Liverpool John Moores University

School of Engineering

Integrative Risk-Based Assessment Modelling of Safety-Critical Marine and Offshore Applications

By

Adokiye Godwill Eleye-Datubo

B.Eng (Hons), MRes

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

May 2005

Dedicated to the loving memory of both
my dad, Chamberlain Alaye Eleye-Datubo, and
my mum, Margaret Makioba Eleye-Datubo.
"I have fulfilled your dream"

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), the Engineering and Physical Sciences Research Council (EPSRC) and the Institute of Marine Engineering, Science and Technology (IMarEST) for their generous financial patronage of the research. In particular, he (the author) would like to express his sincere gratitude to his supervisors, Prof. J. Wang and Dr. A. Wall, as well as Mr. A. Saajedi, in the School of Engineering at LJMU for their stimulating suggestions, constructive comments and constant encouragement. He would like to record his sincere thanks to Shell Global Solutions (UK) for encouraging the idea of a fuzzy-Bayesian network into this research and to the International Maritime Organisation for providing him with an enormous amount of data support on the development of trial application of formal safety assessment. Also, the author has derived a great deal of pleasure working with his colleagues at the Marine and Offshore Technology Research Group of LJMU and he is ever so grateful for their wit that provided the critical forum for the research.

Last but not least, the author would like to give special thanks to his siblings; Elizabeth, Tammy, Eddy, Sandy and Bobby, as well as to his close friends, for all their constant prayers and loving encouragement, especially in times of hardship.

Eleye-Datubo, A.G.

May 2005

Abstract

This research has first reviewed the current status and future aspects of marine and offshore safety assessment. The major problems identified in marine and offshore safety assessment in this research are associated with inappropriate treatment of uncertainty in data and human error issues during the modelling process. Following the identification of the research needs, this thesis has developed several analytical models for the safety assessment of marine and offshore systems/units. Such models can be effectively integrated into a risk-based framework using the marine formal safety assessment and offshore safety case concepts.

Bayesian network (BN) and fuzzy logic (FL) approaches applicable to marine and offshore safety assessment have been proposed for systematically and effectively addressing uncertainty due to randomness and vagueness in data respectively. BN test cases for both a ship evacuation process and a collision scenario between the shuttle tanker and Floating, Production, Storage and Offloading unit (FPSO) have been produced within a cause-effect domain in which Bayes' theorem is the focal mechanism of inference processing. The proposed FL model incorporating fuzzy set theory and an evidential reasoning synthesis has been demonstrated on the FPSO-shuttle tanker collision scenario. The FL and BN models have been combined via mass assignment theory into a fuzzy-Bayesian network (FBN) in which the advantages of both are incorporated. This FBN model has then been demonstrated by addressing human error issues in a ship evacuation study using performance-shaping factors. It is concluded that the developed FL, BN and FBN models provide a flexible and transparent way of improving safety knowledge, assessments and practices in the marine and offshore applications. 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.

Table of Contents

Acronyms and Abbreviations

ALARP	As low as reasonably practicable
AR	Approximate reasoning
BC	Bulk carrier
BN	Bayesian network
BIMCO	Baltic and International Maritime Council
CA	Criticality analysis
CBA	Cost benefit assessment
CCA	Cause-consequence analysis
CCD	Cause-consequence diagram
COGENT	Cognitive event tree system
COLREGS	International Regulations for the Prevention of Collisions at Sea
CPD	Conditional probability distribution
CPP	Controllable pitch propeller
CPT	Conditional probability table
CRCO	Collision risk control option
CREAM	Cognitive reliability and error analysis method
CRI	Composition rule of inference
CURR	Cost per unit reduction in risk
DA	Digraph-based analysis
DAG	Directed acyclic graph
DP	Dynamic positioning
DPS	Dynamic positioning system
DS	Dempster-Shafer
EER	Escape, evacuation and recue
ER	Evidential reasoning
ESD	Emergency shutdown
ETA	Event tree analysis
EU	Expected utility

F.I.	Frequency index
FAM	Fuzzy associative memory
FBN	Fuzzy-Bayesian network
FE	Focal element
FL	Fuzzy logic
FMEA	Failure mode and effects analysis
FMECA	Failure mode, effects and criticality analysis
FPSO	Floating production, storage and offloading unit
FRCO	Fire risk control option
FS	Fuzzy set
FSA	Formal safety assessment
FTA	Fault tree analysis
GrossCAF	Gross cost of averting a fatality
HAZID	Hazard identification
HAZOP	Hazard and operability studies
HCR	Human cognitive reliability
HEART	Human error assessment and reduction technique
HEP	Human error probability
HRA	Human reliability analysis
HRCO	Human factors risk control option
HSC	High-speed passenger catamaran vessel
HSE	Health and Safety Executive
IACS	International Association of Classification Societies
ICAF	Implied cost of averting a fatality
ICFTU	International Confederation of Free Trade Unions
ICLL	International Convention on Load Lines
ID	Influence diagram
IMarEST	Institute of Marine Engineering, Science and Technology
IMO	International Maritime Organisation
INTENT	Quantification of errors of intention
IPSB	International Project Steering Board
ISM	International Safety Management
JPD	Joint probability distribution

LJMU	Liverpool John Moores University
LMIS	Lloyds Maritime Information Service
LOHI	Loss of hull integrity
LP	Likelihood principle
LRCO	Loss of hull integrity risk control option
MA	Mass assignment
MCA	Maritime and Coastguard Agency
MCDA	Multiple criteria decision analysis
MES	Marine evacuation system
MEU	Maximum expected utility
MISO	Multi-input-single output
ML	Maximum likelihood
MTBF	Mean time between failure
NetCAF	Net cost of averting a fatality
NP	Non-parametric
NPV	Net present value
OAT	Operator action trees
ORCO	Organisational factors risk control option
PD	Probability distribution
PHA	Preliminary hazards analysis
PLL	Potential loss of life
PRS	Position reference system
PSF	Performance shaping factor
QRA	Quantitative risk assessment
R.I.	Risk index
RINA	Royal Institution of Naval Architects
RCM	Risk control measure
RCO	Risk control option
RCT	Risk contribution tree
SC	Safety case
S.I.	Severity index
SLIM	Success likelihood index methodology
SOLAS	Safety of Life at Sea

SPAR-H	Standardized plant analysis risk human reliability analysis
SRA	Subjective reasoning analysis
STCW	Standards of Training, Certification and Watchkeeping
SWIFT	Structured what-if technique
THERP	Technique for human error rate prediction
TRCO	Technical factors risk control option

LIVERPOOL
JOHN MOORES UNIVERSITY
AVRIL ROBARTS LRC

Lists of Figures

Lists of Tables

Chapter 1: Introduction

Chapter Summary

It has been ascertained that there is a need for analytical models, which can aid in safety assessment, to be effectively integrated into a maritime risk-based system. In addition, numerous regulations for ensuring maritime safety have been recognised as being reactions to accidents. This makes the system quite deficient in such areas as 'human element' and 'uncertainty' and therefore, the scene of problem definition is set to the root causes of contributory factors that could bring about errors or growth incidents/accidents. To tackle the causes, two risk-based approaches have been recognised and examined in this chapter. Employing any of these approaches should establish whether risks are tolerable or need to be reduced further, based on an up to standard risk acceptance criteria structured within a risk analysis framework. A risk-based framework for maritime safety assessment is then proposed. Finally, this chapter presents the goals of the study described in this thesis and establishes a general characterisation to the structure of the work.

1.1 Background

Ships and offshore installations designed, built, maintained and operated well are capable of long, safe, trouble-free and profitable service over their intended life cycle. Surprisingly, this has not been the achieved reality and in worst cases, several unexpected accidents have occurred. Even with minor examination, a 'proactive' and 'risk-based' stance shows that there is no single previous disaster at sea which could not have been either prevented or suppressed in its scale. Thus, headlines on 'safety' now need a permanent spotlight in the 21st century marine and offshore industry more than it ever revealed itself in the aftermath.

Following many notable marine disasters (e.g. *Piper Alpha*, *Herald of Free Enterprise*, *Estonia*), the International Maritime Organization (IMO) reacted positively to ensure that such accidents did not repeat (IMO, 2001a; Wang, 2002). Nevertheless, worrying accidents did occur again and this made the IMO realise the need for a better resolution. One result of this resolution option is the 'formal safety assessment (FSA) concept' (IMO, 2002b), which represents a fundamental change from what was previously a largely piecemeal and reactive regulatory approach to one that is proactive, integrated, and above all based on risk evaluation and management in a transparent and justifiable manner (THEMES, 2001). Essentially, the concept provides an elegant route to application of well-established risk analysis methods.

Once data and information is provided, some of the novel risk analysis techniques can be developed and used in an integrated manner to yield powerful risk assessments. For example, the time between the occurrences of events can be an important parameter (Nielsen, 1971) and this can be treated using a cause-consequence diagram (CCD). Basically, the CCD method is a tool, which, like fault tree analysis, documents the failure logic but has the extra capability enabling the analysis of systems subject to sequential failures. In addition the CCD identifies the complete set of systems responses to any given initiating event. In principle, incorporate significant features of both fault and event trees. Thus, the CCD could well prove to offer a sophisticated tool for enriching reliability and with respect to risk contribution tree modelling.

The nature of the FSA framework requires that relevant accident scenarios be established to enable hazard identification exercises, which will then feed into the risk assessment of any safety-critical marine and offshore application. Accident databases usually provide statistical input to the scenarios, though the information acquired from these are somewhat subject to inherent uncertainties and may only be acquired incrementally. Decision-making is essential to the risk assessment task and therefore, under the realm of uncertainty, Bayesian network (BN) (Jensen, 1993) can be adopted to enable a powerful marine and offshore decision-support solution. The focal mechanism for this network's inference process relies on the sound Bayes' theorem (Groen & Mosleh, 2001) to perform a probabilistic logic/reasoning of the domain. Also, BN models can be expanded into influence diagrams for use as a communication tool in the decision-making process.

Whilst the analysis, under conditions of uncertainty, can adopt a probability-based approach due to randomness in the modelling data, another feasible choice is a possibility-based approach due to a nature of vagueness. On this note, analysis of safety and reliability capabilities of ships and offshore installations can be undertaken in view of the fact that fuzzy logic (FL) (Zadeh, 1975) has emerged as a uniquely efficient linguistic and numerical tool for safety assessment. In addition to its modelling from fuzzy set theory, FL could be combined with evidential reasoning (Yang & Xu, 2002) to enable a justified weighted ranking in terms for safety and utility. The possibility values of fuzzy set can be transformed into probabilities to enable BN and FL integrative modelling via the theory of mass assignment. In-service behaviour of safety-critical systems in marine and offshore applications can be investigated using these developed modelling techniques. Such techniques can also be applied to address the assessment of safety due to the relevant and thoughtful technological modifications/added features that are made by designers and the vessel operators.

1.2 Problem Definition in the Safety Issue

It is essential for regulations to be set in order to ensure maximum safety to the maritime industry. Unfortunately, regulations have been reactive to accidents and prone to several deficiencies. The time-honoured causation of historic incidents and accidents offers an inadequate setting to resolving safety for complex systems of the likes of maritime vessels and installations.

1.2.1 Deficiencies due to Regulating by Disasters

A huge amount of the change to regulations and procedures in shipping activity has resulted from tragedies. Figure 1.1 gives an event breakdown of the prominent consequences in most marine disasters. Obviously, many important lessons have been learnt from those past maritime accidents.

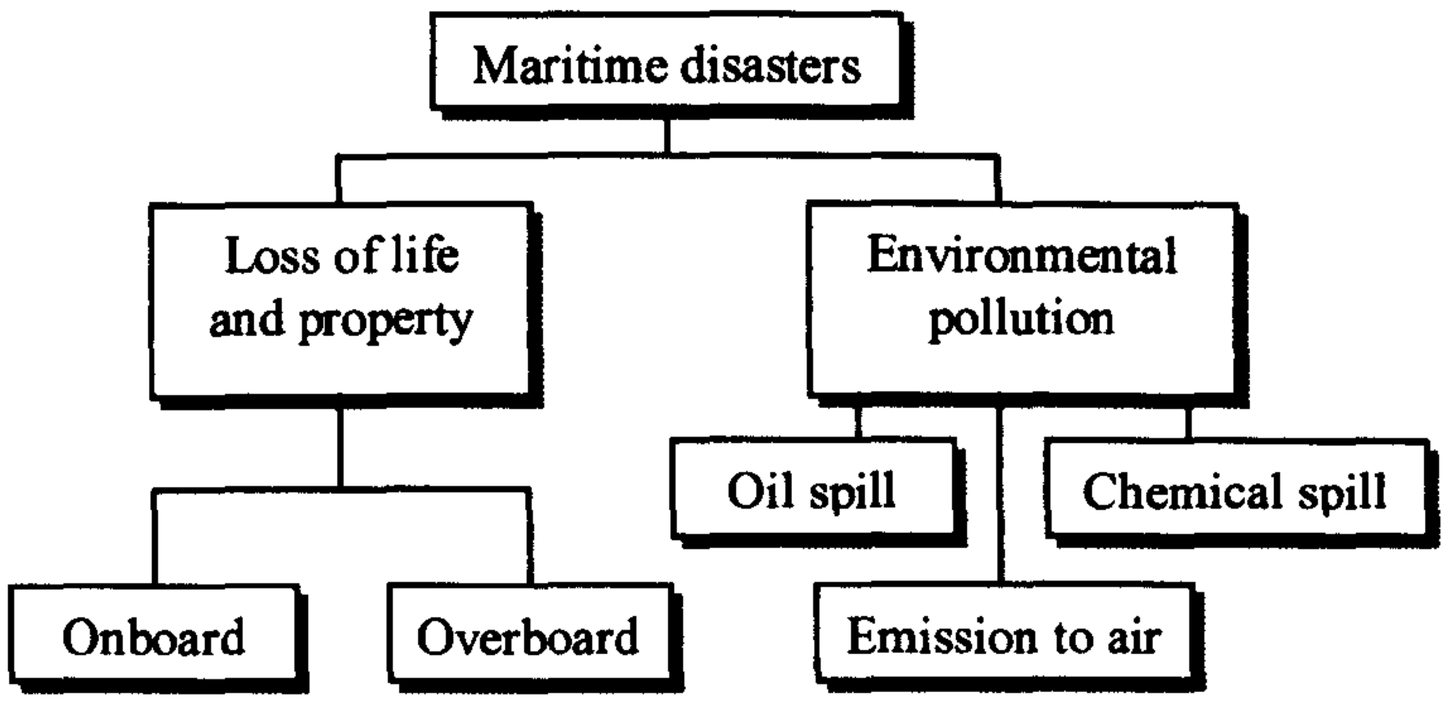


Figure 1.1: Consequences in the majority of marine disasters

Ships such as *Titanic*, *Torrey Canyon*, *Amoco Cadiz*, *Herald of Free Enterprise*, *Exxon Valdez*, *Scandinavian Star*, *Estonia* (Bråfelt & Larsson, 2000; Wang, 2002) and others shown in Table 1.1, represent highly controversial tragic accidents which led to response strategies but left many issues unresolved. The *Exxon Valdez* case (NTSB, 1990), for example, led to the introduction of mandatory requirements for double hulls, notwithstanding the fact that it was largely due to a navigational error. In fact, it did nothing much to address the human element issue. Therefore, as the traditional structure of shipping is being transformed, such an example indicates clearly that a system which merely reacts to disasters is basically flawed.

The accident categories of grounding, stranding, collision, fire and explosion have become a driving force for new legislation and the focus of safety training standards. Nevertheless, it can be acknowledged from such invariably devised responses that the way in which the industry is regulated has evolved in an unstructured manner. Regulation has been so much reactive rather than proactive and regulators clearly struggle to keep up with the rapid pace of technological and operational developments within the industry. As such, a change of regulatory approach is desperately desirable in pursuit of "a safety culture". However, this change has to create a proactive rather than reactive system of controlling maritime safety and environmental protection, and one in which underlying issues such as '*human element*' and '*uncertainty*' are no longer neglected. The system should further allow for model integration of risk-based assessments into the appropriate methodology steps, which are set to meet an acceptable risk criterion.

Table 1.1: Maritime disasters that greatly influenced worldwide maritime regulations

Date	Vessel/Unit	Accident	Location	Consequence	Resolutions
15 April 1912	*Titanic*	Sank after a collision with an iceberg	South of Grand Banks	1,503 lives lost	SOLAS Convention
8 September 1934	*Morro Castle*	Caught fire and grounded	Gulf of New Jersey	134 lives lost	Fire Safety
18 March 1967	*Torrey Canyon*	Grounding and subsequent oil spill	West Coast of England	120,000 tonnes of spilled oil	Civil Liability Convention, MARPOL 73/78
16 March 1978	*Amoco Cadiz*	Grounding	Northern Coast of France	223,000 tonnes of spilled oil	Pollution Liability Limits, STCW 78/95
19 July 1979	*Atlantic Express*	Collision	Trinidad and Tobago	287,000 tonnes of spilled oil	Tanker Safety
9 September 1980	*Derbyshire*	Sank in a typhoon	North Pacific	44 lives lost	Bulk Carrier Safety
6 March 1987	*Herald of Free Enterprise*	Foundered	Zeebrugge	193 lives lost	Passenger Ferry Safety I, ISM Code
6 July 1988	*Piper Alpha*	Fire after an explosion	North-east coast of Scotland	167 lives lost	Safety Case, ALARP Established
24 March 1989	*Exxon Valdez*	Ran to a shoal	West Coast of Alaska	37,000 tonnes of spilled oil	Tanker Construction, OPA 90
6 April 1990	*Scandinavian Star*	Caught fire	Skagerak	158 lives lost	Directional Sound Evacuation
5 January 1993	*Braer*	Grounded in severe weather, following engine failure	The Shetland Isles	85,000 tonnes of spilled oil	Tanker Traffic Routing
27 September 1994	*Estonia*	Sank in a storm	South of Uto (Finland)	852 lives lost	Passenger Ferry Safety II
15 February 1996	*Sea Empress*	Grounding	Milford Haven (South Wales)	72,000 tonnes of spilled oil	HNS Convention
16 January 1998	*Flare*	Split in two during rough weather	Gulf of St. Lawrence	21 lives lost	Bulk Carrier Design & Construction
12 December 1999	*Erika*	Broke in two	West Coast of France	10,000 tonnes of spilled oil	Sub-Standard Tankers
13 November 2002	*Prestige*	Broke in two and sank 6 days later	Northwest Coast of Spain	77,000 tonnes of spilled oil	Establishment of PSSAs

where; SOLAS means is the International Convention for the Safety of Life at Sea
MARPOL is the International Convention for the Prevention of Pollution from Ships
STCW is the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
ISM means International Safety Management
ALARP means As Low As Reasonably Practicable
OPA means Oil Pollution Act
HNS means Hazardous and Noxious Substances
PSSA means Particularly Sensitive Sea Area

1.2.2 Overlooked Contributory Causes of an Undesirable Event

Many lessons still need to be learnt from the past maritime accidents. There is also no doubt that the less dramatic, or less well-publicised accidents, incidents/ near misses, as well as certain unsafe acts bringing about errors and those of recovery occurrences, do have equally valuable lessons to be learnt from. In fact, it is possible that accidents may have propagated from the later and yet these are often overlooked as likely sources of the problem with the safety issue in the maritime industry. Thus, within existing maritime safety regulations, there are several amendments to be undertaken that may prove invaluable in preventing even the likely occurrence of an incident from developing any further.

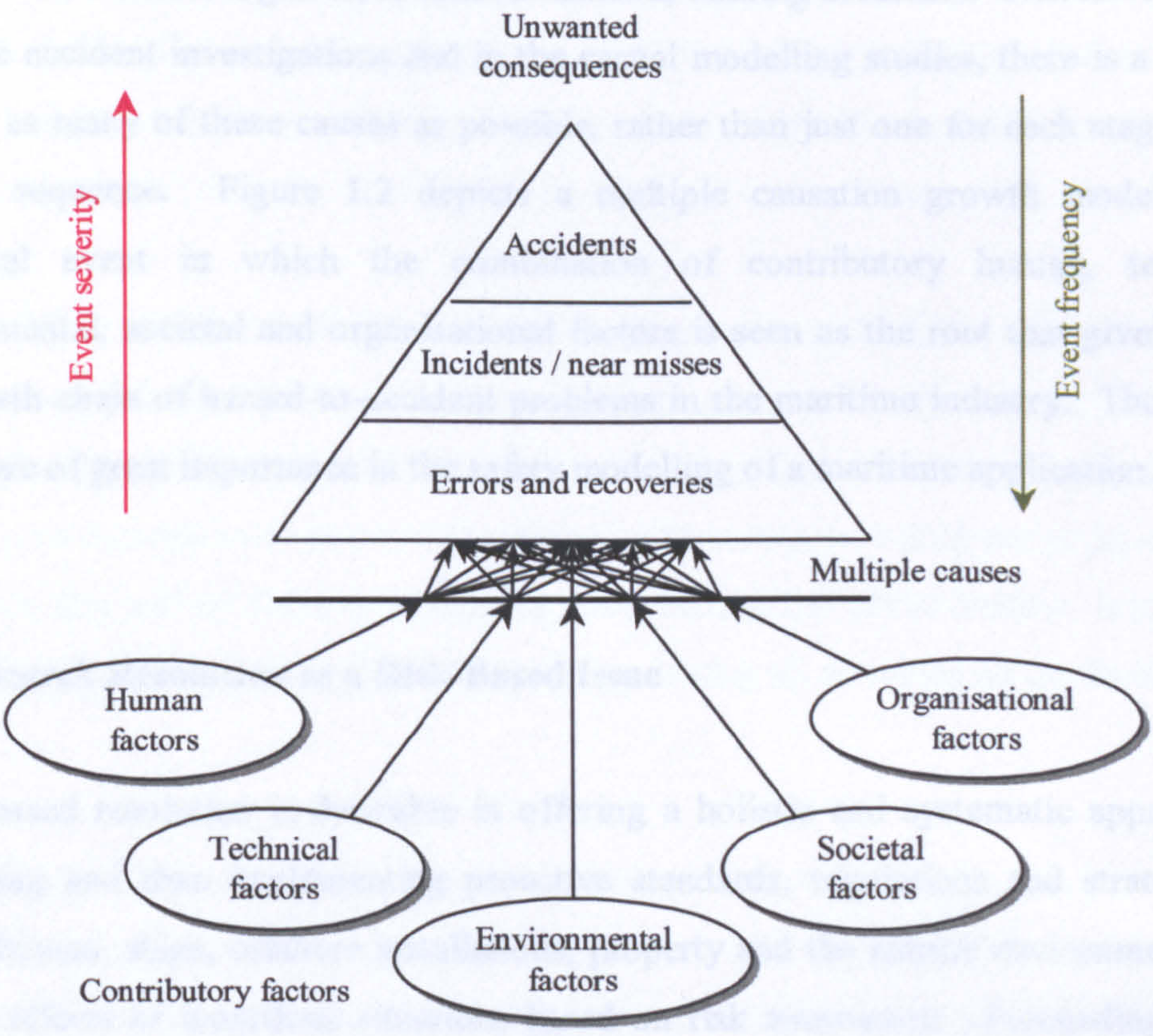


Figure 1.2: A multiple causation growth model of an accidental event

It is extremely difficult to prevent accidents in the absence of an understanding as to how near misses, incidents or accidents are caused. Prior to the 1980's (Peterson,

1996), all the knowledge, tools, and techniques of events existing prior to an accident were built on a set of principles that were first derived by Heinrich (1931). Perhaps the most important of these principles behind a built model of the causes of an accident is the *domino theory of accident causation.* This principle implies that accidents result from a sequence of events and suggests that removal of one single event in this sequence of events will prevent an accident from occurring. As such, the domino model has been noted as a *one-dimensional sequence of events*, which has proved to be inadequate for complex systems like ships and offshore installations.

In complex systems, accidents are usually *multi-factoral* and develop through relatively lengthy sequences of changes and errors. This has led to the principle of multiple causation. According to Peterson (1978), behind every accident there lie many contributing factors, causes and sub-causes. The *theory of multiple causation* is that these factors combine together, in random fashion, causing accidents. Therefore, during maritime accident investigations and in the casual modelling studies, there is a need to identify as many of these causes as possible, rather than just one for each stage of the domino sequence. Figure 1.2 depicts a multiple causation growth model of an accidental event in which the combination of contributory human, technical, environmental, societal and organisational factors is seen as the root that gives rise to the growth chain of hazard-to-accident problems in the maritime industry. Thus, these factors are of great importance in the safety modelling of a maritime application.

1.3 Research Resolution as a Risk-Based Issue

A risk-based resolution is desirable in offering a holistic and systematic approach to developing and thus implementing proactive standards, regulations and strategies to protect human, ships, offshore installations, property and the marine environment from adverse effects of hazardous situations based on risk assessment. Proceeding on the basis of sound criteria, the risks level can be determined for tolerability.

1.3.1 Reviewed State of Proactive Safety Practice

One way of ensuring that action is taken to avert the cause of an incident or accident in the maritime industry is the use of a risk-based concept. This is termed 'safety case' and 'formal safety assessment' approach for offshore and marine systems respectively.

1.3.1.1 Offshore Safety Case Concept

Most international safety legislative regimes were highly prescriptive before the Piper Alpha oil platform disaster in the North Sea, off the UK (in 1988). One of the most significant findings of the inquiry into the disaster, headed by Lord Cullen, was that prescriptive regulation provides no guarantee of excellent safety performance (DOE, 1990). It guaranteed nothing more than compliance to a minimum level. Thus, the Lord Cullen Report recommended the establishment of the objective based *safety case (SC)* regime and its concept has ever since been adopted in the offshore oil and gas industry.

The SC (HSE, 1998) is a detailed document that outlines the types of safety studies undertaken and the results obtained, and the management arrangements to ensure the continued safety of an offshore facility and persons on it. It should demonstrate that the operator knows what technical and human activities occur, how they are to be managed and how safety will be assured throughout the operating life of the facility. It must also identify the methods used for monitoring and reviewing all activities on the facility.

1.3.1.2 Marine Formal Safety Assessment Concept

The House of Lords committee, headed by Lord Carver, asserted in 1992 that modern science and technology were not being adequately applied in the many fields that affect shipping safety and that the time had come for a radical change (House of Lords, 1992). In respect of the regulatory regime for shipping, the Carver Report envisaged the adoption of safety goals based upon a quantified assessment of risks, costs and benefits, coupled with the introduction of a ship SC regime for every commercial vessel.

Although, the idea had considerable merit on the basis of such quantified assessments, the UK government made clear that to contemplate a SC for every individual vessel would be impractical for the foreseeable future as such a regime would put unrealistic demands upon the resources of both the regulator and the regulated operator (MSA, 1996). Hence, the concept of *formal safety assessment (FSA)* was proposed.

FSA (IMO, 2002b) allows a systematic and proactive view to be taken of ship safety enabling informed decisions to be made based on the objective analysis of risk. The concept involves using the techniques of risk assessment and cost benefit analysis, not for individual ships, but as a tool to assist in the International Maritime Organisation's (IMO's) decision-making process in formulating new and amended rules for shipping in general. The UK reasoned that adoption of FSA would enable safety and pollution issues at IMO to be prioritised, and regulations to be derived that are cost effective and proportional to risk.

1.3.2 Basic Definitions to Understanding Risk Evaluation Process

A risk-based approach for a safety-critical maritime system/unit should be one in which any perceived risk to the system can be evaluated so as to reflex where there may be a need for possible risk reductions or design modifications (See Section 1.3.3). The following basic definitions give clarity to fundamental expressions in the risk evaluation process for the system:

(a) Hazard

A hazard is defined as a physical situation with the potential for human injury, damage to property, damage to the environment, economical loss or some combination of these. Hazards are classified according to the severity of their potential effects, either in terms of safety, economics or other consequences. Such classifications alone are purely subjective and usually require qualification and quantification, by definition of the precise form of the hazard and quantified evaluation of the consequences (Warner, 1992).

(b) Risk

Risk is a combination of the probability, or frequency, of occurrence of a defined hazard and the magnitude of the consequences of occurrence on lives, property and the environment. Criteria for acceptability of some predicted risk or measured risk can be set voluntarily by the organisation responsible and/or subjected to the hazard, or be set mandatorily by some regulatory organisation (Warner, 1992).

(c) Safety

Safety is a term that denotes freedom from unacceptable risks/personal harm.

(d) Reliability

Reliability is the probability of failure-free operation for a specified length of time.

1.3.3 Framework for Risk Criteria

The simplest framework for risk criteria is a single risk level that divides tolerable risks from intolerable ones (i.e. acceptable activities from unacceptable ones). Such criteria give attractively simple results, but they need to be used very carefully, because they do not reflect the uncertainties both in estimating risks and in assessing what is tolerable. For instance, if applied rigidly, they could indicate that, an activity, which just exceeded the criteria, would become acceptable as a result of some minor remedial measure that in fact scarcely changed the risk levels. A more common approach to dividing tolerable and intolerable risks is to use two criteria, known as "*maximum tolerable*" and "*negligible*" *levels.* These divide risks into three tiers as shown in Figure 1.3 (HSE, 1992), that is:

- An intolerable region (above the "maximum tolerable" criterion) within which the risk is generally intolerable whatever the benefit may be. Risk reduction measures or design changes are considered essential.

- A middle band (between the "maximum tolerable" and "negligible" criteria) where risk reduction is desirable. In the UK, risks in this region are considered to be tolerable only when they have been made "as low as reasonably practicable" (ALARP). This requires risk reduction measures to be implemented if they are reasonably practicable, as evaluated by cost-benefit analysis.
- A negligible region (below the "negligible" criterion) within which the risk is generally tolerable, and no risk reduction measures are needed.

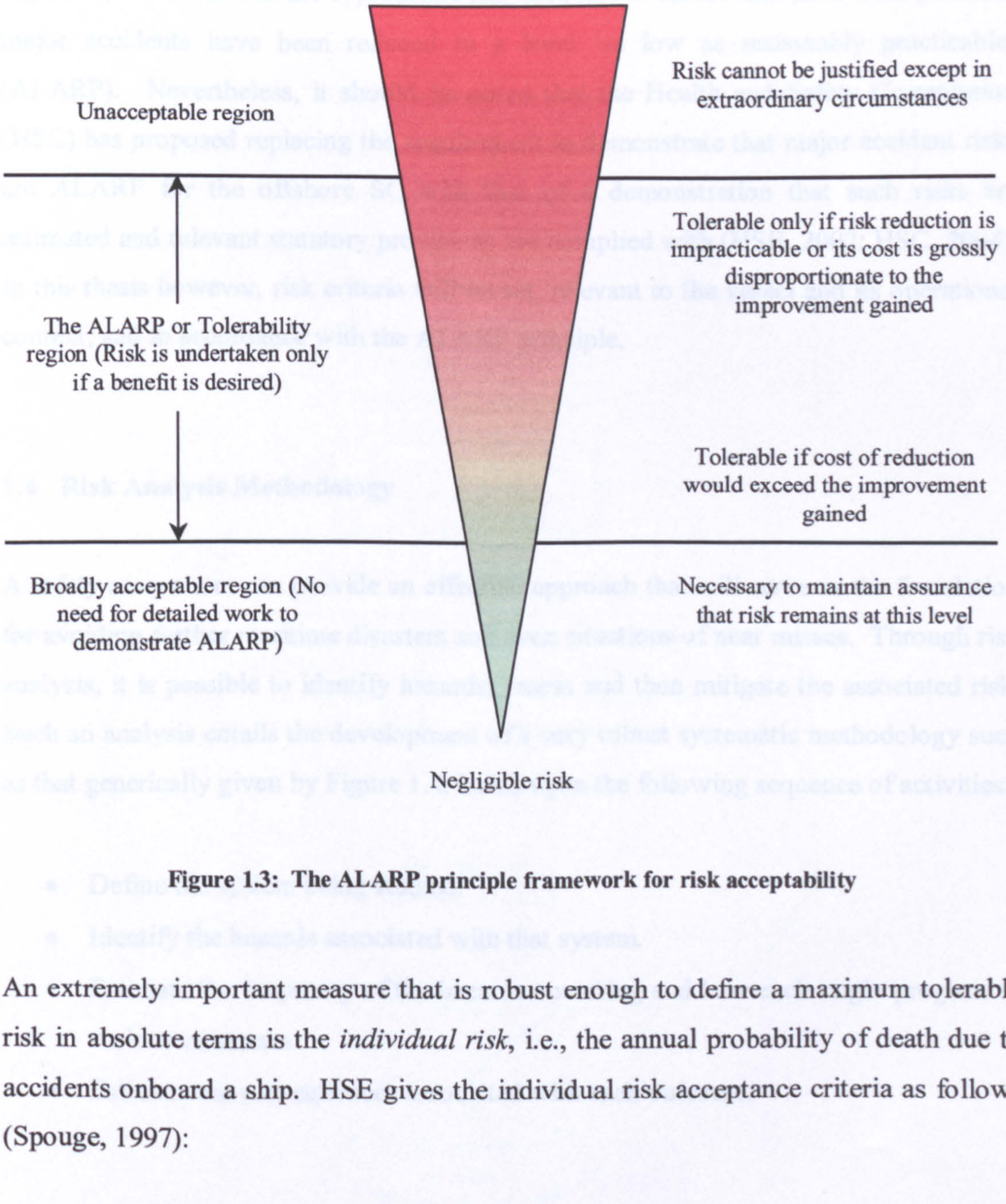


Figure 1.3: The ALARP principle framework for risk acceptability

An extremely important measure that is robust enough to define a maximum tolerable risk in absolute terms is the *individual risk*, i.e., the annual probability of death due to accidents onboard a ship. HSE gives the individual risk acceptance criteria as follows (Spouge, 1997):

- Maximum tolerable risk for *crew members* is 10^{-3} (i.e., 1 in 1,000) per year.
- Maximum tolerable risk for *passengers* is 10^{-4} (i.e., 1 in 10,000) per year.
- Maximum tolerable risk for *public ashore* is 10^{-4} (i.e., 1 in 10,000) per year.

However, if all individual risks are below 10^{-6} per year, this suggests that risks are negligible and cost benefit analysis need not be justified (Spouge, 1997).

One of the main objectives of the SC and FSA approaches is the demonstration (to the regulator) that measures are appropriate and adequate to ensure that risks from potential major accidents have been reduced to a level 'as low as reasonably practicable' (ALARP). Nevertheless, it should be noted that the Health and Safety Commission (HSC) has proposed replacing the requirement to demonstrate that major accident risks are ALARP for the offshore SC with that of a demonstration that such risks are estimated and relevant statutory provisions are complied with (HSE, 2002; HSC, 2004). In this thesis however, risk criteria will be set, relevant to the vessel and its operational context, and in accordance with the ALARP principle.

1.4 Risk Analysis Methodology

A safety assessment can provide an effective approach that will serve as the foundation for avoiding further maritime disasters and even situations of near misses. Through risk analysis, it is possible to identify hazards, assess and then mitigate the associated risk. Such an analysis entails the development of a very robust systematic methodology such as that generically given by Figure 1.4, based upon the following sequence of activities:

- Define the system being studied.
- Identify the hazards associated with that system.
- Estimate the frequency of the hazards occurring and how each might progress to various outcomes.
- Estimate the consequences associated with each outcome.

- Multiply hazard frequency and consequence to obtain the risk associated with each outcome.
- Sum the risks associated with the outcomes to produce an overall risk.
- Check if risk is acceptable based on the criteria as given by the ALARP principle.
- If risk is acceptable, carry out risk mitigation otherwise modify system.

In practice, both the SC and FSA approaches apply this risk assessment methodology. Therefore, the resulting development of this research can be effectively integrated into this aspect of both approaches. It should be noted that the measure of the frequency of the hazards occurring is a function that is deduced from its *possibility*, *evidential* or *probability distribution*. Thus, with the recognition that quantitative risk assessment is not always the most appropriate due to its too prescriptive nature (HSC, 2004), the idea should be that risk analysts use effective risk assessment techniques, selected to be appropriate to the circumstances.

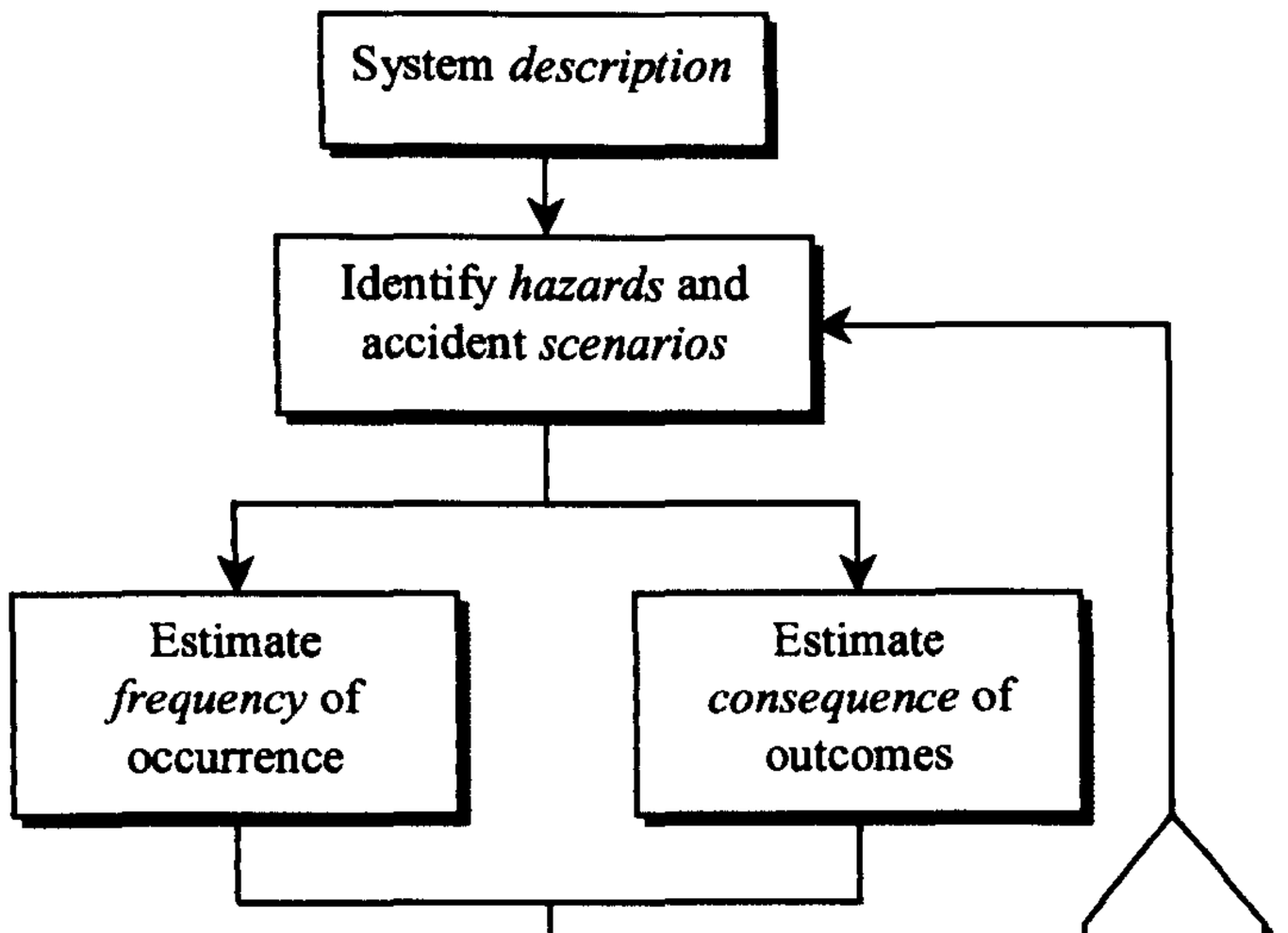


Figure 1.4: Generic process of the risk analysis framework

An obvious benefit of risk assessment is that the results serve as the basis for a cost-effective means for risk mitigation and avoidance. With respect to these, it is often possible to undertake actions that will reduce the potential of the occurrence of an incident or accident.

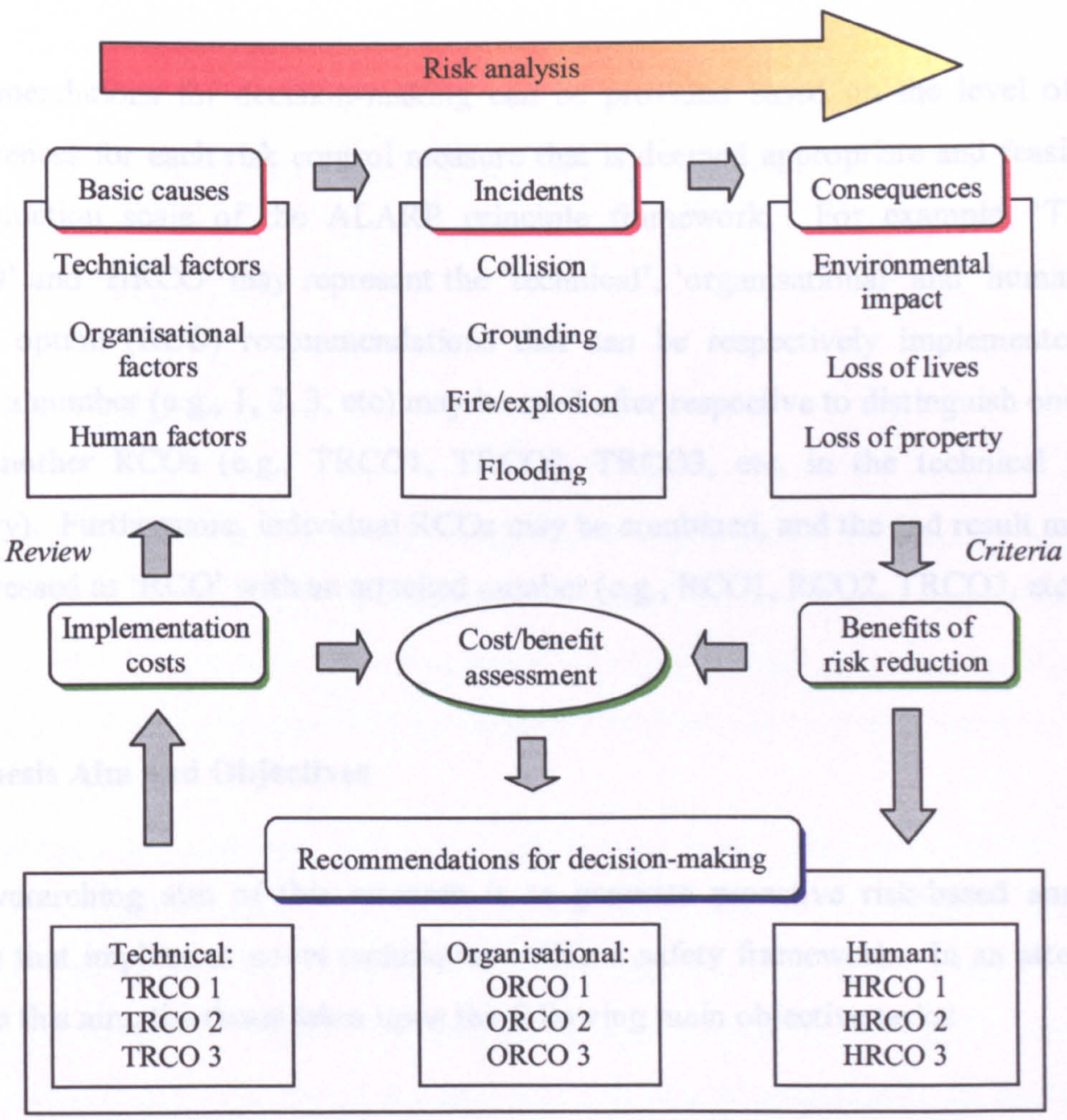


Figure 1.5: Proposed research framework for risk-based assessments

In order to implement the outlined risk analysis methodology effectively, Figure 1.5 gives a proposed framework for which the risk-based assessment settings of this research can also be achieved via a cost effective means. It has been developed by

moulding the multiple causation growth contributory causes of an undesired event (see Section 1.2.2) into the risk analysis process whilst also effecting the treatment of uncertainty (a vital issue of problem definition as stated in Section 1.2.1) for the safety assessment of the maritime application. Following from this, the final risk that would be determined for the application may then be reduced based on the ALARP Principle (Section 1.3.3). Cost effectiveness can thus be demonstrated via the assessment of the benefits of the risk reduction and the implementation costs for greater risk reduction measures (HM Treasury, 1997; Mathiesen, 1997; HSE, 2001) of life saving and environmental protection for the safety-critical maritime application.

Recommendations for decision-making can be provided based on the level of cost-effectiveness for each risk control measure that is deemed appropriate and feasible on risk reduction scale of the ALARP principle framework. For example, 'TRCO', 'ORCO' and 'HRCO' may represent the 'technical', 'organisational' and 'human' risk control option (RCO) recommendations that can be respectively implemented. In theory, a number (e.g., 1, 2, 3, etc) may be used after respective to distinguish one RCO from another RCOs (e.g., TRCO1, TRCO2, TRCO3, etc, in the technical factors category). Furthermore, individual RCOs may be combined, and the end result may just be expressed as 'RCO' with an attached number (e.g., RCO1, RCO2, TRCO3, etc).

1.5 Thesis Aim and Objectives

The overarching aim of this research is to generate proactive risk-based analytical models that implement novel techniques within a safety framework. In an attempt to achieve this aim, the thesis takes upon the following main objective tasks:

- To review the current status of safety practice in both marine and offshore industry.
- To establish appropriate data statistics for carrying out risk-based assessment.
- To identify key risk analysis techniques that are currently in use within the maritime industry.

- To examine formal safety assessment procedures and review the developments of its trial application to ships.
- To facilitate the incorporation of uncertainty treatment into the maritime application domain of risk-based reasoning.
- To demonstrate how the adoption of Bayesian network (BN) can enable a powerful marine and offshore decision-support solution.
- To demonstrate the application of fuzzy logic (FL) towards evidential reasoning synthesis in maritime engineering safety analysis.
- To investigate the integration of BN and FL for the incorporation of the human element into probabilistic risk-based modelling.

These goals are being established more clearly as the work proceeds through each chapter of the thesis.

