SAE (1967) Design Analysis Procedure for Failure Modes, Effects and Criticality Analysis (FMECA). Aerospace Recommended Practice (ARP) 926. Society of Automotive Engineers (SAE). Warrendale. USA.

Santos, E. (1994) "A linear constraint satisfaction approach to cost-based abduction." Artificial Intelligence, Vol.65, pp 1-28.

Scott, D.W. (1992) Multivariate Density Estimation. Wiley & Sons. New York.

Sen, P. & Yang J.B. (1995) "Multiple criteria decision making in design selection and synthesis." Journal of Engineering Design, Vol.6, pp 207-230.

Sen, P. Labrie, C.R., Wang, J. Ruxton, T. & Chan, J. (1993), "A General Safety and reliability analysis Framework for Large Made-To-Order Engineering

Products." Proceeding of 1st Newcastle International Conference on Quality and Its Applications. Newcastle. UK, pp. 499-505.

Shanahan, M. (1989) "Prediction is deduction but explanation is abduction." Proceedings of the International Joint Conference on Artificial Intelligence, Margan Kaufmann. San Mateo, California, pp 1055-1060.

Shafer, G. (1976) A Mathematical Theory of Evidence. Princeton University press, Princeton. New Jersey. USA.

Sharp, J.V. et al. (2002) "Measurement of organizational maturity in designing safe offshore installations." Proceedings of OMAE'02. 21st International Conference on Offshore Mechanics and Artic Engineering. Oslo.

Shimony, S.E. (1994) "Finding MAPs for belief networks is hard." Journal of Artificial Intelligence, Vol.68, pp 399-410.

Sii, H.S. & Wang, J. (2003) "A Statistical Review of the Risk Associated with Offshore Support Vessel/Platform Encounters in UK Waters." Journal of Risk Research, Vol.6, pp 163–177.

Smith, D.J. (1992) Reliability, Maintainability and Risk. 4th Edition. Butterworths-Heinemann Ltd. Basingstoke. UK.

Smith, D.J. (1985) Reliability and Maintainability in Perspective. 2nd Edition. Macmillan Publishers Ltd. London. UK.

Spirtes, P. Glymour, C. & Scheines, R. (1993) Causation prediction and search. Springer-Verlag. New York.

Stansfeld, J. T. (1994) "The Safety Case." Transactions of Lloyd' s Register Technical Association Session 1994-5. Paper No. 3. Lloyd's Register of Shipping.

Strurel, A. (2002) Structural reliability analysis program system. RCP GmbH.

Germany.

Tucker, F.S. Zivan, S.M & Camp R.C. (1987) "How to measure yourself against the best." Harvard Business Review, Vol.65, pp 8-10.

UKOOA (2002) UKOOA FPSO Design Guidance Notes for UKCS Service.

U.N 96/82/EC (1999) Council Directive on the Control of Major-Accident Hazards, Submitted by United Nations Economic Commission for Europe.

U.S Military Handbook 217 (1982) Handbook on Reliability Prediction for Electronic Equipment. State University of New York. New York. USA.

Vellido, A. & Lisboa, P.J.G. (2001) "An Electronic Commerce Application of the Bayesian Framework for MLPs: The Effect of Marginalization and ARD." Neural Computing and Applications, Vol.10, pp 3-11.

Vesely, W.E. Dugan, J. Fragola, J. Minarick III, J. & Railsback, J. (2002) Fault Tree Handbook with Aerospace Applications. Version 1.1. National Aeronatics and Space Administration (NASA). Office of Safety and Mission Assurance. Washington DC. USA.

Villemeur, E. (1992) Reliability, availability, maintainability and safety assessment. John Wiley. Chichester.

Wang, J. & Ruxton, T. (1998) "A review of safety analysis methods applied to the design process of large engineering products." Journal of Engineering Design, Vol.8, pp 131-152.

Wang J. (2002) "A Review of Marine and Offshore Safety Assessment." Marine Technology, SNAME, Vol.39, pp 77-85.

Wang, J. & Yang, J.B. (2001) "A subjective safety based decision making approach for evaluation of safety requirements specifications in software

development." International Journal of Reliability Quality and Safety Engineering, Vol.8, pp 35-57.

Wang, J. (1997) "A subjective methodology for safety analysis of safety requirements specifications." IEEE Transactions on fuzzy Systems, Vol.5, pp 418-430.