1.6 General Scope of Work

The chapters in this thesis have been organised to express a certain flow of thought or line of argument. Figure 1.6 summaries the logical structure of the thesis. Obviously, the structure starts off with this introductory platform chapter that gives light into the much-needed risk-based approach to marine and offshore safety as its Chapter 1.

Sourced data for carrying out safety assessment tasks may need to be treated statistically, which Chapter 2 demonstrates, before they can be well utilised. Chapter 3 presents some typical risk analytical techniques that are used in maritime safety and reliability assessment studies. In Chapter 4, a structured formal safety assessment (FSA) methodology that allows for proactive risk control measures to be permitted is presented and this chapter further provides a review of the noteworthy developments in the trial application of FSA to some ship types. Chapter 5 explores the incorporation of uncertainty treatment into the application domain of risk-based reasoning. Bayesian network (BN) is adopted in Chapter 6 to enable a powerful decision-support solution under the realm of random uncertainty, whilst fuzzy logic (FL) treats the vague uncertainty and then offers a safety analysis solution in Chapter 7 via evidential

reasoning synthesis. In Chapter 8, an integrated risk model of BN and FL is achieved in a fuzzy-Bayesian network of an induced mass assignment paradigm. Chapter 9 concludes the thesis with an overall review and also then presents its principal findings, major limitations and recommendations for future work of the research.

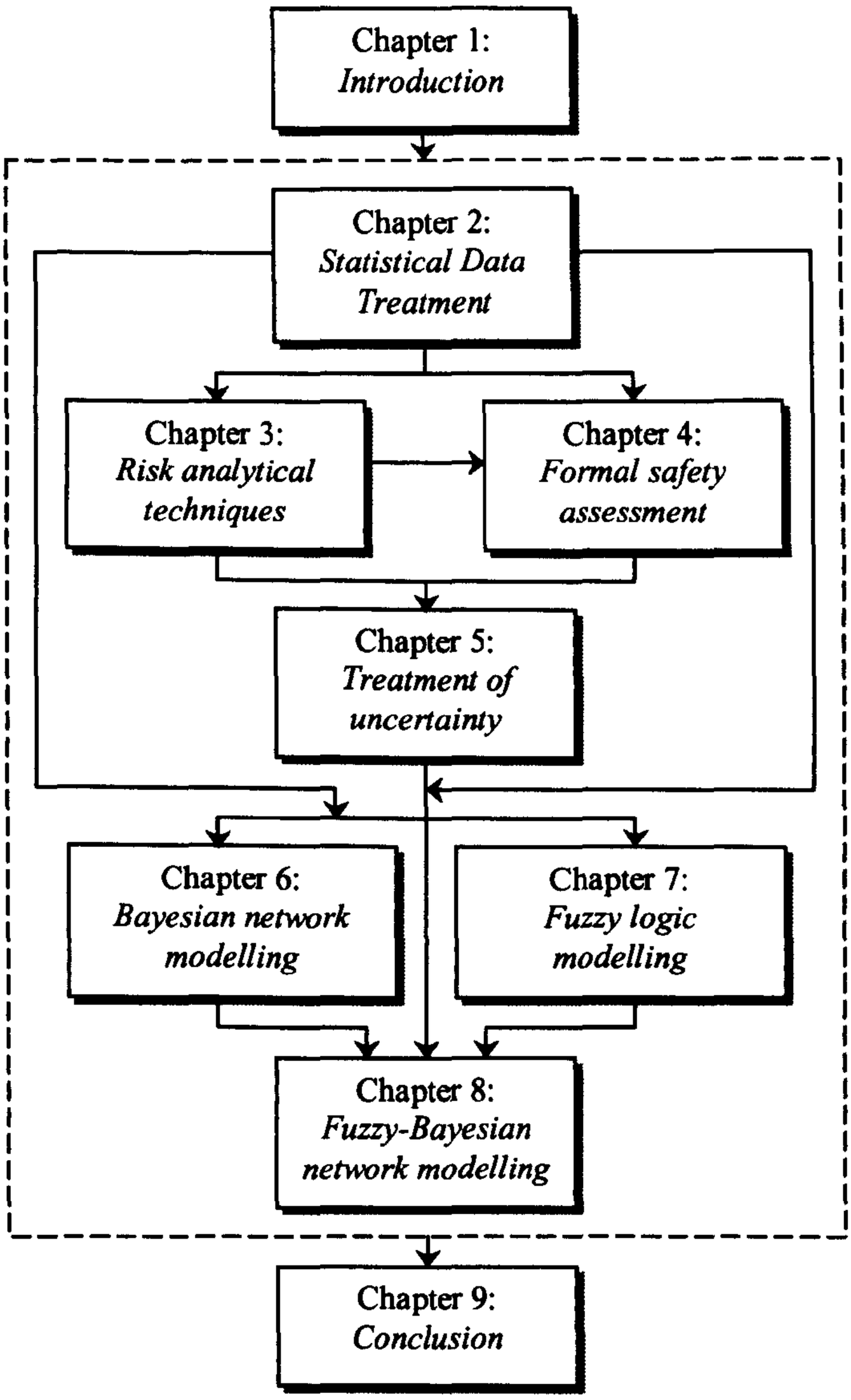


Figure 1.6: Structure of the thesis

1.7 Concluding Remarks

In the field of marine regulations, the high number of casualties and oil pollutions has acted as a catalyst in triggering a positive reaction that led to the adoption of reforms

designed to improve maritime safety. Nevertheless, such systems have often overlooked the areas of several contributory factors (such as the human factor) and their causes, which can result into errors, incidents and accidents. Besides, an account of uncertainty is not habitually taken into consideration. The approach of SC and FSA is currently adopted in the offshore and marine industry respectively to proactively establishing safety at sea.

Preparation and submission of a SC constitute a key strategy in the drive for improved safety in the offshore oil and gas industry, whilst FSA for the marine industry delivers the maximum level of safety and pollution prevention in a cost-effective manner. Both industries apply the ALARP principle as the risk criteria. Furthermore, a risk analysis methodology has been presented, which establishes the generic framework upon that the safety assessments in this thesis are embarked upon.

The research aim is to achieve the generation of proactive and integrative risk-based assessment models within its safety analytical framework. Hence, several goals have been established within a well-structured outline of the chapters in the thesis.

Chapter 2: Statistical Data Treatment

Chapter Summary

Data for risk and uncertainty modelling usually needs to be treated statistically in order to satisfy their use in an application tool. Several useful maritime databases provide reliable failure and repair rates, or information/data on accident category types, such as the nature and number of occurrences of incidents/accidents. Some supplementary data can also be obtained from expert judgement, models or simulations. Failure probability distributions are then used to enable the probabilistic modelling of failure and repair activities. In the related consequence term, the frequency of occurrence of accidents, as obtained from a historical database and the distribution of the numbers of fatalities in such accidents are required to give a frequency-number of fatalities graph. The area under this graph provides a convenient one-dimensional measure of societal risk, which is termed the potential loss of life.

2.1 Introduction

Reliable failure and repair data is a paramount item in developing any kind of safety and reliability assessment. The existence of these prime data will enable any authority to determine the probability of occurrence and the extent of the consequences of a hazardous event or its associated failed components and systems. The available data will also help to determine the nature of risk analysis methods, such as *qualitative* or *quantitative*, to be utilised in the process of the maritime risk-based methodology (e.g., 'safety case' or 'formal safety assessment').

Various authorities or bodies attend to safety issues from different perspective in order to facilitate their own interest. For example, data from *classification societies* will mainly deal from the viewpoint of compliance with various sets of rules and regulations

in force. Meanwhile, data from *protection & indemnity (P&I) clubs* tend to deal with the matter from the viewpoint of financial losses due to lack of safety (Sii & Wang, 2003). When there is insufficient data from the database, then expert judgement, physical models, simulations and analytical models may be used to achieve valuable results (IMO, 2002b). Nonetheless, any data that is obtained, whether from database or otherwise, should always be critically evaluated.

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. 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.

Just as data for every error, incident or accident event are required to be treated, it is imperative that the data for their developing sequence of events and including their final consequences are dealt with. In this sense, every data that would proceed into risk or uncertainty analysis would have been completely justified for its suitable use by such statistical data treatment.

2.2 Collection of Failure and Repair Data

It is essential to obtain reliable statistical failure and repair data of components in order to apply safety assessment techniques. Generally, such failure and repair data of components can be obtained from field experience, life testing under controlled conditions in laboratory and/or laboratory testing of similar components (Misra, 1992). The collection of these data based on life tests of ships and offshore installations is precluded as a very expensive and labour demanding operation. Extensive use is made

of those collected from laboratory tests and field reports on similar components (generic data collection programmes). In addition, repair data may also be compiled from the agreed judgmental estimates of experts (Misra, 1992).

It should be noted that, for some components, there is fairly close agreement between different data banks and in other cases, there is a wide range of failure rates (Smith, 1992). The latter may be due to a number of reasons as, for example:

- Some failure rates involve the replacement of components during preventive maintenance whereas others do not.
- Failure rates are affected by so many factors that a variation in values exists.
- Although nominal environmental and quality levels are described in some databases, the range of parameters covered by these broad descriptions is large.

Great care should be taken to use failure and repair data obtained from data banks to reflect the environment to which the product is designed. 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 (Wang, *et. al*, 1993), although there is uncertainty about the relevant distributions.

How critical the reliability of the failure and the repair data is depends on the aims of the safety analysis. If the safety analysis aims at obtaining the best absolute estimate of system safety, as may be required by statutory requirements, the failure and repair data is obviously critical. In such cases, validation of the data becomes as important as the validation of the safety assessments themselves, and verification procedures should be implemented to ensure that the obtained data for components is reliable. Modification of the obtained data may also be required (Figure 2.1). However, when the estimates of the system safety are used for comparison purposes, the criticality of such data is greatly reduced. Safety analysis is then used to provide the sensitivity of the system safety and to indicate the relative benefits of design changes on system performance.

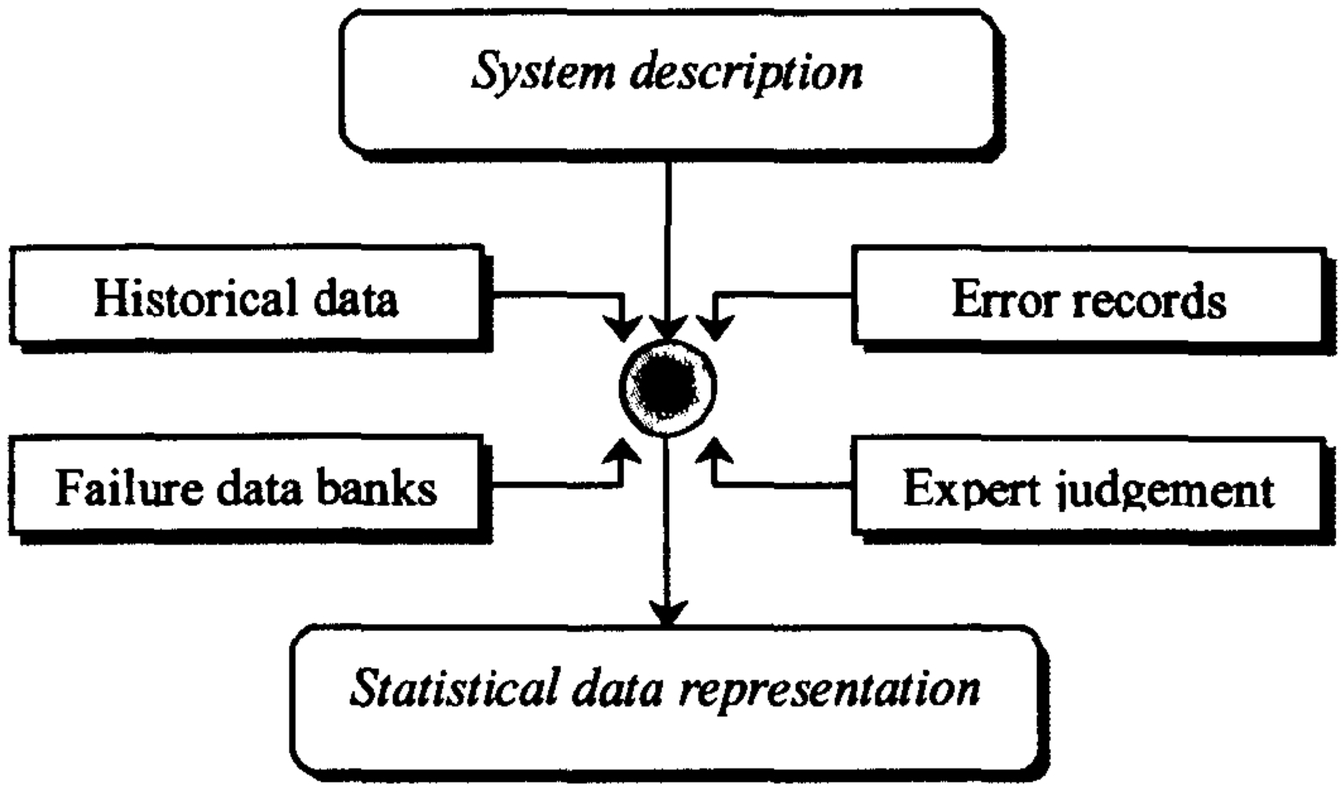


Figure 2.1: Sourcing of data for statistical data treatment and representation

The following sources 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.
- Nonelectronic Parts Reliability Data - NPRD3 (1985): This document is produced by the Rome Air Development Center. It contains field data information of electromechanical, mechanical, hydraulic and pneumatic parts.
- Handbook of Reliability Data for Electronic Components Used in Telecommunications Systems HRD4 (1986): This document is produced, from field data, by British Telecom's Materials and Components Centre.
- Electronic Reliability Data - INSPEC/NCSR (1981): This book, published jointly by the Institute of Electrical Engineers and the National Centre of Systems Reliability (Warrington) in 1981, consists of simple multiplicative models for semiconductors and passive electronic components with tables from which to establish the multipliers according to the environment, temperature and other parameters.

- OREDA- Offshore Reliability Data (DNV, 1992): 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.
- Green and Bourne - Reliability Technology, Wiley, 1972: This book contains failure rate data obtained mostly from US and UK atomic energy sources.
- UK Atomic Energy SRD Data Bank: It contains the generic reliability data of various components and is maintained by the SRD (Systems Reliability Department) at the UKAEA (UK Atomic Energy Authority at Culcheth), Warrington, Cheshire.
- 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 such as (Smith, 1985 and 1992).

It is also becoming useful to record and utilise data from near misses and errors. Furthermore, to ensure that there is an accurate applicability of the safety assessment carried out, novel techniques should integrate expert judgement with the obtained data in a formal manner (See Figure 2.1).

2.3 Categorisation of Hazardous Events

For the available data of any resourceful database(s) to be well utilised in a safety assessment study, accidents, incidents or errors that might affect or impair the seaworthiness of the vessel are categorised according to the nature of their occurrence. There resulting consequences can also be categorised similarly

2.3.1 Category of Major Accidents

Some of the *major maritime accidents* can be associated with one or more of the following categorises (LMIS, 1995):

- **Contact and collision**: Striking or being struck by another ship or external object, regardless of whether underway, anchored or moored. This category includes striking drilling rigs/platforms, regardless of whether in fixed position or in tow but it does not include striking underwater wrecks.
- **Grounding and stranding**: Being aground or hitting/touching shore or sea bottom or underwater wrecks.
- **Fire or explosion**: Accidents where the initial event is an uncontrolled process of combustion characterised by heat or smoke or flame or any combination of these, which engulfs sections of or the entire ship.
- **Missing vessel**: Ship whose fate is undetermined with no information having being received of conditions and whereabouts after a reasonable period of time.
- **War loss and hostilities**: Ship lost or damaged as a result of any hostile acts.
- **Heavy weather damage**: Ship suffering damage caused by severe weather and wave conditions that can occur unexpectedly.
- **Loss of structural integrity**: Structural failure resulting in the ingress of water and/or loss of strength and/or stability.
- **Flooding and foundering**: The ingress of water that leads to ship sinking as a result of causes such as heavy weather, springing of leaks and breaking into two.
- **Miscellaneous**: Lost or damaged ships that cannot be classified into any of the above categories or due to lack of information. For example, an accident starting by the cargo shifting (and not as a consequence of events of any of the above categories) would typically be classified as miscellaneous.

The rate of occurrence of such accidents is usually expressed in terms of *frequency per ship operating year*.

2.3.2 Category of Major Consequences

The accident categories in Section 2.3.1 have also been known to be the initiating event that can lead to one or more of the following *serious consequences* (LMIS, 1995):

- **Ship casualty**: Breakdown resulting in the ship being towed or requiring assistance from ashore, flooding of any compartment and/or structural, mechanical or electrical damage requiring repairs before the ship can continue trading.
- **Total ship loss**: Ship having ceased to exist after a casualty, either due to it being irrecoverable (actual total loss) or due to it being subsequently broken up (constructive total loss). Constructive total loss occurs when the cost of repair exceeds the insured value of the ship.
- **Cargo damage/loss**: Commonly by cargo contact with oil spill, fresh water or seawater and/or entire shipping package being missing at destination arising due to hull penetrations or insufficient/improper securing.
- **Environmental spillages/pollution**: Oil spills, general pollution, ecological destructions and dangerous gas releases. Spills are generally categorised by size (<7 tonnes, 7-700 tonnes and >700 tonnes), although the actual amount spilt is also recorded (ITOPF, 2005).
- **Human injury/fatality**: Human suffering that requires hospital treatment and in the worst of cases, loss of life. In cases were both injury and loss of life are combined, weightings such as, for example, 100 minor injuries are equivalent to 1 fatality; and 10 major injuries are equivalent to 1 fatality, is generally assumed (IMO, 1997c).

This list of consequences is not comprehensive, but rather it provides a representative sample that is meant to reflect some of the most unwanted cases during risk amplification of a critical event. The rate of occurrence of such consequences is usually expressed in terms of *casualty*, *spill* or *fatality rate per ship year*.

2.4 Data Forms of a Risk Variable

A risk variable (e.g., hazardous or consequential event) can be measured numerically measured from obtained data, otherwise it may be presented in qualitative or linguistic form. The measured numerical variable may be either *discrete* or *continuous* (See Figure 2.2, which also shows the distribution of the outcome/occurrence of an event, x).

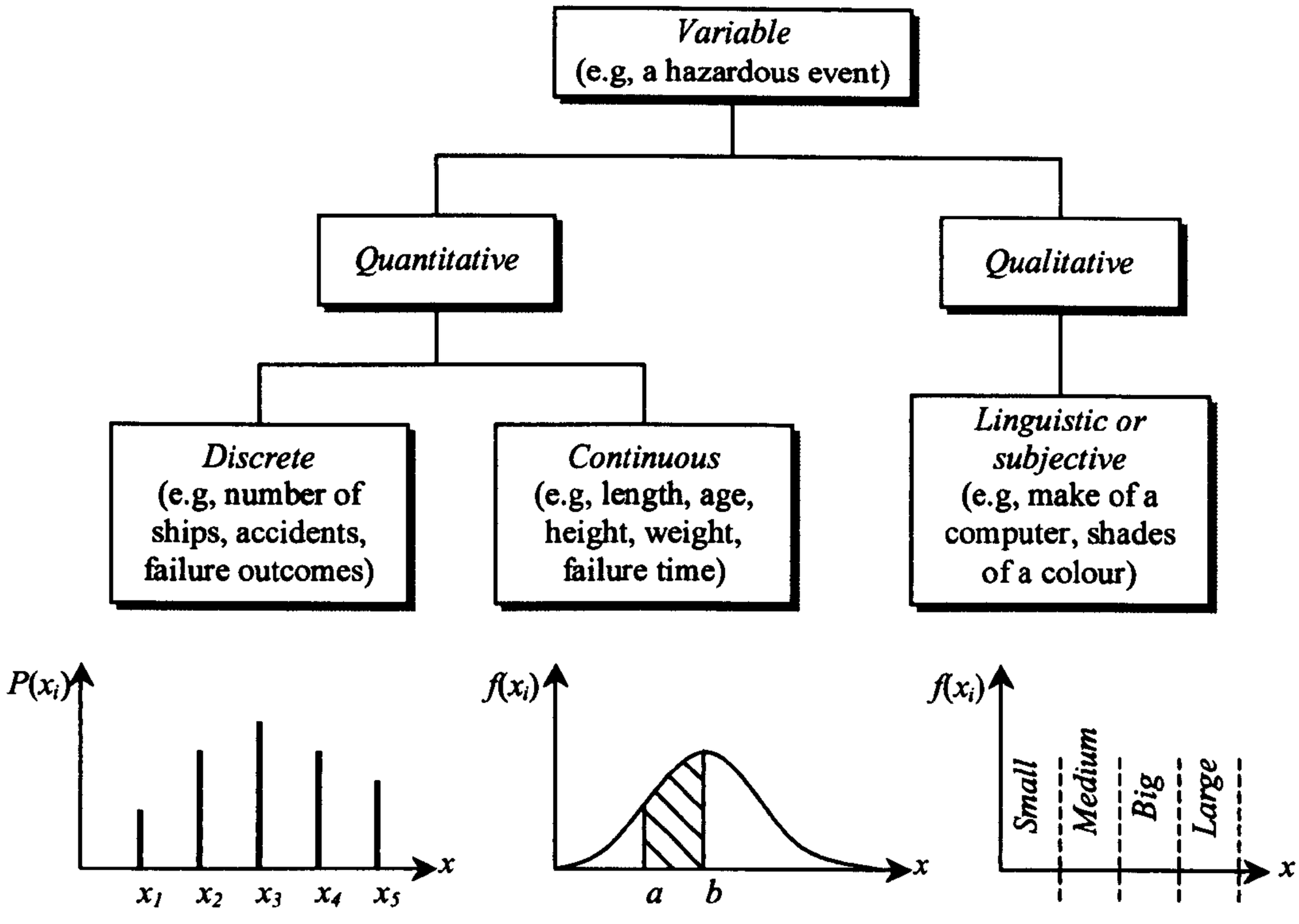


Figure 2.2: Types of variables and their occurrence distribution

As can be seen from Figure 2.2, a discrete variable is one in which its values are countable. In other words, it can assume only certain values (x_i where i = 1, 2, 3, 4, 5, etc) with no intermediate values. In its most basic form, the discrete model defines the probability of each individual outcome, $P(x_i)$. A continuous variable is one that can assume any numerical value over a certain interval (a to b) or intervals. In its most basic form, the continuous model is a mathematical expression (function) useful in computing probabilities of certain outcomes, $f(x_i)$. Time and distance are perhaps the most common continuous variables. A linguistic variable takes on certain grades such as *small*, *medium*, *big* or *large* over that describes a set interval or intervals.

2.5 Failure Probability Distributions

Failure frequency (i.e., rate of occurrence) data supplies the necessary input for carrying out maritime risk and uncertainty analysis. On the basis of such frequency/rate, there are a number of probability distributions for modelling failures. The most widely used

of these for discrete random variables are the *binomial* and the *Poisson* distribution. The exponential and the normal distribution are most extensively applied to continuous random variables. Law & Kelton (1982) and Henley & Kumamoto (1992) are excellent sources for additional detailed information on the distribution types.

2.5.1 Binomial Distribution

The binomial distribution describes the possible number of times that a particular event will occur in a sequence of observation. When there are just two possible outcomes, e.g., success and failure, then the binomial distribution is characterised by the equation:

$$(p + q)^n \tag{2.1}$$

where;

p = probability of event occurring (failure).

q = probability of event not occurring (success).

n = number of failures in the trial sequence of observation.

To get probabilities for any one term, put p and q into the formula:

$$P(x) = \frac{n!}{x!(n-x)!} p^x q^{n-x} \tag{2.2}$$

where;

x is the number of failures.

2.5.2 Poisson Distribution

The Poisson distribution best predicts probabilities of what can be considered 'rare and random events', where the event is rare relative to the number of times it could possibly occur and each event is independent of previous events in the sampling unit (time

period or unit of space). The Poisson equation for predicting the probability of a specific number of defects or failure (x) in time (t) is (Sherwin, 2004):

$$P(x) = \frac{(\lambda t)^n e^{-\lambda t}}{n!} \tag{2.3}$$

where;

n = number of failure in time (t)

λ = failure rate per hour

t = time expressed in hours

$P(x)$ = probability of getting exactly n failures in time t.

While the Poisson distribution governs the occurrence of random events in time, space, volume, etc, the intervals between such events is controlled by the exponential distribution.

2.5.3 Exponential Distribution

For many items, the relationship of failure rate versus time can be modelled by a "bathtub" curve. The idealised "bathtub" curve shown in Figure 2.3 has the following three stages:

- *Initial period*: The item failure rate is relatively high. Such failure is usually due to factors such as defective manufacture, incorrect installation, learning curve of equipment user, etc. Design should also aim at having a short "initial period".

- *Useful life*: In this period of an item, the failure rate is *constant*. Failures appear to occur purely by chance. This period is known as the "useful life" of the item.

- *Weardown period*: In this period of an item, the item failure rate rises again. Failures are often described as wear-out failures.

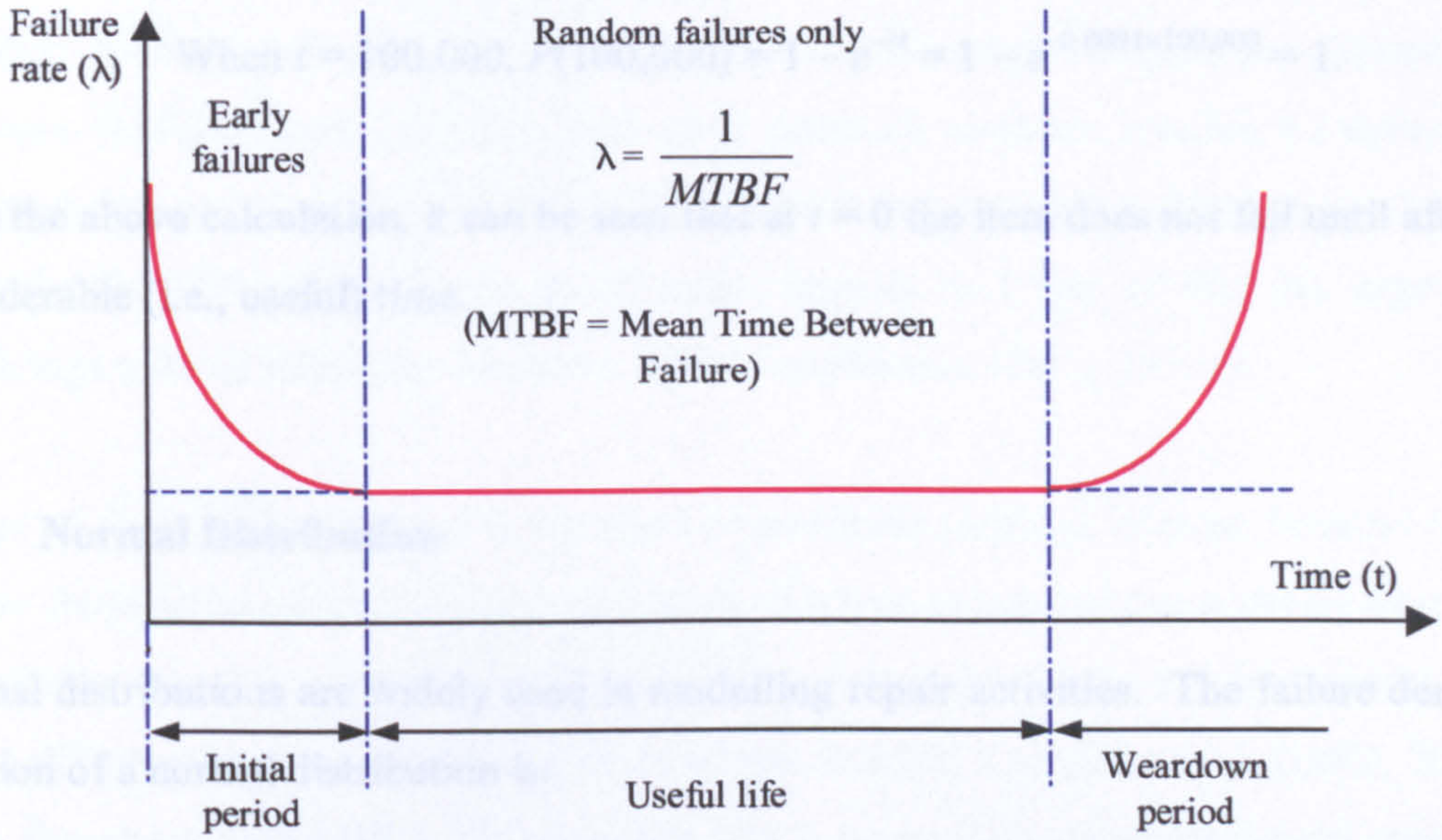


Figure 2.3: The "bathtub" failure rate curve

A risk assessment often concentrates on the useful life region of the curve, for which the failure rate is constant. In other words, a failure could occur randomly regardless of when a previous failure occurred. The failure density function of an exponential distribution is as follows:

$$f(t) = \lambda e^{-\lambda t} \qquad (2.4)$$

where failure rate $\lambda = 1/Mean\ Time\ Between\ Failure\ (MTBF)$ and t = time of interest.

Failure probability of an item at time t is:

$$P(t) = 1 - e^{-\lambda t} \qquad (2.5)$$

For example, given that the MTBF for an item is 10,000 hours, the failure probabilities of the item at t = 0, 10,000 and 100,000 hours if failures follow an exponential distribution can be calculated as follows:

$\lambda = 1/MTBF = 0.00001$ per hour.

When $t = 0$, $P(0) = 1 - e^{-\lambda t} = 1 - e^{0} = 0$.

When $t = 10{,}000$, $P(10{,}000) = 1 - e^{-\lambda t} = 1 - e^{-0.0001 \times 10{,}000} = 0.632$.

When $t = 100{,}000$, $P(100{,}000) = 1 - e^{-\lambda t} = 1 - e^{-0.0001 \times 100{,}000} = 1$.

From the above calculation, it can be seen that at $t = 0$ the item does not fail until after a considerable (i.e., useful) time.

2.5.4 Normal Distribution

Normal distributions are widely used in modelling repair activities. The failure density function of a normal distribution is:

$$f(t) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(t-\mu)^2/2\sigma^2} \qquad (2.6)$$

where μ and σ are mean and standard deviation of t. When $\mu = 0$ and $\sigma = 1$, it is called the standard normal distribution. The failure density for the standard normal distribution is:

$$f(t) = \frac{1}{\sqrt{2\pi}} e^{-t^2/2} \qquad (2.7)$$

2.6 Empirical Frequency-Number of Fatalities Graph

FN-curves are a graphical presentation of information about the frequency of fatal accidents in a system and the distribution of the numbers of fatalities in such accidents. In maritime systems, they plot the frequency per vessel operating year F of accidents against N or more fatalities (IMO, 1997c), where N ranges upward from 1 to the maximum possible number of fatalities in the system. Values of both F and N can sometimes range across several orders of magnitude. In fact, *FN*-graphs are usually drawn with logarithmic scales (HSE, 2003).

There are two general methods for constructing FN-curves. One method calculates the FN-curve directly from empirical frequency data on the past maritime accidents while the other develops and uses a probability model to estimate the frequencies. There is a spectrum between these extremes, and most practical methods involve a mixture of empirical data and modelling (HSE, 2003). In addition, equivalent fatalities for loss of life (equating 100 minor injuries to 10 major injuries to 1 loss of life) are approved weightings utilised within the maritime field of application (IMO, 1997c).

Values of F for high values of N are often of particular political interest, because these are the frequencies of high-fatality accidents. Society in general has a strong aversion to multiple casualty accidents. There is a clear perception that a single accident that kills 1,000 people is worse than 1,000 accidents that kill a single person (IMO, 2004). Thus, frequency and fatality are combined into a convenient one-dimensional measure of societal risk. This is also known as *potential loss of life (PLL)*, which can be calculated as follows:

$$\mathrm{PLL} = \sum_{i=1}^{n} F_i N_i \tag{2.8}$$

PLL is a type of risk integral, being a summation of risk as expressed by the product of consequence (i.e., fatality) and frequency. The integral is summed up over all potential undesired events that can occur. In other words, PLL approximates to the area under the FN-curve, as shown in Figure 2.4 (IMO, 2004), although it is typically measured as fatality per ship-year.

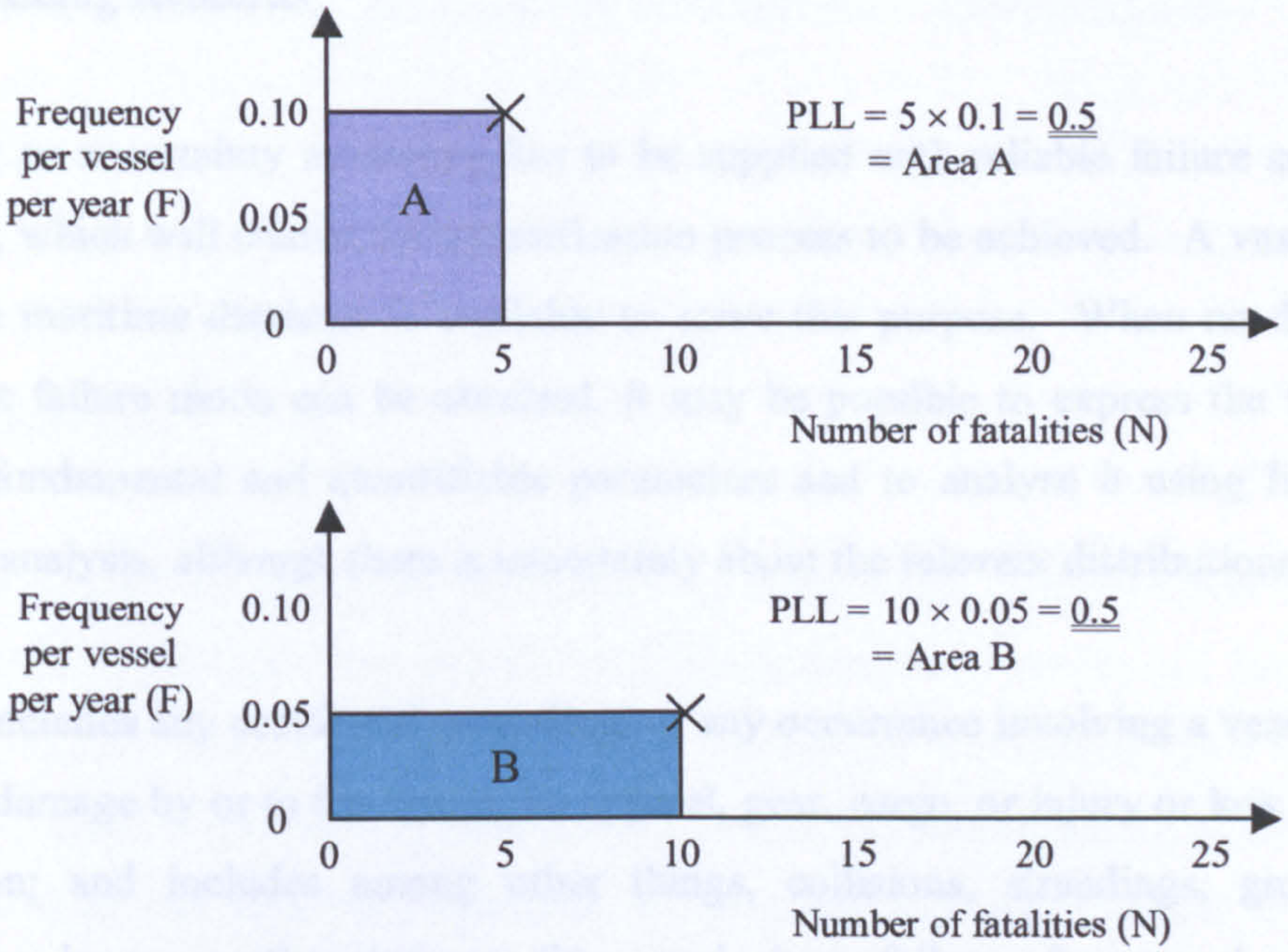


Figure 2.4: Generation of potential loss of life

2.7 Concluding Remarks

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.

Casualty includes any accidental grounding, or any occurrence involving a vessel which results in damage by or 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.

Societal risk data are normally presented in the form of an F-N curve the slope of which is a measure of the risk aversion towards accidents with multiple fatalities. If injuries and fatalities are required to be taken into account in a particular assessment, it is helpful to combine these into a single measure of the number of equivalent fatalities. The maritime industry makes use of relative weightings of 0.1 and 0.01 for major and minor injuries respectively.

Chapter 3: Review of Analytical Techniques

Chapter Summary

Risk-based modelling for safety assessment of marine and offshore units and their systems would necessitate risk analysts to identify hazardous events and enquire into their risk causes and consequences via a variety of dependable risk analytical techniques. Good use of such tools leads to an improved understanding of the systems posing the risks and lays the foundation for planning and taking action to improve safety. A general review is provided of the well-established safety and reliability assessment techniques as these methods have been widely accepted and applied in the industrial setting. A critical review is made of human reliability analysis tools for incorporate the human element into risk-based modelling because, not addressing the risks posed by human operators means that the risk analysis are necessarily underestimates. Finally, literature reviews are undertaken to permit developments for modelling techniques that can analysis and treat uncertainties arising from the domain model of study and its parametric values.

3.1 Introduction

When studying the safety aspects of a large ship or offshore installation, it is almost impossible to treat the system in its entirety, owing to nature of its complex engineering structure (Sen, *et al.*, 1993; Wang & Ruxton, 1998). A logical approach may be to break down the system into functional entities comprising subsystems and components, so that the interrelationships can be examined and finally a system safety model can be formulated to assess the safety parameters. This will therefore necessitate risk analysts to utilise some very well dependable analytical tools and techniques in the formulation of the assessment model.

A large number of techniques/methods exist for the identification of hazards and hazard scenarios as well as for use in risk estimation. These well established methods have seen continuous usage within industries because knowledge about the method is well documented in the literature (Mannan, 2005) and the analyst's own knowledge increases if focused on a basic amount of methods. The methods also lay down foundations for the development of novel techniques and may adjust to new applications (Harms-Ringdahl, 2001) especially as the depth of technology continuous to increase. They differ according to different dimensions (Hauge, 2001), e.g. depth of analysis, way of conducting analysis, whether they are quantitative or qualitative, and search method used. Obviously, safety assessments should be quantified only to the extent that is realistic and practicable (O'Connor, 1993). Which method to use, must be decided for each specific project as this enables the analyst to focus on the issue of concern and allows the analysis to be undertaken to an appropriate level of detail. Besides, use of different techniques might make it easier to both discover new hazards (bottom-up approaches, i.e. inductive/forward logic) and find causes for specific hazards (top-down approaches, i.e. deductive/backward logic) (Hansen, *et al.*, 2002).

Failing to addressing the risks posed by human operators mean that the risk analysis are necessarily underestimates (Redmill, 2002) and therefore, this calls for human reliability analysis (HRA) for the safety-critical maritime application. HRA is the method by which the probability of a system-required human action, task, or job will be completed successfully within the required time period and that no extraneous human actions detrimental to system performance will be performed (Hollnagel, 1994). Results of the HRA can then be used as inputs to probabilistic risk assessments, which analyses the reliability of entire systems by decomposing the system into its constituent components, including hardware, software, and human operators. However, HRA does not contribute fully to risk analysis, not only because of its deficiencies but also because there is a need for engineering risk analysts to become familiar with the techniques and to study human cognition and the models developed to explain human error. This is important with respect to modern systems especially as automation has increased rather than reduced the problems facing a human operator and the need to assess them.

Though tricky, HRA needs to be carried out. Yet, it is omitted from many, if not most, maritime risk analysis and safety assessments, and their techniques are largely unknown

to engineering risk analysts. Further, engineers have little guidance on the subject as most safety standards do not advise on it. For example, the influential international safety standard, IEC 61508-SER (IEC, 2005) addresses hardware and software functional safety in great detail, but offers no advice on human factors. HRA methods are in some respects flawed, but if used with care, they facilitate a significant but overlooked aspect of risk analysis that needs to be incorporated into modern safety-critical marine and offshore applications.

Uncertainties in risk analysis inputs are propagated through the risk assessment and evaluation steps of the safety assessment to obtain estimates of the level of confidence in the assessment outcomes (Chauhan & Bowle, 2003). Such uncertainties require techniques that can handle its treatment efficiently and effectively for the safety-critical maritime systems. The techniques are used to help predict how the systems would behave if they were to be hit by unforeseen catastrophic events such as the likes of fire, explosions, collisions, and loss of hull integrity (See Chapter 2, Section 2.3.1 for more details). Therefore, a review of related work is necessary for the development and application of uncertainty analysis methods that can appropriately deal with qualitative and quantitative factors of the risk assessment study. A method that can deal with both types of uncertainty may be necessary for the incorporation of the human element from an appropriate HRA study.

3.2 Qualitative and Quantitative Safety Assessment

Based on the requirements of safety analysts and the safety data available, either a qualitative or a quantitative analysis can be carried out to study the risks of a system in terms of the occurrence probability of each hazard and its possible consequences. A severe hazard with a high occurrence probability requires priority attention whilst that which is not likely to occur and which results in negligible consequences usually requires minimal attention (Aldwinckle & Pomeroy, 1983).

3.2.1 Qualitative Safety Assessment

Qualitative safety analysis is used to locate possible hazards and to identify proper precautions (design changes, administrative procedures, etc.) that will reduce the frequencies or consequences of such hazards. It should become an integral part of the marine or offshore safety and reliability process. It may be performed with one or more of the following objectives:

- To identify hazards in design and operation.
- To document and assess the relative importance of the identified hazards.
- To provide a systematic compilation of data as a preliminary step to facilitate quantitative analysis.
- To aid in the systematic assessment of the overall system safety.

The general steps in a qualitative system risk assessment are to:

- Identify significant hazards.
- Display the above information in a table, a chart, a fault tree or other format.

The consequences of a hazard can be classified as one of the four severity categories as shown in Table 3.1 (Halebsky, 1989). They range from "*catastrophic*" to "*negligible*". The occurrence probability of a hazard can be described using the levels ranging from "*frequent*" to "*remote*" as shown in Table 3.2 (Halebsky, 1989).

Table 3.1: Hazard consequence classification

Category	Description	Equipment	Personnel	Environment
I	Catastrophic	System loss	Death	Severe damage
II	Critical	Major system damage	Severe injury/illness	Major damage
III	Marginal	Minor system damage	Minor injury/illness	Minor damage
IV	Negligible	< Minor system damage	< Minor injury/illness	Negligible damage

Table 3.2: Hazard probability

Level	Description	Frequency
A	Frequent	Likely to happen
B	Probable	Several times during lifetime
C	Occasional	Likely to happen once
D	Remote	Unlikely but possible during lifetime

Engineering judgement and past experience is required to carry out a qualitative risk assessment. Measures can be taken to eliminate or control hazards based on the information produced from such an assessment. Table 3.3 forms the basis of determining design actions based on the combined consequence severity and occurrence probability of each hazard (Halebsky, 1989). A catastrophic hazard, for example, requires some corrective action regardless of the probability of occurrence, whereas a marginal hazard with a remote probability of occurrence would not normally receive any corrective action.

Table 3.3: Risk assessment matrix

Hazard Severity	Hazard Probability			
	A (Frequent)	B (Probable)	C (Occasional)	D (Remote)
1 - Catastrophic	A-1	B-1	C-1	D-1
2 - Critical	A-2	B-2	C-2	D-2
3 - Marginal	A-3	B-3	C-3	D-3
4 - Negligible	Negligible hazard ← No action required →			

- Design action is required to eliminate or control hazards classified as A-1, A-2, A-3, B-1, B-2, and C-1.
- Hazard consequences must be controlled or hazard probability reduced for hazards classified as B-3, C-2, and D-1.
- Hazard control is desirable if cost effective classified as C-3 and D-2.
- Hazard control is not cost effective for hazards classified as D-3.

3.2.2 Quantitative Safety Assessment

The purpose of a quantitative safety analysis is to help the designer to be aware of the characteristics of the system and to provide the designer with the quantified occurrence probability of each critical failure condition and the associated consequences.

Quantitative risk analysis utilises what is known and assumed about the failure characteristics of each individual component to build a mathematical model that is associated with some or all of the following information:

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

Typical parameters that need to be obtained in a quantitative risk analysis include both:

- The occurrence probability of each system failure event - A system failure 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 failure event 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 failure event can be quantified in terms of possible loss of lives/human injuries, property damage and the degradation of the environment caused by the occurrence of the failure event. With respect to the particular operating situation, experts normally quantify them.

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

- Sensitivity analysis.
- Comparison with prior analysis if possible.
- Model checking.

3.3 Methods for Safety and Reliability Assessment

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

3.3.1 Preliminary Hazards Analysis

A preliminary identification of the system elements or events that lead to hazards is the first step of a risk analysis. If it is extended in a more formal manner to include considerations of the event sequences that transfer a hazard into an accident, as well as corrective measures and consequences of the accident, the study is called a preliminary hazards analysis (PHA). PHA was introduced in the late sixties after the US Department of Defense requested safety studies to be performed at all the stages of product development. They issued guidelines that were applied from 1969 onward (DOD, 1969; DOD, 1999). It is also part of the mandatory activities required by MOD (1996) and SAE (1996).

PHA is a qualitative approach that involves a mixture of inductive and deductive logic. It is conducted on the basis of information such as casualty statistics and comprehensive knowledge of similar systems. A PHA may provide an essential foundation for further analysis of individual hazards, with particular reference to fault tree analysis and event tree analysis (Sen, *et al.*, 1993). The typical steps of a PHA are described as follows:

- Identification of hazardous events.
- Identification of hazardous event causes.
- Identification of hazardous event effects.
- Classification of risks.
- Determination of preventive measures.

The format of a typical PHA is as shown in Table 3.4.

Table 3.4: The format of a typical preliminary hazards analysis

No.: PHA _____.
Subsystem name:
Hazardous condition:
Possible hazardous event:
Probable hazardous result:
Result impacts: People only _____.
Equipment only _____, both _____.
Hazard classification: I ___, II ___, III ___, IV ___.
Recommendations:
Remarks:
Prepared by _____.