Wang, J. (2000) Subjective modelling tool applied to formal ship safety assessment. Ocean Engineering. Pergamon, Vol.27, pp 1019-1035.

Wang, J. Yang, J.B. & Sen, P. (1995) "Safety analysis and synthesis using fuzzy sets and evidential reasoning based on subjective safety and cost analysis." Reliability Engineering and System Safety, Vol.47, pp 103-118.

Wang, J. Yang, J.B. Sen, P. & Ruxton, T. (1996) "Safety based design and maintenance optimisation of large marine engineering systems." Applied Ocean Research, Vol.18, pp 13-17.

Wang, J. Labrie, C. R. & Ruxton, T. (1993), "Computer Simulation Techniques Applied to the Prediction and Control of Safety in Maritime Engineering." Institute of Marine Engineers Transactions, Vol.105, pp 21-34.

Weisbord, R. (1976) "Diagnosing your organization: Six places to look for trouble with or without theory." Group and Organizational Studies, Vol.3, pp 430-447.

Wikipedia (2006) The Free Internet Encyclopedia.
Available from: www.en.wikipedia.org
[Accessed: 4th August 2006]

Yager, R.R. (1987) "On the Dempster-Shafer framework and new combination rules." Information Science, Vol.41, pp 93-137.

Yang J.B. & Singh, M.G. (1994) "An evidential reasoning approach for multiple attribute decision making with uncertainty." IEEE Transaction on Systems. Man and Cybernetics, Vol.24, pp 1-18.

Yang, J.B. & Xu, D.L. (2002), "Nonlinear Information Aggregation via Evidential Reasoning in Multiple Attribute Decision Analysis Under Uncertainty." IEEE Transactions on Systems. Man and Cybernetics Part A: Systems and Humans, Vol.32, pp 376–393.

Yang J.B. & Xu, D.L. (2001) Intelligent decision system software. Cheshire, United Kingdom.

Yang, J.B. (2001) "Rule and utility based evidential reasoning approach for multiple attribute decision analysis under uncertainty." European Journal of Operational Research, Vol.131, pp 31-61.

Yang, J.B. Dale B.G. & Siow, C.H.R. (2001) "Self-assessment of excellence: An application of the evidential reasoning approach." International Journal of Production, Vol.39, pp 3789-3812.

Zadeh, L.A. (1965) "Fuzzy sets." Journal of Information and control, Vol.8, pp 338-353.

Zimmermann, H.J. (1990) "Problems and tools to model uncertainty in expert and decision support systems." Mathematical Computational Modelling, Vol.14, pp 8-20.

Appendix I

Common hazard categories on board

A. Shipboard hazards to personnel

1. Asbestos inhalation.
2. Burns from caustic liquids and acids.
3. Electric shock and electrocution.
4. Falling overboard.
5. Pilot ladder/pilot hoist operation.

B. Hazardous substances on board vessel

Accommodation areas:

1. Combustible furnishings.
2. Cleaning materials in stores.
3. Oil/fat in galley equipment.

Deck Areas:

4. Cargo.
5. Paint, oils, greases etc. in deck stores.

Machinery spaces:

6. Cabling.
7. Fuel and diesel oil for engines, boilers and incinerators.
8. Fuel, lubricating and hydraulic oil in bilges, save alls, etc.
9. Refrigerants.
10. Thermal heating fluid systems.

C. Potential sources of ignition

General:

1. Electrical arc.
2. Friction.
3. Hot surface.
4. Incendiary spark.
5. Naked flame.
6. Radio waves.

Accommodation areas (including bridge):

7. Electronic navigation equipment.
8. Laundry facilities - irons, washing machines, tumble driers, etc.

Deck areas:

9. Deck lighting.
10. Funnel exhaust emissions.
11. Hot work sparking.

Machinery spaces:

12. Air compressor units.
13. Generator engine exhaust manifold.

D. Hazards external to the ship

1. Storms.
2. Lightning.
3. Uncharted submerged objects.
4. Other ships.

Appendix II

Structured interview on marine systems involving duality

The following set of questions was asked in the sequence presented to the following industry's experts (Technical manager of Interunity Management Corporation, Chief engineer of LPG vessel and company's senior technical superintendent) in an attempt to identify a number of possible examples stating dependency and dependent failures.

1. Based on your experience of on-board engineering systems please indicate any situations you have encountered where either a component or a system can operate in a dual manner.

2. Please state if applicable, any cases where failure of a system or component can cause a demand to deal with more than one system simultaneously.

3. Apart from component and system failure are there any other external factors linked with the required operability of a component or a system?

4. Would you be able to mention some factors you consider important either internal or external, ranging from the design to the operation phase of a system that if applied can cause dependent failures within a components or a system or even a number of systems.

5. Do you believe that all-dependent failures involve independent equipment?

Appendix III

Structured interview on vessel selection process

Section A

In order to derive the assessment grades for the first, second, third, fourth and fifth level criteria a structured interview has been presented to the director of Interunity Management Corporation, a company managing LPG vessels bound to operate within very strict safety levels. Similar interviews took place in the premises of two broker companies involved in cases of vessel selection, Clarksons and Himatiki Marine Ltd. Finally the opinion of a Bureau Veritas' field surveyor was taken into consideration through the structured interview. The questions used for the structured interview were as follows:

1. If you would like to assess a vessel for transporting a specific cargo at a specific port in the west USA, how many describing variables would you use in order to describe it accurately and what would these linguistic variables be?

2. What, in your opinion, are the most significant factors influencing the selection process of a vessel? Having defined those factors what kind of description variables would you use in order to assess them as accurately and in a holistic way as possible?

3. The most significant factors in the vessel selection process identified in the previous question, are a bit generic in their form as they stand. Trying to focus into more specific areas contained in each factor separately, what would you think that these specific areas would be? How far would you consider that an analysis of factors should proceed in terms of subsequent levels of expanding detail, in order to reach a stage where one can claim that each factor is thoroughly examined?

4. Again, after having identified the depth of analysis in terms of describing variables, how many and what kind of assessment grades would you think that each describing variable would need in order to be defined accurately?

Section B

This section is used to give a description of the 2nd level's assessment grades. The description of each of these criteria is given in Step 1 in section 4.5.1. The identification of these assessment grades was a result of the structured interview of section A. In a similar manner the rest of the criteria and their sub-sequent assessment grades are produced.

As far as the 2nd level of criteria is concerned the assessment grades are explained as follows:

Integrity	V. bad	bad	Average	Good	V. good

Very bad: The vessel's integrity both at a mechanical and structural level is unacceptable. There are a lot of class outstanding remarks and a probable detention between the last two special surveys. The majority of the vessel's certificates have expired.

Bad: The vessel's integrity condition can be at a very bad state at either the mechanical or the structural side. Class outstanding remarks that have not been resolved yet will be noted in the vessel's class records. Some certificates will have expired.

Average: The vessel's integrity condition is at such a state that can barely pass the margin between being acceptable or unacceptable. The majority of its certificates are still valid but more work is required it to bring it to the pass region.

Good: The vessel' integrity is above the average condition within the acceptable region. The vessel's certificates are updated and in the vessels' class records some recommendations may appear.

Very good: The vessel is newly built within the last five years. It is insured at a reputable classification society, with no remarks in its class records.

Pollution Prevention	Worst	Poor	Average	Good	V. good	Excellent

Worst: The vessel has a recorded history of major pollutions. The pollution prevention plan is non existent. SOLAS (Safety of Life At Sea) and other international regulations on pollution safety are not followed. Various coast guards do not permit entrance of the vessel in several ports.

Poor: The vessel has a history of a couple very minor pollutions. The sludge and bilge networks are connected thus giving raise to the possibility of discharge of sludges at sea. Coast guards have not denied access to the vessel in ports but have it in a black list for extensive check over when it arrives. Emissions are usually above permitted limits.

Good: The vessel does not have a recorded history of pollutions. Class remarks in terms of sludge and bilge networks appear in the vessel's class history. The state of the vessel indicates some negligence in terms of pollution training as far as personnel is concerned. Emissions are at a marginal level of passing the permitted limits.

Very good: The vessel is in a state both mechanically and structurally very sound in terms of pollution. The vessel has double bottoms and double side skins installed bearing in mind the reduction of the probability of spillage of cargo in cases of light collision.

Excellent: The vessel is newly built within the last 3 years with the latest technology in pollution prevention and cargo purification systems. Automation controls are installed monitoring the piping networks for oil contents. Personnel are trained at a very high level in terms of pollution prevention and pollution fighting.