Hazard classifications I, II, III and IV stand for catastrophic, critical, marginal and negligible, respectively. PHA may be very useful in the problem definition and hazard identification phases of the safety and reliability assessment process. It is strongly suggested that PHA be carried out in the initial stages of the marine and offshore system design process.

3.3.2 What-if Method

The intention of "what-if" approach (CCPS, 1992) is to ask questions that will cause a multi-disciplinary team to consider potential failure scenarios and ultimate consequences that such failures might create. It has also been referred to as scenario analysis or deterministic simulation (Groumpos & Merkuryev, 2002). It uses a mixture of inductive and deductive logic.

"What-if" studies may often begin with the words "How could", "Is it possible", etc. Other forms of questions are perfectly acceptable. Some studies of this method incorporate checklists (DOD, 2000) at the end of the brainstorming to act as "sweeper questions", in order to ensure that potential hazards are not omitted. For example, a piece of work commissioned by the UK Department of Trade and Industry in 2003

required a group of risk experts to utilise a *structured what-if technique (SWIFT)* to ascertain hazards that may result from leaks of CO_2 from geological formations (Vendrig, *et al.*, 2003). The SWIFT follows a procedure that combines brainstorming, structured discussion and checklists to determine potential hazards. As its name suggests, SWIFT will generate answers more quickly than HAZOP (see Section 3.3.5) but is less thorough in looking at the detail (RINA, 2002). Furthermore, "What-if" analysis of a model considers the question: "What happens to the result if a particular change to a parameter is made"? If the change of a parameter is small this is also called *sensitivity analysis*: "How sensitive is the result to a small change of a parameter"?

Generally, the "What-if" approach may be very useful in the problem definition and hazard identification phases of the safety and reliability assessment process.

3.3.3 Parts Count

The inductive parts count method is often used to produce an upper bound of failure probability of a large and complex system. Parts count analysis models predict reliability of a system (EPSMA, 2004) by summing the part failure rates, while accounting for conditions, such as the environment, stress, and quality of workmanship. The failure rates used in the analysis are based on historical data. This analysis is used to evaluate configurations in the preliminary design phase when the number of parts is reasonably fixed. In addition, the overall complexity is not expected to change appreciably during later development and production. This analysis can also be used to provide verification data and have generally been used to predict the reliability of electronic components. However, the models can be extended to mechanical subsystems when appropriate data is available. A parts count analysis assumes the time to failure of the parts is exponentially distributed (that is, a constant failure rate). It also assumes that all elements of the item reliability model are in series or can are assumed to be in series for purposes of approximation. Thus, the general expression for item failure rate, λ_{item}, with this method is given as (DOD, 1995; Telcordia Technologies, 2001; FAA, 2005):

$$\lambda_{item} = \sum_{i=1}^{n} N_i \lambda_{gi} \pi_{Qi} \qquad (3.1)$$

where;

n = number of different generic parts categories;

N_i = quantity of ith generic part;

λ_{gi} = generic failure rate for the ith generic part; and

π_{Qi} = quality adjustment factor for the ith generic part.

Quality adjustment factors are usually applied to the failure rates to account for items, such as differences in application, temperature, and stress (FAA, 2005). For other parts such as non-electronics, $\pi_{Qi} = 1$ providing that parts are procured in accordance with applicable parts specification. The parts count technique may be very useful in the hazard identification and risk estimation phases of the safety and reliability assessment process.

3.3.4 Failure Mode, Effects and Criticality Analysis

Failure mode, effects and criticality analysis (FMECA) is one of the oldest and most frequently applied hazard identification methods. It is a combination of failure mode and effects analysis (FMEA) and criticality analysis (CA). FMECA was developed in 1967 by Society of Automotive Engineers to offer criticality analysis for the FMEA process (SAE, 1967). The FMEA technique was originally developed in the US Department of Defense in 1949 as a mechanism for improving the quality control of its weapons and military equipment (Pentti & Atte, 2002). FMEA was used as a reliability evaluation technique to determine the effect of system and equipment failures (Coutinho, 1964). Failures were classified according to their impact on mission success and personnel/equipment safety. The formal application of the technique was quickly adopted by the aerospace industry, where it was already used during the 1960s Apollo space missions. In the early 1980's, US automotive companies began to formally incorporate FMEA into their product development process (Pentti & Atte, 2002).

FMECA can be carried out at any indenture level required to examine each failure mode of an item and its possible consequences. An FMECA may consist of the following steps (DOD, 1980):

- Define the constraints and assumptions of the analysis.
- Break down the system to its indenture levels such as the sub-system level and the component level.
- For each item at the level analysed, identify all possible modes of failures and respective causes.
- For each identified failure mode, identify or provide the following information:
  - All the distinctive operating conditions under which failure may occur.
  - The failure rate of the identified failure mode.
  - The effects (consequences) on the safety and operability of the higher levels (including the level analysed).
  - The possible means by which failure may be identified.
  - Design provisions and/or actions in operation to eliminate or control the possible resulting effects.
  - The severity class of the possible effects where such a class may be defined by one of the following linguistic variables:

    Catastrophic: Involving death, system loss and/or severe environmental damage.

    Critical: Involving severe injury, major system damage and/or major environmental damage.

    Marginal: Involving minor injury, minor system damage and/or minor environmental damage.

    Negligible: Involving no injury and negligible damage to the system and the environment.
- Failure consequence probability defining the likelihood that the effects of the identified failure mode will occur, given that the failure mode has taken place.
- Criticality analysis

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. So 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:

$$C = \sum_{i=1}^{N} E_i L_i t \qquad (3.2)$$

where;

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; and

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 display shows the distributions 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, where available, for individual items. It can be integrated into the hazard identification phase of the safety and reliability assessment process and information produced from it may also be used to assist in construction of fault trees and also in construction of Boolean representation tables (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, the 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). Furthermore, guidance for dynamically positioned vessels FMEA has been provided by IMCA (2002) to provide a practical amalgamation of current regulations, operating procedures and good practice.

3.3.5 Hazard and Operability studies

A HAZard and OPerability (HAZOP) study is an inductive technique usually regarded as an extended FMECA (see Section 3.3.4) that can be applied by a multidisciplinary team to stimulate systematic thinking for identifying potential hazards and operability problems, particularly in the process industries (Henley & Kumamoto, 1992). Its basis was laid by Imperial Chemical Industries Ltd in 1963 from so-called "critical examination" techniques (Kletz, 1974; Lawley, 1974) at the time in which its application first became known as operability and hazard studies (Hendershot, *et al.*, 1998). It was soon after improved upon and to emphasize the importance of process safety, the name HAZOP (HAZard and OPerability) was coined (CIA, 1977). The technique was then used to run a pilot study on an agricultural chemical manufacturing plant that proved a great success (Hendershot, *et al.*, 1998). It went on to arouse greater interest and within ten years it had become widely acknowledged as one of the most powerful hazard identification technique (CIA, 1977; Henley & Kumamoto, 1992). The distinctive features of the HAZOP methodology are:

- A focus on state variables rather than mechanical components.
- An emphasis on an expert team approach.
- An explicit consideration of operator effects.
- A good foundation for subsequent quantitative risk analysis.

A HAZOP study investigates the proposed scheme systematically for every conceivable deviation, and looks backward for possible causes and forward for the possible consequences. It is normally based on a word model and the flow sheet or diagram of the system to be examined. The level of detail, depending on the time and merits, determines HAZOP study planning and as such, good knowledge of the system is essential. HAZOP studies involve normal plant operation, foreseeable changes in normal operation, start-up and shutdown, suitability of plant materials and failures of equipment and instrumentation. A HAZOP study may involve the following basic steps (McKelvey, 1988):

1. Define the scope of the study.
2. Select the correct analysis team.
3. Gather the information necessary to conduct a thorough and detailed study.
4. Review the normal functioning of the process.
5. Subdivide the process into logical, manageable sub-units for efficient study and confirm that the scope of the study has been correctly set.
6. Conduct a systematic review according to the established rules for the procedure being used and ensure that the study is within the special scope.
7. Document the review proceedings.
8. Follow up to ensure that all recommendations from the study are adequately addressed.

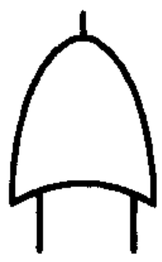
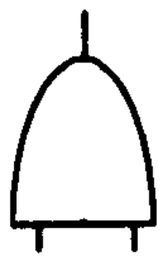
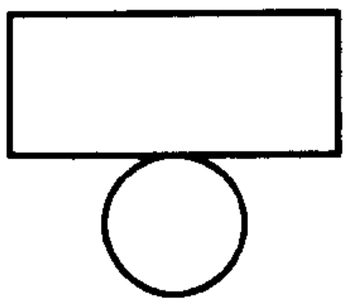
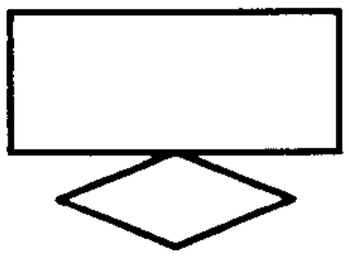
HAZOP studies can be integrated into the hazard identification phase of the safety and reliability assessment process and is one of the most commonly used hazard identification techniques in the marine and offshore industry (HSE, 2002). The form of HAZOP notes closely parallels the requirements of fault tree analysis (see Section 3.3.6) as a HAZOP study yields a clear identification of top events and a detailed description of failure sequences and associated operating conditions. FMECA (refer to Section 3.3.4), cause-consequence analysis (refer to Section 3.3.9) and Boolean representation analysis (refer to Section 3.3.7) can also make use of the information produced from HAZOP studies. In recent years, HAZOP studies have become increasingly recognised as an essential part of the process plant design by both the process industries (Kennedy & Kirwan, 1998; Tweeddale, 2003) and the regulatory authorities (Andrews & Moss, 1993). Thus, it is strongly suggested that HAZOP studies be conducted in the initial stages of the process plant design process.

3.3.6 Fault Tree Analysis

The idea of analysing potential faults using fault trees was first envisaged by Watson (1961) of Bell Telephone Laboratories, as a plan to evaluate the safety of the launch control system for the Minuteman missile. Scientists at the Boeing Company led by Haasl (1965) improved the technique to a modern theory and then applied it to the entire Minuteman Missile System. Other divisions within Boeing realised the usefulness of

the results from the Minuteman program and began using the fault tree technique during the design of commercial aircraft. In later years the technique was adopted by the nuclear power industry (Veseley, *et al.*, 1981) and nowadays its grown to become one of the most widely used methods in system reliability analysis (Veseley, *et al.*, 2002; FAA, 2005).

Table 3.5: Commonly used fault tree symbols

Types	Symbol	Description
Logic gates	 OR-gate	The OR-gate indicates that the output event occurs if any of the input events occurs
	 AND-gate	The AND-gate indicates that the output event occurs only if all the input events occur at the same time
Input events (states)		The basic event represents a basic equipment failure that requires no further development of failure causes
		The undeveloped event represents an event that is not examined further because information is unavailable or because its consequences are insignificant
Description of state		The comment rectangle is for supplementary information
Transfer symbols	Transfer out  Transfer in 	The transfer-out symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer-in symbol

The fault tree analysis (FTA) is probably the most widely applied technique for hazard identification and risk evaluation. Such an analysis is a process of deductive reasoning that can be applied to the safety assessment of a system of any size. It is particularly suitable for the risk assessment of large marine and offshore engineering systems for which the associated undesired (top) events can be identified by experience, from previous accident and incident/accident reports of similar products, or by some other means. The top events of a system to be investigated in FTA may also be identified through PHA (see Section 3.3.1), incident/accident reports, system Boolean representation modelling (see Section 3.3.7), etc. The information produced from FMECA (see Section 3.3.4) may be used in construction of fault trees.

FTA provides an engineering capacity to identify potential problem areas, to evaluate their overall system impact, and to numerically assess the level of safety inherent in the system design. Careful consideration must be given to the selection of the top event; it must be sufficiently defined to constrain the fault tree to the specific conditions to be investigated. Intimate knowledge of the system design is required to perform a fault tree analysis as the analyst must be familiar with the various modes of system operations and the types of component failures that can occur. Since a fault tree construction is event-based, human error (caused by operators, design or maintenance), hardware or software failures, environmental conditions or operational conditions can be taken into account (Sen, *et al.*, 1993). The steps in FTA are outlined as follows:

- Identification of top events.
- Representation of each top event by means of a fault tree.
- Evaluation of the occurrence probability of each top event.
- Determination of critical failure modes.

Fault trees are built using gates and events (blocks). The symbols used for the most common of these (and as used in this research) are given in Table 3.5. In an FTA, an event with a catastrophic nature or an event that cannot be tolerated, such as total loss of a system, is usually selected as a top event for investigation. The selected top event is placed at the top of the logic diagram, and the failure events that lead to the top event

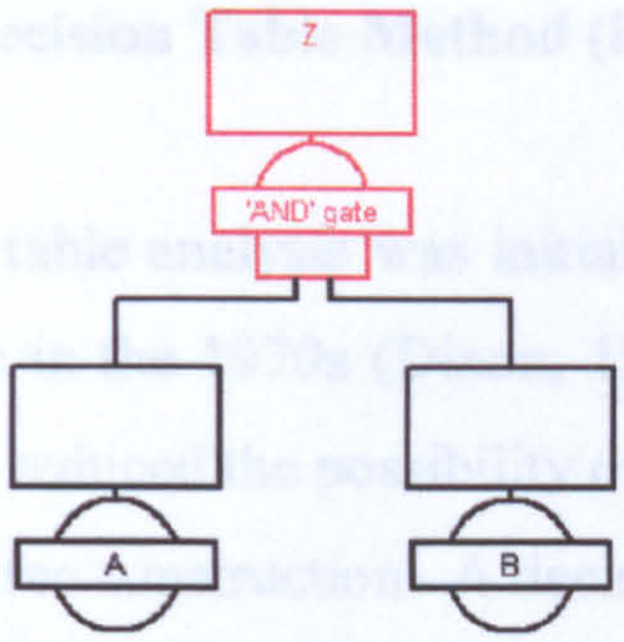
are located immediately below in successive levels. The pathways through the fault tree diagram represent all the events that give rise to the top event. These pathways are known as "cut sets" or "implicant sets" (Bozzano & Villafiorita, 2003). After the simplification rules have been applied, the irreducible pathways can be obtained and these irreducible pathways are referred to as "minimal cut sets" or "minimum implicant sets" (Wang, *et al.*, 2000; 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 " $\bar{B}$ " represents the events of "not A" and "not B" respectively, then the typical Boolean algebra rules are described as in Table 3.6.

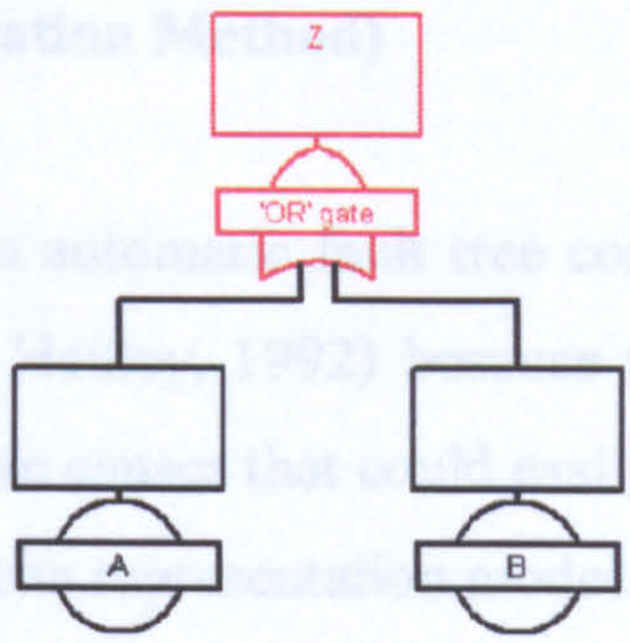
Table 3.6: Basic rules of Boolean algebra

Name of the rule	AND form	OR form
Identity law	$A \cdot 1 = A$	$A + 0 = A$
Null (or dominance) law	$A \cdot 0 = A$	$A + 1 = 1$
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	$A + (B \cdot C) = (A + B) \cdot (A + C)$	$A \cdot (B + C) = A \cdot B + A \cdot C$
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. The following two mini-trees in Figure 3.1 are used to demonstrate this.



(a) Event occurrence due to an "AND" gate



(a) Event occurrence due to an "OR" gate

Figure 3.1: Logic gate representation in a fault tree

Suppose $P(A)$ and $P(B)$ are the occurrence probabilities of events A and B respectively. If both these event are independent of each other, the occurrence probability of top event Z due to an "AND" gate as shown in Figure 3.1(a) is given by:

$$P(Z) = P(A \cdot B) = P(A) \times P(B) \tag{3.3}$$

However, the occurrence probability of top event Z due to an "OR" gate as shown in Figure 3.1(b) is:

$$\begin{aligned} P(Z) &= P(A + B) = P(A) + P(B) - P(A \cdot B) \\ &= P(A) + P(B) - P(A) \times P(B) \end{aligned} \tag{3.4}$$

FTA can be used in both reliability and risk 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 serious consequences. It may be carried out in the hazard identification and risk estimation phases of the safety and reliability assessment process to identify the minimal cut sets associated with system top events and to assess the occurrence probability of each top event in order to assist in design decision making.

3.3.7 Decision Table Method (Boolean Representation Method)

Decision table analysis was initially introduced as an automatic fault tree construction technique in the 1970s (Dixon, 1964; Fussel, 1973; Henley, 1992) because its logical approach reduced the possibility of omissions of failure causes that could easily occur in the fault tree construction. A decision table is a Boolean representation model.

An engineering system can be described in terms of components and their interactions. A component can be described by a set of input events and a set of output events. Each output event specifies the state of the output and a set of input events specifies the states of inputs. Each event may have several states. For instance, output pressure from a valve may be assigned to one of the five states such as "*too high*", "*high*", "*normal*", "*low*" and "*too low*", each of which corresponds to a range of values. The interactions of components can be modelled by studying the system process diagram.

Given sufficient information about a system to be analysed, this approach can allow a rapid and systematic construction of a Boolean representation table of the system on the basis of the Boolean representation models of the components and their interactions. Once components and their interactions have been modelled, Boolean representation modelling can be started initially at the component level, progressed up to the subsystem level if necessary, and finally to the system level in order to obtain the final system Boolean representation description. The final system Boolean representation table contains the possible system top events and the associated prime implicants (cut sets). Although the construction of such a table is not diagrammatic, as FTA can be, it can allow a less cumbersome representation of failure modes for components having multiple states, and it can also allow systems with feedback loops to be easily modelled (Henley, 1992; Kumamoto & Henley, 1979; Wang, *et al.*, 1993). This method is extremely useful for analysing systems with a comparatively high degree of innovation since their associated top events are usually difficult to obtain by experience, from previous accident and incident reports of similar products, or by other means.

3.3.7.1 Simplification of Boolean Representation Tables

Events or variables used in Boolean representation modelling can be classified in the following two categories:

1. Intermediate events/variables: These are the outputs from a component within the system
2. Primary (basic) events/variables: These are the events/variables that are inputs from the system environment or an internal mode of a component. An internal mode of a component represents its functioning for which the failure data is known.

Each primary variable or intermediate variable may have several states. Suppose the number of the states of a variable *A* and a variable *B* both equal three, as given by *F*, *W* and *N*, which stand for "*failed*", "*working*" and "*normal*", respectively. Then the rules for Boolean representation simplification, which are absorption (see Table 3.7(a)) and merging (see Table 3.7(b)), can be applied to obtain the output of a variable *C*. The symbol " * ", as used in Table 3.7, represents a "*don't care*" state. Such a state is used to signify that it makes no difference whichever state the specified input variable is in.

Table 3.7: Simplification rules for Boolean representation

(a) Absorption

A	*B*	C_{output}
N	*	High
N	N	High

→

A	*B*	C_{output}
N	*	High

(b) Merging

A	*B*	C_{output}
F	F	High
F	W	High
F	N	High

→

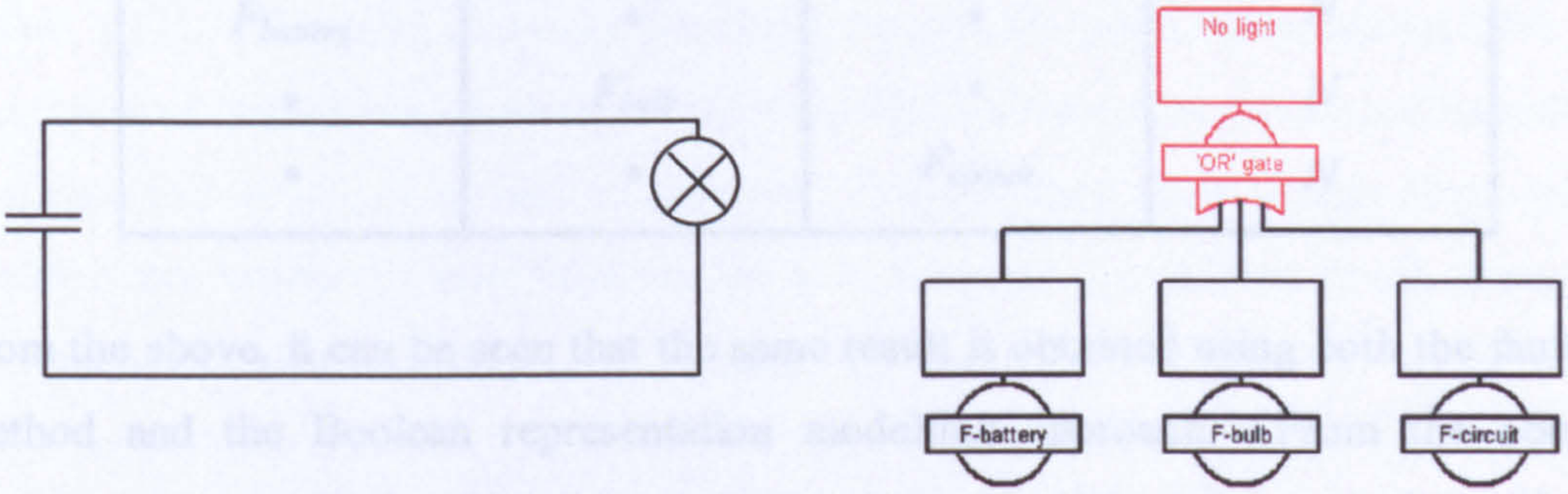
A	*B*	C_{output}
F	*	High

The input entries of a final system Boolean representation table should be primary variables. Therefore, intermediate variables should be eliminated by substitution with primary variables. During the elimination process, some intermediate variables may be used to replace other intermediate variables. Gradually, all intermediate variables are eliminated and a Boolean representation table in which all the entries are primary

variables is obtained. At this stage, the simplification of the Boolean representation table can be carried out. If the number of the entries of a Boolean representation table is large the simplification process may prove time-consuming. Therefore, it is suggested that the simplification rules be applied after each intermediate variable is eliminated.

3.3.7.2 Relationship Between Fault Tree and Boolean Representation Model

To demonstrate the relationship between fault tree modelling and Boolean representation modelling, a simplified example is used. Suppose that an electrical circuit system is composed of the three components: "*battery*", "*bulb*" and "*circuit*", as shown in Figure 3.2(a), for which the desired outcome is "*light*". Each of these components may be in either a *working* (*W*) or *failure* (*F*) state. The top event that indicates the failure of the electrical circuit system is "*no light*". Therefore, the fault tree leading to this top event is built as shown in Figure 3.2(b), where the basic events $F_{battery}$, F_{bulb} and $F_{circuit}$ stand for the failure state of the respective subscripted component. The "OR" gate in the fault tree indicates that if any of $F_{battery}$, F_{bulb} and $F_{circuit}$ happens, then the top event "*no light*" occurs.



(a) Circuit's line diagram

(b) Circuit's fault tree

Figure 3.2: Fault tree illustration of an electrical system

Also, let $W_{battery}$, W_{bulb} and $W_{circuit}$ stand for the working state of the respective subscripted component. By studying all the possible combinations of the both working and failure states of the three components, the preliminary Boolean representation table is built as shown in Table 3.8. Note that "*Y*" and "*N*" represent "*yes*" and "*no*" respectively for "*light*". After the rules for simplifications and deducing extra prime

implicants have been applied to Table 3.8, the final Boolean representation table is obtained as shown in Table 3.9. From Table 3.9, it can be seen that if any of $F_{battery}$, F_{bulb} and $F_{circuit}$ happens, top event "*no light*" occurs.

Table 3.8: A preliminary Boolean representation table of an electrical system

Battery	Bulb	Circuit	Light
$W_{battery}$	W_{bulb}	$W_{circuit}$	Y
$W_{battery}$	W_{bulb}	$F_{circuit}$	N
$W_{battery}$	F_{bulb}	$W_{circuit}$	N
$W_{battery}$	F_{bulb}	$F_{circuit}$	N
$F_{battery}$	W_{bulb}	$W_{circuit}$	N
$F_{battery}$	W_{bulb}	$F_{circuit}$	N
$F_{battery}$	F_{bulb}	$W_{circuit}$	N
$F_{battery}$	F_{bulb}	$F_{circuit}$	N

Table 3.9: A concluding Boolean representation table of an electrical system

Battery	Bulb	Circuit	Light
$W_{battery}$	W_{bulb}	$W_{circuit}$	Y
$F_{battery}$	*	*	N
*	F_{bulb}	*	N
*	*	$F_{circuit}$	N

From the above, it can be seen that the same result is obtained using both the fault tree method and the Boolean representation modelling approach. From the obtained Boolean representation table, it can also be seen that the working condition for the system is modelled. In general, the fault tree model is a special case of the Boolean representation model, and its analysis process only deals with failure events. Thus, when modelling events with multiple state variables, the Boolean representation approach is considered to be more appropriate. The Boolean representation approach may also be more appropriate to model systems with complicated interrelations between components. In terms of the ways the two approaches are applied, the major difference is that fault tree analysis is a deductive reasoning process while the Boolean representation approach uses the inductive logic, as described previously.

3.3.8 Event Tree Analysis

In many accident scenarios the initiating (accidental) event may have a wide spectrum of possible outcomes, ranging from no consequences to catastrophes. In most well designed systems, a number of safety functions, or barriers, are provided to stop, or mitigate the consequences of potential accidental events. The safety functions may comprise technical equipment, human interventions, emergency procedures, and combinations of these. Examples of safety functions are: fire and gas detection systems, emergency shutdown (ESD) systems, fire-fighting systems, firewalls and evacuation systems. The consequences of the accidental event are determined by how the accident progression is affected by subsequent failure or operation of these safety functions, by human errors made in responding to the accidental event, and by various factors like weather conditions, time of the day, etc.

The accident progression is best analysed by an inductive/bottom-up method. The most commonly used method is the so-called *event tree* analysis (ETA), which was originally developed when the risk analysis for the WASH-1400 nuclear power system was done (NRC, 1975). The safety team for the nuclear power system tried to make a FTA from the top even "accidental release of radioactivity" but the tree became tremendously complex and finally they had to give up. Instead they adapted the more general decision-tree formalism from business, so as to break up the problem in smaller pieces, and this method became the ETA (Leveson, 1995).

ETA is a logic tree diagram (Halebsky, 1989) that starts from a basic initiating event and provides a systematic coverage of the time sequence of event propagation to its potential outcomes or consequences (i.e., forward logic) step-by-step. In the development of the event tree, each of the possible sequences of events that result is followed from assuming failure or success of the safety functions (Henley, 1992; NRC 1991) affected as the accident propagates. Each event in the tree will be conditional on the occurrence of the previous events in the event chain. The outcomes of each event are most often assumed to be binary ('true' or 'false' – 'yes' or 'no'), but may also include multiple outcomes (for example, 'yes', 'partly' or 'no').

ETA has been used in the safety and reliability assessment of a wide range of technological systems. This analytical technique is a natural part of most risk analysis, but may also be used as a design-tool to demonstrate the effectiveness of protective systems in vessels. This technique is also used for human reliability assessment.

The ETA may be qualitative, quantitative, or both, depending on the objectives of the analysis and may be developed independently or follow on from fault tree analysis. It (ETA) is usually carried out in the following six steps:

1. Identification of a relevant initiating (accidental) event that may give rise to unwanted consequences.
2. Identification of the safety functions that are designed to deal with the initiating event.
3. Construction of the event tree.
4. Description of the resulting accident event sequences.
5. Calculation of probabilities/frequencies for the identified consequences.
6. Compilation and presentation of the results from the analysis.

Figure 3.3 shows an event tree for an initiating event "major overheat" in an engine room of a ship. If a failure occurs, then this overheat may propagate through the system and result in some possible consequences. From this event tree, it can be seen that when initiating event "*major overheat*" takes place, if there is *no fuel present to aid combustion*, then the consequences will be *negligible* in terms of fire risks. If there is *fuel present*, then it is required to look at if the "*detection fails*". If the answer is "*no*", the consequences are "*minor damage*", otherwise it is required to investigate if the "*sprinkler fails*". If the *sprinkler works*, then the consequences will be "*smoke*"; otherwise it is required to see if the *alarm system works*. If the alarm system works, then the consequences will be "*major damage*"; otherwise "*injuries/deaths*" may result.

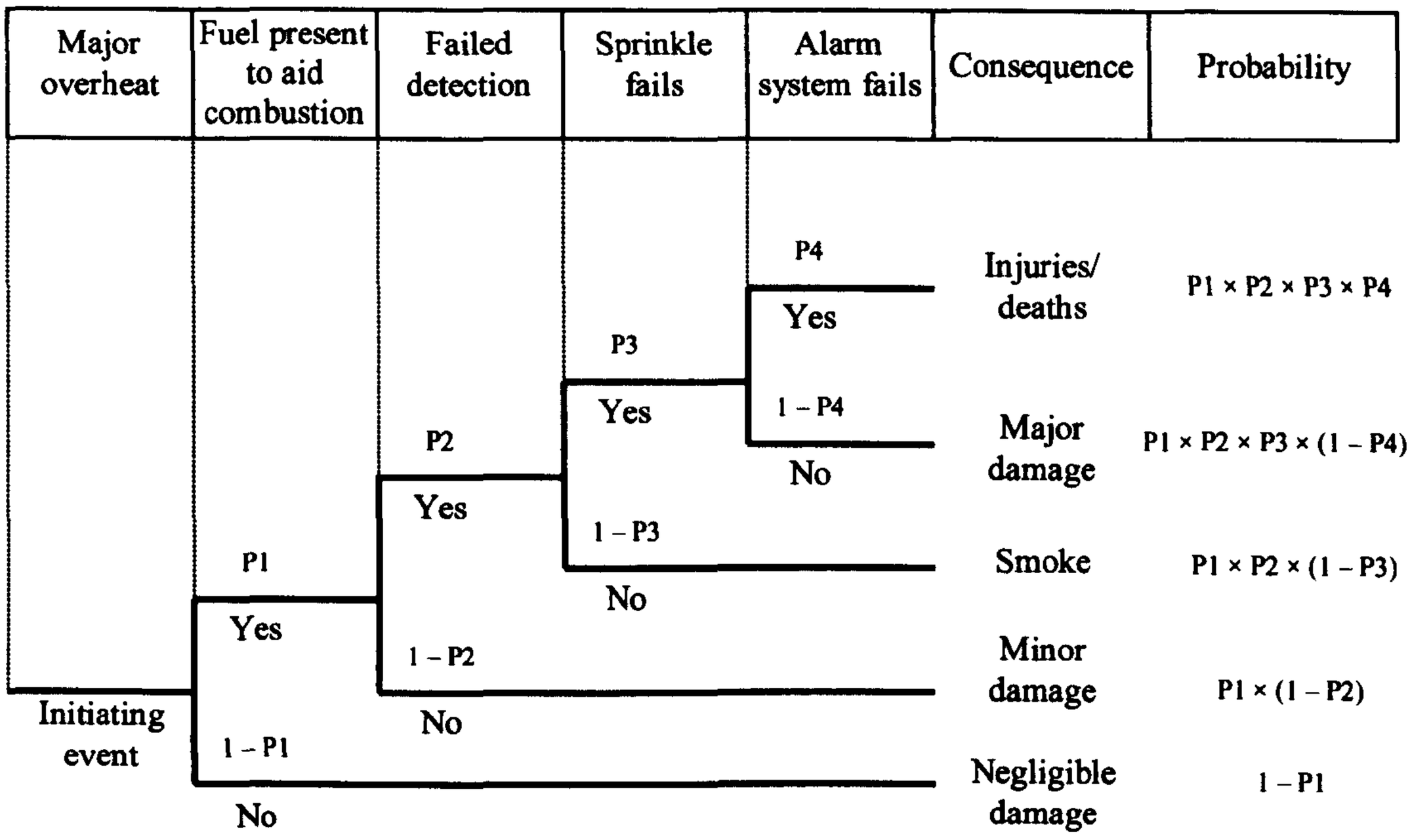


Figure 3.3: Example event tree for an initiating event in a ship's engine room

Quantitative analysis can be carried out on the event tree to assess the occurrence probability of each possible resulting consequence. As shown in Figure 3.3, P1, P2, P3 and P4 are the probabilities for the "*yes*" condition of "*fuel present to aid combustion*", "*failed detection*", "*sprinkle fails*" and "*alarm system fails*", respectively. 1 – P1, 1 – P2, 1 – P3 and 1 – P4 are their "*no*" condition probabilities. The ETA also gives the calculated probabilities of occurrence for all the consequences, i.e., "*injuries/deaths*", "*major damage*", "*smoke*", "*minor damage*" and "*negligible damage*", that results from the analysis. The sum of all probabilities of occurrence for all the resulting consequences is equal to 1.

Such an analysis can be integrated into the hazard identification and risk estimation phases of the safety and reliability assessment process.

3.3.9 Cause-Consequence Analysis

A technique that possesses the ability to identify the causes of an undesired event and from this event develop all possible system consequences is the Cause-Consequence

Diagram (CCD) method. This analytical diagram method, also termed Cause-Consequence Analysis (CCA), was developed in the 1970s at RISØ National Laboratories in Denmark (Nielsen, 1971) to specifically aid in the reliability and risk analysis of nuclear power plants in Scandinavian countries (Villemeur, 1992a). The method was created to assist in the cause-consequence accident analysis of the nuclear plants, which involved identification of the potential modes of failure of individual components and then relating these causes to the ultimate consequences for the system (Nielsen, & Runge, 1974). It has been perceived as being superior to the ETA (Villemeur, 1992a) and in addition to this, can account for time delays, which is not a feature available in the ETA method. Nielsen (1971) stated that as well as being a tool for illustrating the consequences of particular failures, the method could also serve as a basis from which the probability of occurrence of the individual consequences could be evaluated. The consequences evaluated include those that illustrate the system functioning as intended and those that illustrate an undesirable failure sequence.
The technique has been used as the main analysis tool for conducting safety assessment (Nielsen, 1975; Nielsen, *et al.*, 1975; Nielsen, *et al.*, 1977; Taylor, 1977) and for assessing the reliability of sequential systems (Andrews, & Ridley, 2001).

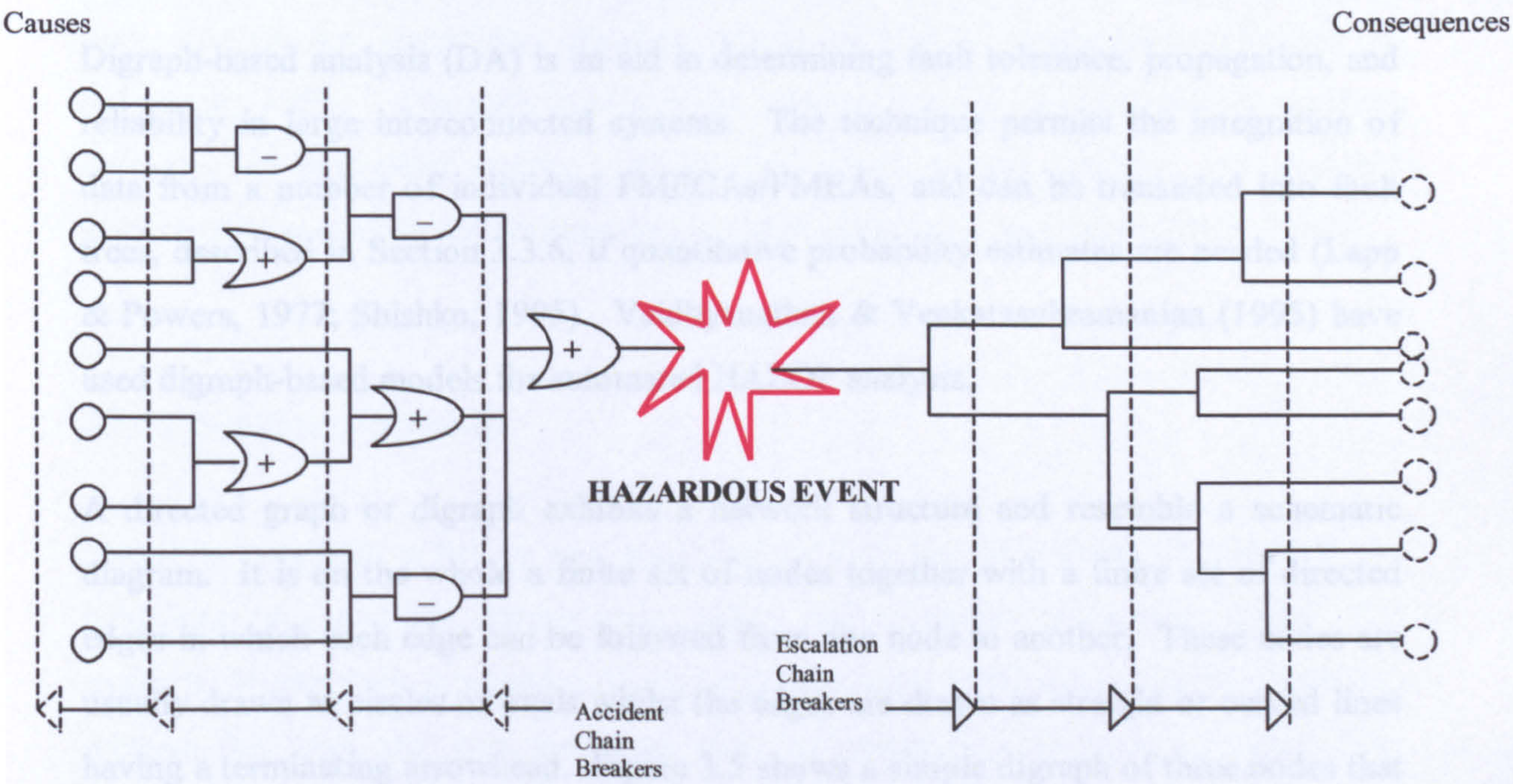


Figure 3.4: Cause-consequence diagram of a hazardous event

CCA is a marriage of fault tree analysis (to show causes) and event tree analysis (to show consequences) (Henley & Kumamoto, 1981). CCA is a diagrammatic approach as shown in Figure 3.4. Construction of cause-consequence diagrams starts with a choice of a critical event. The "consequence tracing" part of a CCA involves taking the initial event and following the resulting chains of events through the system. The "cause identification" part of a CCA involves drawing the fault tree and identifying the minimal cut sets leading to the identified critical event. CCA is extremely flexible as it can work forward using event trees and backward using fault trees.

Although CCA incorporates features from FTA and ETA, it is not commonly used since the CCD for a fairly simple process is detailed and somewhat cumbersome. It is mostly used when the logic model for the concerned event is simple enough for a graphical display. The detailed description and applications of this approach are the same as discussed in FTA and ETA.

3.3.10 Digraph-Based Analysis

Digraph-based analysis (DA) is an aid in determining fault tolerance, propagation, and reliability in large interconnected systems. The technique permits the integration of data from a number of individual FMECAs/FMEAs, and can be translated into fault trees, described in Section 3.3.6, if quantitative probability estimates are needed (Lapp & Powers, 1977; Shishko, 1995). Vaidhyanathan & Venkatasubramanian (1995) have used digraph-based models for automated HAZOP analysis.

A directed graph or digraph exhibits a network structure and resemble a schematic diagram. It is on the whole a finite set of nodes together with a finite set of directed edges in which each edge can be followed from one node to another. These nodes are usually drawn as circles or ovals whilst the edges are drawn as straight or curved lines having a terminating arrowhead. Figure 3.5 shows a simple digraph of three nodes that are represented by *A*, *B* and *C*. An edge begins from an influencing node and terminates at an influenced node. Also, $A \rightarrow B$ signifies that "*A* influences *B*".

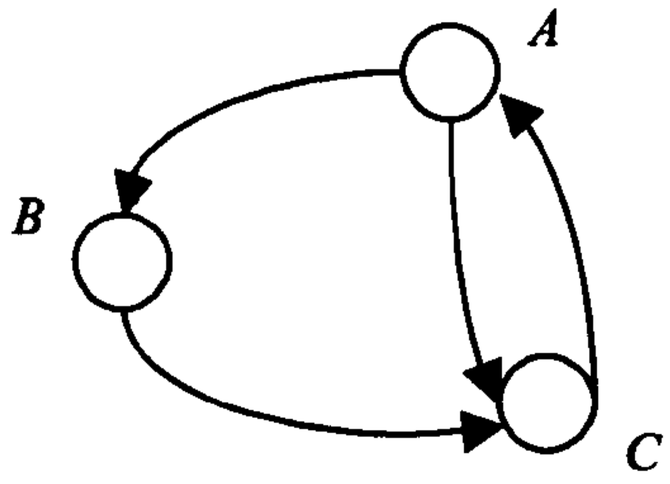


Figure 3.5: A simple digraph

In a DA, the nodes correspond to the state variables, alarm conditions or failure origins, and the edges represent the causal influences between the nodes. Digraph representation provides explicit causal relationships among variables of systems with feedback loops. From the constructed digraph, the causes of a state change and the manner of the associated propagation can be easily found (Umeda, *et al.*, 1980). The rules generated from such an analysis can be used as knowledge of an expert system for plant operations.

DA is a bottom-up event-based qualitative technique. DA may be integrated into the hazard identification phase of the safety and reliability assessment process and may be very efficient for identifying possible causes of process disturbances (Kramer & Palowitch, 1987). Digraphs can also be used to model and reconstruct accident scenarios of hazardous events. As a result, both hazard analysis and accident investigation processes can be improved via modelling event sequences (FAA, 2005).

3.3.11 Simulation Analysis

Simulation analysis refers to any analytical method that is capable of imitating the behaviour of a real-life system under safety and reliability assessment study. For example, Monte Carlo simulation (Cortazar & Schwartz, 1998) is an eminent simulation method that uses the idea 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 observations 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 solution/outcome to the problem. Together, these scenarios give a range of possible solutions/outcomes, some of which are more probable and some less probable. Unfortunately, this also means that it is computer intensive and best avoided if simpler solutions are possible. Therefore, the most appropriate situation to use Monte Carlo methods is when no other solutions exist or they are difficult to use.

Monte Carlo analysis methods are used in the oilfield to estimate the risks involved in new exploration projects, evaluation of development schemes and evaluation of validity of reservoir models (Cortazar & Schwartz, 1998; Armstrong, *et al.*, 2005).

3.3.12 Subjective Reasoning Analysis

Whenever data are sparse for safety and reliability assessment, it may become very difficult for the risk analyst to precisely obtain the parameters of basic failure events to carry out quantitative analysis using the probabilistic analytical methods outlined above since a great deal of uncertainty is involved. Therefore, the need for models that reflect subjective reasoning or understanding will dominate choices in parameterisation.

Subjective reasoning analysis (SRA) may prove relatively easier to deal with such problems with uncertainty. An example of SRA is where subjective descriptors such as cold, cool, warm or hot is used by the safety analyst to present the value state at which the temperature of a room is at. Clearly, it is not accurate to define a transition from a quantity such as 'warm' to 'hot' by the application of one degree centigrade of heat. In the real world a smooth (unnoticeable) drift from warm to hot would occur. This natural phenomenon can be described more accurately by fuzzy set theory (See Chapter 7 for more details).

It can be combined with FMECA to form mixed approaches for modelling the safety and reliability assessment of a system more efficiently and conveniently. This method can be used in the hazard identification and risk estimation phases of the safety process.

3.4 Selection of Safety and Reliability Methods

Each phase in the safety and reliability assessment process involves the use of the analytical methods outlined previously. Best practice dictates the use of a combination of the different methods, since each provides different information about the system under consideration. It is realised that use of these safety and reliability assessment methods in an integrated manner may make risk assessment comparatively efficient and convenient since safety information and the advantages of each method may be more efficiently explored by doing so (Wang, *et al.*, 1993). In such integration, one method may be used to process the information produced using another method.

To make full use of the risk assessment methods, an analysis of their input requirements and outcomes is required. The possible inter-relationships of the various methods are identified as shown in Figure 3.6. This network of data flows (as collected from Chapter 2) and these analytical methods constitute a general framework within which the safety of a system may be assessed as the design evolves. The outlined analytical methods, classified as either top-down or bottom-up event-based as described previously, may be applied to study the system states, operational conditions, environmental conditions and other design considerations which contribute to the occurrence likelihood of the hazardous conditions associated with a ship or an offshore installation and define the magnitude of possible resulting consequences.