Vessel's Running Costs	V. high	high	Average	Low	V. low	Minimum

Very high: Main engine and auxiliary engines operate with lots of leakages. Personnel are overpaid. Oil consumption keeps on increasing on a monthly basis. No automation machinery is installed on board thus more personnel are required.

High: Either the main engine or the auxiliary engines have faults increasing their daily consumption of fuel. Bad maintenance also increases the monthly oil consumption. Automation controls are primitive thus more personnel are required.

Average: There is a fragile balance between consumption and maintenance. The main engine and auxiliary engines are maintained at an acceptable level giving raise to a mediocre amount of money required to keep them running at appropriate levels. There are automated controls for the significant cargo procedures.

Low: The vessel is well maintained at an engineering level. Both main engine and auxiliary engines operate without significant problems that require large down time to be resolved. Fuel and oil consumption levels are within acceptable limits.

Very low: The vessel is at a very good condition with the technical department monitoring consumptions on a daily basis. New parts are used to substitute worn parts at intervals stated by the manufacturer leaving very small margins for functional failures. Automated systems control the majority of cargo and engineering processes on board the vessel. Personnel are reduced due to automated systems installed and paid at an average market price.

Minimum: The vessel is newly built within the last 2 years. It is fully automated thus having only the minimum manning requirements. Main and auxiliary engines are brand new with sensors installed indicating if the associated systems function as required. Oil and fuel consumptions are at optimized levels.

Restrictions on Vessel	**Bad**	**Average**	**Good**

Bad: The vessel exceeds the maximum permitted geographical elements of the destination port such as the maximum permissible draft. Additionally for the particular case examined the vessel even if it matches the required size does not meet the maximum permissible breadth requirement of the Panama Canal.

Average: The vessel is just at the limit of the elements governing the position of a port making it the captain's responsibility, if selected to carry the cargo, to ensure the safety of the vessel itself as well as of its cargo.

Good: The vessel fulfills all the navigational requirements leading to the designated port of call.

Section C

This section contains some general information concerning the overall condition of each vessel in question.

Vessel 1: This vessel has a good maintained overall structure and engineering systems such as the main and the auxiliary engines. Just had a major servicing period after a special survey dry dock which resulted in 300 tones of steel to be changed where needed and a full overhaul of the main and auxiliary engines bringing above the average selection standards. It is exactly due to the special survey amendments that pollution control systems have been checked and updated accordingly making it a strong candidate for the USA port of call. Due to the fact that a complete overhaul is made to its engines it is expected to maintain reasonably low daily running costs. It complies with all the geographical requirements in terms of draft and breadth as it is due to pass from the Panama Canal.

Vessel 2: This vessel has moderately decent auxiliary engines but the main engine need overhauling in cylinders 4 and 6. The structural integrity of the vessel is in an average state with a number of brackets and longitudinal frames needing immediate replacement due to extensive rust levels. Cargo tanks have lost almost 80% of their protective coating and side ballast water tanks have lost the majority of their anodes thus having very increased level of cavitations especially at their lower levels. Due to the badly maintained main engine current emission levels are above the permitted limits imposed by the U.S Coast Guard. Currently the vessel has high daily running costs as the main engine works inefficiently. The vessel has a breadth similar to the breadth of the Panama Canal making it a questionable candidate for the cargo to be transported.

Vessel 3: This vessel is in its last charted voyage. Owners are considering scrapping it after delivery of the next cargo. Both structurally and mechanically the vessel is in a bad condition with numerous steel plates requiring immediate replacement both in cargo as well as in external areas of the vessel. Both main and auxiliary engines have passed the overhauling limits in an attempt from the owners side to save some funds.

Emissions are beyond the acceptable limits due to improper operation of the main engine and the cargo's purifiers require cleaning. Sludge and bilge networks have not been checked for a number of months leaving questions as to where the sludges are disposed. Being a very old vessel automation control are non existent thus having more personnel on board. Daily running costs have made this vessel not worthy of sea going passage and that is why owners decided to scrap it. The design characteristics of this vessel do not meet the Panama Canal requirements but it was put among the other vessels due to its capacity.

Vessel 4: This vessel is in a good condition even though it is near its first decade of age. It is well maintained and recently was converted from single to double side skin. Main engine and auxiliary engines meet the manufacturer's inspection criteria thus having a few problems during their operation. It is mainly due to the properly maintained main engine that emissions are kept just below the permitted limits. Sludge and bilge networks have had some piping parts changed and a new three way valve has been installed along with an oil content measuring device in an attempt to try and reduce given sludges to minimum levels. The overall vessel's running costs are kept in a low level as automated controls are installed for cargo handling operations. Average fuel and oil consumption are kept within reasonable levels and with proper engineering maintenance they can be kept stable.

Vessel 5: This is a newly built vessel, well maintained from the very beginning both in structural and engine aspects. It was delivered with a special structural coating thus the overall condition of its cargo and ballast tanks is very good. The emission levels are kept way below the permitted limits and individual manuals have been prepared for both sludge and bilge networks along with the vessel's pollution certificates and the automated controls ensuring that the level of oil content in bilges is kept to an absolutely minimum level. It is due to the installation of a number of automated systems that personnel is kept at an absolute minimum. With generally no problems in the engine's operation the overall vessel's running costs are very low and the vessel leaves a respectable profit to its owner at every voyage. It meets all the geographic and structural criteria of the designated port of call.

Section D

The maximum and minimum utility values are given from the following equations:

Min. Utility =
{[(Degree of belief assigned under grade very bad + unassigned degree of belief) x utility of grade very bad] +
(Degree of belief assigned under grade bad x utility of grade bad) +
(Degree of belief assigned under grade average x utility of grade average) +
(Degree of belief assigned under grade good x utility of grade good) +
(Degree of belief assigned under grade very good x utility of grade very good) +
(Degree of belief assigned under grade excellent x utility of grade excellent)}.

The maximum utility is given as follows:

Max. Utility =
{[(Degree of belief assigned under grade very bad x utility of grade very bad) +
(Degree of belief assigned under grade bad x utility of grade bad) +
(Degree of belief assigned under grade average x utility of grade average) +
(Degree of belief assigned under grade good x utility of grade good) +
(Degree of belief assigned under grade very good x utility of grade very good) +
[(Degree of belief assigned under grade excellent + unassigned degree of belief) x utility of grade excellent]}.

PAGE NUMBERING AS ORIGINAL

Appendix IV

Structured interview on organizational maturity of self assessment

Section A

In order to derive the assessment grades for the first, second, third and fourth level criteria a structured interview has been presented to the director of Interunity Management Corporation, a company managing LPG vessels bound to operate within very strict safety levels. The same set of questions have been presented to a safety and quality surveyor from Bureau Veritas as well as to the owner of Safetec Developments, a newly built company operating in the area of marine and port safety in Greece. All three interviewees had a briefing from the author of this thesis concerning the six-box Weisbord model and the factors it incorporates, as it was necessary for the construction of main criteria and their subsequent level of criteria. The questions used for the structured interview were as follows:

1. If you would like to assess the level of maturity of a company dealing with marine and port safety issues, how many describing variables would you use in order to describe it accurately and what would these linguistic variables be?

2. Having discussed the basic factors used in Weisbord's six-box model and leaving leadership aside, what kind of short descriptions would you use for the rest of them if you were trying to associate them with the operation of a company dealing with marine and port safety issues?

3. Having defined the description for each of the remaining factors of Weisbord's six-box model, how many assessment grades would you think would be appropriate to be used for each one of the discussed descriptions and what would these be?

4. The described factors from Weisbord's six-box model are a bit generic in their form as they stand. Trying to focus into more specific areas contained in each factor separately, what would you think that these specific areas would be? How far would you consider that an analysis of factors should proceed in terms of subsequent levels of expanding detail, in order to reach a stage where we can claim that each factor is thoroughly examined?
5. Again, after having identified the depth of analysis in terms of describing variables, how many and what kind of assessment grades would you think that each describing variable would need in order to be defined accurately?

Section B

This section is used to give a description of the 3rd and 4th level criteria along with an explanation of what do the respective assessment grades mean in 2nd and 3rd level criteria.

As far as the 2nd level of criteria is concerned the assessment grades are explained as follows:

Safety Data, Information and Knowledge	**Very little**	**Little**	**Average**	**Enough**	**More than enough**

Very little: The company uses less than minimal if not at all historical statistical data relevant to a case examined. It is very unlikely to do any research in failure databases or other places that may contain statistical data.

Little: The company uses only the minimal of statistical data relevant to the case examined. Research is only in terms of a couple of major incidents relevant to the case examined.

Average: The company uses statistical data from only a few major past cases well renowned for their statistical results. Research is only to the level of outcome reports from these major cases.