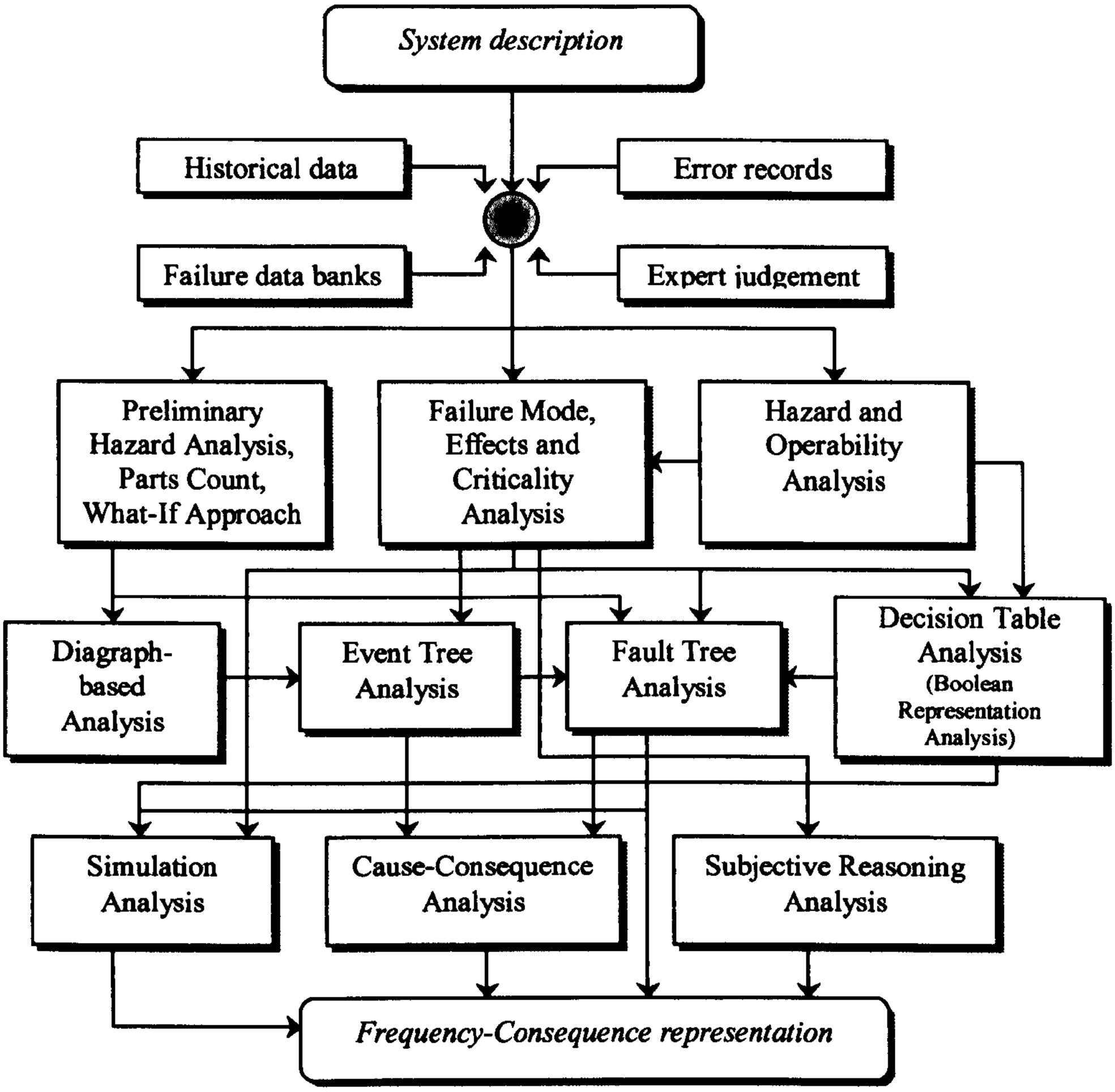


Figure 3.6: Information flow diagram of risk assessment methods

The selection of the outlined methods, or the decision as to which methods are more appropriate for the risk assessment of a particular product, is dependent on the following considerations:

- The level (system, subsystem or component level) of the product breakdown at which the hazard identification is carried out.
- The degree of complexity of the inter-relationships of the items at the investigated level of the product breakdown.
- The degree of innovation associated with the product design (the availability of product failure data for risk assessment).

The applicability of each risk assessment method has been discussed with reference to the phases of the safety and reliability assessment process. When there is a lack of knowledge or experience regarding the design solution and its possible effects on product safety, inductive bottom-up methods, although more time-consuming, should yield a higher level of confidence that hazardous system states and respective failure modes are identified, otherwise top-down methods may prove more convenient and efficient. If, however, it is difficult to describe the basic failure events of a system using probabilistic risk analysis methods, subjective reasoning analysis may be more appropriate to assess the safety of the system.

3.5 Critical Review on Human Reliability Analysis Techniques

As early as the 1960s, the importance of human reliability was realised by Rook (1962) who defined as the probability that an agent accomplish successfully his mission under fixed time and fixed conditions. Attempts followed to classify human error in industrial settings (Swain, 1963; Farmer, 1967). Then during the 1970s and early 1980s, there was an increasing awareness of the importance of human-error as a factor in incidents and accidents involving complex technologies. This offered significant advances to be made in the knowledge of human behaviour so as to quantify the propensity of humans to make errors under the conditions of interest. An early model to explain error mechanisms was developed by Rasmussen (1983) whilst analysing the errors made by seasoned operators on the basis of an extensive review of incident and accident reports from hazardous industries. Rasmussen's framework proposed three types of error: skill-based, rule-based, and knowledge-based. This framework was built on by Reason (1990), who defined the basic error types as being *slips*, *lapses* and *mistakes*. Since this time, various approaches have been taken to this area in the past and detailed accounts of the history of HRA are given in Villemeur (1992b) and Reason (1990). Recently, Kletz (2001) went on to included *violations* and *mismatches* to the types of human error.

In parallel with attempts to model the causes and mechanisms of human error, risk analysts sought to develop methods and techniques (Caccuabue, 1997) to quantify the reliability of a human operator as a system component, in order for human-error to be accounted for in an overall assessment of the risk associated with a system. Such

techniques included: Technique for Human Error Rate Prediction (THERP) (Swain, & Guttmann, 1983), Human Cognitive Reliability (HCR) (Hannaman, *et al.*, 1984), Operator Action Trees (OATS) (Hall, *et al.*, 1982), Success Likelihood Index Methodology (SLIM) (Embrey, *et al.*, 1984) and Human Error Assessment and Reduction Technique (HEART) (Williams, 1988). Reason (1990) provides an overview, and critique of these techniques. Their differences are noticed when considering their goals (identify, quantify or reduce errors (see Kirwan, 1992)), their features and the consequences of their applications (Gerdes, 1995).

In the first place, the techniques approximate to hazard identification methods in that they provide ways of analysing operators' tasks and working environments and identifying likely causes of error. In the second place, they approximate to hazard analysis methods by attempting to attach probabilities to the identified hazards. This quantitative approach was not unnatural given that, at the time the techniques were developed, industrial risk analyses were mostly probabilistic and HRA techniques were intended to achieve similar aims of identifying and analysing risks. Although the hazard identification processes were qualitative and based largely on human judgement, the techniques were not seen as complete if they did not provide ways of attributing probabilities to error occurrences. Besides this quantitative analysis formation on a qualitative and judgmental foundation, such first-generation HRA techniques are weak because they do not embrace the most recent knowledge of human behaviour. The human factors experts have for a long time acknowledged this and called for the development of a new generation of techniques. Williams (1985) stated that these methods were neither accurate nor easily usable by non-specialists, while at the same time its developers have yet to demonstrate, in any comprehensive fashion, that their methods possess much conceptual, let alone, empirical validity. Swain (1988) declared that all HRA models had serious limitations, are often ill-founded relative to human behaviour and the task of calibrating the models had not been seriously addressed. Dougherty (1990) agreed and in asserting that inadequate HRA modelling can lead to increased risk, called for second-generation methods to be developed and for advances in error psychology and cognitive science to be accommodated within the HRA framework. Later, Hollnagel (1996) complained of the obsolescence of the state of the HRA art and Dearden & Harrison (1996) expressed the fact that all these approaches suffer from their inability to adequately take into account aspects of the human-machine

interface that might affect the probability of human-error. However, reliable second-generation methods have not yet replaced the first-generation methods. The second-generation methods includes, Quantification of Errors of Intention (INTENT) (Gertman, *et al.*, 1992), Cognitive Event Tree System (COGENT) (Gertman, 1993), Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel, 1998) and Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) method (Gertman, *et al.*, 2004).

In spite of the serious flaws of current HRA methods within their scope of applicability, the HRAs have been highly successful in terms of identifying significant deficiencies related to human performance. Thus, genuine success for analysing manual and repetitive tasks due to numerous modifications such as new procedures, revision of procedures or technical specifications, revised training, installation of additional hardware and operator support systems or automated capabilities, and modifications of systems (including actuation logic) have resulted from the HRA modelling. These findings are in most cases considered as robust in spite of the normally large numerical uncertainties. Fortunately, some of these techniques are still being updated, combined and evaluated as to their relative effectiveness as a perspective means of improving safety culture. It is envisaged that their qualitative effects and incorporation into quantified form, based on the consideration of uncertainty, can be enabled via the development of a fuzzy-Bayesian network (FBN) modelling. A literature review is provided for the FBN in Section 3.6.3.

3.6 Literature Review on Uncertainty Treatment Techniques

The previous sections in this chapter have outlined several risk analysis methods that are widely applied in maritime risk analysis. Nevertheless, in some situations where there is a lack of data, it may be difficult to apply them with confidence to the assessment task. Over the recent years, some techniques such as Bayesian network (BN), fuzzy logic (FL) and fuzzy-Bayesian network (FBN) have attracted much attention in safety assessment and in situations where traditional risk analytical tools cannot be applied with confidence due to the high level of uncertainty in data. This research work will investigate such techniques. Detail descriptions and case study

application of these developed techniques to marine and offshore systems will be given in more detail in Chapters 6, 7 and 8.

In this section, a brief review of the BN, FL and FBN is given herein to highlight the research progress in the development of such techniques.

3.6.1 A Review on Bayesian Network

Until twenty years ago, the issue of ordering possible beliefs, both for belief revision and for action selection, was seen as increasingly important and problematic, and at the same time, dramatic new developments in computational probability and decision theory directly addressed perceived shortcomings. The key development (Pearl, 1988) was the discovery that a relationship could be established between a well-defined notion of conditional independence in probability theory and the absence of arcs in a directed acyclic graph (DAG). This relationship made it possible to express much of the structural information in a domain independently of the detailed numeric information, in a way that both simplifies knowledge acquisition and reduces the computational complexity of reasoning. The resulting graphic models have come to be known as *BNs*.

BNs are at the cutting edge of expert systems research and development. Unlike the traditional rule-based approach to expert systems, they are able to replicate the essential features of plausible reasoning (reasoning under conditions of uncertainty) and combine the advantages of an intuitive visual representation with a consistent, efficient and mathematical basis in Bayesian probability. Critically they are capable of retracting belief in a particular case when the basis of that belief is explained away by new evidence. Because of the development of propagation algorithms (Pearl, 1988; Russell & Norvig, 2003), followed by availability of easy to use commercial software and growing number of creative applications, BN has caught the sudden interest of research in different research fields since early 90's. Perhaps the greatest testament to the usefulness of Bayesian problem-solving techniques is the wealth of practical applications that have been developed in recent years. After about ten years' research, BNs have succeeded in creating models for practical applications in areas of intelligent decision, safety assessment, information filtering, autonomous vehicle navigation,

weapons scheduling, medical diagnosis, pattern recognition, and computer network diagnosis. For a nice collection of papers on applications of Bayesian techniques, see the March 1995 special issue of the Communications of the ACM (Heckerman, *et al.*, 1995). Since most real life problems involve inherently uncertain relationships, BN is a technology with huge potential for application across many domains.

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 in *Hugin* is described in Jensen, *et al.* (1994). The *Hugin* software (Jensen, 1993) 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.

3.6.2 A Review on Fuzzy Logic

Forty years ago, it was conceived that items in the real world are better described by having partial membership in complementary sets rather than by having complete membership in exclusive sets and this notion that gave rise to the theory of fuzzy set (Zadeh, 1965). This theory was then applied to traditional logic to develop the concept of FL (Zadeh, 1975), a modelling technique which employs human analysis to provide an approximate and yet effective means to describe the behaviour of situations that are too complex or too ill-defined to allow precise mathematical analysis. Every since, the technique has been further developed to include methodologies such as modelling, evaluation, optimization, decision-making, control, diagnosis and information (Terano, *et al.*, 1992).

Zadeh (1973) presented fuzzy algorithms for complex systems and decision processes. Whilst using this algorithm in an attempt to control a steam engine and boiler combination by synthesizing a set of linguistic control rules obtained from experienced

human operators, Mamdani (1975) proposed a fuzzy inference system (FIS) in which the rule consequence is defined by fuzzy sets. Takagi, Sugeno and Kang (Sugeno, 1985) later went on to propose an inference scheme in which the conclusion of a fuzzy rule is constituted by a weighted linear combination of the crisp inputs rather than a fuzzy set. For this reason, Takagi-Sugeno FIS may only need a smaller number of rules since their output is already a linear function of the inputs rather than a constant fuzzy set. However, the Mamdani-type scheme has emerged as the most commonly used FIS owing to the fact that FL systems do not necessarily require mathematical equations to establish a relationship between input and output parameters. Such a relationship can be set via simple IF-THEN rules that are defined by a knowledge basis. Kosko (1992) uses another approach to generate fuzzy IF-THEN rules and shows that the fuzzy sets can be viewed as points in a multidimensional unit hypercube. This makes it possible to represent a set of inference rules by the guise of a fuzzy associative memory (FAM) in an inference matrix or table. This FAM matrix can thus give the risk matrix for a risk assessment task.

FL modelling can be particularly useful where there is no analytical model of the relation under consideration and/or where there are insufficient data for statistical analysis (Salski, et al., 1996), as it provides a logical means for linguistic computation. As such, the logic can be applied to problems in the domains of engineering, business, medical and related health sciences, and the natural sciences. Whilst it cannot substitute for deterministic modelling techniques, FL does complement the set of such techniques and can be coupled to them, thus enabling a better and more extensive risk assessment in cases of vague and incomplete project information.

After an aggregation process of the Mamdani FIS rule consequences, there is a fuzzy set for each output variable that needs defuzzification. If the defuzzification is carried out, this transforms the fuzzy reality into a crisp one. The emerging crisp reality carries less information than the underlying fuzzy reality and moreover, there is an irreversible loss of information that may be vital or significant in the assessment task for a safety-critical application. With Dempster-Shafer evidence theory (Shafer, 1976) holding a connecting relationship to fuzzy set theory, an evidential reasoning (ER) approach (Yang & Xu, 2002) may best utilise the aggregated fuzzy output set to establish the most useful and practical results of a risk analysis. Besides, the ER approach shows

great potentials in handling multiple attribute/criteria decision analysis (Yang & Singh, 1994; Yang & Xu, 2002) and also in hierarchical evaluation problems (Yang & Sen, 1993) under uncertainty. In following this setting therefore, FL modelling can thus permit the risk-based modelling of safety-critical marine and offshore application domains.

3.6.3 A Review on Fuzzy-Bayesian Network

The combination words "fuzzy-Bayesian" have seen increasing usage owing to developments achieved whilst tackling both vague and random uncertainties within a modelling domain. Clark & Kandel (1990) recognised that a FBN may provide a more holistic, graphical approach that lends itself well to implementation in expert systems on personal and small computers. With Pan & McMichael (1998) putting up thoughts on a causal model that could possibly provide a high-level generic architecture for fusing data incoming from multiple sensors, an ideal integration of Bayesian probability theory (Bayes, 1763) and FL lead to fuzzy causal probabilistic networks (another term in the ideology behind FBNs). This was followed through by Pan & Liu (1999) study on hybrid BNs (the most general form of BNs demanded by practical applications), in which continuous variables and discrete ones may appear anywhere in a DAG. In such BNs, discretization of continuous distributions can allow approximate inference in the network without limitations on relationships among continuous and discrete variables. As explained by Pan & Liu (2000), although all the variables are defined to be discrete, the subset of some variables, such as temperature or pressure, for example, can be genuinely continuous. On the other hand, it considers FL as an approximate reasoning formalism that may be easy to use and possibly sufficient in many ordinary applications. Thus, the proposition presented that FBNs may quite possibly realise anything FL can do and as well, may inherit the entire rigor, flexibility and other superior properties of probabilistic approaches (Pan & Liu, 2000). Furthermore, there is the tendency to combine BN and FL modelling techniques so that one will complement the shortfall of the other.

Viertl (1987) explains the necessity of developing a fuzzy Bayesian inference and this paved way for the first works on this inference, which come from safety project studies

in structural reliability researches (Chou & Yuan, 1993; Frühwirth-Schnatter, 1993; Itoh, & Itagaki, 1989). The research results based on two examples, a reinforced concrete beam and a structural frame, showed that the fuzzy-Bayesian approach is a viable enhancement to the safety assessment of existing structures (Chou & Yuan, 1993). Nonetheless, that inference suffered from numeric stability problems in trying to achieve a justified fuzzy-probability transformation and further overlooked the conditional cases that can arise between fuzzy/possibility distribution events. The developed theory of mass assignment (MA) by Baldwin, *et al.* (1996) provide a bi-directional transformation platform between Bayesian probability theory and possibility/fuzzy set theory, and Dubois & Prade (1997) introduce a Bayesian conditioning operation in possibility theory, adapted to the idea of focusing on a body of knowledge for a reference class described by some evidences.

The work carried out so far on FBN cannot suitably be applied in the maritime domain, since the renowned leap in possibility-probability distribution inference process, as brought about by the theory of MA, is worthy of appropriate modifications to previous methodologies. With such modifications in place, the innovative FBN can now rightly be based on a more realistic inference process and may as well offer a stable practical solution for those domains containing continuous and discrete variables and also those of random and vague uncertainties.

3.7 Concluding Remarks

As followed from the collection of reliable failure and repair data for which a number of useful database sources are ascertained, typical risk analytical methods need to be applied in order to conduct safety and reliability assessments. Such an assessment can then be carried out qualitatively or quantitatively depending on how much data is or has made been obtainable/available, in addition to the competence of expert judgement that can be provided to the safety analyst.

Some of the analytical methods, such as PHA, what-if, part count, FMECA and HAZOP are most usefully applied from hazard identification phase, whilst others like FTA, decision table, ETA, CCA and DA are used mainly in performing risk estimation. Best

practice dictates the use of a combination of different methods, since each method provides different information about the system under consideration. These safety and reliability techniques can also be used in an integrative manner to produce a more efficient and convenient safety assessment, and therefore, they have gained substantial acceptance for use in formal maritime safety practice, as can be noticed in Chapter 4.

Human-error also can be accounted for in an overall assessment of the risk associated with a safety-critical maritime system via HRA techniques. First-generation HRA techniques such as THERP, HCR, OATS, SLIM and HEART have been developed to quantify the reliability of a human operator, although the hazard identification processes were qualitative and based largely on human judgement. Their use leads to an increased understanding of the human sources of risk that transpired into genuine success for analysing manual and repetitive tasks. It is realised that they do not embrace the most recent knowledge of human behaviour and therefore, there has been a growing demand for the development of new generation methods. Reliable second-generation methods have included INTENT, COGENT, CREAM and SPAR-H, but these have not yet replaced the first-generation methods. Nevertheless, both qualitative and quantitative effects of human influences need to be incorporated into the risk analytical domain model.

The developed techniques of BN, FL and FBN are used in situations where these traditional risk analytical tools cannot be applied with confidence due to the high level of uncertainty in data. The FBN may also provide the platform for which the human element of the safety assessment can be incorporated into risk-based models. More details on these developed techniques can be found in Chapters 6, 7 and 8. It is envisaged that the use of uncertainty analysis in conjunction with risk assessment would provide enhanced information for decision makers.

Chapter 4: Formal Safety Assessment (FSA)

Chapter Summary

Formal safety assessment (FSA) as a method supporting the decision-making for maritime legislation offers a more rational approach than the traditional "regulation by disaster" method. Its adoption for shipping represents a fundamental cultural change, from a largely reactive and piecemeal approach, to one that is integrated, proactive, and soundly based upon the evaluation of risk. The incentives that FSA can offer have prompted its trial application to high speed passenger catamaran ferries and bulk carrier ships for which this chapter briefly reviews the outcome of their risk analysis. In spite of highlights reached in these FSA trial developments so far, there are still many important hurdles to cross. The chapter further discusses these problems and delineates the road that lies ahead in advancing and properly setting FSA in place.

4.1 Introduction

In general, improvements in safety have been driven by accidents, that is, the traditional "regulation by disaster" approach to safety. It is as though there is the need for the shock of a catastrophe to force some corrective action to be taken, and even then the results achieved are often proportionate to the political, media and public outrage and pressures generated. By introducing a more structured risk analysis process through a formal safety assessment procedure, regulators are compelled to examine potential hazards and to introduce appropriate measures or standards before a tragedy occurs.

Formal safety assessment (FSA) is a process of identifying hazards, assessing the associated risks, studying alternative ways of managing those risks, carrying out cost-benefit assessment of alternative management options, and finally making decisions on which option to select (MSA, 1996). The concept of FSA provides an elegant route to

application of well-established risk analysis methods (see Chapter 3), already widely used in other industries within shipping activities, whereas the proposition of moving rapidly towards a safety case regime would be extremely difficult, putting unrealistic demands on both the regulator and the regulated.

In addition to a direct involvement in the FSA Methodology (Section 4.4), the application of safety assessment techniques has for many years been actively considered, hence promoting the use of such methods in the marine industries (Aldwinckle & Pomeroy, 1983; Pomeroy, 1985). In parallel the experience gained in the preparation of safety cases for offshore installations has provided experience of the application of the key techniques of analysis (Stansfeld, 1994).

It is important to recognise that any approach suitable for assisting IMO in setting the international framework of rules for shipping must be equally valid when looking at the Rules for classification. Changes to the Rules for classification are proposed for many reasons, including changes in technology and as a consequence of service experience, the proposed changes could be tested by using a generic ship type risk model. It is possible to set up a number of generic models for this purpose and to assess the benefit of the changes. This approach would give greater transparency and objectivity to the rule making process of the classification societies.

4.2 Adoption of Formal Safety Assessment

In 1992, Lord Carver's report into marine safety raised the issue of a more scientific approach to ships and recommended that emphasis be given to a performance-based regulatory approach. This introduced the concept of formal ship safety assessment. In general, over the last several years the application of formal ship safety assessment has reached an advanced stage as a result of several serious marine accidents (IMarE, 1997) such as those mentioned tragedies in Chapter 1, Section 1.2.1. The established statutory safety regulations that govern ship safety have been in use for many years and these are prescriptive in nature. However, they do not reflect the requirements of individual ships and a "goal setting" approach involving FSA was thought to be of vital importance.

The UK government reasoned that adoption of FSA would enable safety issues at IMO to be prioritised, and regulations derived that are cost effective and proportional to risk. Thus, in 1993, the UK proposed to the IMO that FSA should be applied to ships to ensure a strategic oversight of safety and pollution prevention. The UK Maritime Safety Agency (now the Maritime and Coastguard Agency, MCA) developed the concept of the FSA, recognising that the uniformity and minimum standards of the existing prescriptive requirement must be maintained.

The principle that FSA should be adopted as a systematic and rational process for assessing risks associated with any sphere of activity, and for evaluating the benefits of mitigation options has been accepted by IMO and the interim guidelines were approved in 1997 (IMO, 1997a). These interim guidelines had since been replaced by an IMO approved formal guideline in 2002 (IMO, 2002b).

4.3 Problem Definition to the Vessel Type

Prior to undertaking an FSA the problem under analysis and its boundaries should be carefully defined. The definition should be consistent with operational experience and current requirements taking into account all relevant aspects (IMO, 1997a). In order to achieve this, written submissions discussing aspects of the problem definition are sought from a number of technical experts. These are presented to a working meeting comprising a wider range of expertise in shipping, its operations, and also in human factors so as to gain a consensus view.

4.3.1 Preparation for the Study

Those aspects that may be considered relevant when addressing ships are:

- Ship category (e.g. type, length or gross tonnage range, new or existing, type of cargo).
- Ship systems or functions (e.g. layout, subdivision, type of propulsion).
- Ship operation (e.g. operations in port and/or during navigation);

- External influences on the ship (e.g. vessel traffic system, weather forecasts, reporting, routing).
- Accident category (e.g. collision, explosion, fire).
- Risks associated with consequences such as injuries and/or fatalities to passengers and crew, environmental impact, damage to the ship or port facilities, or commercial impact.

4.3.2 The Generic Ship Type

In order to set the context for application of FSA to specific ship types, it is useful to define a "generic ship type risk model". This means those features, characteristics and attributes which are common to all ships, or relevant to the problem under consideration. The generic model can thus be a collection of systems, including organisational, management, operational, human, electronic and hardware, which fulfil the defined function, and not as an individual ship in isolation. Identified generic ship functions are as shown in Figure 4.1 (IMO, 1998).

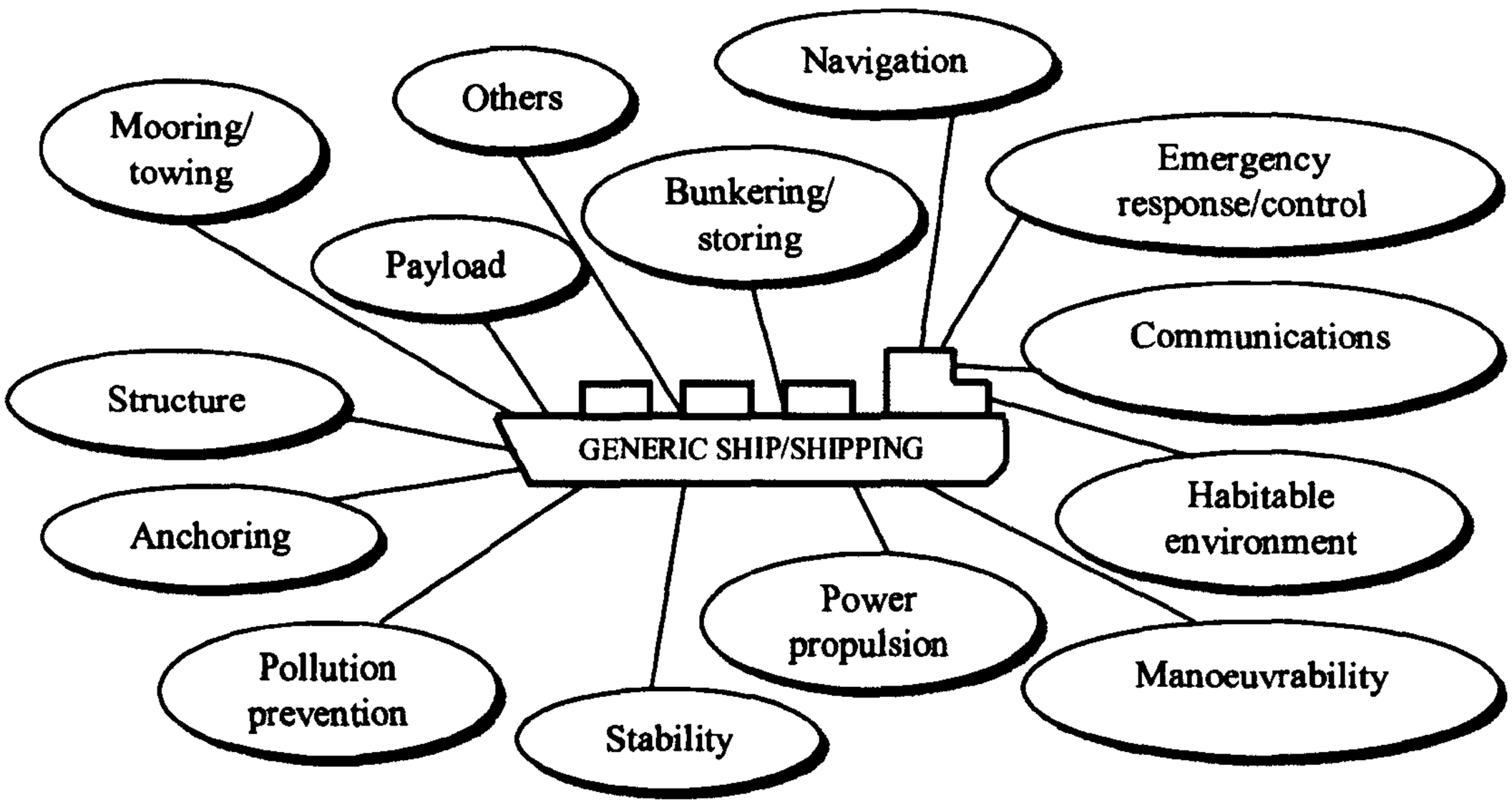


Figure 4.1: Generic ship functions

The life cycle of the generic ship comprises:

- Design, construction and commissioning.

- Entering port, berthing, unberthing and leaving port.
- Loading and unloading.
- Passage.
- Dry dock and maintenance period.
- Decommissioning and disposal.

Generic ship definitions are also used to assist in identification of hazards, underlying causes, risk assessments and risk control options.

4.4 The Formal Safety Assessment Methodology

FSA is a risk-based tool for the management of safety. The word "risk" is used here to encompass consideration of both the likelihood and the consequences of an unwanted event.

The FSA process consists of *five individual steps* as shown in Figure 4.2 (Riding, 1997; IMO, 1997a; 1997b; 2002b). These are:

Step 1: Identification of hazards (a list of all relevant accident scenarios with potential causes and outcomes).

Step 2: Assessment of the risks associated with those hazards (evaluation of risk factors).

Step 3: Consideration of alternative ways of managing the risks (deriving regulatory measures to control and reduce the identified risks).

Step 4: Cost-benefit assessment of alternative risk-management options (determining cost effectiveness of each risk control option).

Step 5: Recommendations for decision-making (information about the hazards, their associated risks and the cost effectiveness of alternative risk control options is provided).

In this context, it is recognised that nowhere in the 5 steps defined above is there a point at which a judgement of acceptability is made. Some people have reasoned that, as part

of the FSA process, a target level of risk ought first to be established, and that before starting on *Step 3* a judgement be made on whether any risk reduction measures are needed at all. There is clearly logic in this approach, particularly at a detailed level. However, in the first instance it is more important to be able to identify all hazards, and to rank them relative to each other, so that attention can first be given to the more significant contributors to total risk.

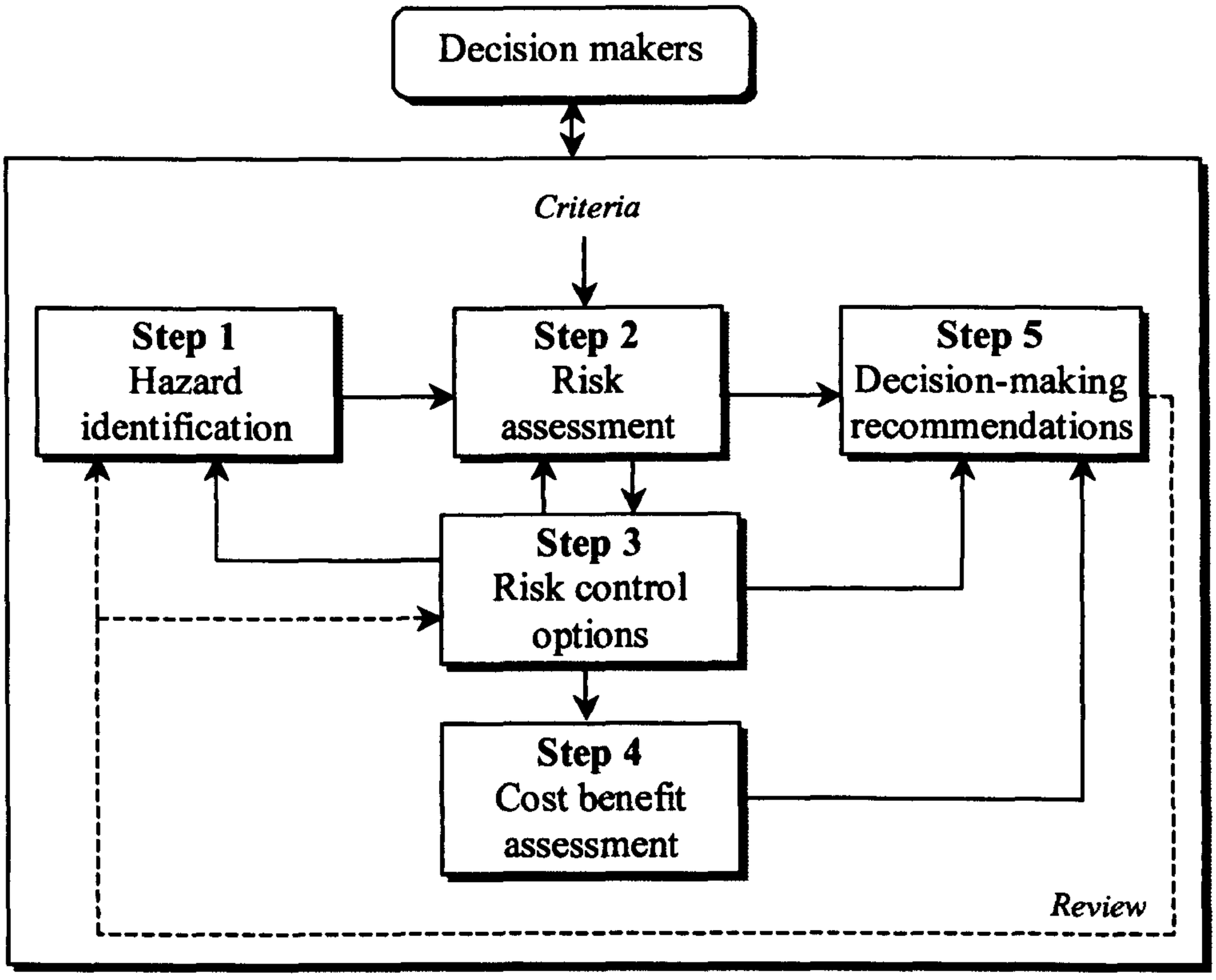


Figure 4.2: Flow chart of the FSA process

It should also be pointed out that even with inclusion of risk targets and acceptability judgements, the overall safety management process is not complete. To manage risk effectively, there needs to be a loop established, whereby the effects of changes based upon the decision making of *Step 5* are monitored to ascertain whether the desired level of safety is being achieved, and if not, further options are examined. However, the core process comprises the five steps set out above. It is these objective and rational analyses that facilitate systematic judgement, and effective management, of risk (Peachey, 1995).

4.4.1 FSA Step 1 - Identification of Hazards

Hazards may or may not have already been realised as accidents. With the passage of time, changing technology, and the influence of human factors, new hazards will arise, and existing hazards may materialise into accidental events not previously experienced. Identification of hazards is therefore a vital first step in the FSA process. Its objective is to describe the activity, and identify the hazards that might impair the functions of the generic ship type (or subject undergoing FSA analysis). This is achievable by the use of standard techniques, such as *brainstorming*, to identify hazards that can contribute to accidents, and by screening these hazards using a combination of available data and expert judgement in preparation for *Step 2*.

Various techniques exist for hazard identification. The most common of these in the shipping industry are:

- *Failure modes, effects and criticality analysis (FMECA)*, described in Section 3.3.4 of Chapter 3, which is particularly suitable for hardware systems such as machinery controls.
- *HAZard and OPerability studies (HAZOP)*, described in Section 3.3.5 of Chapter 3, which is particularly appropriate for identifying hazards in "soft" systems involving activities and operations.
- *Compartment studies* in which the effect of an event such as fire or flooding on every system or piece of equipment within a compartment, is systematically examined.

Details of other typical hazard identification techniques can be found in Chapter 3.

4.4.1.1 Hazard Screening

The purpose of the *hazard screening* during step 1 is to provide a quick and simple way of ranking hazards. It is a process for establishing, in broad terms, the risk of all identified accident categories and accident subcategories, prior to the more detailed quantification that will be used in *Step 2*.

Lists of accident categories that have been determined by the Marine Accident Investigation Branch (MAIB) as a guide for safety analysis of the generic ship are (Brennan & Peachey, 1996; Loughran, *et al.*, 2002; and see also Chapter 2, Section 2.3.1):

- Collision (striking between ships).
- Contact (striking between ship and other objects).
- External hazards (natural).
- External hazards (others).
- Grounding/stranding.
- Hazardous substances.
- Explosion.
- Fire.
- Flooding.
- Machinery failure.
- Payload related.
- Loss of hull integrity.

Having identified the accident categories, their causes are then sorted into risk exposure groups of the identified generic ship functions.

4.4.1.2 Risk Matrix Ranking

This stage consists of analysis of incident and accident data coupled with expert judgement. In order to check the robustness of the resulting hazard rankings and to assist in the resolution of the rankings in cases where several hazards have similar ranking level, the *risk matrix* approach is used.

The FSA guidelines (IMO, 1997a; 2002b) propose a two-dimensional qualitative risk matrix as shown in Figure 4.3:

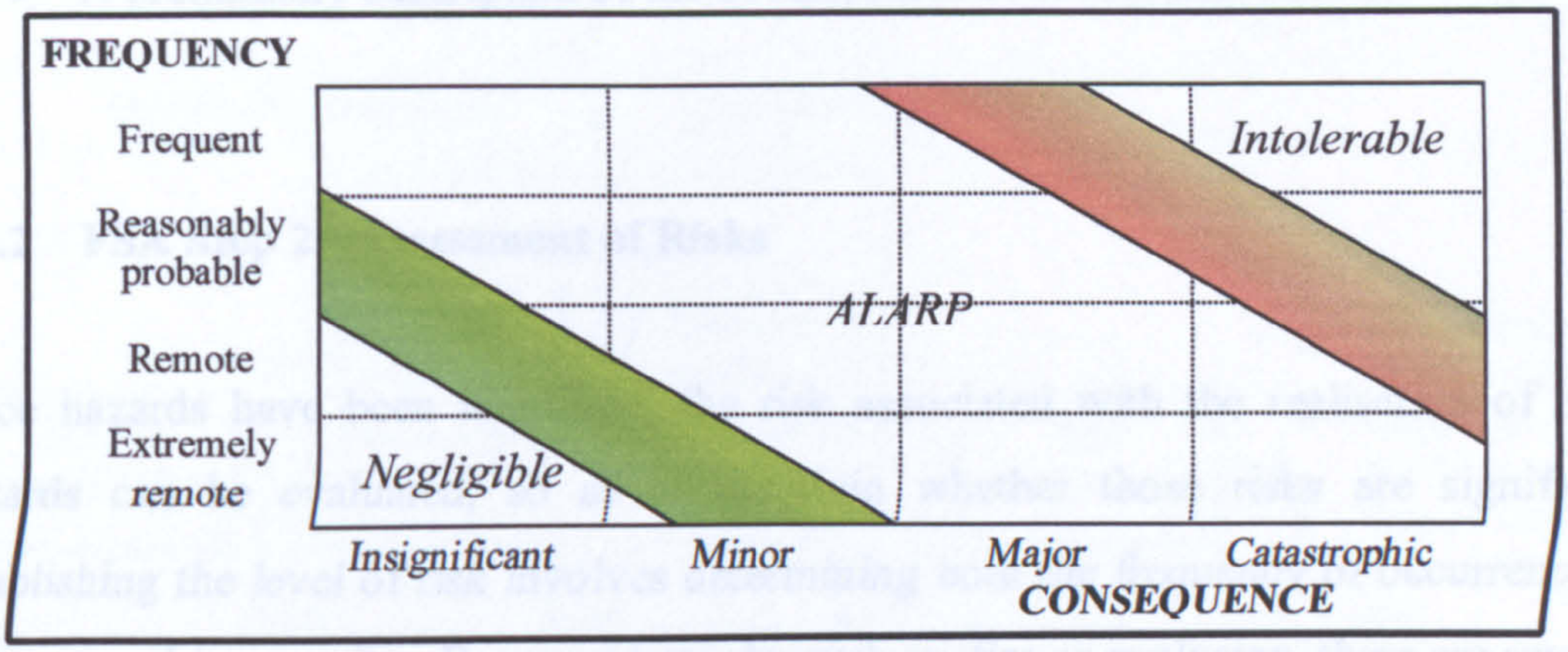


Figure 4.3: A two-dimensional qualitative risk matrix

Risk level boundaries (Negligible/ALARP/Intolerable) in Figure 4.3 are purely illustrative. *ALARP* is used to refer to where a risk has to be shown that it is "*As Low As Reasonably Practicable*" (See Chapter 1, Section 1.3.2). The FSA guidelines leave the selection of the definition of frequency, consequence and the risk level boundaries to the member or organisation undertaking the FSA study.

The risk matrix in the FSA guidelines uses qualitative definitions of frequency and consequence that are generally understandable to those interpreting data or making future projections. However it leaves definition of the risk level boundaries open as there is no IMO or other internationally agreed guidance on defining these boundaries. It is proposed for the generic ship FSA study that a risk matrix, based on that in the Interim Guidelines is used, but with risk ranking in place of defining risk boundaries. Qualitative definitions of frequency and consequence can then be defined from the definition of the ship operations and the accident categories selected for the ship's FSA study.

4.4.1.3 Results of Step 1

The output of *Step 1* comprises:

- A prioritised list of hazards and their associated scenarios prioritised by risk level.

- A preliminary description of the development of causes and effects.

4.4.2 FSA Step 2 - Assessment of Risks

Once hazards have been identified, the risk associated with the realisation of those hazards can be evaluated, so as to ascertain whether those risks are significant. Establishing the level of risk involves determining both the frequency of occurrence of the event and its severity. For most hazards, such as, fire or explosion, there are several possible initialising events, and several possible outcomes, depending upon circumstances. This leads to there being numerous different scenarios to evaluate.

4.4.2.1 Qualitative and Quantitative Risk Assessment

The process of risk assessment is initially performed qualitatively and later extended quantitatively to include data when it becomes available. The interactions and outcomes of both these process are seen in Figure 4.4 (ABS, 2000).

Estimating risk in a qualitative way is done by categorising each of the two components of risk descriptively. For example, the likelihood of an event could be described as "frequent", "unlikely", "extremely improbable", etc. and its consequence as "minor", "major", "catastrophic", etc. The result of a qualitative risk assessment can be presented in the form of a risk matrix.

Qualitative risk assessment can be done using historical data (which reflects past experience), and judgement (which can take a forward look), or a combination of the two. Subsequently, this qualitative evaluation can be improved upon by quantifying the result using appropriate data (for example, error rates, reliability data, accident statistics) and analysis or modelling methods (for example, of fire growth) where these are available. Quantification is not necessary, however, and meaningful judgements, particularly of risk ranking can be made based upon qualitative assessment of risk.

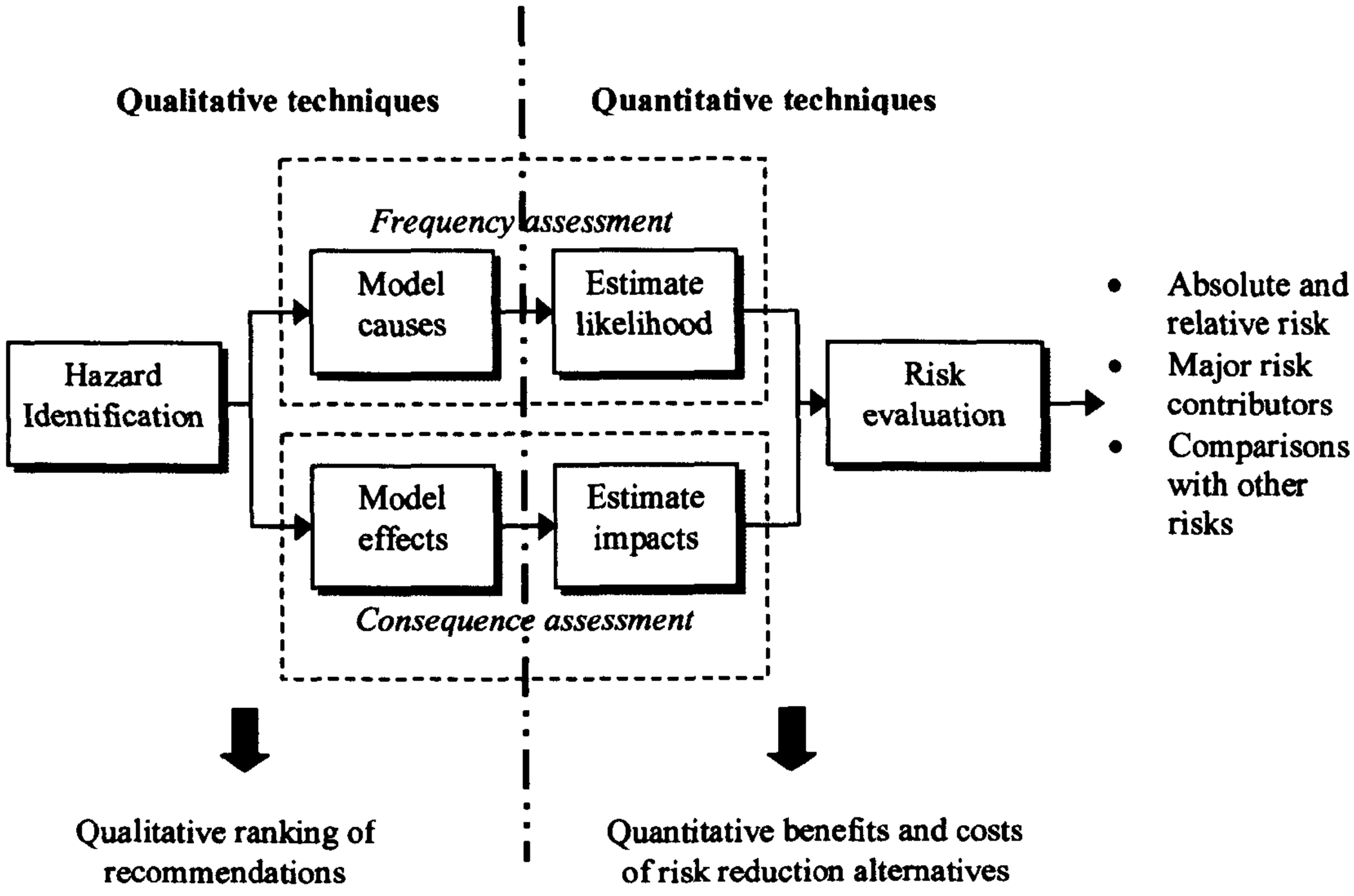


Figure 4.4: Modelling process via qualitative and quantitative analysis

Quantitative risk assessment utilises what is known and assumed about the failure characteristics of each individual component to build a mathematical model. From this assessment, typical parameters including the probability of occurrence of each failure system and possible consequences need to be obtained. Normally quantified by experts with respect to the particular situation, consistency checking is required to validate the results produced from quantitative analysis. Also, there will inevitably be uncertainty in such assessment of risk. This uncertainty does not negate the value of the assessment, but needs to be taken into account when considering the results.

Human error is generally recognised as being a significant factor in many accidents. Likewise, human intervention can prevent an incident occurring, or control or reduce the degree of escalation. Human factors therefore need to be fully taken into account during the risk assessment stage. The objective nature of the risk assessment techniques mentioned above, in which contributory factors and alternative outcomes are systematically examined, facilitates an objective evaluation of both the negative effect of human error and the potentially positive effect of appropriate human intervention.

Systematic techniques, such as *task analysis* (Kirwan & Ainsworth, 1992), are available for analysing human behaviour, enabling explicit account to be taken of this factor, even if at this time reliable data on human performance is scarce and the resulting uncertainty is relatively high.

4.4.2.2 Risk Modelling

As with *Step 1* of FSA (hazard identification), techniques for the assessment of risk are also well established and proven. They include, for example:

- *Fault tree analysis (FTA)*, described in Section 3.3.6 of Chapter 3, which systematically looks at the combinations of circumstances and failures that can lead to an accidental event.
- *Event tree analysis (ETA)*, described in Section 3.3.8 of Chapter 3, which is a systematic and logical means of exploring the escalation potential of an accidental event to establish all possible outcomes and their severity.

The construction and quantification of both such event and fault trees can be used to build a risk model. An example of a conceptual risk model is the *risk contribution tree (RCT)*. The RCT provides a mechanism for displaying diagrammatically the distribution of risk amongst accident categories and subcategories, as shown in Figure 4.5.

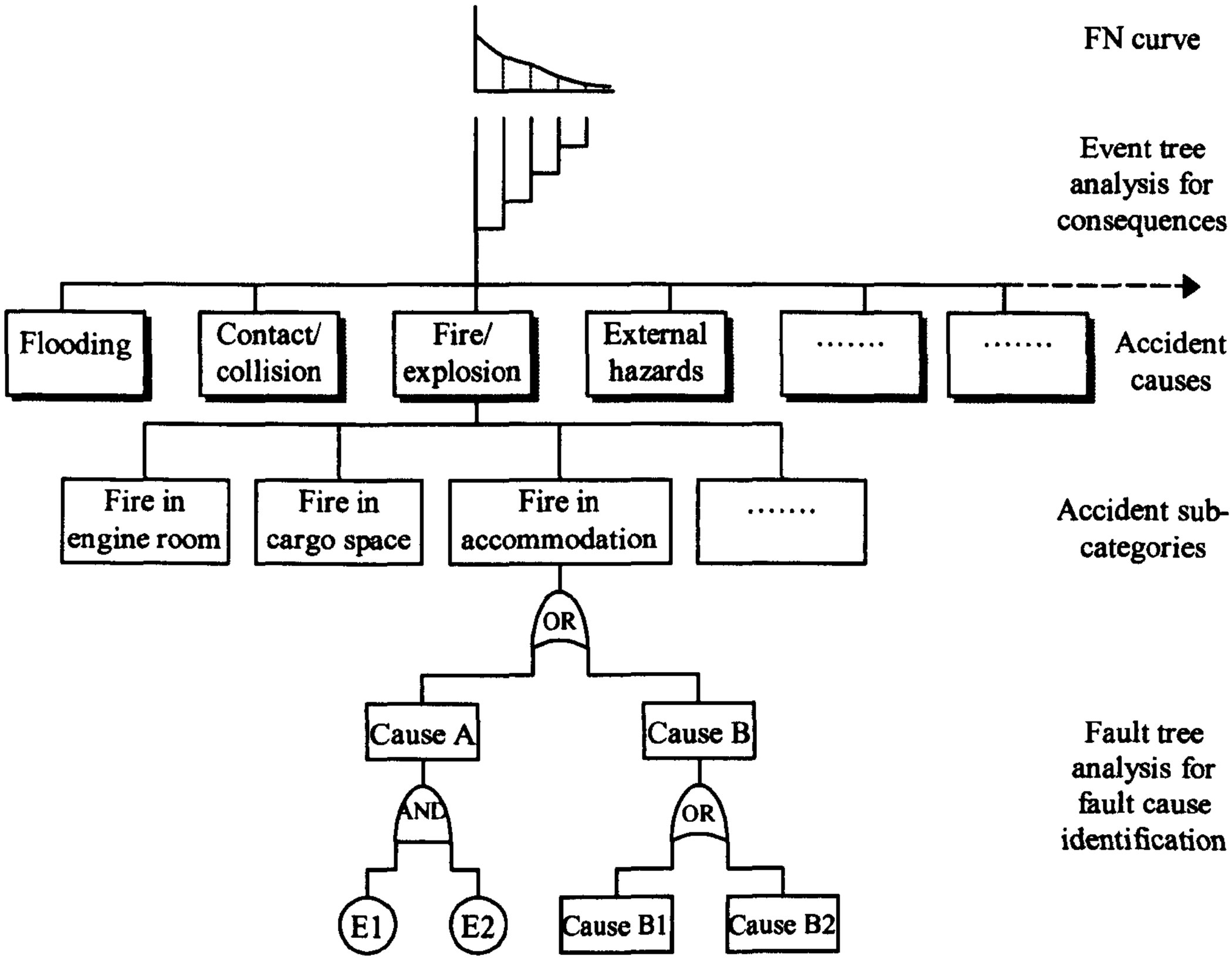


Figure 4.5: Example of a risk contribution tree

Whilst the example makes use of fault and event tree techniques, other established methods could be used if appropriate.

4.4.2.3 Factors which Influence Risk

Factors which *influence risk* include:

- *Stakeholders* – "interested entities".
- *Influence diagrams* – " regulatory impact diagrams".

Stakeholders

Stakeholders are any persons, organisations, company or nation state (as in Figure 4.6), which are directly affected by shipping accidents or the cost effectiveness of the

industry. Their attitudes and actions are probably the greatest single influence over safety. Hence, FSA includes stakeholder identification, and consideration of the impact and equality of potential regulatory options for each stakeholder.

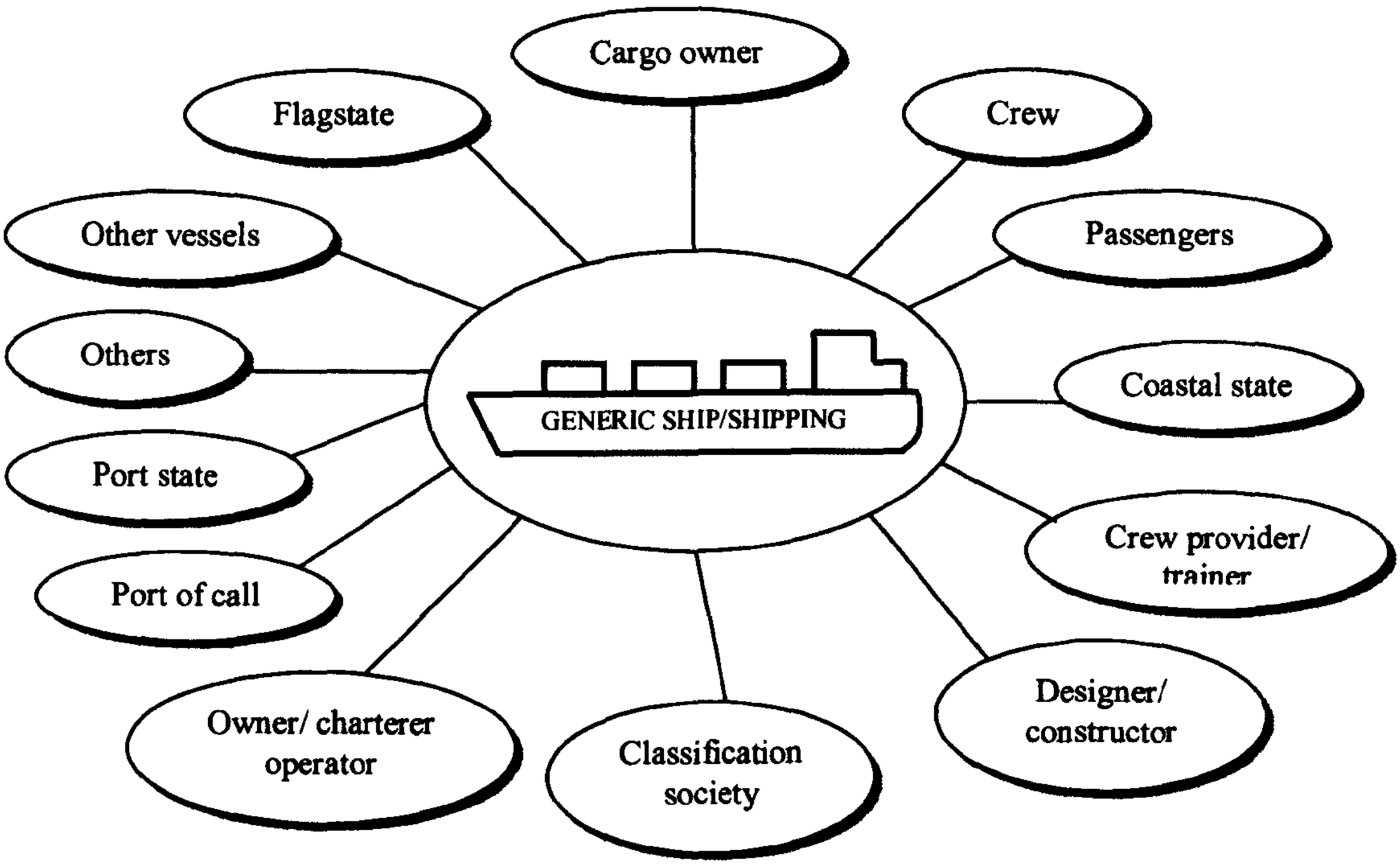


Figure 4.6: Typical stakeholders in shipping venture

Influence Diagrams

An influence diagram identifies the influences that affect the likelihood of an accident, and enables those influences to be quantified. An influence diagram also provides information for use in Step 3 of the FSA process. In the context of developing an overview of risk, influence diagrams are complementary to fault and event trees in the construction of the RCT.

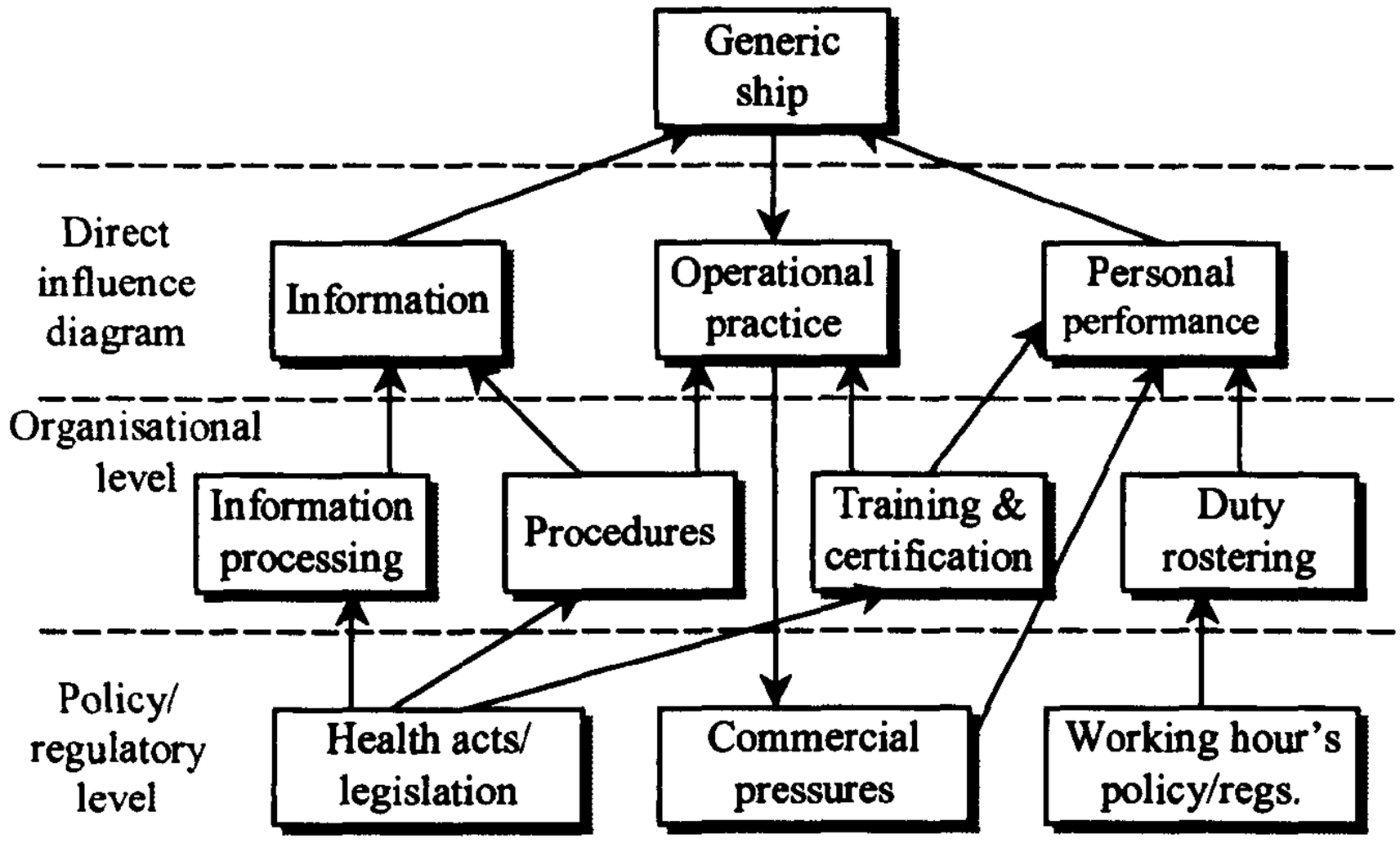


Figure 4.7: A generic influence diagram

An influence diagram takes account of three different types of influence. These are those due to:

- Human failures.
- Hardware failure.
- External events.

Influencing factors are assumed to exist at three levels as shown in Figure 4.7, that is:

- *Direct level*: Factors that directly influence the likelihood of occurrence.
- *Organisational level*: Company/organisational level factors that underlie the direct level factors.
- *Policy level*: The level at which rules and regulations are made, with a view to influencing the organisational and direct level factors.

4.4.2.4 Results of Step 2

The results from *Step 2* can be summarised as follows:

- An identification of high risk areas to be controlled.
- An identification of the principal influences that affect the level of risk.

4.4.3 FSA Step 3 – Risks Control Options

Having concentrated on identification and assessment of high-risk areas/events, *Step 3* begins the process of managing risk by developing causal chains along the lines, which may be expressed as in Figure 4.8 (IMO, 2002b).

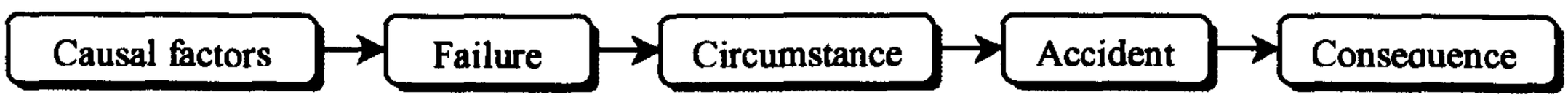


Figure 4.8: Casual chain of a failure event

Causal chains are required for all potential likely high-risk scenarios in enabling a range of risk control measures (RCMs) to be identified. These are either 'preventive' control measures or those that provide a measure of 'mitigation'. In order to assist logical thought process about RCMs they are divided into three categories (Canter, 1997).

- Category A: Fundamental type of risk control, for example, preventive or mitigating.
- Category B: Type of action required and its cost, for example, engineering/ design/ procedural/ human.
- Category C: Confidence placed on measures, for example, passive/active, independent/dependent, auditable/non-auditable, quantitative/ qualitative etc.

(a) **Areas Needing Control**

It is aimed to screen the output of *Step 2* so that effort is focused on the areas that need the most control. The main aspects of this assessment are to review the following:

- Review risk level.
- Review severity.
- Review probability.
- Review confidence.

(b) **Risk Control Measures Log**

Generation of RCMs is aimed to:

- Reduce the frequency of failure.
- Mitigate of the effort of failure.
- Alleviate circumstances where failure may occur.
- Mitigate the consequences of accidents.

Creating this log involves the following steps:

(i) Identifying existing RCMs as identified in *Step 2*.

(ii) Developing new RCMs for high risk areas identified in *Step 2* that are not sufficiently covered by existing measures;

(iii) Ensuring the RCMs are comprehensive and cover all the possible hazards and risks. The two tools, 'risk attribute' and 'causal chains', can be used for both steps (ii) and (iii);

(iv) Entering the RCMs identified into 'risk control measures log'. Then, they are reviewed with reference to the influence of each individual RCM on other high risk areas identified by *Step 2*.

(v) Draft of 'risk control measures log' is reviewed before generating 'risk control option log'. Examples of these logs are shown in Table 4.1 and Table 4.2 (IMO, 1996).

(vi) At any stage of the process above, it is necessary to refer back to *Step 1* or *Step 2* of FSA for more information or further analysis.

Table 4.1: A typical risk control measures log form

Ref.	Risk profile element	Description of measures	Attributes	Assumptions/reasoning
	Outcomes			
	Initiating event (1)			
	Initiating event (2)			
	Initiating event (n)			
	Magnitude factors			
	Event tree node (1)			
	Event tree node (2)			
	Event tree node (n)			
	Progression factor			
	Fault tree base event (1)			
	Fault tree base event (2)			
	Fault tree base event (n)			
	Initiating factors			
	Fault tree base event (1)			
	Fault tree base event (2)			
	Fault tree base event (n)			
	Human factors			
	Influence diagram event (1)			
	Influence diagram event (2)			
	Influence diagram event (n)			
	Step 1 hazards			
	Hazards (1)			
	Hazards (2)			
	Hazards (n)			

Table 4.2: A typical risk control options log form

Ref.	Description of risk control	Attributes	Benefit		Supporting information
			Quantitative Δf-n	Qualitative	

Note that Δf-n represents the change in frequency of fatal accident (f) versus number of fatalities (n) (See Chapter 2, Section 2.6 for more details).

(c) **Risk Control Options**

The output result of risk control option (RCO) details the cost of the options in terms of cost types defined by *Step 4*. It should also show sufficient data on who bears the risk, who benefits from the risk reduction and who has to implement the measures. This provides the sources of information for the subsequent principles of "risk imposer pays" and stakeholders.

4.4.3.1 Results of Step 3

The output from *Step 3* comprises:

- A wide range of RCOs, which are assessed for their effectiveness in reducing risk.
- An inventory of interested entities affected by the identified RCOs.

4.4.4 FSA Step 4 - Cost Benefit Assessment

Cost benefit assessment (CBA) in risk assessment is normally used to assess the marginal return of additional safety measures comparing:

- The cost of implementing the measure.
- The benefit of the measure, in terms of the risk that would be averted.

The purpose of CBA is to show whether the benefits of a measure outweigh its costs, and thus indicate whether it is appropriate to implement the measure. CBA cannot provide a definitive decision, because factors other than risks and costs may be relevant, but provide a useful guide. There are several indices that can express cost effectiveness in relation to safety of life. In order to compare different RCOs, the risks and costs are expressed as a ratio, known as the *implied cost of averting a fatality (ICAF)*. The definition is:

$$\text{ICAF} = \frac{\textit{Net annual cost of measure}}{\textit{reduction in annual fatality rate}}$$

The potential loss of life (PLL) values, given in units of lives/vessel/year (see Chapter 2, Section 2.6), can then be determined for the system *before*, *b*, and *after*, *a*, the introduction of a risk reduction measure respectively. Then, the reduction in PLL can be calculated as:

$$\text{Reduction in annual fatalities rate} = \text{PLL}_b - \text{PLL}_a$$

where,

PLL_a = PLL *after* RCO is implemented.

PLL_b = PLL *before* RCO is implemented.

Other indices based on damage to and affect on property and the environment may be used for a CBA relating to such matters. Calculating these indices should also provide comparisons of cost effectiveness for the RCOs.

Costs are estimated as life cycle costs, including initial, operation, training, inspection and certification costs. Benefits include reduction of costs for fatalities, injuries, environmental damage, clean-up, liability claims, ship deterioration, etc.

4.4.4.1 Results of Step 4

The result of the *Step 4* comprises:

- Costs and benefits for each RCM identified in *Step 3* from an overview perspective.
- Costs and benefits for those interested entities which are the most influenced by the problem under concern.
- Cost effectiveness expressed in terms of suitable indices, such as ICAF.

4.4.5 FSA Step 5 – Recommendations for Decision Making

The overall aim of *Step 5* is to collate all the information generated by *Steps 1 to 4*, to assist in the choice of cost effective and equitable changes to regulations. For example, information about risk levels before and after implementation of risk control would be recorded alongside justification to iterate any part of the process. This step recognises FSA to be a tool, not a decision maker, and seeks to enhance the quality of information by first considering the cost effectiveness of a proposed option on an industry wide basis. A second stage examines whether the effect on all interests involved is equitable (that is, one or more interests may be carrying a risk or cost at a level disproportionate to expected returns). Given this information, the normal decision making process can proceed, taking into account all the social, political and cultural influences that are a necessary part of obtaining consensus on an international basis. Hence, there is a systematic, robust and auditable basis to guide decision makers.

4.4.5.1 Results of Step 5

The results of *Step 5* will include:

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

4.4.6 Incorporation of the Human Element

In deriving the generic ship model that forms the basis of FSA it rapidly becomes apparent that human factors dominate many of the risk scenarios. Casualty data confirms that the general assumptions, which often suggest that around sixty to eighty percent of casualties result directly from human error (The Nautical Institute, 2003), are valid. It comes as no surprise to any safety analyst that it simply is not possible to

separate technical safety from the influence of operators, in the widest sense. The FSA methodology does not allow consideration of a technical solution without due regard being paid to the interactions with people.

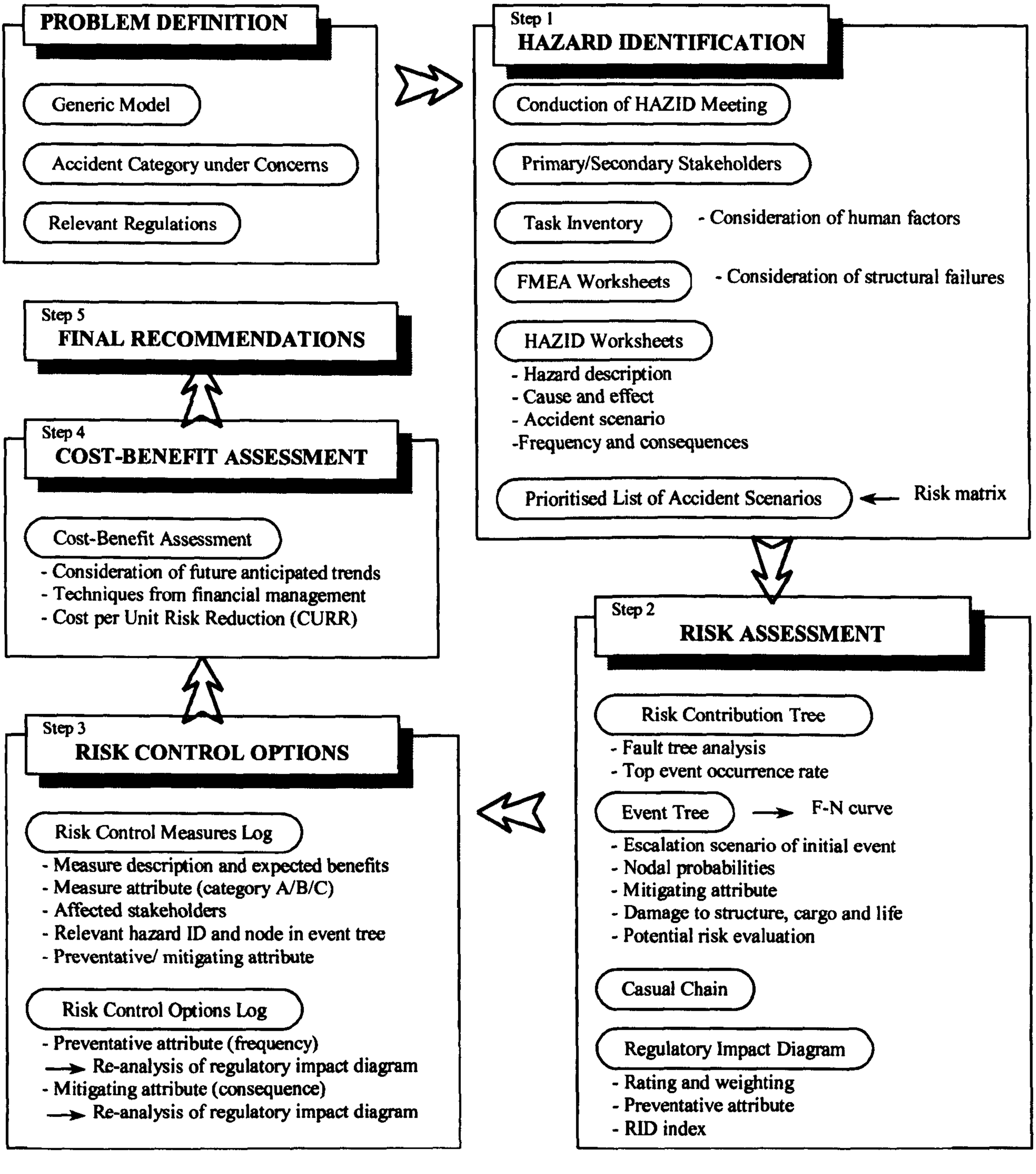


Figure 4.9: Procedures of formal safety assessment

As a result of failure to address such human factors issues, casualty cases have been put ever so often in the spotlight. In order to make a step improvement however, any new approach to safety needs to target the human factor in a rational and systematic manner. FSA adopts this approach by allowing for the human element to be incorporated into its process from a human reliability analysis that takes details squarely with the contributing factors to human error.

4.5 Procedure Summary of Formal Safety Assessment

Figure 4.9 summarises the procedures of FSA as discussed in Sections 4.4.1 to 4.4.5 and the flow of inputs/outputs at each procedure.

Additionally, absolute decisions about acceptability require a degree of confidence in both the results of risk analysis, and in the acceptable level of risk, which are probably not justified at the present time for an industry as diverse as shipping. This is due partly to the paucity of data and resulting uncertainties, and also to the lack of experience of using FSA in the shipping industry. The FSA process is therefore probably best seen and relied upon as a comparative rather than an absolute method for the time being.

4.6 Incentive for Utilising Formal Safety Assessment

FSA involves much more scientific aspects than previous conventions. The benefits of adopting FSA as a regulatory tool include (MSA, 1993):

- A consistent regulatory regime, which addresses all aspects of safety in an integrated way.
- Cost effectiveness, whereby safety investment is targeted where it will achieve the greatest benefit.
- A proactive approach, enabling hazards that have not yet given rise to accidents to be properly considered.

- Confidence that regulatory requirements are in proportion to the severity of the risks.
- A rational basis for addressing new risks posed by ever changing marine technology.

Furthermore, application of FSA in ship design and operation may offer great potential incentive that could:

- Improve the performance of the current fleet, be able to measure the performance change and ensure that new ships are of good designs.
- Ensure that experience from the field is used in the current fleet and that any lessons learned are incorporated into new ships.
- Provide a mechanism for predicting and controlling the most likely scenarios that could result in incidents.

4.7 Brief Review of FSA Trial Application to Key Generic Ships

On an international acclaim, large-scale FSA studies have been mainly undertaken for high speed passenger catamaran ferries (HSC) and bulk carrier (BC) ships. These vessels have been considered an appropriate basis for the FSA approach as they embody new technology largely without an extensive historical basis of experience. To this end, focus of the studies is deployed only to highlight a brief review to the results in their significant progress.

4.7.1 Trial FSA Application to High Speed Passenger Catamaran Ferries

The final report of the FSA to HSC (IMO, 1997c), as undertaken by the United Kingdom, focused on the safety of passengers and crew. To provide a broad perspective, both of hazards and of a variety of different aspect of HSC design, construction and operation, the following accident categories were selected for trial study:

- Collision and contact;
- Fire; and
- Loss of hull integrity (including structural failure)

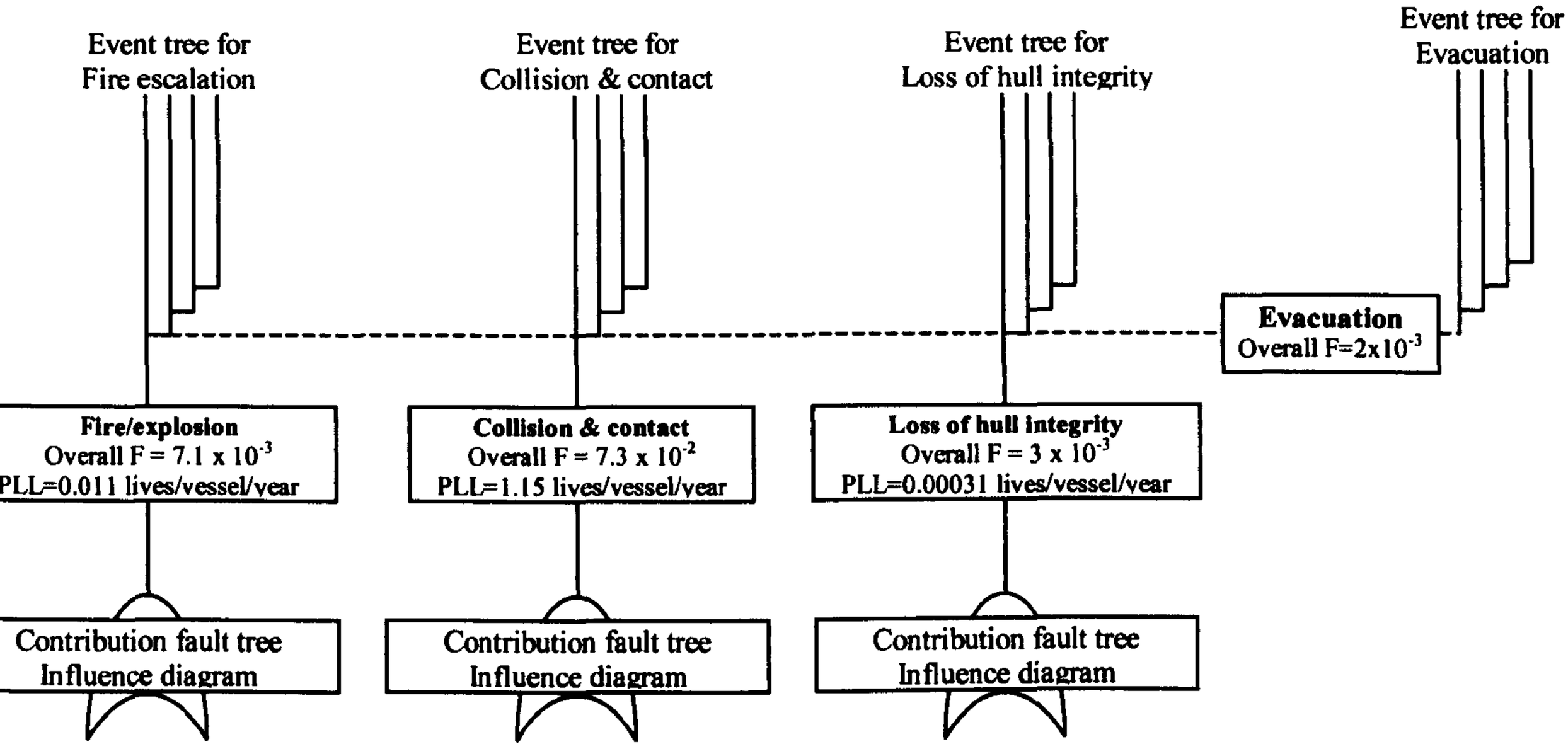


Figure 4.10: Components of HSC risk contribution tree

Following causes and outcomes of the accident scenarios being identified for consideration, the risk analysis of the HSC trial study presents the risk contribution tree (RCT), which is briefly outlined in Figure 4.10 (IMO, 1997c), for the three accident categories. Overall frequency (F) figures of 7.1×10^{-3} per vessel year for the fire category, 7.3×10^{-2} per vessel year for the collision and contact category and 3.0×10^{-3} per vessel year for the loss of hull integrity (LOHI) category have been derived from the sorted incident database (IMO, 1997c). Injury weightings have been applied to determine equivalent fatalities and the PLL caused by the occurrence of these failure events have then been determined from FN curves. These PLL values are given as 0.011 lives/vessel/year for the fire category, 1.15 lives/vessel/year for the collision and contact category and 0.00031 lives/vessel/year for the LOHI category (IMO, 1997c). These results provide an approximation to risk that appear to be realistic for the fire and LOHI events but may not be a true representation of risk for collision and contact events. The study also assumes that the maximum estimated PLL reduction could be

achieved and therefore, seven risk control options (RCOs) were finally ranked for their implementation in the trial application of the FSA process (IMO, 1997c).

Although expert judgement was applied to account for areas of uncertainty, the study acknowledges that there remain uncertainties with regards to the numerical evaluations for the overall frequency and assumed maximum PLL.

4.7.2 Trial FSA Application to Bulk Carrier Vessels

Serious concerns have been expressed about the safety of bulk carriers since a spate of sinking in the early 1990's. IMO prompted an international programme of research and development culminating in the 1997 IMO SOLAS Conference on Bulk Carrier Safety (IMO, 1999). The research had shown that the ships at greatest risk comprised those of over 15 years of age, and 150m in length, carrying dense cargoes such as coal or iron ore, and built with single side skin construction. The most likely cause of loss was considered to be side shell failure causing flooding of cargo holds and leading to overall structural failure of the ship due to overloading of the structure. For trial FSA of BC vessels, the key hazards relate to failure of watertight integrity (IMO, 2002c), which thus implies LOHI. These result from failure related to:

A: The closing devices provided.
B: The hull envelope itself.
C: Inappropriate operations aspects.

Fault trees and event trees had to be developed for the failure related to A, B and C, in order to achieve a RCT for the trial FSA on bulk carrier vessels. These tree-type analyses were developed from the statistical base of events contributing potentially to the LOHI and their frequency of occurrence over the period 1978 to 2000 (IMO, 2002a). In the expanded fault tree case of Figure 4.11 (see IMO, 2002c), branch B (hull envelope) have been clearly prevailing and suggest the most significant high-level event to be that of side shell failure due to fatigue/wastage with 146 identified cases, across all sizes of BC, resulting in 113 lives lost. While side shell failure due to collision, escalating to loss of structural integrity and sinking, accounts for 26 cases, but has

LIVERPOOL
JOHN MOORES UNIVERSITY
AVRIL ROBARTS LRC
TEL. 0151 231 4022

caused 130 fatalities, hatch cover failures account for a total of 40 incidents, which have resulted in 565 fatalities. The later appear to be the result of covers being dislodged (possibly due to failing securing devices or unsecured hatches), however, their structural failure is apparent and cannot be ruled out.

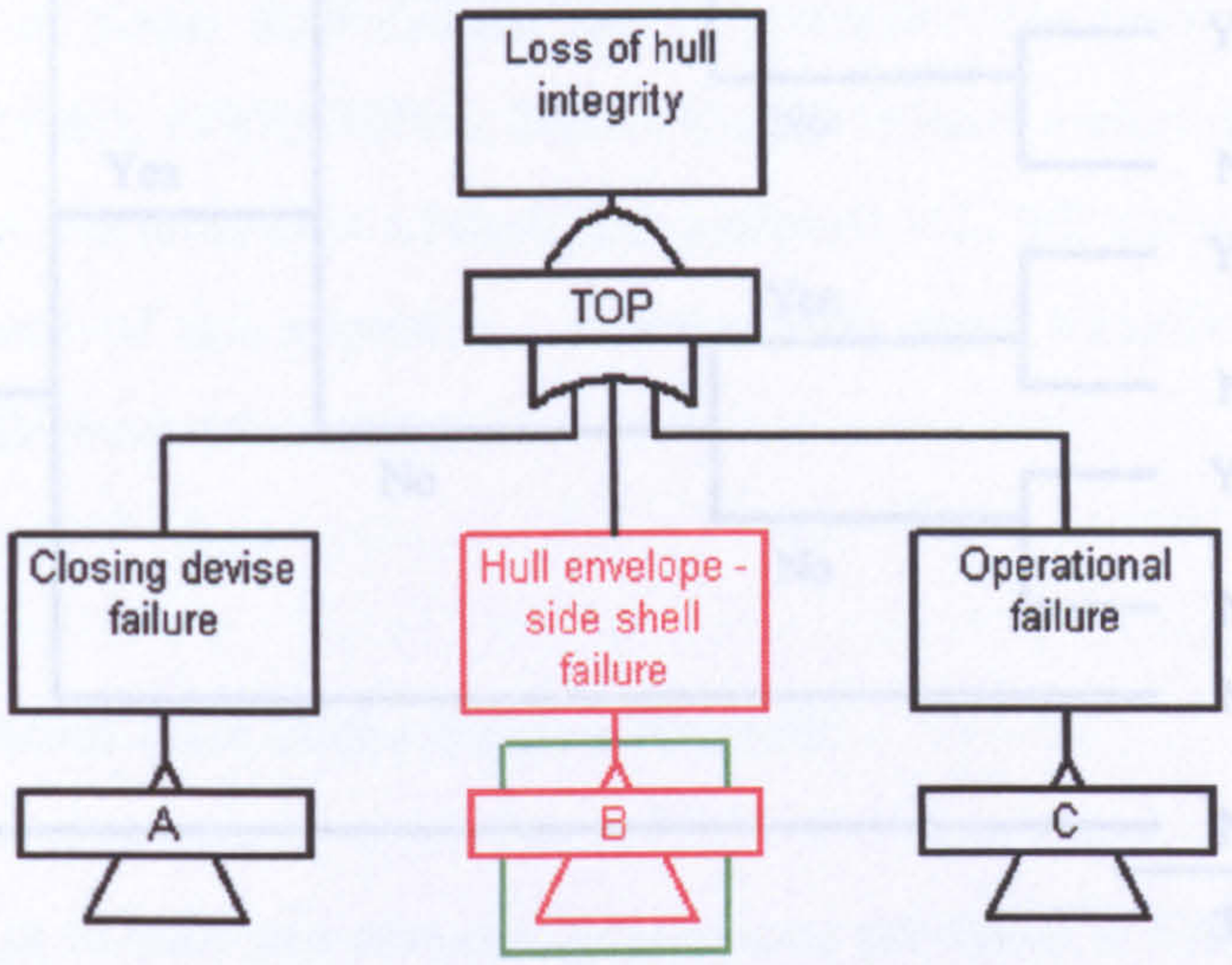


Figure 4.11: Fault tree of the first level to BC failure of watertight integrity

Side shell failure in branch B of the LOHI event leading to rapid flooding and consequent loss of ship generated a PLL of 2.34×10^{-3} fatalities per ship year (i.e., 94% of total PLL, according to IMO (2002c), see Figure 4.12)). The predominance of PLL of hatch cover and side shell failure incidents is flagrant with a dramatic impact on loss of life from hatch cover incidents which results in approximately 1.5 times more fatalities than side shell incidents with 4 times less occurrence. The overall value of risk is 1.22×10^{-2} fatalities per ship year (IMO, 2002c). A large number of risk control measures (RCMs) have eventually been derived for BCs, including a total of 98 derived from the international community (IMO, 2002d). These assessed RCOs are divided into three branches given by the ETs and ETs of A, B and C, for which a screening process was applied to sort and review potential RCMs and RCOs. In addition to those, two evacuation RCOs, i.e., free-fall lifeboat and float-free accommodation, have been considered.

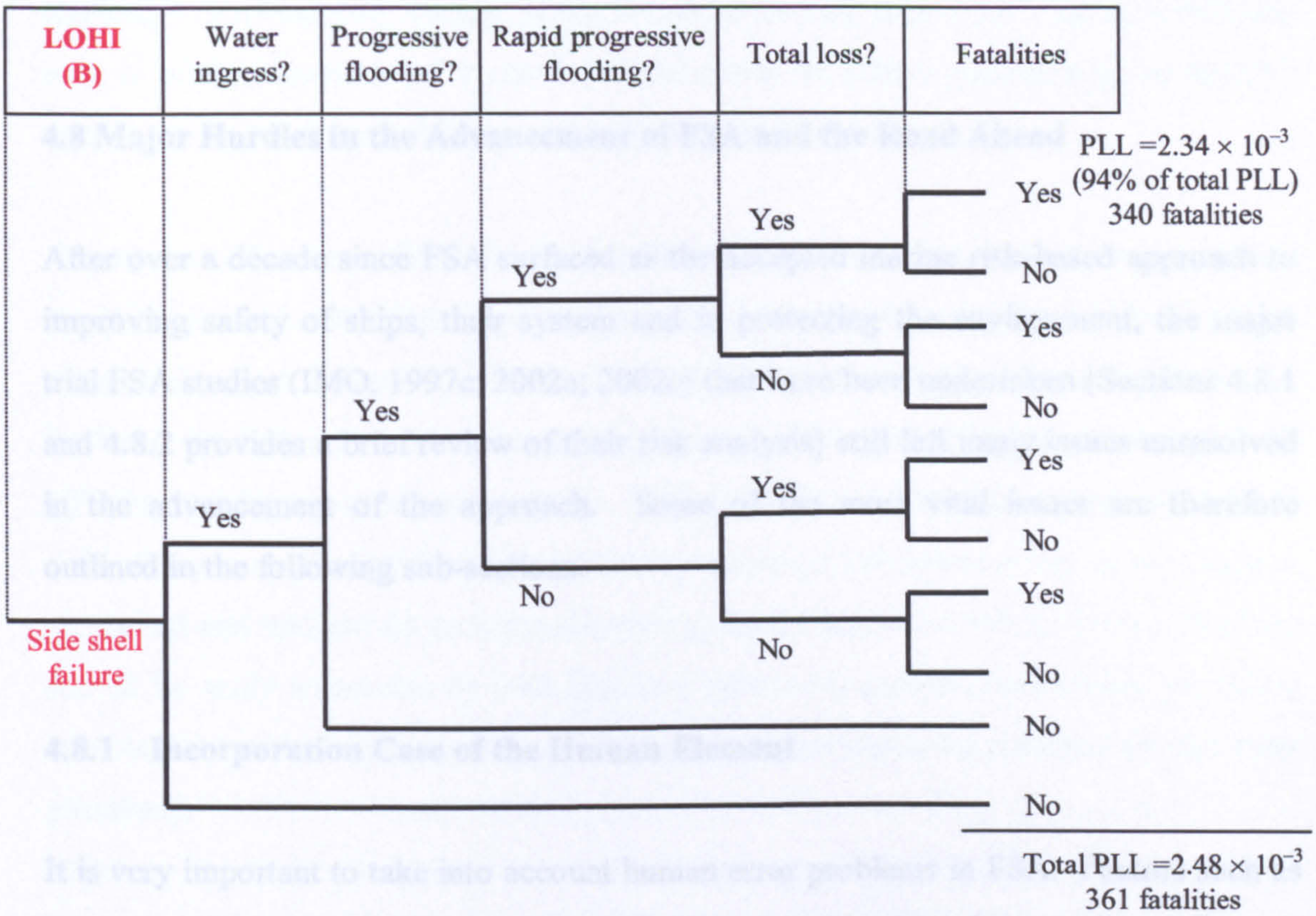


Figure 4.12: Event tree showing sequence of events for BC side shell failure

Cost benefit assessment (CBA) study was applied to calculate and rank 75 of the 98 derived RCOs for BCs of Handy (Handysize & Handymax), Panamax and Capesize types in terms of their cost effectiveness with respect to potential risk reduction available (ShipTech A/S, 2002). These have been analysed, quantified and ranked according to their net cost of averting a fatality (NetCAF). The criteria on which a RCO was selected for recommendation are generally those assessed by the trial application of FSA to BC vessels to have a NetCAF being <$3 million US dollar or to provide an estimated reduction in risk (i.e., PLL) of the order of 10^{-4} or better (ShipTech A/S, 2002).

The estimates given above are encumbered with statistical uncertainty. Even though the risk contribution from the water ingress scenarios in general is a significant estimate, the break down on the underlying scenarios is more uncertain, e.g. the importance of the side shell failure scenarios may be over-estimated, whereas the importance of the hatch cover failure scenarios may be under-estimated (IMO, 2001b).

4.8 Major Hurdles in the Advancement of FSA and the Road Ahead

After over a decade since FSA surfaced as the accepted marine risk-based approach to improving safety of ships, their system and in protecting the environment, the major trial FSA studies (IMO, 1997c; 2002a; 2002c) that have been undertaken (Sections 4.8.1 and 4.8.2 provides a brief review of their risk analysis) still left many issues unresolved in the advancement of the approach. Some of the most vital issues are therefore outlined in the following sub-sections.

4.8.1 Incorporation Case of the Human Element

It is very important to take into account human error problems in FSA. Factors such as language, education, training, etc., that affect human error, have increased over the past years, especially with the introduction of multi-national crews. Such problems largely contribute to marine casualties. On the other hand, crew reductions have increased the workload of operators, which in connection with the reduced opportunities for port stay and recreation equally increases the probabilities for errors.

It becomes apparent that FSA's success largely depends on two essential conditions. The first condition is the development of a safety culture at all levels of the industry's infrastructure, from company managers to vessel operators. The second one is the inclusion into the FSA framework itself of further guidance on how human factors would be integrated in a feasible manner.

4.8.2 Availability and Reliability of Data

The confidence of FSA greatly depends on the reliability of failure data. The availability and accuracy of data defines the ease and accuracy with which a project such as this can be carried out. The more expert judgement that is used in developing risk analysis studies the more subjective the results become and the more open to

challenge. Furthermore, the risk analysis task of the reviewed FSA studies, which has been briefed in Sections 4.7.1 and 4.7.2, proved to be quite a challenging and lengthy one due to the obvious deficiencies in casualty data.

Nonetheless, it is rare for a study, particularly in the marine environment, to have comprehensive data and the approach is almost always one of using data backed up with expert judgement; the two approaches are complementary. The application of FSA may facilitate the collection of useful data on operational experience that can be used for effective pre-active safety assessment. However, international co-operation and co-ordination are required with the intention that a new global database will be established, controlled and updated by an international regulatory body (i.e. IMO). Such a database should be easily accessible by both administrations and analysts/researchers, providing reliable data with defined parameters upon which the incoming information has been processed.