Enough: The company has a well documented file containing data from major and minor incidents relevant to the case examined. It will have done research on a regular basis to make sure that the majority of similar incidents are documented and verified from reputable sources. It will use the data acquired in the process of risk estimation.
More than enough: The company keeps a monthly record of all major, minor and near misses that have been documented in any way. It keeps log data going several years back thus been able to produce trend lines for a case examined. The level of uncertainty is greatly reduced due to a wealth of statistical data.

Innovation & Research	**Very basic**	**Basic**	**Normal**	**Advanced**	**Excellent**

Very basic: The company has not appointed anyone for dealing with research and development issues. Complex cases cannot be dealt appropriately, thus loosing time and money.
Basic: The company does not have anyone appointed for dealing with research and development issues. It uses personnel based on recent relevant past experience or first degree relevant to the basics of safety.
Normal: The company filters its employees and appoints a couple of persons, usually those with the greater experience to tackle the complex issues raised. The educational levels of employees go slightly beyond the first degree.
Advanced: There is a small group of persons specialized in specific areas working together in order to resolve complex issues. All of them have degrees in Masters level any their leader usually holds a PhD in the safety area that the company is dealing with.
Excellent: The company has a dedicated R&D department parted from personnel at PhD level. Usually, it co-operates with universities and other scientific and academic sources to ensure that all complex issues are dealt woth high standards of knowledge.

Management and H.R	Very bad	Bad	Average	Good	Very good

Very bad: The company has no standards on selecting employees nor does it provide a defined role for each employee within the company. The company faces great problems in resolving problems of personnel.

Bad: The company has indifferent standards in the selection process of its employees. There is a basic hierarchy structure which cannot be followed due to insufficient managerial knowledge. Problems are dealt and resolved with a lot of delays.

Average: The company has some selection standards mainly based on past experience of its employees. There is an appointed human resources manager who operates on his own trying to deal with personnel problems.

Good: The company has set specific standards to be met by its personnel according to the position in question. There is a human resources department trying to resolve any issues raised from personnel.

Very good: The company filters all personnel trying to identify the best person based on academic qualifications and past experience for each individual position. There is a structured hierarchy as to the way that problems are handled and a dedicated department well organized with processes and appointed personnel trying to resolve problems in the fastest possible manner.

Measurement and Benchmarking	Very bad	Bad	Average	Good	Very good

Very bad: The company does not have any intention to assess its performance in the marine and port safety field either on its own or compared with a better company.

Bad: The company does not have any way to measure its own performance and always seems to lack behind as it tries to compare itself in terms of clients with leading companies in the area.

Average: The company struggles to assess its own performance using very simplistic models based for example on annual revenue but is aware of its status compared to similar or better companies.

Good: The company has appointed a person dealing with internal quality issues trying to develop basic self assessment reports which are examined usually at the end of

each year. It has a solid knowledge as to where it stands compared with similar companies and a good view of the targets it needs to set to improve upon them.

Very good: The company has a separate department dealing with internal quality issues. Analytic self assessment reports are received from each department and assessed at regular intervals through the year. The gaps are identified and work is done to improve upon them. The company stands as a benchmark for others to use.

Safety Strategy and Planning Processes	**Reactive approach**	**Stable approach**	**Pro-active approach**

Reactive approach: The company cannot propose possible future scenarios and new hazards that may give rise to a specific situation as it only operates on granted evidence.

Stable approach: The company maintains a stability between reactiveness and pro-activeness. It records the data after the occurrence of an incident trying to identify some key future scenarios which could give rise to similar consequences. It develops a list of highly possible future hazards leaving others without further examination.

Pro-active approach: The company has a well recorded hazard list from past experience and due to high level of innovation and research it is enabled to identify different categories and future hazardous scenarios giving a better approach to future safety planning.

The 3rd level criteria are as follows:

3rd level criteria	**Assessment Grades**				
Port Security Measures	Very loose	Loose	Normal	Strict	Very strict
Organisational Updates	Not very often		Often		Regular
Comparison Sources	Independent				
Educational Background and Further Training	Very poor background	Poor background	Average background	Good background	Very good background
Supply Management	Very bad	Bad	Average	Good	Very good
Design Management	Very bad	Bad	Average	Good	Very good
Application of Technical Standards	Very loose	Loose	Normal	Strict	Very strict
Self-Assessment Tools	Very few	A few	Average	Enough	More than enough

Organisational Updates	**Not very often**	**Often**	**Regular**

Organisational updates: The company ensures to distribute to its employees documents concerning new rules, new methodologies and generally new tools that can assist in the improvement of overall personnel knowledge.