4.8.3 Risk Criteria Acceptance and Cost Effectiveness

The acceptability of risk is a problematic question and likewise, risk communication may also be a problematic issue. Large variations also exist in the risk criteria that are set around the world, as they depend mainly on local regulators. Up to today, much effort is being made by administrations individually, without any co-ordination among them. Considering that internationally trading vessels move constantly from one jurisdiction to another, it becomes apparent that this lack of co-ordination is bound to produce further confusion to the industry, which does not seem willing to accept it.

The establishment of universally acceptable risk criteria for ships may be achieved through a compromise between qualitative and quantitative figures. When quantitative risk assessment (QRA) is performed, it is required to use numerical risk criteria. It is generally noted that no quantitative criteria in FSA exist even for a particular type of ship although the trial applications have used QRA to a certain extent. Therefore, numerical risk criteria for FSA application needs to be reviewed for possibility of its incorporation in future studies. Nonetheless, the application of numerical risk criteria may not always be appropriate/suitable to use as inflexible rules because of

uncertainties in inputs. Accordingly, acceptance is unlikely to be based solely on a numerical risk assessment. It can therefore only assist judgements and be used as guidelines for decision-making.

It is appropriate to consider the acceptability of risk, as in broad terms, there is risk attached to every activity. At one end of the scale, there is a risk level that would be considered intolerable, that is, an activity giving rise to the risk can/should not be justified. At the other end of the scale, a risk may be so low that the cost and trouble involved in further reducing it may be quite unreasonable. Indeed, it would be wrong to devote resource to risks that are already acceptably low, when the same investment would be better expended on reducing other, greater risk.

In the decision-making process, criteria may be used to determine if risks are acceptable/tolerable, unacceptable/intolerable or need to be reduced to ALARP. In the regions between the maximum tolerable and broadly acceptable levels, risks should be reduced to ALARP, taking costs and benefits of any further risk reduction into account.

4.8.4 Complexity Owing to the Use of Cost-Benefit Analysis

The cost-benefit approach remains controversial when applied to the safety of life and the environment, although its use as a platform on which a given option is finally selected for implementation is an appealing proposal. In practice, however, it can be quite complicated, especially in cases where human lives are involved. The fact that ships are manned with multi-national crews, usually officers from developed countries and crews from developing ones, and obliged to trade in all parts of the world creates a difficulty in selecting the proper human life value for cost benefit analysis. Furthermore, the use of different values on different nationalities would have an adverse and undesirable effect on both international relations and working conditions onboard ships.

A feasible solution to this problem would involve an international agreement on a reliable method of estimating the current value of human life. The international regulatory bodies should not only be responsible for the initial deliberations, but also for

the constant follow up of the international economic, political and social trends that influence that value.

4.8.5 Treatment of Uncertainty and Expert Judgement

Accident and incident databases, if available, are very useful for the risk assessment exercise. Uncertainty problems however, do arise with older data or data concerning distant occurrences (THEMES, 2001). The environmental conditions, cultural habits and other singularities like adherence to rules, may differ quite a lot between different areas and cultures of the world. Some special types of accidents need an enlargement of the scope.

The FSA procedure utilises expert judgements and expert sessions. The suitable experts must represent a broad range of knowledge, domain experience and skills. However, it is possible to reduce the use of expert judgement by utilising objective data based on engineering analysis as far as possible.

4.9 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 route recommended in that it aims to support the rule making process at a generic level and to provide a logical methodology to establishing 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 depends on the level of risk.

In reviewing the risk analysis carried out on the trial application of FSA to HSC and BC ships, it has become apparent that there is still plenty of space for improvement on FSA application to the maritime field. Areas on which such improvement can be achieved include risk criteria acceptance, cost-benefit, life-saving equipment, information availability and/or expert judgement, uncertainty treatment and human reliability. The later two areas are extremely vital for the practical use of FSA yet these were often not tackled in the trial studies. In the proceeding three chapters, the treatment and reasoning under conditions of uncertainty is embarked upon. Another chapter, which follows after these three, deals with both uncertainty treatment and human reliability.

Chapter 5: Treatment of Uncertainty

Chapter Summary

Risk cannot be uniquely determined because of various types of uncertainty. The costs of ignoring uncertainty can be very high in terms of unwelcome surprises and poorly calculated risk-taking behaviour. Thus, it is important to reduce this uncertainty to a manageable level and much crucial for maritime risk assessment and decision-making to be conducted in the presence of uncertainty.

There are many potential sources of uncertainty affecting risk. Available knowledge that needs to be utilised may be unreliable, incomplete, imprecise, vague and/or inconsistent. Moreover, inherent uncertainty is associated with even the most comprehensive and useful data for quantified risk assessment in safety-critical maritime domains. Various theories have been developed to accommodate the different characteristics of uncertainty forms for risk-based modelling.

5.1 Introduction

All maritime activities desire the lowest level of risk possible in order to pave way for the highest probability of success, profit, or some form of gain (e.g. high performance, safety and reliability). Therefore, even when the risk assessment result of a safety-critical marine and offshore application indicates the risk level is negligible, acceptable or as low as reasonably practicable (ALARP) in criteria (HSE, 1992), such risk acceptance must incline towards minimal uncertainty.

Nearly every assessment encounters situations where data are unavailable or where information is available on parameters that are different from those of interest for the assessment. The very heart of risk analysis is the responsibility to use whatever

information is at hand or can be generated to produce a number, a range, a probability distribution - whatever expresses best the present state of knowledge about the effects of hazards in some specified setting (NRC, 1994 and 2000). Simply to ignore the uncertainty in any analytical process is almost sure to leave critical parts of the process incompletely examined, and hence to increase the probability of generating a risk estimate that is incorrect, incomplete, or misleading. Therefore, uncertainty is clearly a key factor in risk-based modelling. By incorporating uncertainty into the risk assessment process, alternative-planning strategies can be viewed more realistically.

Also, to arrive at a decision in the presence of absolute certainty with respect to all the relevant facts and considerations is a luxury rarely afforded to human beings. Assumptions must be made about data values and/or about events, which may or may not have occurred, and about consequences likely to flow from a given decision. In the real world, the consequences of any decision choice made cannot be fully known before that choice is made, which means that the ideas of uncertainty and risk have to be examined. Many of these assumptions may be made unconsciously or subconsciously. Some may be made explicitly, with whatever degree of justification may be adduced. Mathematics may be prayed in aid of some assumptions made on statistical bases. Otherwise, rule of thumb and accrued experiences serve as a guide (Graham & Jones, 1988). Thus, decision-making under uncertainty (the theory of how to take those uncertainties into account in an optimal manner in decisions) has to also govern an important part of risk management. Failure to do so is likely to result in adverse impacts on performance, and in extreme cases, impede safety.

5.2 Uncertainty in Risk Analysis

The term 'uncertainty' has come to encompass a multiplicity of concepts. It typically refers to situations in which many outcomes of a particular choice are possible but the likelihood (or probability) of each outcome is unknown. Risk is rather different in that it can only be measured accurately on the assumption that all the possible outcomes and the likelihood (probability) of each outcome occurring are known. Risk can be estimated in a variety of ways by assigning probabilities to various possible outcomes. In fact, in risk analysis, the uncertainty can be put across as a lack of certainty/precise

knowledge as to what the truth is, whether qualitative or quantitative (NRC, 1994 and 2000), which in turn has important implications to the results of the assessment and to what can be achieved at the decision-making. Sometimes these implications are 'risk' in the sense of 'significant potential unwelcome effects on the safety-critical performance of the domain application'. Nonetheless, that lack of knowledge creates an *intellectual problem* - that one does not know what the "scientific truth" is; and a *practical problem* - one needs to determine how to assess and deal with risk in light of that uncertainty (NRC, 1994 and 2000).

Scientific truth is always somewhat uncertain and is subject to revision as new understanding develops (NRC, 1994 and 2000). In the realistic viewpoint, uncertainty in maritime quantitative risk assessment (QRA) might be uniquely large, so it requires special attention by risk analysts - one that calls for a clear understanding of where the uncertainty comes from, in what form, what repercussion it possesses and how it can be dealt with in order to decrease its presence. Therefore, it is crucial for risk assessment to be conducted in the face of it.

5.3 Sourcing and Representing Uncertainties

It is an essential prerequisite for risk analysts and decision makers to understand the nature of perceived threats and opportunities in order to identify hazards, assess and manage the attendant risk. Thus, those uncertainties that may give rise and shape the risk, threat and opportunity, have to be well sourced and represented in order for them to be dealt with appropriately.

5.3.1 Sources of Uncertainties

The natural world is the ultimate source of all uncertainty. Therefore, even before the risk assessment commences, there are uncertainties attributable to the complexity of requirements or implementation (INCOSE/PMI, 2002) and that of people issues in the least of cases. Through the course of a risk analysis, there are many potential sources of

uncertainty that safety-critical maritime systems must be able to cope with, though most can be attributed to one of:

- *Imperfect Domain Knowledge*: The theory of the domain may be vague or incomplete. Incompleteness necessitates the use of rules of thumb (or heuristics), which may not always give optimal or correct results. Even if the domain theory is complete, an expert may use approximations or heuristics to save time or simplify the problem solving.

- *Imperfect Case Data*: Data is collected in the field with different levels of accuracy; so naturally, the knowledge accrued ends up being implicitly imperfect. Also, data gaps are usually bridged based on a combination of scientific data or analyses, expert judgement, and through the use of some analogous data that may be the only option available. Therefore, experts, the risk analysts and other professionals may disagree over which data is relevant to include in risk models, especially when there is conflicting data. This lack of consensus can increase uncertainty. Human reports may be ambiguous or inaccurate. Evidence from different sources may be missing or in conflict. Even if exact data were available, it could be too costly in time or resources to get it. Confidence can be increased through consensus building techniques such as peer reviews, workshops, and other methods to elicit expert opinion. Cost-effective data-acquisition strategies can be developed to achieve decision closure where there is adequate data or where further reduction of uncertainty is needed and is feasible.

Whatever the source of uncertainty, safety-critical maritime systems need to be able to deal with it. Opportunities for reducing these sources of uncertainty should be noted and carried through to risk characterisation.

5.3.2 Representation of Uncertainty

As far as knowledge representation schemes are concerned, a good mechanism for representing uncertainty ought to have the following properties (Graham & Jones, 1988):

- Consistent and natural semantics.
- An appropriate level of granularity as required.
- It should allow appropriate assumptions about independence.
- An intelligent, meaningful dialogue and knowledge representation manage.
- Easy and intelligent tracing of aggregation and propagation of uncertainty.
- It should be store the reasons for its support for or arrival at hypotheses.
- Second-order measures of uncertainty.
- It must be able to resolve conflict.
- For large or real-time knowledge-based system, heuristic control strategies must be possible.
- Cognitive emulation of how experts handle uncertainty may be desirable in some cases and should be possible.
- Its logic should be context dependent.

At this point it is appropriate to remark on granularity: RULES ARE SUMMARIES. In other words the chunking of knowledge represents abstraction, and often this is how human experts reduce or eliminate uncertainty. This is very like the idea of disposition – implicit quantifiers (Graham & Jones, 1988). Experienced experts often insist that they use a rule of thumb that assigns linguistic labels to ranges of numerical inputs.

Uncertainty expresses a measure of confidence. The three basic methods of representing uncertainty are *numeric*, *graphic*, and *symbolic* (Turban, 1992).

Numeric: The most common method of representing uncertainty is numeric using a scale with two extreme numbers. For example, 0 may be used to represent complete uncertainty while 1 or 100 represents complete certainty. Although such representation seems to be easy to some people, it may be very difficult to others. For example, ship

speed, for a given distance and travelling time, may vary considerable depending on waves and weather conditions.

Graphic: Although many experts can describe uncertainty in terms of numbers, such as "it is 85 percent certain that …", some have difficulties in doing so. By using horizontal bars, for example, it is possible to assist experts in expressing their confidence in certain events. Such a bar is shown in Figure 5.1. Experts are asked to place markers somewhere on the scale. Thus, expert A may express very little confidence of the likelihood of occurrence of an event, whereas expert B has much more confidence.

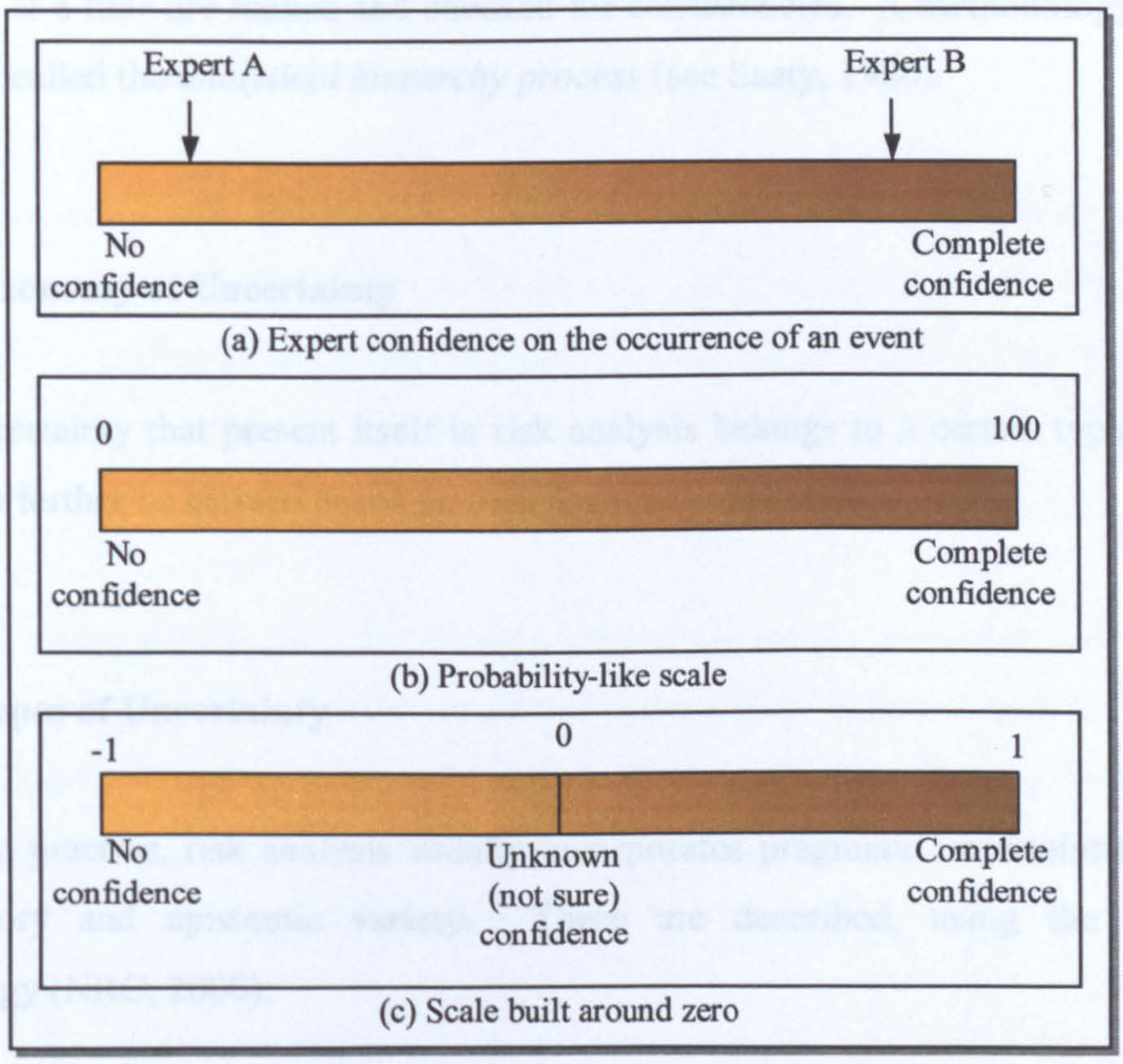


Figure 5.1: Confidence scales for graphic representation of uncertainty

Even though some experts prefer graphic presentation, the graphs are not as accurate as numbers. Another problem is that most experts do not have experience in marking graphic scales (or setting numbers on the scale). Thus, many experts, especially managers prefer ranking over graphic or numeric methods.

Symbolic: There are several ways to represent uncertainty by using symbols. Most experts use a *Likert scale* approach to express their opinion. For example, an expert may be asked to assess the likelihood of occurrence of an event on a five-point scale: very unlikely, unlikely, neutral, likely, and very likely. *Ranking* is a very popular approach among experts with non-quantitative preferences. Ranking can be either ordinal (i.e., listing items by the order of their importance) or cardinal (ranking complemented by numeric values). Managers are often comfortable with ordinal ranking. When the number of items to be ranked is large, people may have a problem with ranking and also tend to be inconsistent. One method that can be used to alleviate this problem is a pair-wise comparison combined with a consistency checker in which two items at a time are ranked and checked for consistencies. A methodology for such ranking is called the *analytical hierarchy process* (see Saaty, 1980).

5.4 A Taxonomy of Uncertainty

Every uncertainty that present itself in risk analysis belongs to a certain type or types, which can further be classed based on their form or parameter.

5.4.1 Types of Uncertainty

In modern practice, risk analysis usually incorporates pragmatic uncertainties of both the aleatory and epistemic variety. These are described, using the following terminology (NRC, 2000):

5.4.1.1 Aleatory uncertainty

Aleatory uncertainty is attributed to inherent randomness, natural variation, or chance outcomes in the physical world; in principle, this uncertainty is irreducible as the knowledge of experts cannot be expected to reduce aleatory uncertainty although their knowledge may be useful in getting a better estimate of the magnitude of the variability.

This uncertainty is sometimes called, random variability, stochastic variability, natural variability, objective uncertainty, or external uncertainty (Parry, 1996 and NRC, 2000).

Sources of aleatory uncertainty can commonly be singled out from other contributors to uncertainty by their representation as randomly distributed quantities that can take on values in an established or known range, but for which the exact value will vary by chance from unit to unit or from time to time. The mathematical analysis most commonly used for aleatory uncertainty is probabilistic. When substantial experimental data are available for estimating a distribution, there is no debate that the correct treatment modelling for aleatory uncertainty is by way of a probability distribution.

5.4.1.2 Epistemic uncertainty

Epistemic uncertainty is attributed to lack of data, lack of knowledge about events and processes that limits our ability to model the real world; in principle, this uncertainty is reducible with sufficient study and therefore, expert judgement may be useful for its reduction. This uncertainty is sometimes called, subjective or internal uncertainty (Parry, 1996 and NRC, 2000).

Epistemic uncertainties can be divided into two major sub-categories: model uncertainty and parameter uncertainty (See Figure 5.2). Model uncertainty has to do with the degree to which a chosen mathematical model accurately mimics reality; parameter uncertainty has to do with the precision with which model parameters can be estimated. The mathematical analysis used for treating epistemic uncertainty is typically non-probabilistic.

5.4.2 Sub-Categories of Uncertainty

Uncertainties may arrive singly or in groups, whether data is collected manually or automatically (Graham & Jones, 1988). Policy and risk analysis community has classified uncertainty into quantity/parameter and model-based uncertainty (Morgan & Henrion, 1990). Figure 5.3 illustrates this classification.

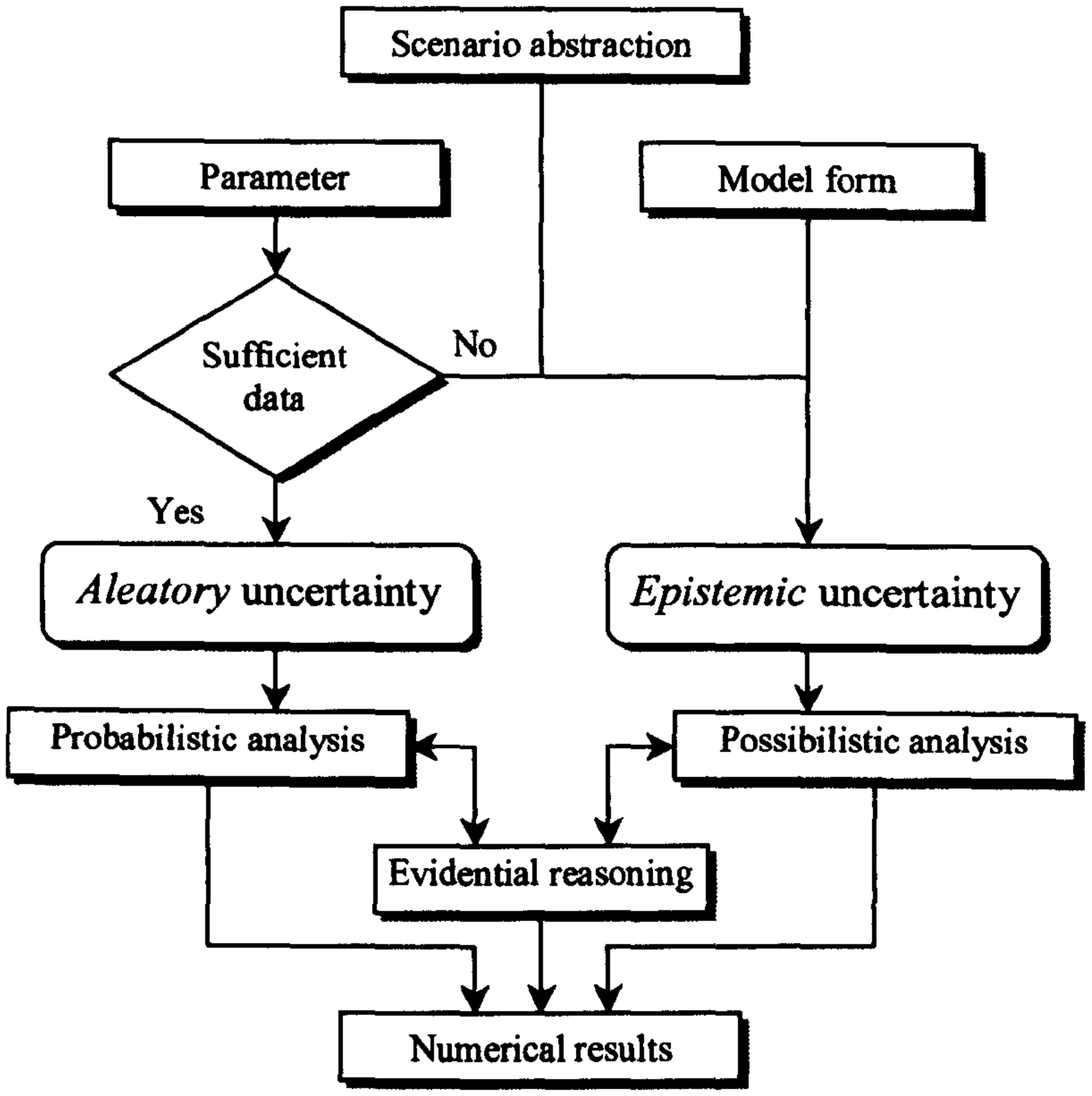


Figure 5.2: Processing and treatment of types of uncertainty in risk analysis

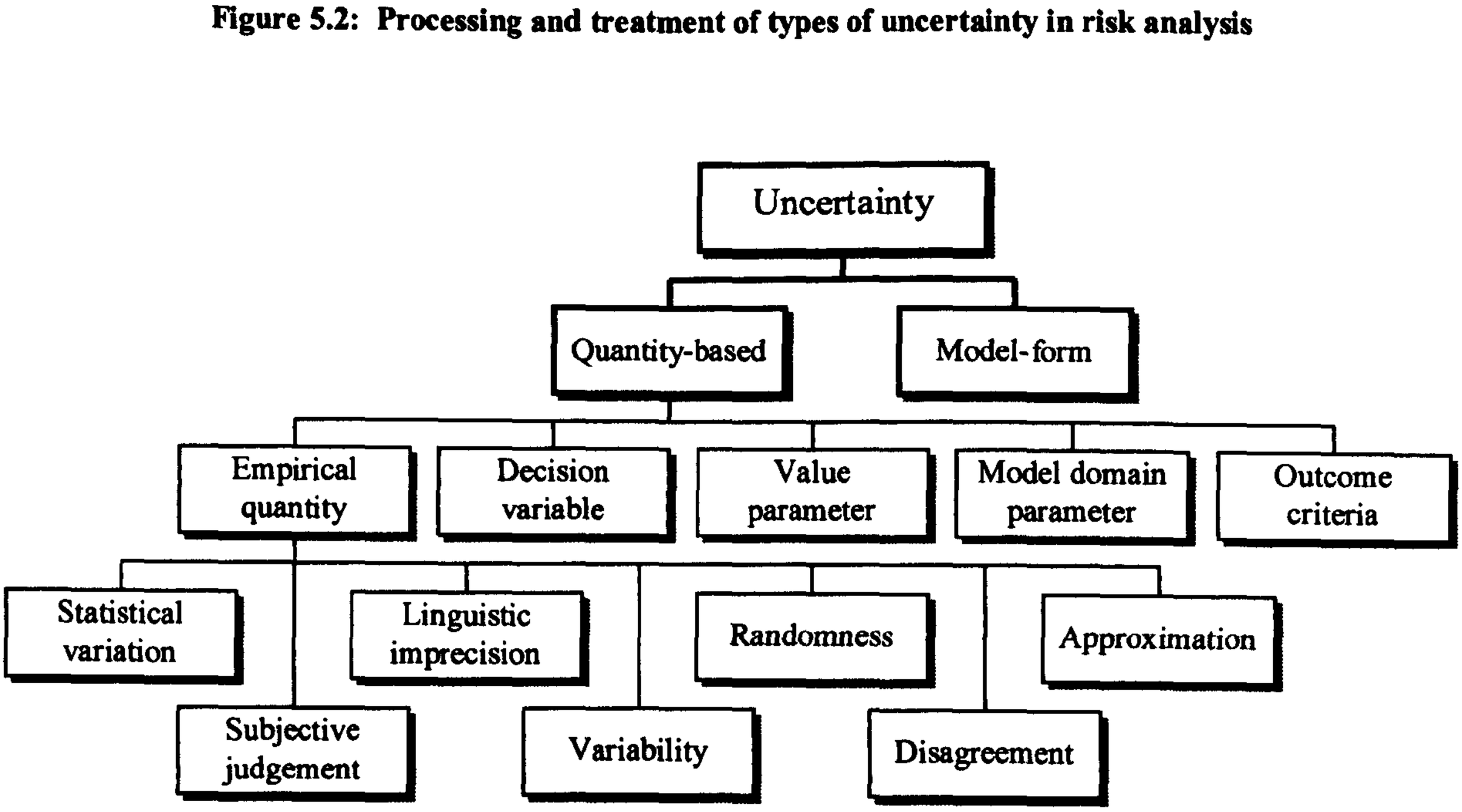


Figure 5.3: Uncertainty classification in risk analysis

5.4.2.1 Parametric-Based

The *parametric/quantity-based* group is given in Table 5.1, which briefly defines/explains each sub-classification in the group (Morgan & Henrion, 1990).

Table 5.1: Quantity type uncertainty definitions in policy and risk analysis

Uncertainty	Sub-classification	Definition/explanation
Empirical quantity	Statistical variation	Arises from random error in direct measurements of a quantity
	Subjective judgment	Teamed with systematic error as the difference between the true value of a quantity of interest and the value to which the mean of the measurements converges as more measurements are taken
	Linguistic imprecision	Refers to quantities that are not well-specified and could not be empirically measured in principle
	Variability	Refers to quantities that are variable over time and space
	Randomness	Uncertainty that is irreducible even in principle
	Approximation	Difference between the assumed quantity value and the real-world value
Decision variable	n/a	Quantity over which the decision maker exercises direct control
Value parameter	n/a	Parameter that represents aspects of the preferences, such as those giving benefits, of the decision maker
Model domain parameter	n/a	Specifies the domain or scope of the system being modelled
Outcome criteria	n/a	Variable used to rank or measure the desirability of possible outcomes

All of the quantity-based uncertainties vary in magnitude, location, or time of occurrence as well as in their interactions with each other and have the ability to accumulate during the whole process, from data collection through all the different assumptions and uncertainties connected to the applied methodology and models. Properly designed studies will specify sample sizes that are sufficiently large to detect important signals. Unfortunately, many studies have sample sizes that are too small to detect anything but gross changes (Smith & Shugart, 1994; Peterman, 1990).

5.4.2.2 Model-Form

Uncertainty associated with the *model-form* refers to the approximations that a model provides to a real-world system. In other words, it represents that uncertainty about the degree to which a model is an adequate representation of the world for the problem at hand. Model form uncertainty is differentiated from (quantity form) model domain parameter uncertainty by referring to the actual model itself as opposed to the quantities assumed in the model (Morgan & Henrion, 1990). Any model is unavoidably (and by definition) a simplification of reality. A real-world system contains phenomena or behaviours that cannot be produced by even the most detailed model. The difference between the real-world system and such a model is "model form uncertainty".

Opinions of experts on the appropriate conceptual model configuration may differ. Sources of uncertainty that arise primarily during development and application of models include:

- The structure of process models due to errors introduced by *oversimplified representations* of reality (e.g., representing a three-dimensional strut and bracket with a two-dimensional mathematical model).

- The description of the *relationship between two or more variables* in empirical models (e.g., incorrectly inferring the basis for correlations between offshore structure and ship-based activity).

Moreover, any model can be incomplete if it excludes one or more relevant variables (e.g., relating ignition to fire without considering the effect of gas release on both those exposed to ignition and those unexposed), uses surrogate variables for ones that cannot be measured (e.g., using wind speed at the nearest port as a proxy for wind speed at the offshore facility), or fails to account for correlations that cause seemingly unrelated events to occur much more frequently than would be expected by chance (e.g., two separate components of a marine engine are both missing a particular washer because the same newly hired assembler carried out the assemble work on them).

5.5 Theoretical Methods of Handling Uncertainty

Methods for analysing and describing uncertainty can range from simple to complex for which some appropriate mathematical treatments need to be explored. Selecting the appropriate statistics depends on the amount of data available and the degree of detail required. Often included are methods of combining and propagating uncertain information within a mathematically rigorous structure. More complicated methods become necessary when multiple sources of uncertainty must be combined (Phillips & LaPole, 2003).

Some of the more common approaches to representing and handling uncertainty used by various reasoning systems today are based on (Klir, 1994; Dubois & Prade, 1988; Graham & Jones, 1988; Baldwin, 1996):

- Probabilistic analysis
    - Classical set theory
    - Probability theory
    - Bayes' theory
- Evidential reasoning
    - Dempster-Shafer theory
    - Mass assignment theory
- Possibilistic analysis
    - Interval mathematics
    - Possibility theory
    - Fuzzy set theory

As with the reasoning technologies they are typically associated with, each approach has various strengths and characteristics regarding its representational capabilities. Each has different representational characteristics and propagation models. When a modelling approach is used, sensitivity analysis can be used to evaluate how model output changes with changes in input variables, and uncertainty propagation can be analysed to examine how uncertainty in individual parameters can affect the overall uncertainty of the assessment.

5.5.1 Probabilistic Reasoning Under Uncertainty

The calculation of one or more point estimates is one of the most common approaches to presenting analysis results; point estimates that reflect different aspects of uncertainty can have great value if appropriately developed and communicated (EPA, 1996). Nonetheless, one aspect that most uncertainty management schemes agree on is that single point values of risk are worse than representing both variability and uncertainty. Common ways to more adequately express uncertainty are:

- To represent the level of uncertainty by modifying the probability for propositions.
- To treat it as a separate entity that is affixed to each probability.
- To represent it as a range of opinions.

Opinion pooling is particularly effective at assessing the usefulness of information produced by human experts (Kahn, 2004). When applied in a hierarchical model, it can provide a natural and flexible way to incorporate dependencies among experts while acknowledging that they may justifiably disagree. In these models, uncertainty in a probabilistic value is represented by a collection of estimates of the quantity and the degree of certainty or uncertainty is measured by means of the distribution of values in the collection of estimates.

5.5.1.1 Probability Theory

If an event has yet to occur, and there is more than one possible outcome, then there is clearly some uncertainty about its outcome. Probability theory provides an ideal way of handling such uncertainties. Probability gives a measure of the likelihood of an event resulting in one possible outcome under one set of conditions. Also, the outcome itself is restricted to a binary state {*true*, *false*}. Given some history of previous outcomes for this type of event one can determine a measure of the probability of this event being true when it occurs. If there is no history of previous outcomes and one has no insight into

the event itself, then there is total uncertainty with regard to the event outcome. This complete uncertainty, which is represented by a uniform prior probability distribution, may be assigned to each of the possible outcomes.

In almost all cases the uniform prior probabilities are unrepresentative of the actual outcome probabilities. A better method of obtaining these probabilities is by taking a frequency of occurrence approach where it is assumed that the number of times the event is encountered tends to infinity. Such an approach is more accurate than a uniform prior probability approach but requires a large history of event outcomes.

For any event A, one can assign a number $P(A)$, called the *probability of the event A*. This number satisfies the following three conditions that act as the *axioms of probability* (Papoulis, & Pillai, 2002):

(i) $P(A) \geq 0$

(ii) $P(X) = 1$, where X is the (finite) sample space.

(iii) If $A \cap B = \varnothing$, then $P(A \cup B) = P(A) + P(B)$

Note that probability axiom (iii) states that if A and B are *mutually exclusive* events, the probability of their union is the sum of their probabilities.

The following conclusions follow from these axioms:

(a) Since $A \cup \bar{A} = X$, in using probability axiom (ii) one obtains $P(A \cup \bar{A}) = P(X) =$ 1. But $A \cap \bar{A} \in \varnothing$ and in using probability axiom (iii), one obtains:

$$P(A \cup \bar{A}) = P(A) + P(\bar{A}) = 1 \qquad (5.1)$$

(b) Similarly, for any A, $A \cap \{\varnothing\} = \{\varnothing\}$. Hence it follows that $P(A \cup \{\varnothing\}) = P(A) + P(\varnothing)$. But $A \cup \{\varnothing\} = A$, and thus:

$$P(\varnothing) = 0 \qquad (5.2)$$

Whilst such a probability approach is useful for many simple cases, a more complicated problem arises when events are not mutually exclusive. (and this means that Equation 2.7 in Section 2.5.6 of Chapter 2 applies). In these cases *conditional probabilities* can be calculated from Equation 5.3 (the rule of conditional probabilities):

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \tag{5.3}$$

where | denotes "given", so that $P(A|B)$ is the conditional probability that A is true given that B is true.

In one way the conditional probability equation gives some elementary reasoning under uncertainty. There may be the uncertainty as to whether A is true, but if it is known that B is true, then the conditional probability rule of Equation 5.3 can at least estimate the probability $P(A|B)$.

The rule of conditional probability is extended to give the rule of total probabilities. This is shown in Equation 5.4.

$$P(B) = P(B|A).P(A) + P(B|\bar{A}).P(\bar{A}) \tag{5.4}$$

The rule of total probabilities provides more power in reasoning about discrete events that are not mutually exclusive.

5.5.1.2 Bayes' Theory

Bayes' theorem extends the rules of conditional probability and total probability. It provides a means of dealing with inference and belief updating in uncertainty situations. As can be read from Equation 5.5, the theorem defines a method of calculating the conditional, or *posterior*, probability $P(H|E)$ from known probability $P(E|H)$ and prior probabilities $P(E)$ and $P(H)$.

Basically, Bayes theorem enables the probability distribution across all independent and mutually exclusive H_i given new evidence E to be updated.

$$P(H_i|E) = \frac{P(E \mid H_i).P(H_i)}{\sum_{n=1}^{k} P(E|H_n)P(H_n)} \tag{5.5}$$

where;

$P(H_i|E)$ = probability that hypothesis H_i is true given evidence E,

$P(E|H_i)$ = probability of observing evidence E given hypothesis H_i,

$P(H_i)$ = a priori probability of hypothesis H_i being true, and

k = number of hypotheses.

In practice $P(E|H_i)$ in Equation 5.5 may be computationally expensive to calculate if all evidence is not independent. If the assumption is made that all evidence is independent this is referred to as *naïve Bayes*.

If on the other hand new evidence e, is encountered and E and e are not independent, then conditional joint probabilities needs to be taken into account in order to calculate $P(H_i|E, e)$. This is shown in Equation 5.6.

$$P(H|E, e) = P(H|E).\frac{P(e \mid E, H)}{P(e \mid E)} \tag{5.6}$$

where;

$P(H|E)$ = probability that hypothesis H is true given evidence E,

$P(H|E, e)$ = probability that H is true given E and new evidence e,

$P(e|E, H)$ = probability of observing e given H and E, and

$P(e|E)$ = probability of observing e given E.

The problem with modifying simple Bayes theorem (Equation 5.5) to the conditional evidence case (Equation 5.6) is in calculating the joint probabilities. For n pieces of evidence there are 2^n joint probabilities to be calculated. For reasons of computational

speed, storage and knowledge acquisition, the conditional evidence case of Bayes theorem is frequently intractable.

5.5.2 Evidential Reasoning Under Uncertainty

This section looks at two key uncertainty reasoning theories which use more humanistic terms in dealing with information. These theories, namely Dempster-Shafer theory and the more sophisticated mass assignment theory, use terms such as evidence, belief and plausibility.

5.5.2.1 Dempster-Shafer Theory

In a finite discrete space, Dempster-Shafer theory can be interpreted as a generalization of probability theory where probabilities are assigned to *sets* as opposed to mutually exclusive singletons. In traditional probability theory, evidence is associated with only one possible event. In Dempster-Shafer theory, evidence can be associated with multiple possible events, e.g., sets of events. As a result, evidence in this theory can be meaningful at a higher level of abstraction without having to resort to assumptions about the events within the evidential set. Where the evidence is sufficient enough to permit the assignment of probabilities to single events, the Dempster-Shafer model collapses to the traditional probabilistic formulation. One of the most important features of this theory is that the model is designed to cope with varying levels of precision regarding the information and no further assumptions are needed to represent the information. It also allows for the direct representation of uncertainty of system responses where an imprecise input can be characterized by a set or an interval and the resulting output is a set or an interval.

Belief, *Bel* **and Plausibility,** *Pl*

Dempster-Shaffer theory allows for the allocation of probability-like weights to a set of events to be made in a way that allows statements of ignorance about likelihood of some

of the events. From the allocation of weights, two numbers that represent the uncertainty data can be obtained: the degree to which an event is supported by evidence (*belief*), and the degree to which there is a lack of evidence to the contrary (*plausibility*). These two numbers are the basis on which any belief-based decision is made.

For any event A, the degree of belief in A, $Bel(A)$, and degree of plausibility in A, $Pl(A)$, must satisfies the following conditions that act as the *axioms of evidence* (Shafer, 1976):

(i) $Pl(A) \geq Bel(A) \geq 0$

(ii) $Bel(X) = Pl(X) = 1$, where X is the (finite) sample space.

(iii) $Bel(A) + Pl(\bar{A}) = 1$

(iv) $Bel(A \cup B) \geq Bel(A) + Bel(B)$, if A and B are mutually exclusive events

(v) $Pl(A \cup B) \leq Pl(A) + Pl(B)$, if A and B are mutually exclusive events

The following conclusions follow from these axioms:

(b) Since $A \cup \bar{A} = X$, in using evidence axiom (ii) one obtains $Bel(A \cup \bar{A}) = Bel(X) = 1$. But $A \cap \bar{A} \in \varnothing$ and in using evidence axiom (iv), one obtains $Bel(A \cup \bar{A}) = 1 \geq Bel(A) + Bel(\bar{A})$. Thus:

$$Bel(A) + Bel(\bar{A}) \leq 1 \tag{5.7}$$

(c) Similarly, for any A, $A \cap \{\varnothing\} = \{\varnothing\}$. Hence it follows that $Bel(A \cup \{\varnothing\}) = Bel(A) + Bel(\varnothing)$. But $A \cup \{\varnothing\} = A$, and thus:

$$Bel(\varnothing) = 0 \tag{5.8}$$

(d) Since $A \cup \bar{A} = X$, in using evidence (ii) one obtains $Pl(A \cup \bar{A}) = Pl(X) = 1$. But $A \cap \bar{A} \in \varnothing$ and in using evidence (iv), one obtains $Pl(A \cup \bar{A}) = 1 \leq Pl(A) + Pl(\bar{A})$. Thus:

$$Pl(A) + Pl(\bar{A}) \geq 1 \tag{5.9}$$

(e) Similarly, for any A, $A \cap \{\varnothing\} = \{\varnothing\}$. Hence it follows that $Pl(A \cup \{\varnothing\}) = Pl(A) + Pl(\varnothing)$. But $A \cup \{\varnothing\} = A$, and thus:

$$Pl(\varnothing) = 0 \tag{5.10}$$

Within a belief-plausibility interval lies the precise probability of the event A (in the classical sense) such that:

$$Bel(A) \leq P(A) \leq Pl(A) \tag{5.11}$$

A belief measure (or a plausibility measure) becomes a *probability measure* when all focal elements are *singletons* or the evidences are disjoint. In this case:

$$Bel(A) = P(A) = Pl(A) \tag{5.12}$$

This corresponds to classical probability, where all the probabilities, $P(A)$ are uniquely determined for all subsets A of the universal set X (Ramer, 1987).

The definition of *conditional belief* is different from the definition of conditional probability as given by Equation 5.13 (Halpern & Fagin, 1992):

$$Bel(A|B) = \frac{Bel(A \cup \overline{B}) - Bel(\overline{B})}{1 - Bel(\overline{B})} \tag{5.13}$$

The *conditional plausibility* of A given B is (Halpern & Fagin, 1992):

$$Pl(A|B) = \frac{Pl(A \cap B)}{Pl(B)} \tag{5.14}$$

If *Bel* is a Bayesian belief function, then:

$$Bel(A|B) = \frac{Bel(A \cap B)}{Bel(B)} = Pl(A|B) \tag{5.15}$$

which coincides exactly with the classical conditional probability $P(A|B)$ defined in Equation 5.3.

Probability Assignment, *m*

Dempster-Shafer theory also adds a third measure called the *basic probability assignment (bpa)* that is often denoted by *m*, which attempts to relate the measures *Bel* and *Pl* directly to probability theory. This theory's *m* is unlike the basic probability distribution, which is defined over the universe *X*, in that *m* is defined over the power set of *X*, $P(X)$. That is:

$$m : P(X) \rightarrow [0, 1] \tag{5.16}$$

such that, $m(\varnothing) = 0$ and $\sum_{A \in P(X)} m(A) = 1$.

Every set for $A \in P(X)$ for which $m(\varnothing) > 0$ is usually called a focal element of *m*. As the name suggests, focal elements are subsets of *X* on which the available evidence focuses. When *X* is finite, m can be characterised by a list of its focal elements *A* with the responding values $m(A)$. The pair $\langle \Im, \text{m} \rangle$, where $\Im$ and *m* denote a focal element and the associated basic assignment, respectively is often called a *body of evidence* (Türksen, 2004).

A subset of $P(X)$ containing only the singleton sets, $\{x\}$ $\forall x \in X$, is analogous to the basic probability density function. The basic probability density function is therefore a restricted case of the Dempster-Shafer theory basic probability assignment.

It is important to note that the definition of *m* does not require that $m(X) = 1$ (as the basic probability density function does) or that $m(A) \leq m(B)$ when $A \subset B$. The later of these two cases is important because it gives us more representation power then the basic probability density function. Furthermore, no relationship between $m(A)$ and $m(\bar{A})$ is required.

Bel, *Pl* and *m* are related by Equations 5.17 and 5.18, where *A* is a subset of *P*(*X*)

$$Bel(A) = \sum_{B \subseteq A} m(B) \tag{5.17}$$

$$Pl(A) = \sum_{B \cap A \neq \varnothing} m(B) \tag{5.18}$$

The inverse procedure is also possible. Given, for example, a belief measure *Bel*, the corresponding basic probability assignment *m* is determined for all $A \in P(X)$ by the formula:

$$m(A) = \sum_{B \subseteq A} (-1)^{|A-B|} Bel(B) \tag{5.19}$$

Total ignorance (Türksen, 2004), is expressed in terms of the basic assignment by $m(X) = 1$ and $m(A) = 0$ for all $A \neq X$. In terms of the corresponding *Bel* measure, it is exactly the same: $Bel(X) = 1$ and $Bel(A) = 0$ for all $A \neq X$. However, it is quite different in terms of the corresponding *Pl* measure: $Pl(\varnothing) = 0$ and $Pl(A) = 0$ for all $A \neq \varnothing$.

Dempster Evidence Combination

Evidence obtained in the same context from two independent sources, e.g., from two experts in the field of inquiry, and expressed by two basic assignments m_1 and m_2 on some power set *P*(*X*) must be appropriately combined to obtain a joint basic assignment $m_{1,2}$. In general, evidence can be combined in various ways (Sentz, & Ferson, 2002), some of which may take into consideration the reliability of the sources and other relevant aspects. The standard way of combining evidence is expressed by the formula:

$$m_{1,2}(\mathrm{C}) = \frac{\sum_{A \cap B = C} m_1(A).m_2(B)}{1 - \sum_{A \cap B = \varnothing} m_1(A).m_2(B)} \quad , C \neq 0 \tag{5.20}$$

Equation 5.20 is known as *Dempster's rule of combination*. According to this rule, the degree of evidence $m_1(A)$ from the first source that focuses on set A $\in P(X)$ and the degree of evidence $m_2(B)$ from the second source that focuses on B $\in P(X)$ are combined by taking the product $m_1(A)$. $m_2(B)$, which focuses on the intersection $A \cap B$. This is exactly the same way in which the joint probability distribution is calculated from two independent marginal distributions and, consequently, it is justified on the same grounds (Türksen, 2004).

In order to obtain a normalised basic assignment $m_{1,2}$, the denominator of Equation 5.20 acts as a normalising factor. Some of the intersections of Dempster's combination rule may be empty and the renormalisation of the final probability assignment to redistribute probability assigned to the empty set is a contentious operation. The theory of mass assignment (Baldwin, 1992) overcomes this problem through the mass assignment definition and combination methods.

5.5.2.2 Mass Assignment Theory

Mass assignment (Baldwin, 1992 and 1996) unifies probability, possibility and fuzzy sets into a single theory. Since this is a large topic for just one section, only the underlying theory of mass assignment with respect to probability theory will be considered here. Mass assignment approach to fuzzy sets, and hence possibility theory, can be found in Section 8.4.1.1. of Chapter 8.