Not very often: The company distributes updates to its personnel a couple of times per years.

Often: The company distributes updates to its personnel on a 3-month period.

Regular: There is a dedicated person who deals with updates and distributes them around the department on a monthly basis.

Educational Background and Further Training	**Very poor background**	**Poor background**	**Average background**	**Good background**	**Very good background**

Educational background and further training: The company is assessed based on the educational level of its employees and the intention to further train them in order to improve their level of knowledge and thus improve the overall service quality provided by the company.

Very poor background: The company has employees with no academic qualifications. It spends no amount of money to further train them.

Poor background: The company has very few employees with first degree academic qualifications and aims in training only a small percentage of them.

Average background: The company has the majority of its personnel with first degree academic qualifications and tries to train further those that demonstrate overall good performance.

Good background: The company has set very high standards in selecting its personnel. The majority of the personnel are educated to a Masters level and aims in training as many as costly possible on a yearly basis.
Very good background: The company aims to the highest of educational standards at a PhD level and dedicates a significant capital to further train its employees with regular training updates within the year.

Supply Management	Very bad	Bad	Average	Good	Very good

Supply management: The company ensures that all employees have the appropriate tools to maximize their potential in terms of the quality if service provided.

Very bad: The company does not provide the employees with any tools such as laptops, cars or mobile phones.
Bad: The company has provided only a few persons with items such as a laptop and those are mainly department managers.
Average: The company has updated the information technology area within its premises giving no importance to external tools.
Good: The company has latest technology tools which are distributed according to the needs of each department. The employees working far from the office premises are provided with laptops and mobiles phones.
Very good: The company has taken great care in providing car, mobile phone, laptop and all necessary means for an employee to operate to the required standard either within or out of office premises.

Design Management	Very bad	Bad	Average	Good	Very good

Design management: The company ensures that appropriate and revised plans are drawn at the design phases of implementation of a project so that no other modification will be required at the commission or operation phase of the same project.

Very bad: The company pays minor attention to the design process leaving gaps and problems that will be encountered at further stages.
Bad: The company pays attention to the degree that only the vital systems of a project work properly leaving the majority of sub-systems with a simple check over.
Average: The company tries up to a point to make sure it has covered all major possible problems no matter if it is a major or a minor system. It is mainly due to lack of expertise that omissions are found at a later stage.
Good: The company has an appropriate department dealing only with the design stage. All systems are treated with equal importance trying to avoid as many problems at a later stage as possible.
Very good: The dedicated design department operates on a pro-active approach during the design stage considering and eliminating as many as possible of the problems that may be encountered at a later stage.

Application of Technical Standards	**Very loose**	**Loose**	**Normal**	**Strict**	**Very strict**

Application of technical standards: The company ensures that all research and application is within the certified technical standards recommended by either the European Union or any other governmental organizations.

Very loose: The company does not care about any of the standards imposed thus creating non certifiable projects in the majority of cases.
Loose: The company only considers the absolute necessary standards than need to be followed:
Normal: The company maintains a balance of the standards that need to be followed. It applies the significant leaving space for free movement in several cases.
Strict: The company produces results within the strict limits defined by the required standards leaving very few cases for deviation from them.
Very strict: The company follows the law letter by letter in all cases making no exceptions in any project. All standards are met and the work produced is certified by the respective governmental organization.

Self-Assessment Tools	Very few	A few	Average	Enough	More than enough

Self-assessment tools: The methods and processes utilized to assess its own performance against benchmarked companies.

Very few: The company's self assessment tools are limited to one or two mainly based on annual income and expenses.

A few: The company's self assessment tools are limited on revenue and the annual report given by the board of directors or general manager.

Average: The company's self assessment tools contain simple assessment reports made from internal personnel, mainly department managers trying to assess on very simple criteria such as overtime the quality of employees.

Enough: The company has developed numerous forms covering each department which are then passed to the quality department where gaps and problems are identified and improved upon.

More than enough: The company has developed methodologies measuring its department's performance and then combined to give the overall performance. Problems and gaps are identified no matter how important or insignificant they are and the managerial directive is continuous improvement of quality and services.