The mass assignment is similar to Dempster-Shafer theory's probability assignment, but is extended to enable mass to be assigned to the empty set. Equation 5.21 defines the mass assignment m over the powerset of universe X, $P(X)$.

$$m : P(X) \rightarrow [0, 1] \tag{5.21}$$

such that, $m(\varnothing) \geq 0$ and $\sum_{A \in P(X)} m(A) = 1$

A mass assignment over the power set $P(X)$ defines a family of probability distributions over the universe X. The most general mass assignment defines *complete uncertainty* and is shown in Equation 5.22. The most specific mass assignment defines *complete certainty* and is shown in Equation 5.33.

$$m(X) = 1 \text{ and } m(A) = 0, \forall A \in P(X), A \neq X \tag{5.22}$$

$$m(A) = 1 \text{ and } m(B) = 0, \forall B \in P(X), B \neq A \tag{5.23}$$

Note in Equation 5.21 the special condition $m(\varnothing) \geq 0$ which is less restrictive than the $m(\varnothing) = 0$ restriction applied to probability assignment. The probability assignment is therefore a special case of the mass assignment. The mass assignment is said to be *complete* when $m(\varnothing) = 0$ and *incomplete* otherwise. As with probability assignment, incompleteness arises from inconsistency between two pieces of evidence.

The *focal elements A* of $P(X)$ are defined as those elements of $P(X)$ which have non-zero mass. In contrast to probability assignment, $\varnothing$ can be a focal element.

A mass assignment across focal elements is expressed as in Equation 5.24 where $\mathfrak{I}_i$ is the i^{th} focal element and m_i is the mass assignment to $\mathfrak{I}_i$.

$$m = \mathfrak{I}_i : m_i \mid i = 1, \ldots, n \tag{5.24}$$

Given a universe X the inverse $\bar{m}$ of mass assignment m is defined by Equation 5.25.

$$\bar{m} = X - \mathfrak{I}_i : m_i \mid i = 1, \ldots, n \tag{5.25}$$

The properties of mass assignment also follow the basic rules of Boolean algebra (See Table 2.6 of Chapter 2).

Mass assignment and probability distributions

A mass assignment represents a family of probability distributions. It is often useful to generate one specific probability distribution called the *least prejudiced distribution*. As the name suggests, this distribution is the case when there is the assumption that mass assigned to a set A is equally likely to belong to any element in A. As a result, mass assigned to A can be distributed equally across all elements in A. More formally, given a mass $m(A)$:

$$m(\{B\}) = \frac{m(A)}{|A|} \quad \forall B \in A \tag{5.26}$$

In order to obtain a least prejudiced distribution of mass to generate a single probability distribution, masses assigned to singletons $\{B\}$ are now summed and assigned as probabilities for B. A probability $P(B)$ is therefore defined as:

$$P(B) = \sum_{B \in A, A \in P(X)} \frac{m(A)}{|A|} \tag{5.27}$$

5.5.3 Possibilistic Reasoning Under Uncertainty

This section looks at the theories of Possibility and fuzzy set for reasoning about an epistemic state. Both theories are associated with terms such as fuzzy, possibility and necessity. The rules of these theories utilises max/min or max/product calculus, which are not found in probability theory.

5.5.3.1 Possibility Theory

A special branch of evidence theory that deals with bodies of evidence whose focal elements are nested is referred to as *possibility theory*. Special counterparts of belief and plausibility measures in possibility theory are called *necessity* and *possible measures*, respectively.

The possibility measure, Π, is defined in the powerset $P(X)$ or universe X and is a mapping from $P(X)$ to the unit interval [0, 1]:

$$\Pi : P(X) \rightarrow [0, 1] \tag{5.28}$$

A *possibility distribution*, π, on the universe X can be defined such that the following mapping holds:

$$\pi : X \rightarrow [0, 1] \tag{5.29}$$

and π is defined for all $x \in X$ as,

$$\pi(x) = \Pi(\{x\}) \tag{5.30}$$

The necessity measure is the dual of possibility and is defined in terms of the possibility measure.

$$\mathrm{N} : P(X) \rightarrow [0, 1] \tag{5.31}$$

For any set A, the possibility of A, $\Pi(A)$, and necessity of A, $N(A)$, must satisfies the following conditions that act as the *axioms of possibility*:

(i) $\Pi(A) \geq N(A) \geq 0$

(ii) $N(X) = \Pi(X) = 1$, for any collection of subsets on the universal set X.

(iii) $N(A) + \Pi(\bar{A}) = 1$

(iv) $\Pi(A) + \Pi(A) \geq 1$

(v) $N(A) + N(\bar{A}) \leq 1$

(vi) $\Pi(A \cup B) = max[\Pi(A), \Pi(B)]$

(vii) $N(A \cap B) = min[\mathrm{N}(A), \mathrm{N}(B)]$

The concept of *conditional possibility distribution function* is essential for defining possibilistic independence. Two marginal possibilistic body of evidence are said to be

independent if and only if the conditional possibilities do not defer from the corresponding marginal probabilities. This is expressed by the equations:

$$\Pi(A|B) = \Pi(A) \tag{5.32}$$

$$\Pi(B|A) = \Pi(B) \tag{5.33}$$

for all $x \in X$ and all $y \in Y$, where $\Pi(A|B)$ and $\Pi(B|A)$ denote conditional possibilities on $X \times Y$.

For more information on possibility theory, see Laviolette & Seaman (1994) and Dubois, & Prade (1988).

5.5.3.2 Fuzzy Set Theory

Fuzzy sets theory defines real-world concepts and deals with uncertainty that may be due to human interpretation or machine measurement. The linguistic term *warm*, for example, has different meanings for different people, and is an example of fuzziness due to human interpretation. Measurement of a physical quality, on the other hand, may be restricted to a low precision measure by using inexpensive measurement devices, and leads to fuzziness in the measured quantity.

A classical set can be regarded as a grouping together of elements, all of which have at least one common characteristic. If an element possesses this characteristic, it belongs to the set. If an element does not possess this characteristic, it does not belong to the set. In fuzzy set theory, the set is no longer restricted to this binary (yes/no) definition of set membership, but rather allows a graduated definition of membership. This means that a degree of membership to a set can be specified for each element. This set is then referred to as a *fuzzy set*.

A fuzzy set F over the universe X is characterized by its membership function $\mu_F(x)$. The membership function μ is defined in Equation 5.34.

$$\mu : X \rightarrow [0, 1] \tag{5.34}$$

where $x \in X$.

For $x \in X$, a number of operations have been defined for fuzzy sets including *intersection*, *union* and *complement*, as given by Equations 5.35, 5.36 and 5.37, respectively.

$$\mu_{A \cap B}(x) = min[\mu_A(x), \mu_B(x)] \tag{5.35}$$

$$\mu_{A \cup B}(x) = max[\mu_A(x), \mu_B(x)] \tag{5.36}$$

$$\mu_{\bar{A}}(x) = 1 - \mu_A(x) \tag{5.37}$$

Zadeh's fuzzy set algebra is defined in more detail in (Kosko, 1994).

A fuzzy set F defined on universe X also induces a possibility distribution on X such that,

$$\mu_F(A) = \pi(A), \forall A \in X \tag{5.38}$$

In this way a fuzzy set and its corresponding possibility distribution are linked.

5.6 Comparison and Selection of Theory for Inference Processing

Inference processes generally concern a situation (see Figure 5.4), a part of reality that has an interest. In building an understanding of some portion of reality, models are created, which consist of simplified representations of situations, in terms of a limited number of variables, representing distinct aspects of the situation, and dependencies between those variables (Groen & Mosleh, 2001).

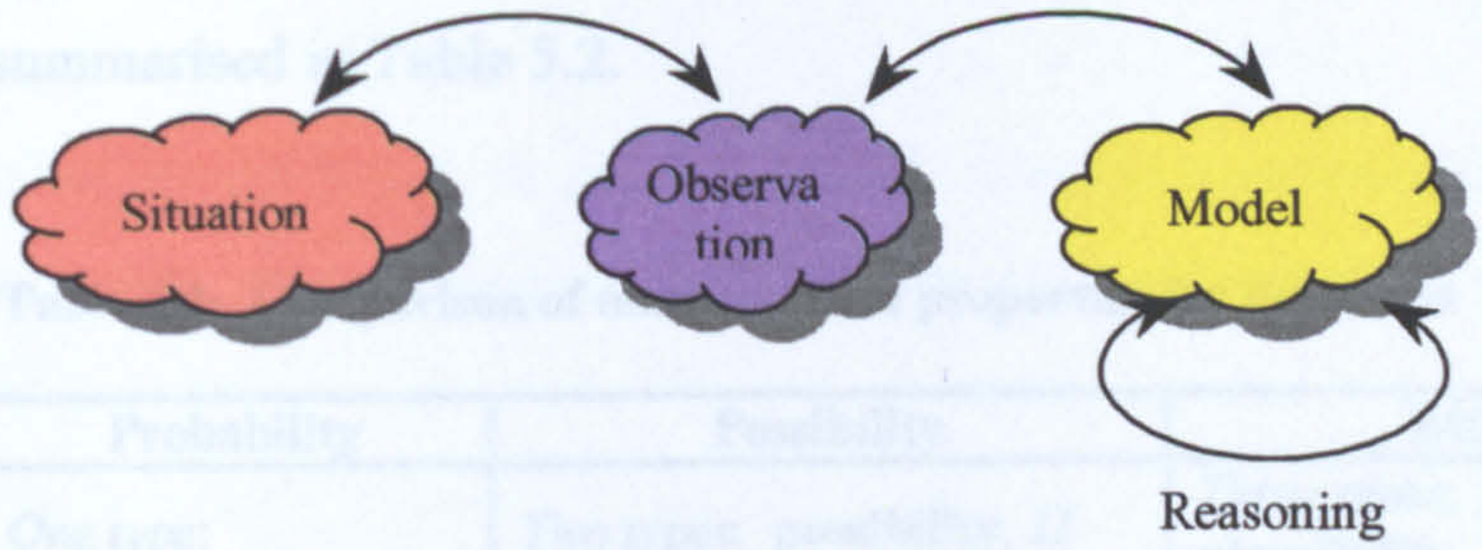


Figure 5.4: Idealised view of inference process

In order to reason through a risk-based model under conditions of uncertainty, it is important to understand the similarities and differences between probability theory and possibility theory. Both theories form the basis of the more restrictive evidence theory that can be effectively summarised by the representative Figure 5.5.

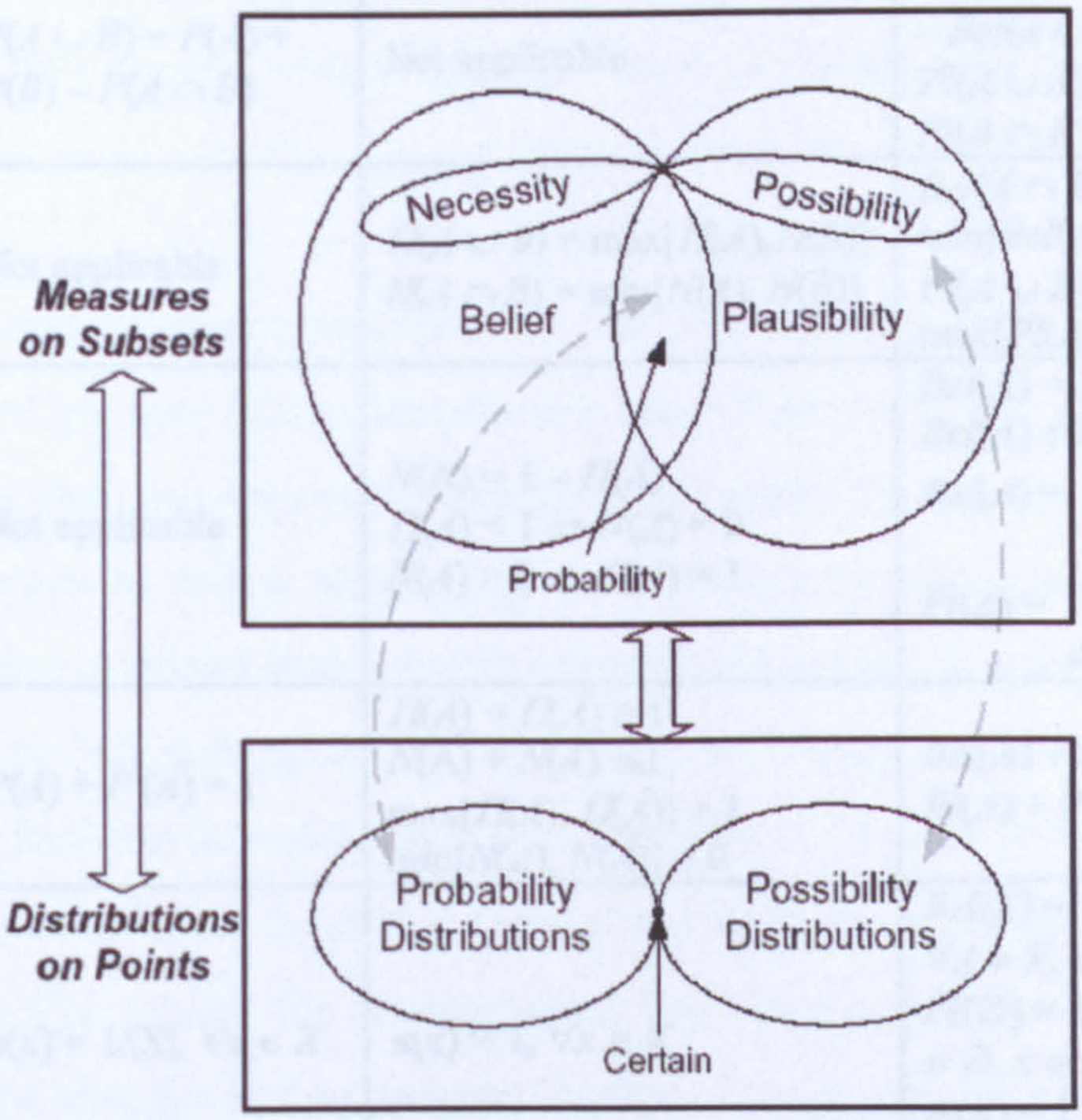


Figure 5.5: Summary of Dempster-Shafer evidence theory

Hence, evidence theory can be used as the *unified theory* to handle both types of uncertainty satisfactorily.

Basic mathematical properties of all three theories (i.e., probability, possibility and evidential) are summarised in Table 5.2.

Table 5.2: Comparison of mathematical properties for finite sets

	Probability	**Possibility**	**Evidence**
Measures	*One type*: **probability**, P	*Two types*: **possibility**, Π and **necessity**, N	*Three types*: **belief**, Bel, **plausibility**, Pl and **probability assignment**, m
Body of evidence	Consists of *singletons*	Consists of a *family of nested subsets*	When events in X are *singletons*: $Bel(A) = P(A) = Pl(A)$ When X contains only *nested subsets*: $Bel(A) = N(A)$ and $Pl(A) = \Pi(A)$
Unique representation	$p : X \rightarrow [0, 1]$ via the formula $P(A) = \sum_{x \in A} p(x)$	$\pi : X \rightarrow [0, 1]$ via the formula $\Pi(A) = \max_{x \in A} \pi(x)$	$m : X \rightarrow [0, 1]$ via the formula $m(A) = \sum_{x \in P(A)} m(x)$
Normalization	$\sum_{x \in X} p(x) = 1$	$\max_{x \in X} \pi(x) = 1$	$\sum_{x \in P(X)} m(x) = 1$
Additivity	$P(A \cup B) = P(A) + P(B) - P(A \cap B)$	Not applicable	$Bel(A \cup B) \geq Bel(A) + Bel(B) - Bel(A \cap B)$ $Pl(A \cup B) \leq Pl(A) + Pl(B) - Pl(A \cap B)$
max/min rule	Not applicable	$\Pi(A \cup B) = \max[\Pi(A), \Pi(B)]$ $N(A \cap B) = \min[N(A), N(B)]$	$Bel(A \cap B) = \min[Bel(A), Bel(B)]$ $Pl(A \cup B) = \max[Pl(A), Pl(B)]$
Measures connectivity	Not applicable	$N(A) = 1 - \Pi(\bar{A})$ $\Pi(A) < 1 \Rightarrow N(A) = 0$ $N(A) > 0 \Rightarrow \Pi(A) = 1$	$Bel(A) = 1 - Pl(\bar{A})$ $Bel(A) \leq Pl(A)$ $Bel(A) = \sum_{B \subseteq A} m(B)$ $Pl(A) = \sum_{B \cap A \neq \emptyset} m(B)$
Complement	$P(A) + P(\bar{A}) = 1$	$\Pi(A) + \Pi(\bar{A}) \geq 1$ $N(A) + N(\bar{A}) \leq 1$ $\max[\Pi(A), \Pi(\bar{A})] = 1$ $\min[N(A), N(\bar{A})] = 0$	$Bel(A) + Bel(\bar{A}) \leq 1$ $Pl(A) + Pl(\bar{A}) \geq 1$
Total ignorance	$p(x) = 1/\|X\|, \forall x \in X$	$\pi(x) = 1, \forall x \in X$	$Bel(X) = 1$ and $Bel(A) = 0$, $\forall A \neq X, x \in X$ $Pl(\emptyset) = 1$ and $Pl(A) = 0$, $\forall A \neq \emptyset, x \in X$ $m(X) = 1$ and $m(A) = 0$, $\forall A \neq X, x \in X$
Conditioning	$P(A\|B) = \frac{P(A \cap B)}{P(B)}$	$\Pi(A\|B) = \begin{cases} \Pi(A), & \forall \Pi(A) < \Pi(B) \\ [\Pi(B), 1,] & \forall \Pi(A) \geq \Pi(B) \end{cases}$	$Bel(A\|B) = \frac{Bel(A \cup \bar{B}) - Bel(\bar{B})}{1 - Bel(\bar{B})}$ $Pl(A\|B) = \frac{Pl(A \cap B)}{Pl(B)}$

5.7 Dealing with Uncertainty via Conceptualised Modelling

The ideal situation would use a single universally capable and accepted uncertainty model. Unfortunately, such a model does not currently exist and is unlikely to be developed any time soon.

Process model description should include key assumptions, simplifications, and aggregations of variables, although empirical model descriptions should include the rationale for selection, and statistics on model performance (e.g., goodness of fit). Uncertainty in process or empirical models can be quantitatively evaluated by comparing model results to measurements taken in the system of interest or by comparing the results obtained using different model alternatives. If important relationships are missed or specified incorrectly, risks could be seriously under- or overestimated in the risk characterization phase. While simplification and lack of knowledge may be unavoidable, risk assessors should document what is known, justify the model, and rank model components in terms of uncertainty (Smith & Shugart, 1994).

Developing alternative conceptual models for a particular assessment to explore possible relationships can reduce uncertainty associated with conceptual models. In cases where more than one conceptual model is plausible, the risk assessor must decide whether it is feasible to follow separate models through the analysis phase or whether the models can be combined into a better conceptual model. It is important to revisit, and if necessary revise, conceptual models during risk assessments to incorporate new information and recheck the rationale. It is valuable to present conceptual models to risk managers to ensure the models communicate well and address key concerns the managers have. This check for completeness and clarity provides an opportunity to assess the need for changes before analysis begins.

5.8 Implications of Not Addressing Uncertainty

Uncertainty must be handled appropriately with a good mix of strategies. If uncertainties are not considered, then unrealistic risk estimates are more likely to be

obtained. Furthermore, if such information is not provided to decision-makers, there is a danger that the assessments made will be considered as fully reliable. The outcome of such a result is often a poor/inappropriate decision being made, leading to missed goals and opportunities. For example, one major reason for cost overruns is the uncertainty inherent in various aspects of the work. This uncertainty can result in a wide range of outcomes that in turn may impact project cost and schedule in unfavourable ways. Moreover, getting it wrong, even slightly, increases likelihood of unwelcome surprises and can often lead to civil or even criminal liability due to negligence.

Also, if further risk assessments are later performed, yielding different conclusions with apparently equal certainty, it may cause a loss of confidence in the risk assessment technique.

5.9 Concluding Remarks

Both risk and uncertainty are always present in any real-world decision among different courses of action. Therefore, developing different courses of action for a decision maker, selecting among those courses of action with different costs and benefits, and implementing those choices effectively require risks and uncertainties to be accurately and objectively recognized, estimated, incorporated, and managed.

Situations of inherent and/or subjective uncertainties are encountered in a maritime risk analytical process. These uncertainties mainly arise due to some variation of the event occurrence parameter and the approximation of the model form. Any effective risk-based model should be capable of treating its inherent or subjective uncertainties via the inference of probabilistic (e.g., probability and Bayes') or possibilistic (e.g., possibility and fuzzy set) theories. Dempster-Shafer theory or the theory of mass reasoning may also be utilised for reasoning evidentially after either a probabilistic analysis or a possibilistic analysis have been conducted. Basically, a good mix of strategy should be applied to handle these uncertainties, otherwise there is bound to be a danger that the assessments made will be considered as fully reliable. This can lead to inappropriate decisions being made, which can result into missed goals and opportunities.

Chapter 6: Bayesian Network Modelling

Chapter Summary

A powerful practical solution is the most desired output when making decisions under the realm of uncertainty on any safety-critical marine or offshore units and their systems. A Bayesian network (BN) is shown to realistically deal with those encountered uncertainties whilst at the same time making risk assessments easier to build, check and also update with data and information typically being obtained incrementally. For its application, a well-matched methodology is proposed to formalise the reasoning in which the focal mechanism of inference processing relies on the sound Bayes' rule/theorem that permits the logic. In this chapter, the method is illustrated and its feasibility is shown in a number of applicable maritime cases of interest, developed via a commercial computer tool. Some influencing nodal parameters in BN models are also further expanded with additional nodes to output influence diagrams that are highly intuitive in their effects on the decision. The test cases, although kept easy, demonstrates how a BN can facilitate the process for a sounder assessment of reliability and safety.

6.1 Introduction

If all the information that could be known about a maritime hazardous event/situation were obtainable for its risk assessment, then the results of such studies that are accurately carried out would not be subject to uncertainty. Instead, data and information is typically obtained incrementally. Thus, it is necessary to model the assessment domain such that the probabilistic measure of each event becomes more reliable in light of the new information being received. In view of this, the domain that is represented can be put out in an intuitive visual format as a Bayesian network (BN) model. The BN reasoning system can be viewed as the generalisation of prepositional

logic and resolution theorem-proving that incorporates the treatment of uncertainty for the structure of the complex argument. Probability theory ensures that inferences based on a network are sound.

Reasoning with incomplete knowledge is one of the fundamental features of human intelligence and one that is very essential to the risk-based marine community. Therefore, competent expert and engineering judgement (to compensate for any lack of mature data) incorporated in a BN can aid in providing its solid knowledge base. Also, it is worth evaluating the use of BNs as a means of optimisation that combines information from diverse sources and permits model reduction. The generic nature of this technique means that it can be developed further and applied widely in marine and offshore applications. With this philosophy in a logical framework, adopting BN to formalise reasoning about system dependability will make assessments easier to build, check and certainly update.

The analogy of BN models can further be expanded/transformed to output influence diagrams that are highly intuitive in the decision-making process. Such diagrams aid the visibility of a large number of interacting issues and their effects on the decision. They can also offer the benefit of a robust practical solution that is required for achieved safety at an affordable cost. Hence, the final scheme of the BN can give a model in which reasoning is justified whilst it enables a powerful marine decision-support solution that is easy to use, flexible, and appropriate for the assessment task.

6.2 Semantics of a Bayesian Network

Fundamental to the idea of *Bayesian networks (BNs)* is the concept of modularity, whereby a complex system is built by combining simpler parts of components that are related in a causal manner. A BN provides factorised representation of a probability model that explicitly captures much of the structure typical in human-engineered models. More generally, a BN is a *directed acyclic graph (DAG)* that encodes a *conditional probability distribution (CPD)* at its nodes on the basis of arcs received. Therefore, by definition:

"BN" = "DAG" encoded with "CPD"

The key feature of BNs is that they enable modelling and reasoning about uncertainty (Pearl, 1988). This uncertainty can be due to imperfect understanding of the domain, incomplete knowledge of the state of the domain at the time where a given task is to be performed, randomness in the mechanisms governing the behaviour of the domain, or a combination of these.

6.2.1 Probability Directed Acyclic Graph

In a directed graph, an edge (*arc*) goes from one vertex (*node*), the *source*, to another, the *target*, and hence makes connection in only one direction. Acyclic implies that such a graph contains no cycle. Therefore, if there is a route from one node to another node in the graphical structure then there is no way back.

In a BN structure (i.e. the DAG), *nodes* (usually drawn as either circles or ovals) represent random (i.e., chance) variables, such as events, that take values from the given domains. *Arcs* (normally drawn as either curved or straight lines having a terminating arrowhead) are used to represent the direct probabilistic dependence relations among the variables. Each influence relationship is described by an arc connecting an influencing (parent) node to an influenced (child) node and has its terminating arrowhead pointing to the child node. If a node has no parents, then its probability distribution is said to be *marginal* (as lack of a link signifies *conditional independence*), otherwise it is *conditional*. The graphical network therefore constitutes a description of the probabilistic relationships among the system's variables that amount to a factorisation of the joint distribution of all variables into a series of marginal and conditional distributions.

For example, the interest in an event A (e.g., an *effect*) might arise knowing that another event B (e.g., a *cause*) in the same model domain has occurred. As shown in Figure 6.1, the BN expresses the fact that A is directly dependent on B (i.e., $A \leftarrow B$ or $B \rightarrow A$). This indicates that B influences A partially or in total, and that A and B are functionally related, or they are statistically correlated.

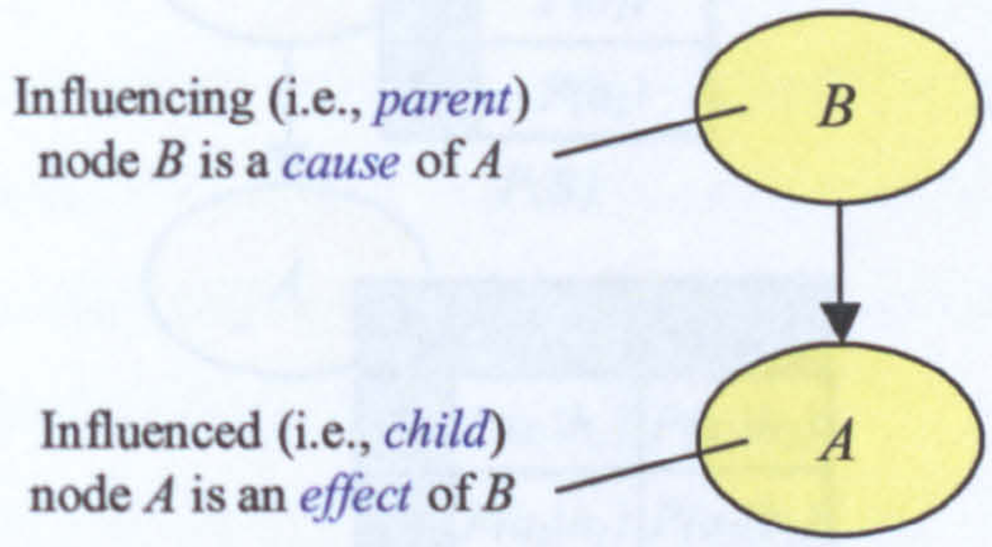


Figure 6.1: A simple events BN structure of two nodes and an arc

One of the best features of BNs is that one can incorporate *new node(s)* as the data becomes available. Thus, it follows that one 'effect' can be a 'cause' of a new/another node and a 'cause' can also be the 'effect' of a new/another node.

Basically, the graphical structure of a BN depicts a qualitative illustration of the interactions among the set of variables that it models. In a task for risk assessment, these variables can be propositions about events or events themselves. These events may be causal and thus get chained together by the arcs in the network. The structure of such a modelled domain in this case would gives a useful, modular insight into the interactions among the events and allows for prediction of effects of external manipulation.

6.2.2 Conditional Probability Distribution

A BN also represents the quantitative relationships among the modelled variables. Numerically, it represents the *joint probability distribution (JPD)* among them. This distribution is described efficiently, exploring probabilistic independencies among the modelled variables. Each node is described by a probability distribution conditional on its direct predecessors that has its values entered into a *conditional probability table* (*CPT*) associated with the node. The encoded nodes with no predecessors are described by prior probability distributions. Those with predecessors are described by posterior probability distributions.

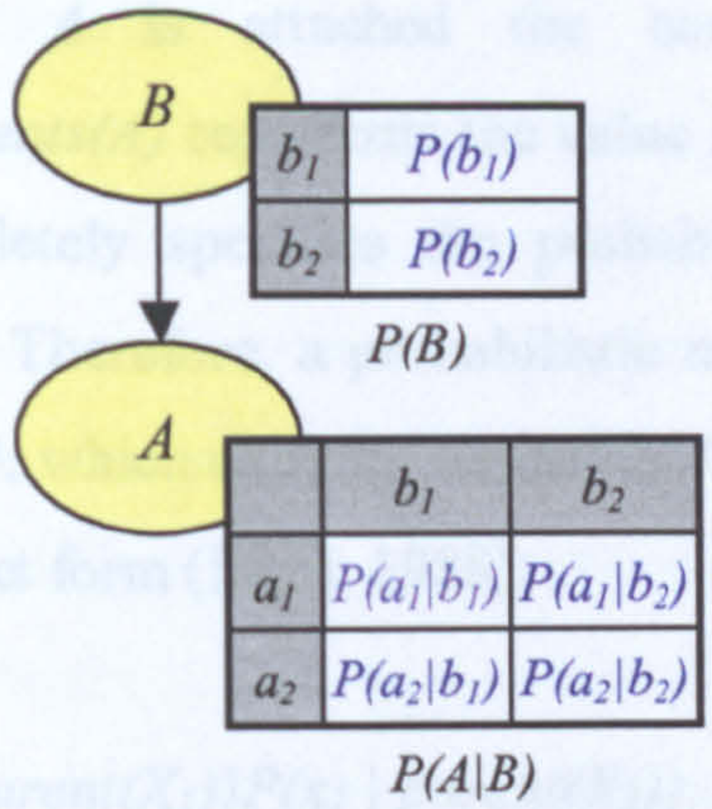


Figure 6.2: A simple BN with its nodes having a CPT containing two states

Basically, a typical CPT is a *matrix of conditional probabilities.* A conditional probability is a probability of one event, given that another event has occurred. For example, the conditional probability of a *parameter,* θ, given an *observed data,* x, would be written as $P(\theta|x)$, where the "|" vertical bar is read as "*given that*" or "*given*" (the indication of *conditionality*). A typical CPT in a BN associated with an event A being directly dependent on an event B is described by its matrix format in Figure 6.2. The subscripts "1" and "2" have been used to give clarity in signifying 2 states of the specified variable. Thus, a_1 and b_1 could say represent a "*reliability*" state for the events A and B respectively whilst a_2 and b_2 could represent a "*failure*" state. To obtain the quantified value with respect to these states, B is described by prior probabilities $P(b_1)$ and $P(b_2)$. Since B has an effect on A, then A is conditionally described by its posterior probabilities $P(a_1|b_1)$, $P(a_1|b_2)$, $P(a_2|b_1)$, and $P(a_2|b_2)$.

More generally, for variable A with a set of states $\{a_1, a_2, \ldots, a_n\}$ and variable B with a set of states $(b_1, b_2, \ldots, b_m)$, the conditional probability matrix $P(a|b)$ represents the conditional probability of A given B as follows:

$$P(a|b) = \begin{bmatrix} P(a_1|b_1) & P(a_1|b_2) & \ldots & P(a_1|b_m) \\ P(a_2|b_1) & P(a_2|b_2) & \ldots & P(a_2|b_m) \\ \vdots & \vdots & \vdots & \vdots \\ P(a_n|b_1) & P(a_n|b_2) & \ldots & P(a_n|b_m) \end{bmatrix} \tag{6.1}$$

More generally, to node A is attached the conditional probability matrix $P(A \mid parents(A))$, where $parents(A)$ represents the value combinations of the parents of A and a global JPD completely specifies the probability assignments to all such propositions in the domain. Therefore, a probabilistic model may consists of a set of variables $X = \{X_1, X_2, ..., X_n\}$, which exploits *conditional independence* to represent the JPD over X having the product form (Pearl, 1988):

$$P(x_1, ..., x_n) = P(x_1 \mid parent(X_1))P(x_2 \mid parent(X_2))...P(x_n \mid parent(X_n))$$
$$= \prod_{i=1}^{n} P(x_i \mid parents(X_i)) \qquad (6.2)$$

$P(x_1, x_2, ..., x_n)$ gives the JPD and like the CPD, it is a table of values where one entry is made for each possible combination of values that its variables can jointly take. The JPD for a problem captures the probability information of every possible combination of a set of variables, and their states. Once a JPD has been defined for a problem, then it is possible, using it along with the axioms of probability, to answer any probabilistic query regarding any of the variables. This includes their value given additional evidence, that is, their posterior probabilities, although, the space, and consequently, time complexity required in representing and manipulating the JPD is exponential in the number of variables considered (D'Ambrosio, 1999). For example, the JPD required to represent a system with 20 binary values would have 2^{20} (1,048,576) values. This causes a problem in the elicitation, storage and manipulation of these values, thus making the use of JPDs unfeasible for any practical use. Fortunately, when modelling most real systems, advantage is taken of any inherent structure the system has by modelling the system as a graph (D'Ambrosio, 1999).

The number of dimensions and the total size of a CPT are determined by the number of parents, the number of states of each of these parents, and the number of states of the child node. Essentially, there is a probability for every state of the child node for every combination of the states of the parents. Nodes that have no predecessors are specified by a prior probability distribution table, which specifies the prior probability of every state of the node.

6.3 Bayesian Inference Mechanism

Bayesian inference is a process by which observations of a real-world situation are used to update the uncertainty about one or more variables characterising aspects of that situation. It relies on the use of *Bayes' rule/theorem* as its rule of inference, defining the manner in which uncertainties ought to change in light of newly made observations. This subjective probability theory is only part of the Bayesian inference mechanism. Together with the applicable results of such probability concepts as the product and sum rules, the concept of conditional independence and the techniques of marginalization, it provides the basic tool for both Bayesian belief updating and in treating probability as logic. In order to apply these tools, the prior probabilities and the likelihood probabilities must be obtained.

6.3.1 Bayes' Theorem/Rule

The theorem of Bayes (1763) is one that has been proven to be a coherent method of mathematically expressing a decrease in uncertainty gained by (or proportional to) an increase in knowledge. As an imperative phase of the probability analysis, this is achieved by combining probability distributions or functions of different parameters (such as events or specific outcomes) and revising their probabilities when new information/data is obtained. The more new information is used, the smaller the parameter of uncertainty about those events or their outcomes becomes.

In order to make probability statements about the model parameters the analysis must begin with providing an initial or *prior probability* estimates for specific outcomes or events of interest. Then from sources such as a special report, a database, a case study, etc., some additional information (i.e., data or evidence) about the event, or an entirely new event(s), is obtained. In light of this new information providing new data belief, it is desirable to improve the state of knowledge and thus the prior probability values are updated by calculating revised probabilities, referred to as the *posterior probabilities* (These probabilities provide basis for action). *Bayes' theorem* provides a means for making these probability calculations. Essentially, it is a relation among conditional and marginal probabilities.

Conditional probabilities are essential to a fundamental rule of probability calculus, the *product rule*. The product rule defines the probability of a conjunction of events (e.g., for two events, A and B):

$$P(A|B)P(B) = P(A,B) = P(B|A)P(A) \tag{6.3}$$

Therefore, in dividing Equation 6.2 by $P(B)$, one obtains:

$$P(A|B) = \frac{P(B \mid A)P(A)}{P(B)} \tag{6.4}$$

which is the theorem conventionally known as *Bayes' theorem*.

Each term in Bayes' theorem has a conventional name. The term $P(A)$ is called the *prior probability of A*. It is "prior" in the sense that it precedes any information about B and this is what causes all the arguments. $P(A)$ is also the *marginal (total) probability of A*. The term $P(A|B)$ is called the *posterior probability of A, given B*. It is "posterior" in the sense that it is derived from or entailed by the specified value of B. The term $P(B|A)$, for a specific value of B, is called the *likelihood function for A given B* and can also be written as $L(A|B)$. The term $P(B)$ is the *prior* or *marginal (total) probability of B* but also one that provides *evidence* of interest for the probability update of A. Its inverse is usually regarded as a *normalising constant*. With this terminology, the theorem may be paraphrased as:

$$posterior = \frac{likelihood \times prior}{evidence} \tag{6.5}$$

In the general case, a JPD over a set of variables, $X = \{X_1, X_2, \ldots, X_n\}$, can be defined recursively using the product rule (Equation 6.6):

$$\begin{aligned} P(X_1, X_2, \ldots, X_n) &= P(X_1|X_2, \ldots, X_n)P(X_2, \ldots, X_n) \\ &= P(X_1|X_2, \ldots, X_n)P(X_2|X_3, \ldots, X_n)P(X_3, \ldots, X_n) \\ &= P(X_1|X_2, \ldots, X_n)P(X_2|X_3, \ldots, X_n)\ldots P(X_{n-1}|X_n)P(X_n) \end{aligned} \tag{6.6}$$

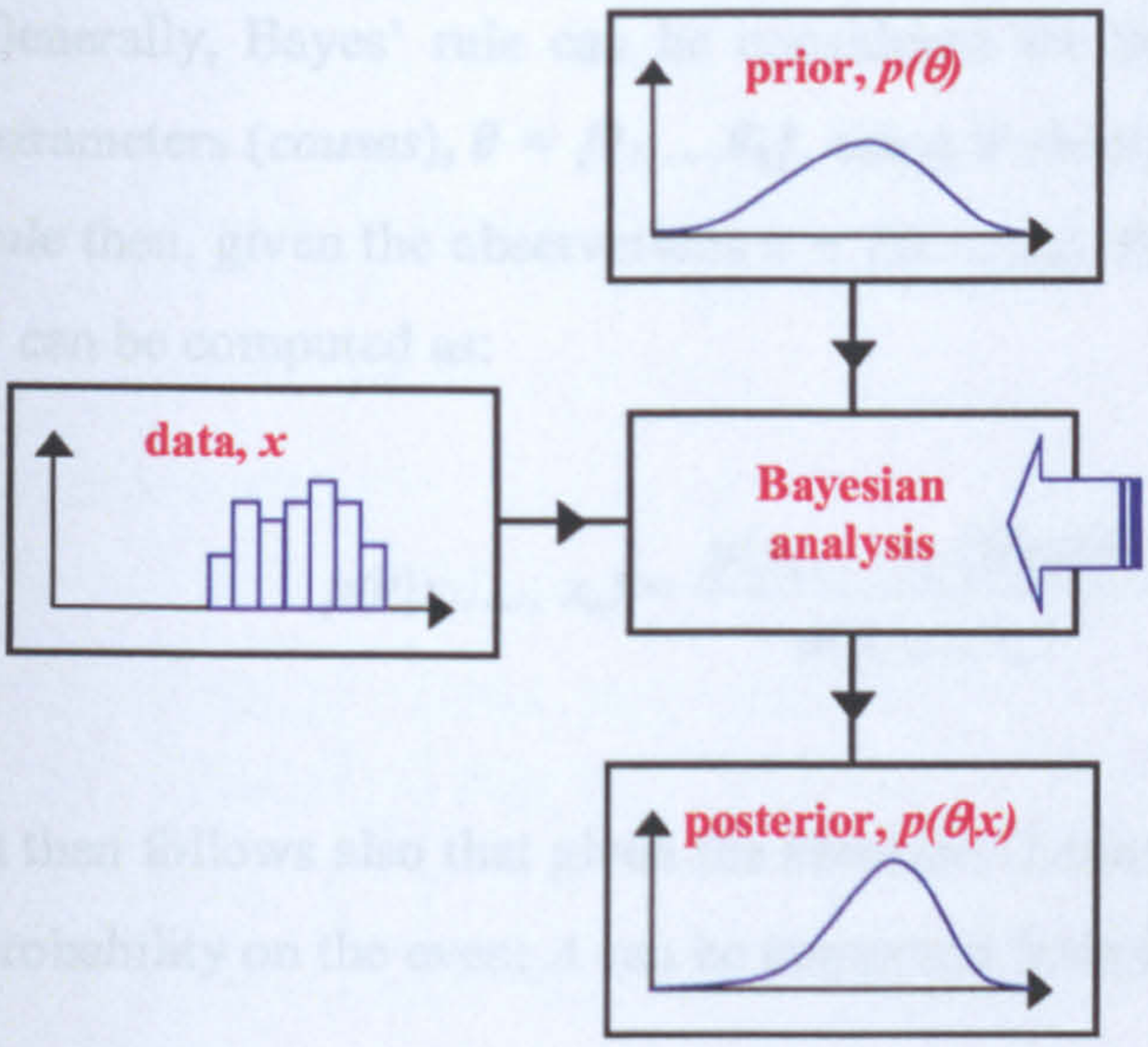
This factorisation property of JPDs is referred to as the *chain rule* of probabilities and is one that allows any ordering of variables in the factorisation. Such a rule is especially significant for BNs because it provides a means of calculating the full JPD from conditional probabilities, which is what a BN stores. For example, the JPD for three events, A, B and C, can be expressed more compactly as:

$$P(A|B,C)P(B,C) = P(A,B,C) = P(B|A,C)P(A,C) \tag{6.7}$$

Then, in applying Equation 6.6, Bayes' theorem specifies for the probability of an event A, given the condition that an event B and an event C both occur ($B \rightarrow A \leftarrow C$) as:

$$P(A|B,C) = \frac{P(B \mid A,C)P(A \mid C)}{P(B \mid C)} \tag{6.8}$$

Bayes' rule/theorem states that:
"The probability distribution of a model parameter, θ, after observing data, x, is proportional to the likelihood of the data, x, assuming that θ is true, times the prior probability distribution of θ."



Symbolically, this is written as:

$$p(\theta|x) = \frac{p(x|\theta)\,p(\theta)}{p(x)}$$

Conventionally, this is read as:

$$posterior = \frac{likelihood \times prior}{evidence}$$

Inverse of the "*Evidence*" term is a *normalising constant*, $\propto$. The "*Likelihood*" term expresses a measure of confidence degree and can be written as $l(\theta|x)$.

Thus, in Likelihood Principle:

$$posterior = \propto likelihood\ (l(\theta|x)) \times prior$$

Figure 6.3: An illustration of probability update via Bayes' theorem

From a statistical viewpoint, the uncertainty associated with a *parameter*, θ, reduces due to the influence of an associated incoming *data*, x, and Bayes' theorem depicts such a

fact as shown in Figure 6.3. Thus, risk assessment of events can be carried out on this basis to enhance reasoning that will enable reliable decision-making.

Bayesian inference proceeds by summarizing the posterior distribution, $p(\theta|x)$. As depicted in Figure 6.4, after observing the data, the wide prior distribution is converted into the more narrow posterior distribution using the Bayes' rule.

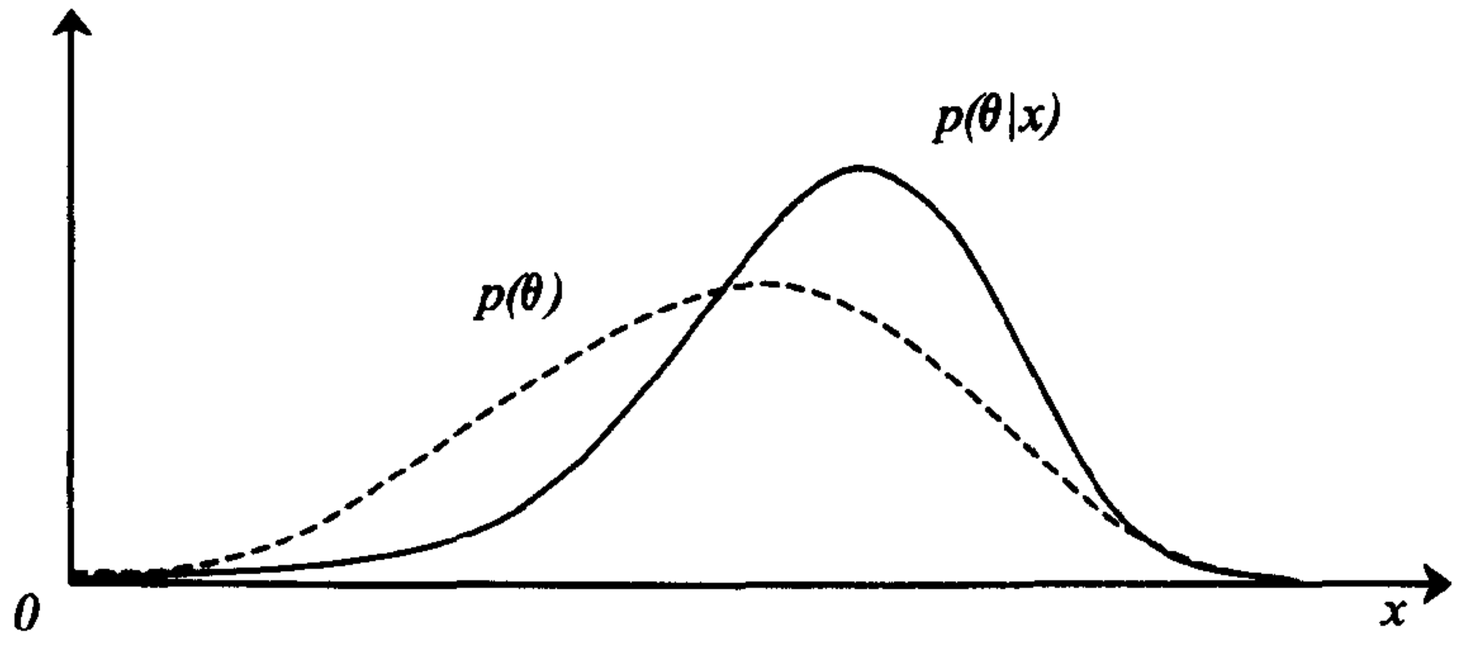


Figure 6.4: Conversion of the wide prior distribution into a more narrow posterior distribution

Generally, Bayes' rule can be considered for the problem of estimating values of k parameters (*causes*), $\theta = \{\theta_1,...,\theta_k\}$, using n observations (*effects*), $x = \{x_1,...,x_n\}$. In the rule then, given the observations $x = \{x_1,...,x_n\}$, the posterior probability distribution on θ can be computed as:

$$p(\theta|x_1,..., x_n) = \frac{p(x_1,...,x_n|\theta)p(\theta)}{p(x_1,...,x_n)} \tag{6.9}$$

It then follows also that given the situation if event B has states $\{b_1,...,b_m\}$, the posterior probability on the event A can be computed from the Bayes' rule as:

$$P(A|b_1,..., b_m) = \frac{P(b_1,...,b_m|A)P(A)}{P(b_1,...,b_m)} \tag{6.10}$$

The process of Bayes' theorem is repeated every time new or additional information becomes available, so that as Lindley (1970) puts it, "today's posterior probability is tomorrow's prior." As the number of pieces of evidence increases, the dependence of

the posterior on the original estimated prior decreases. This is indeed true and the main task of the theorem answers the following question, "Given observations (evidence), what is the probability of a particular cause (or variable of interest)?"