Port Security Measures	Very loose	Loose	Normal	Strict	Very strict

Port security measures: The strategy and measures required to ensure adequate safety levels within a port environment.

Very loose: Security measures are inadequate both for cargoes and for personnel.

Loose: Security levels are operating to the absolute minimal. Typical checks only at main gate.

Normal: The port is surrounded by protective wall. Regular checks at the main gate, lighting installations at loading and unloading docks.
Strict: The port is surrounded by a protective wall. Regular checks at the main gate, lighting installations at loading, unloading and stacking docks. Regular patrols from security officers. Close circuit television (CCTV) installed to monitor the movements within the port premises.
Very strict: The port is monitored and checked 24 hours a day. Regular patrols at short periods of time in order to monitor movements from close range. CCTV is installed to cover all the ports areas and 24 hour security officers recording any unusual movements.

Independent Comparison Sources	**Not very often**	**Often**	**Regular**

Independent comparison sources: The company assigns to 3rd parties to assess their performance either as a stand alone company or compared to other companies and produce a ranking report stating the strengths and weaknesses that need to be improved upon.

Not very often: The company uses a 3rd party to asses its performance compared to other similar or leading companies once every 10 years.
Often: The company uses a 3rd party to assess its performance compared to other similar or leading companies once every 3 years.
Regular: The company uses a 3rd party to assess its performance compared to other similar or leading companies once every 1 year.

In a similar sense and based on the description of the 3rd level criteria the 4th level criteria are described and assessed.

Section C

This section contains a brief description on the profile of each one of the four Greek safety oriented companies examined in the test case. It is due to reasons of anonymity

that the real names of the companies are not given, as the assessment data for those companies was kindly provided by Bureau Veritas, which maintains a very high level of self assessment and benchmark levels.

Company 1: This company is in a transitional period. It has invested in the quality of its personnel in terms of past experience and academic qualifications. The last few years it has turned from a stable strategy tending to become reactive sometimes to a more pro-active strategic approach for a variety of cases. Due to the high level of qualifications of personnel and due to the restructuring of human resources company 1 is at a constantly increasing path. Self assessment tools and benchmarking against companies like company 4, assisted company 1 in identifying gaps and problems and try to improve them.

Company 2: This company uses the managerial directive of pro-activeness wherever possible. It has proper benchmarking tools and invests in the quality of employees specially when it comes to areas like innovation and strategy. It lacks a bit to the human resources organizations because even though it is a safety oriented company it pays more attention to the creation of software related software rather than the implementation of safety methodologies themselves.

Company 3: This company does not quite meet the criteria required to lead the area of marine and port safety. It retains an average quality level of employees giving little attention to matters of innovation and identification of possible future scenarios for various cases. It tends to follow a reactive path when it comes to the company's strategy in assessing hazardous situations, something that questions the validity of the outcomes of the projects it undertakes.

Company 4: This company utilizes the excellent internal organizational structure it has developed in terms of human resources. It maintains a very high level of quality of employees in terms of qualifications. It has very good self awareness compared to the other 3 companies and by keeping stability between reactive and pro-active approach invests in the identification of possible future scenarios based on the case examined.

Appendix V

Publications being part of the work of this thesis

The following publications have been created as part of this thesis:

Maistralis E., Wang J., Bonsall S., "Safety issues and procedures concerning cargo handling of oil tankers", Journal of UK Safety and Reliability Society, Vol.23, No.2, 2003, 39-46 (ISSN: 0961-7353).

Maistralis E., Wang J., "A subjective methodology for self-assessment of organizations", Proceeding of the 5th IMA International Conference on Industrial Maintenance and Reliability (MIMAR, 2004), Salford, 5-7 April 2004.

Wang J., Maistralis E., Sii H. S., Kim S. W., Wong C., Kwon Y. S., Jung G. M., "Some control engineering techniques and their application to risk modelling and decision making", Automation and Computer Science Conference in UK '2001 (CACSCUK'2001), 22 September 2001, University of Nottingham, England 255-260 (ISBN: 0 9533890 2 3).

Wang J., Sii H. S., Yang J. B., Pillay A., Yu D., Liu J., Maistralis E, Saajedi A., "Use of advanced in technology in marine risk assessment", Risk Analysis, Vol.24, No.4, 2004, 1011-1033 (ISSN: 0272-4332).