Bayes' theorem has been particularly useful in estimating knowledge about the frequency of rare events or making reliability predictions where there is sparse or no directly applicable data (Frank, 2000). This has remained evident in dealing with uncertainty in expert systems. Being such a robust and extensible method, Bayes' theorem can likewise aid in marine and offshore risk assessment for predictive reasoning under uncertainty, and therefore, to arrive at a logically justifiable prediction.

6.3.1.1 Marginalization of Probabilities

From a table $P(A, B)$ of probabilities $P(a_i, b_j)$ the probability distribution $P(A)$ can be calculated. Let a_i be a state of A. There are exactly m different events for which A is in state a_i, namely the mutually exclusive events $(a_i, b_1), \ldots, (a_i, b_m)$. Therefore:

$$P(a_i) = \sum_{j=1}^{m} P(a_i, b_j) = \sum_{j=1}^{m} P(a_i \mid b_j) P(b_j) \tag{6.11}$$

In other words:

$$\begin{bmatrix} P(a_1) \\ P(a_2) \\ \vdots \\ P(a_n) \end{bmatrix} = \begin{bmatrix} P(a_1 \mid b_1) & P(a_1 \mid b_2) & \ldots & P(a_1 \mid b_m) \\ P(a_2 \mid b_1) & P(a_2 \mid b_2) & \ldots & P(a_2 \mid b_m) \\ \vdots & \vdots & \vdots & \vdots \\ P(a_n \mid b_1) & P(a_n \mid b_2) & \ldots & P(a_n \mid b_m) \end{bmatrix} \cdot \begin{bmatrix} P(b_1) \\ P(b_2) \\ \vdots \\ P(b_m) \end{bmatrix} \tag{6.12}$$

This calculation is called *marginalization* (summing out) and expresses the fact that the variable B is marginalized out of the JPD, $P(A, B)$ (resulting in $P(A)$) (Russell & Norvig, 2003). The notation is:

$$P(A) = \sum_{B} P(A, B) = \sum_{j} P(A \mid B = b_j) P(B = b_j) \tag{6.13}$$

Similarly, if *P(B, A)* is a CPT over *A* and *B*, then a CPT over the state space of just *B* can be produced by marginalizing over *A*, so that, for example:

$$P(b_1) = \sum_{i=1}^{2} P(a_i, b_1) = P(b_1|a_1)\,P(a_1) + P(b_1|a_2)\,P(a_2) \qquad (6.14)$$

Marginalization is of utmost importance for all inference in Bayesian probability: "integrating out" all "superfluous" variables derives the information about a subset of the system's variables. Furthermore, the process of marginalization tackles the problem of decision uncertainty explicitly, by preventing overoptimistic predictions (Vellido & Lisboa, 2001).

6.3.1.2 Normalization of Probabilities

In estimating values of an event $A = \{a_1,\ldots,a_n\}$ that is directly dependent on another event *B*, the denominator of the right-hand side of Bayes' theorem gives the probability of event *B* as *P(B)*. True probabilities of an event are supposed to sum to one over its entire state space, hence (as from the axioms of probability): $P(a_1) + ,\ldots, + P(a_n) = 1$. This formula can be applied to conditional probabilities, as well: $P(a_1|B) + ,\ldots, + p(a_n|B) = 1$. Using this fact and Bayes' rule for $P(a_1|B)$ and $P(a_n|B)$, the following equation can be obtained:

$$P(B) = P(B|a_1)\,P(a_1) + ,\ldots, + P(B|a_n)\,P(a_n) \qquad (6.15)$$

The inverse of Equation 6.15 is known as a *normalising constant,* α, that ensures the posterior probability over the entire state space ($i = 1, 2,\ldots, n$) sums up to 1. In other words;

$$\alpha^{-1} = P(B) = \sum_{i=1}^{n} P(B \mid a_i)P(a_i) \qquad (6.16)$$

Given that event $B = (b_1,...,b_m)$, the term can be computed by summing the numerator over all possible event values (See "marginalization" in Section 6.3.1.1) whereby:

$$\propto^{-1} = P(b_1,..., b_m) = \sum_{i=1}^{n} P(b_1,...,b_m \mid a_i)P(a_i) \qquad (6.17)$$

The process that had just been explained is called *normalization* since it allows the sum of the probabilities of all exhaustive and mutually exclusive values (i.e., marginal and conditional terms) to equal 1. As a result of this process, Bayes' theorem can be expressed as:

$$P(A|B) = \propto P(B|A)\, P(A) \qquad (6.18)$$

Normalization can alter conclusions with respect to probability inferences. Thus, without the process of normalization there would never exist a unique maximum likelihood (ML) (See Section 6.3.2.2).

6.3.2 The Likelihood Principle

The *Likelihood Principle (LP)* (Fisher, 1922 and Edwards, 1992) states that *all* the relevant information in the model is contained in the likelihood function (which is of fundamental importance in the theory of Bayesian inference). Likelihood and log-likelihood functions are the basis for deriving estimators for parameters, given data. While the shapes of these two functions are different, they have their maximum point at the same value. In fact, the value of a parameter that corresponds to this maximum point is defined as the maximum likelihood estimate. This is the value that is "mostly likely" relative to the other values. This is a simple, compelling concept and it has a host of good statistical properties.

6.3.2.1 The Likelihood Function

Sometimes $P(B|A)$ is called the *likelihood of A given B*, and is denoted $L(A|B)$. The reason for this is that if, for example, $a_1, \ldots, a_n$ are possible states of event A with an effect on the event B in which b is known, then and $P(b|\ a_i)$ is a measure of how likely it is that a_i is the cause. Likewise, $l(\theta|x)$ denotes the *likelihood of* θ, *given* x.

"Likelihood" as a solitary term and one of several informal synonyms for "probability" is actually the shorthand for "*likelihood function*", a measure of how well (i.e., confidence degree) a given parameter *predicts* the data. Thus, the most important difference between $p(x|\theta)$ and $l(\theta|x)$ is that $p(x|\theta)$ is the *probability* of x (for a given parameter θ), while $l(\theta|x)$ is a function of θ (for given observations x). It follows from Equation 6.18 then that:

$$p(\theta|x) = \propto l(\theta|x)\, p(\theta) \tag{6.19}$$

As given by Equation 6.19, likelihood function is the instrument to pass from prior probability distribution to posterior probability distribution via Bayes' formula (See Figure 6.5). Therefore inference must obey the principle about such a function. LP essentially holds that the likelihood function, $l(\theta|x)$, is the sole basis for Bayesian inference as the information brought by an observation x about a parameter, θ, is entirely represented and contained in this function. Thus the likelihood plays an important role in Bayes' theorem, as it is the function that expresses the degree through which the data, x, modifies prior knowledge of θ.

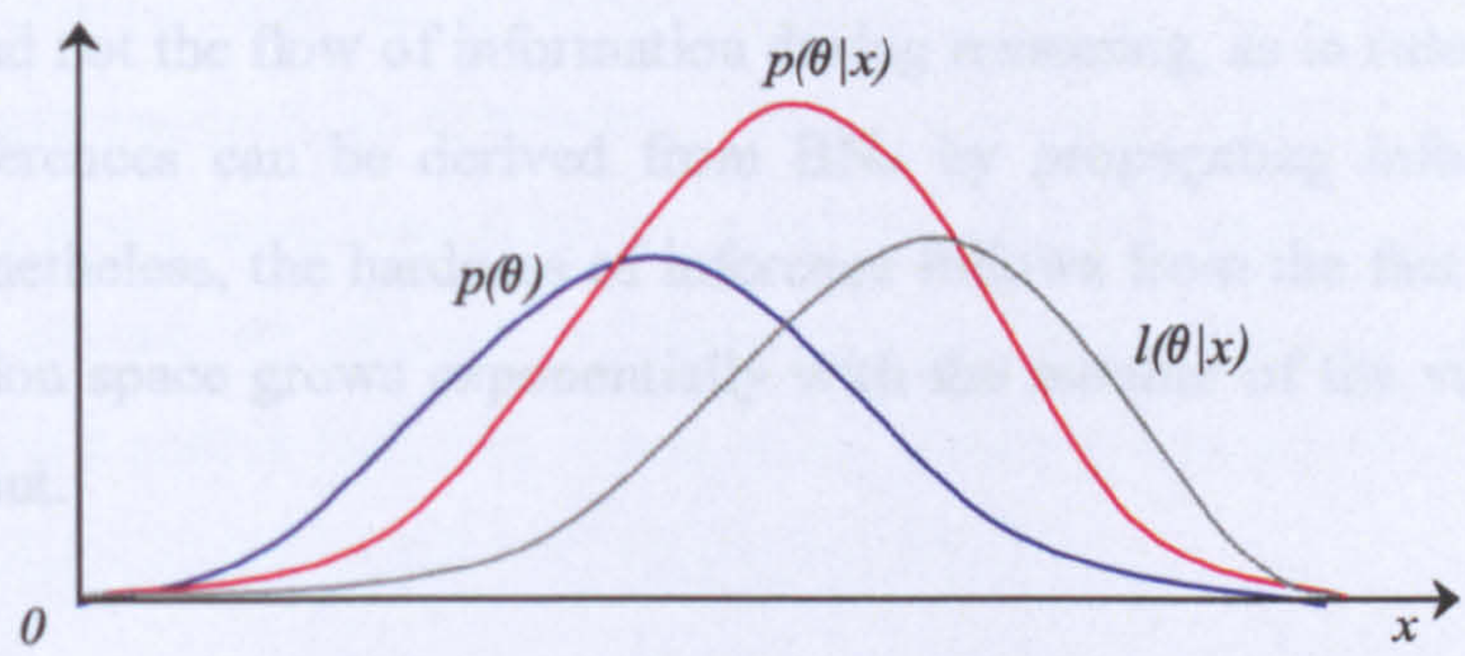


Figure 6.5: Updating from prior distribution to posterior distribution via likelihood function

Since the natural logarithm function, ln, is strictly increasing, the maximum value of $l(\theta|x)$, if it exists, will occur at the same points as the maximum value of $\ln[l(\theta|x)]$. This latter function is called the *log likelihood function* and in many cases is easier to work with than the likelihood function (usually because the probability distribution $p(x|\theta)$ has a product structure).

6.3.2.2 Maximum Likelihood Estimation

In the method of *maximum likelihood (ML)*, one tries to find a value $\theta(x)$ of the parameter θ that *maximises* $l(\theta|x)$ for each x being observed. If this can be done, then $\theta(x)$ is called a *maximum likelihood estimate* for θ. Thus:

$$\theta(x) = \max_{\theta} l(\theta \mid x) \tag{6.20}$$

The method is intuitively appealing and represents the backbone of statistical estimation (Fisher, 1922) in which one tries to find the values of the parameters that would have *most likely* produced the data were in fact observed.

6.3.3 Propagation of Information Concepts

Perhaps the most important aspect of BNs is that they are direct representations of the world, not of reasoning processes. The arrows in the diagram represent real causal connections and not the flow of information during reasoning, as in rule-based systems. Therefore, inferences can be derived from BNs by propagating information in any direction. Nonetheless, the hardness of inference follows from the fact that the size of the configuration space grows exponentially with the number of the variables that are marginalized out.

A graphical model can greatly simplified the representation of the JPD capturing dependencies and independencies between variables. For any BN model, conditional

independencies and dependency-separation (i.e., d-separation) are key factors that are exploited to make inference tractable in order for evidence propagation and belief update to be achieved. In fact, d-separation is another method to determine conditional independence. However, conditional independence is defined in terms of probabilities and d-separation in terms of paths in a graph. On their basis, large computational savings in fast BN update algorithms are also achievable.

6.3.3.1 Conditional Independence

Any probability of interest can be calculated from the JPD of the variables. However, a BN not only outputs the graphical representation of a joint probability of the variables, it also captures properties of conditional independence (i.e., missing arrows that imply no direct influence) between variables (See Section 6.2.2). It is able to take advantage of the conditional independencies first to represent joint probabilities more compactly and efficiently, before the actual conditional probability distributions are numerically specified. It is this combination of qualitative information with quantitative information of the numerical parameters that makes probability theory so expressive. In other words, this combination takes care of reducing the complexity of the probability to be computed, by simplifying probabilistic inference of the network. Conditional independence also reduces the size of CPTs.

For example, given two events A and B, A is *independent* of B if $P(A|B) = P(A)$. Independence is symmetric, and therefore it follows that $P(B|A) = P(B)$. The independence of A and B can also be expressed as $P(A,B) = P(A)P(B)$. Also, A is *conditionally independent* of B given another event C if $P(A|B,C) = P(A|C)$. Conditional independence is symmetric, and therefore it follows that $P(B|A,C) = P(B|C)$. Now, when many variables are conditionally independent (as in the case of Equation 6.6), calculation of joint probabilities using the chain rule can be simplified significantly. As a simple example, if A is conditionally independent of B given C, then $P(A,B,C) = P(A|B,C)P(B|C)P(C) = P(A|C)P(B|C)P(C)$.

6.3.3.2 D-Separation

Conditional independence characteristics may also be experienced for two variables in a BN if evidence about one cannot influence the other. To determine conditional independence in this setting, one must also consider all the undirected paths between the two nodes. Any node on any of the paths may "block" the dependence along that path, and therefore if all the paths between the two variables are blocked at least once, the two nodes will be independent (i.e., *dependency separated* or *d-separated*). As such, the question as to whether two nodes in a BN can influence each other will depend on two issues: the type of connections used on paths between the nodes and the kind of evidence that has been received. The evidence transmitted will either be in a form considered as follows:

- *Hard evidence* (i.e., *instantiation*) for a node X is evidence that the state of X is definitely a particular value; or
- *Soft evidence* (i.e., *a new distribution*) for a node X is any evidence that enables the update of the prior probability values for the states of X.

In considering a node on a path in the network, one can distinguish three types of connection: *serial*, *diverging*, and *converging*, as shown in Figure 6.6. Each connection has its own propagation properties as follows:

- In a serial (head-to-tail) connection (i.e., $B \rightarrow C \rightarrow A$), any evidence entered at node A or node B can be transmitted along the directed or undirected path respectively (as in Figure 6.6(a)(i)) providing that no intermediate node C on the path is instantiated (which thereby blocks further transmission by d-separation as in Figure 6.6(a)(ii)).
- In a converging (head-to-head) connection (i.e., $B \rightarrow C \leftarrow A$), entering hard evidence at node B will update node C but will have no effect on node A (Figure 6.6(b)(i)). Evidence can only be transmitted between parents, i.e, nodes A and B, when the child (converging) node C has received some evidence (which can be soft or hard. See Figure 6.6(b)(ii)).

- In a diverging (tail-to-tail) connection (i.e., $B \leftarrow C \rightarrow A$), evidence can be transmitted between child nodes, i.e, nodes *A* and *B*, of the same parent, i.e., node C, providing that the parent is not instantiated (Figure 6.6(c)(i)). Otherwise, nodes *A* and *B* are *conditionally independent* (i.e., due to d-separation) given evidence at node *C* (Figure 6.6(c)(ii)).

More generally, it can be said that two variables *A* and *B* are d-separated if for all paths between *A* and *B* there is an intermediate variable *C* such that either the connection is:

- serial or diverging and the state of *C* is known, or
- converging and neither *C* nor its descendants have received evidence.

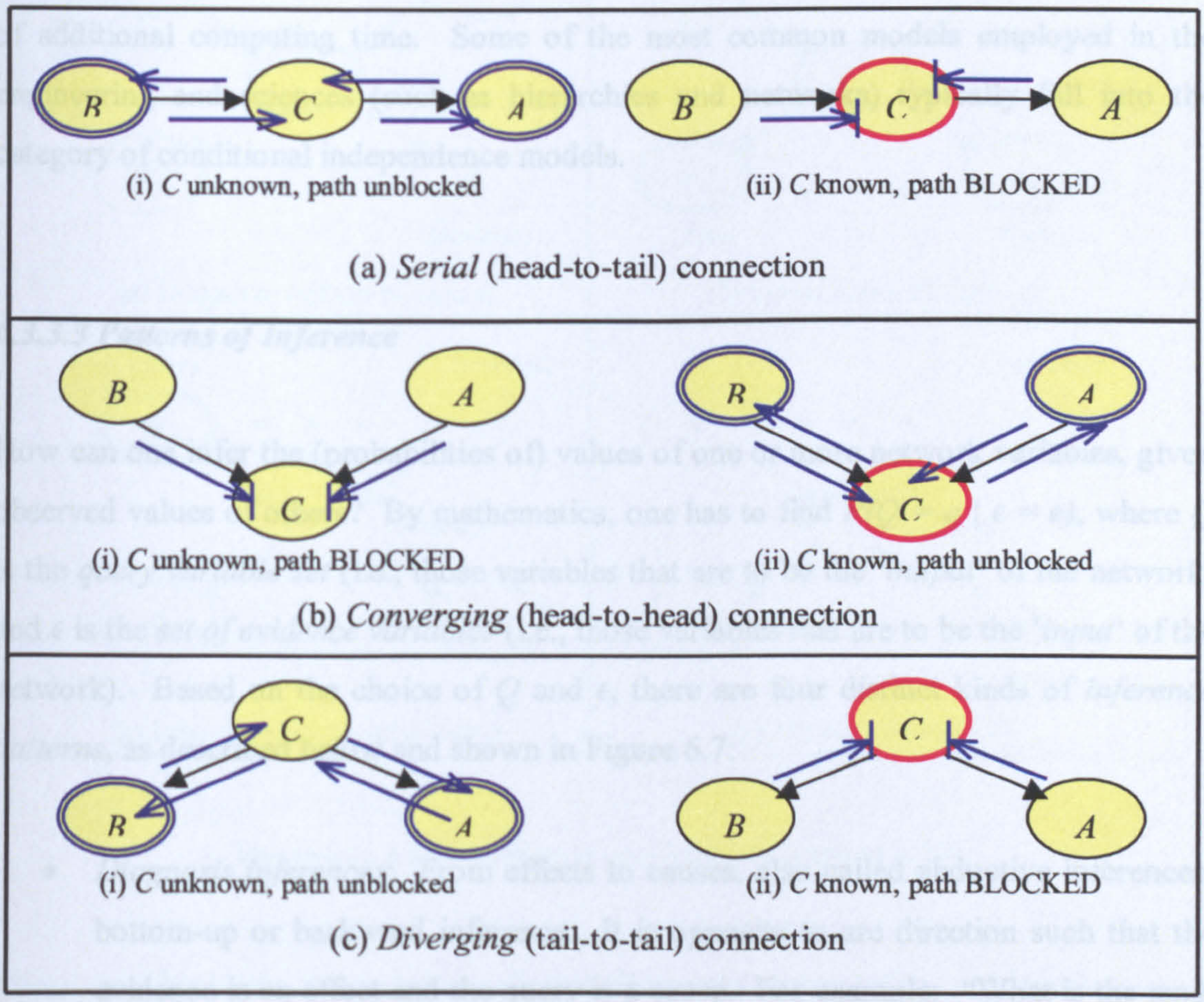


Figure 6.6: Serial, diverging and converging connections to a node *C* on a path

The *smallest set* of nodes that d-separates two nodes, *A* and *B*, is called the *cut-set* of *A* and *B* (Pearl, 1988). As demonstrated also, d-separation characterises independence arising from lack of evidence as well as evidence. Note that any system for reasoning under uncertainty must capture these properties, as they are basic attributes of human reasoning (Jensen & Lauritzen, 2000). Thus, the notion of d-separation is crucial for understanding how the algorithms for probability propagation in BNs actually work. Two variables that are not d-separated are said to be *d-connected*.

A significant benefit of the Bayesian paradigm is that additional parameters can easily be added to a model without seriously adding to the complexity of the statistical analysis, provided that those parameters fit into a conditional independence structure. This means that provided the dependence of the new parameters to the existing data and parameters can be made explicit, assessing the new parameters is often a simple matter of additional computing time. Some of the most common models employed in the engineering and sciences (such as hierarchies and networks) typically fall into the category of conditional independence models.

6.3.3.3 Patterns of Inference

How can one infer the (probabilities of) values of one or more network variables, given observed values of others? By mathematics, one has to find $P(Q = q \mid \epsilon = e)$, where Q is the *query variable set* (i.e., those variables that are to be the '*output*' of the network) and ϵ is the *set of evidence variables* (i.e., those variables that are to be the '*input*' of the network). Based on the choice of Q and ϵ, there are four distinct kinds of *inference patterns*, as described below and shown in Figure 6.7:

- *Diagnosis inferences*: From effects to causes, also called abductive inferences, bottom-up or backward inference. It is opposite to arc direction such that the evidence is an effect and the query is a cause. For example: "What is the most probable explanations for the given set of evidence?"
- *Causal inferences*: From causes to effects, also called predictive inferences, top-down or forward inferences. It is same as arc direction such that the evidence is

a cause and the query is an effect. For example: "Having observed a parent node B, what is the expectation of its child node A?"

- *Inter-causal inferences*: Between causes of a common effect. For example: "If C's parents are $B_1,\ldots, B_m$, then what is the expectation of B_1 given both C and B_m?" Namely, what is the belief of the occurrence of one cause on the effect given that the other cause is true? The answer is that the presence of one makes the other less likely (This phenomenon has been termed "*explaining away*" (Wellman & Henrion, 1993)).
- *Mixed inferences*: Combining two or more of the above.

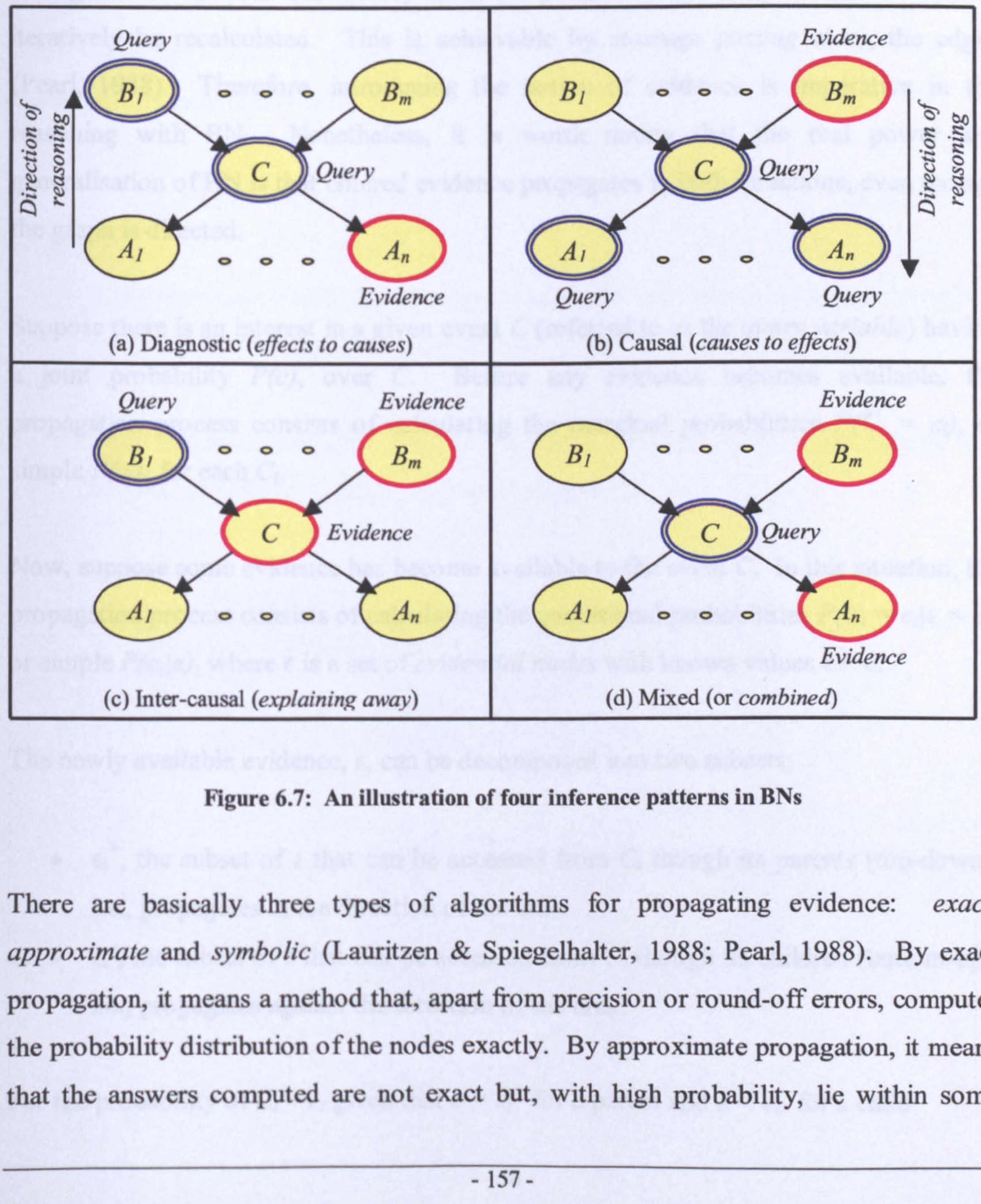


Figure 6.7: An illustration of four inference patterns in BNs

There are basically three types of algorithms for propagating evidence: *exact*, *approximate* and *symbolic* (Lauritzen & Spiegelhalter, 1988; Pearl, 1988). By exact propagation, it means a method that, apart from precision or round-off errors, computes the probability distribution of the nodes exactly. By approximate propagation, it means that the answers computed are not exact but, with high probability, lie within some

small distance of the correct answer. Finally, symbolic propagation, which computes the probabilities in symbolic form, can deal not only with numerical values, but also with symbolic parameters.

6.3.3.4 Belief Update

Evidence is new information about a random variable that causes a change to its probability distribution. Newly available evidence is brought about when a particular state of an event happens. The effect of such new evidence will certainly propagate throughout the network and thereby cause the posterior probabilities of other events to iteratively be recalculated. This is achievable by *message posting* along the edges (Pearl, 1988). Therefore, introducing the notion of evidence is imperative in the reasoning with BN. Nonetheless, it is worth noting that the real power and generalisation of BN is that entered evidence propagates in both directions, even though the graph is directed.

Suppose there is an interest in a given event C (referred to as the *query variable*) having a joint probability $P(c)$, over C. Before any evidence becomes available, the propagation process consists of calculating the marginal probabilities $P(C_i = c_i)$, or simple $P(c_i)$, for each C_i.

Now, suppose some evidence has become available to the event C. In this situation, the propagation process consists of calculating the conditional probabilities $P(C_i = c_i | \epsilon = e)$, or simple $P(c_i|e)$, where ϵ is a set of *evidential nodes* with known values $\epsilon = e$.

The newly available evidence, ϵ, can be decomposed into two subsets:

- ϵ_i^+, the subset of ϵ that can be accessed from C_i though its parents (top-down), i.e., propagates in the direction of the arcs.
- ϵ_i^-, the subset of ϵ that can be accessed from C_i though its children (bottom-up), i.e., propagates against the direction of the arcs.

For the probability of $C_i = c_i$ given that $e = e_i^+$ for a parent and $e = e_i^-$ for a child:

$$P(c_i|e) = P(c_i|\, e_i^-,\, e_i^+) = \frac{P(e_i^-\,|\,c_i, e_i^+)P(c_i\,|\,e_i^+)}{P(e_i^-\,|\,e_i^+)} \tag{6.21}$$

Since C_i d-separates ϵ_i^- from ϵ_i^+ (i.e., $\epsilon_i^- || \epsilon_i^+$, where $||$ stands for d-separation), conditional independence can be used to simplify the first term in the numerator and then $1/P(e_i^-|\, e_i^+)$ can be treated as a normalizing constant, $\propto$, so that:

$$P(c_i|e) = \propto P(e_i^-|c_i)\, P(c_i|\, e_i^+) \tag{6.22}$$

According to the Bayes' theorem conventional interpretation (Equation 6.3), posterior is prior scaled by likelihood and normalized by evidence (so Σ (posteriors) = 1), thus Equation 6.22 can be rewritten as:

$$P(c_i|e) = \propto \lambda_i(c_i)\, \pi_i(c_i) \tag{6.23}$$

where;

$\lambda_i(c_i)$ represents $P(e_i^-|c_i)$, a message passed onto c_i as *likelihood evidence*; and

$\pi_i(c_i)$ represents $P(c_i|e_i^+)$, a message passed onto c_i as *prior evidence*.

To compute the functions $\lambda_i(c_i)$ and $\pi_i(c_i)$, suppose a typical node C_i has parents $B = \{B_1,...,B_m\}$ and children $A = \{A_1,...,A_n\}$ (see Figure 6.8).

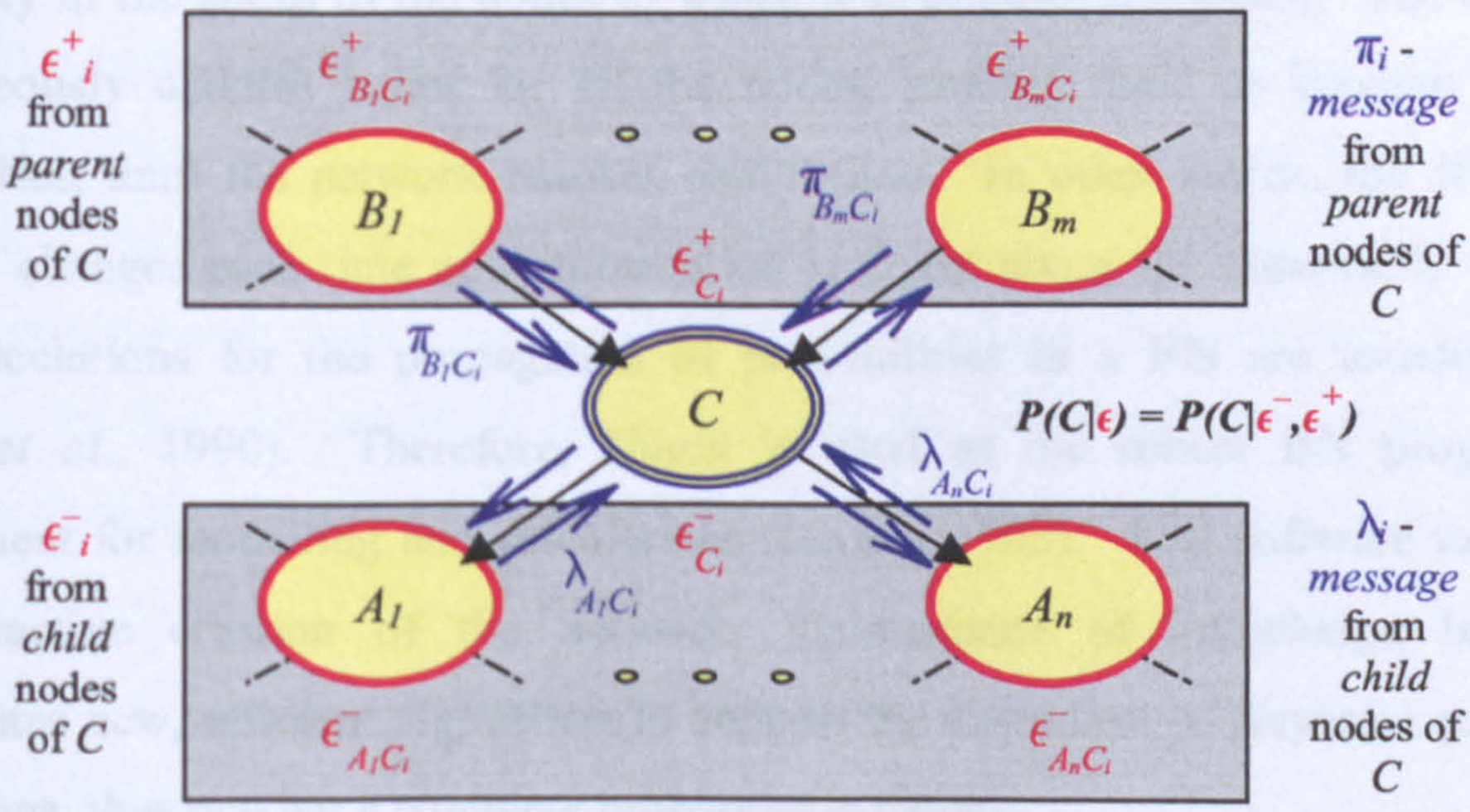


Figure 6.8: Evidence propagation via message posting

The evidence ϵ_i^+ can be partitioned into m disjoint components, one for each parent of C_i:

$$\epsilon_i^+ = \{\varepsilon^+_{B_1C_i},\ldots,\varepsilon^+_{B_mC_i}\} \tag{6.24}$$

where the evidence $\varepsilon^+_{B_jC_i}$ is the subset of ϵ_i^+ contained in the B_j-side of the link $B_j \rightarrow C_i$.

Similarly, the evidence ϵ_i^- can be partitioned into n disjoint components, that is:

$$\epsilon_i^- = \{\varepsilon^-_{A_1C_i},\ldots,\varepsilon^-_{A_nC_i}\} \tag{6.25}$$

where the evidence $\varepsilon^-_{B_jC_i}$ is the subset of ϵ_i^- contained in the A_j-side of the link $A_j \leftarrow C_i$.

Then, given an instantiation of $b = \{b_1,\ldots,b_m\}$ of the parents of C_i, $\pi_i(c_i)$ can be computed (i.e., *top-down propagation*) via a recursive solution (Pearl, 1986: Castillo, *et al.*, 1997). Likewise, given an instantiation of $a = \{a_1,\ldots,a_n\}$ of the children of C_i, $\lambda_i(c_i)$ can be computed (i.e., *bottom-down propagation*).

The CPTs of the events *never* change by entering new evidence; only the new-fangled/belief probability in each of its possible states is determined by the belief probability in the states of the nodes to which it is directly connected. The algorithm simultaneously updates belief for all the nodes, causing them to become posterior probabilities, until the network reaches equilibrium. In other words, the JPD of the variables changes each time new information is learnt about the observable variables. Such calculations for the propagation of probabilities in a BN are usually tedious (Jensen, *et al.*, 1990). Therefore, *Hugin* is used as the robust BN programming environment for modelling and calculations (Jensen, 1993). This software tool allows for interactive creation of the network, maintenance of knowledge bases and incorporates new, efficient algorithms to support the execution of Bayesian probability calculations, thus making a complete probabilistic model.

A runtime system provides facilities for easy entering and propagation of information. This makes it easy to insert the quantitative data into the network. By running *Hugin* in the compiled mode, it is possible to interact with the network and test whether it works properly. In this mode, *Hugin* calculates prior probabilities for each state in each node of the network based on either the qualitative or the quantitative specification of the network. Evidence can be entered to the network by manually setting probabilities in the network. Each time an input for evidence of change is entered, all the probabilities are recalculated. The algorithm repeats until the network reaches equilibrium. In BN terminology, this is called *propagation of evidence* through the network.

The notion of Bayesian propagation has been around for a long time. However, it is only in the last few years that efficient algorithms (Lauritzen & Spiegelhalter, 1988; Pearl, 1988) and tools to implement them (Jensen, 1993; SERENE, 1999) have been developed. Hence it is only recently that it has been possible to perform propagation in networks with a reasonable number of variables. The recent explosion of interest in BNs is due to these developments, which mean that for the first time realistic size problems can be solved.

6.4 Influence Diagram

An *influence diagram (ID)* was originally a compact representation of a decision tree for a symmetric decision scenario: One is faced with a specific sequence of decisions, and between each decision one observes a specific set of variables. Nowadays, an ID is a BN expanded with *utility functions* and with *variables representing decisions*, in order to provide decision-making capabilities within the model. The utilities and decisions are both represented using nodes of distinguishing shapes in contrast to that of BN variables. In fact, the subset of an ID that consists of only *chance nodes* is a BN. Therefore, by definition:

$$\text{“ID”} = \text{“BN”} + \{\textit{decisions} \ \& \ \textit{utilities}\}$$

An ID that uses only these elements is a simple but powerful communication tool, and one that can also be used to perform a quantified assessment of the decision problem. It

provides an intuitive graphical representation of the decision problem and for it to be solved, a *strategy* (i.e., a decision preference) yielding the *highest expected utility* has to be computed. A strategy is a set of functions; to each decision variable is specified a function from which the relevant past returns a decision. The algorithms for probability updating can be modified to solving IDs.

6.4.1 Preferences and Utilities

Similarly to BNs, IDs are very useful in showing the structure of the domain, that is, the structure of the decision problem (Gámez, *et al.*, 2004). The network must be acyclic, and there must exist a directed path that contains all decision nodes in the network. These decision nodes (usually drawn as rectangles or squares) represent variables that are under control of the decision maker and model the decision alternatives available to the decision maker. The nodes include a specification of the available decision options (i.e., choices). Edges into decision nodes indicate time precedence: an edge from a random variable to a decision variable indicates that the value of the random variable is known when the decision will be taken, and an edge from one decision variable to another indicates the chronological ordering of the corresponding decisions.

"Utility" is a figure of merit for a decision alternative that reflects how successfully the decision-maker's values and preferences will be addressed by implementing that alternative. Since decision-makers are interested in making the best possible decisions (i.e., the preferences) for an application, utilities are therefore associated with the state configurations of the network. Utility nodes (normally drawn as diamond-shaped or hexagons) represent these utilities. Each utility node has a utility function that to each configuration of states of its parents associates a utility (Utility nodes do not have children). Making decisions influences the probabilities of the configurations of the network. One can therefore compute the expected utility of each decision alternative (the global utility function is the sum of all the local utility functions). The alternative with the highest expected utility is chosen; this is known as the *maximum expected utility (MEU) principle*.

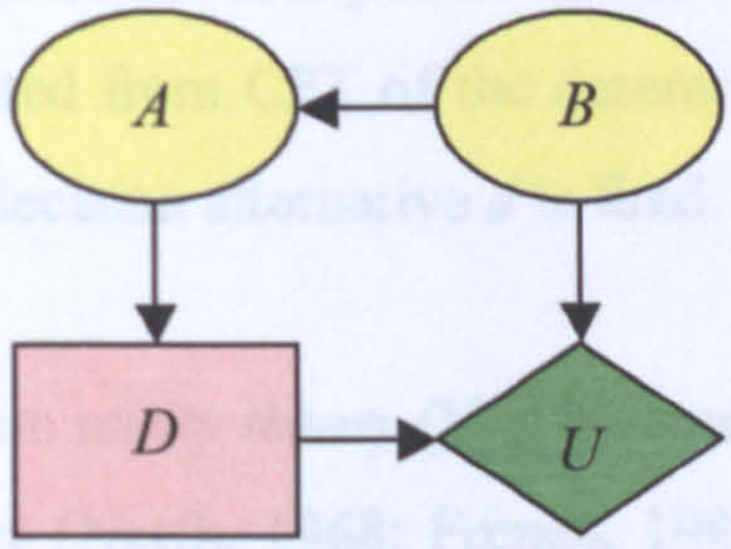


Figure 6.9: A simple Bayesian decision model

Figure 6.9 shows a simple ID in which the prior probability distribution of the influencing node B determines the conditional probability of the influenced node A. The decision D is based on the probability of A, and the utility U is a function of D, given the state of B. B and D are independent of each other.

6.4.2 Maximum Expected Utility

For an outcome state, S, the *expected utility (EU)* of a given alternative is that utility of a decision-maker facing uncertainty calculated by considering utility in each possible outcome state and constructing a weighted average, where the weights are the decision-maker's estimate of the probability of each outcome state. In theory then, one can imply that:

"Decision Theory = Probability Theory + Utility Theory"

In order to assess the decision alternatives in D, a utility table $U(D, S)$ is needed to yield the utility for each configuration of decision alternative and outcome state for the determining variable. The *expected utility (EU)* of a given decision alternative d is calculated by:

$$EU(d) = \sum_{S} P(S \mid d)U(d,S) \qquad (6.26)$$

where $U(d, S)$ are the entries of the utility table in the value node U. The conditional probability $P(S|d)$ is computed from CPT of the determining variable having outcome states, $s \in S$, given that the decision alternative d is fired.

There is the presumption from *utility theory* (Von Neumann & Morgenstern, 1964), and as well from *decision theory* (North, 1968; French, 1988), that humankind is *rational* when inferring subjective value (or utility) from choices (or preferences). This implies that decision-makers maximise their utility wherever possible. Based on this, two principles are then used to determine the existence of the utility function:

- *Utility principle*: If a decision-maker obeys the axioms of utility, then there exists a real-valued function, U, that operates on states such that $U(X) > U(Y)$ if and only if X is preferred to Y and $U(X) = U(Y)$ if and only if there is no preference between X and Y.

- *Maximum expected utility (MEU) principle*: This implies that a rational decision-maker should choose an action that maximises expected utility of outcome states. Thus, given that $d_1, d_2, \ldots, d_k$ are the mutually exclusive decision alternatives of D, the decision alternative d that gives MEU is:

$$MEU(d) = \max_{d}\{EU(d_1), EU(d_2), \ldots, EU(d_k)\} \qquad (6.27)$$

Evaluation of the ID is done by setting the value of the decision node to a particular choice of action (i.e., best *risk control option (RCO)*), and treating the node just as a nature node with a known value that can further influence the values of other nodes. The action's utility is calculated, first by calculating the conditional probabilities for the parents of the utility node using standard inference algorithm, and then feeding the results to the utility function. *Hugin* will calculate these utilities on the assumption that all future decisions will be made in an optimal manner (using all available evidence at the time of each decision). Similar considerations also apply to the remaining decisions.

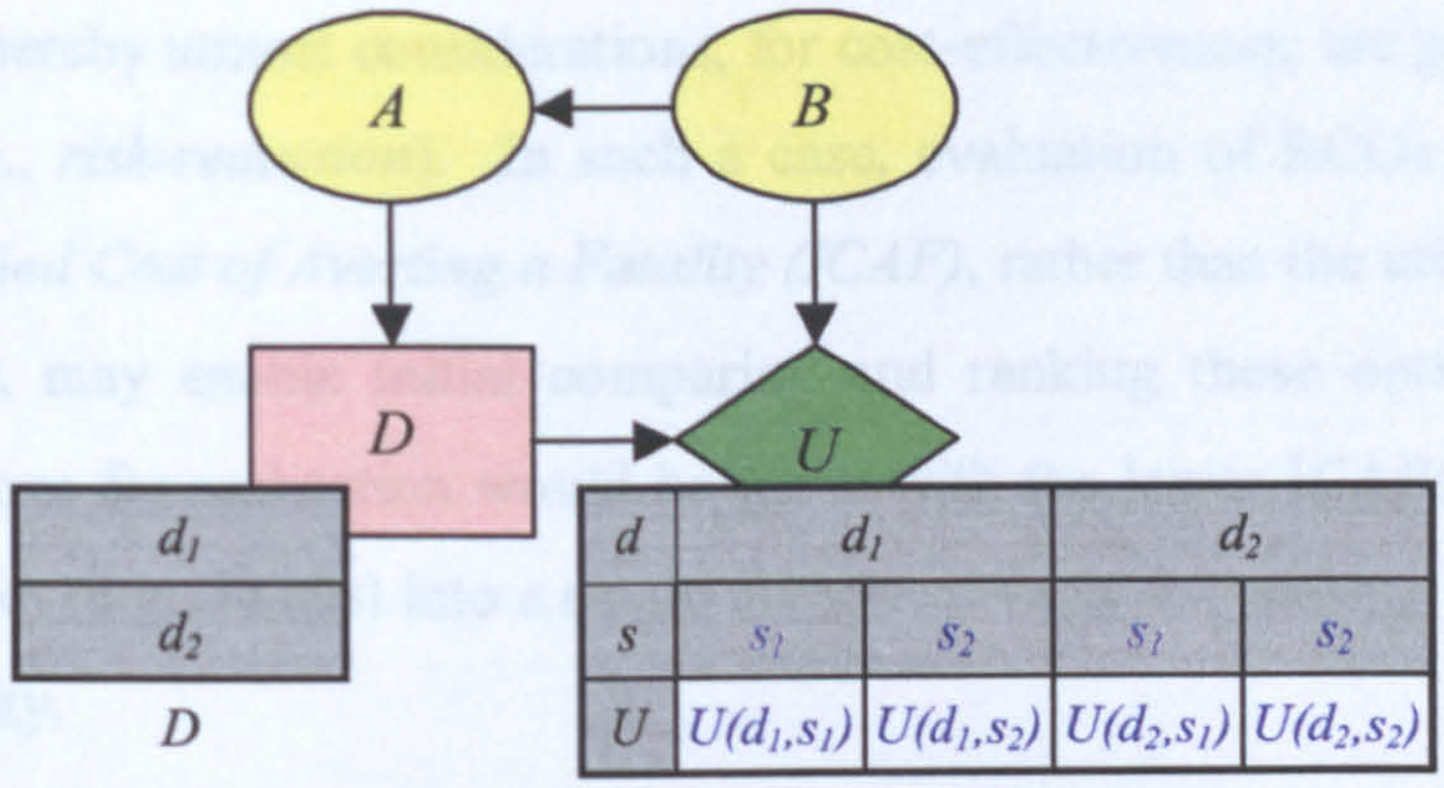


Figure 6.10: ID showing decision alternatives and quantified utility

Figure 6.10 shows the encoded node table for a decision node, D, and a utility node, U. D has two alternatives: d_1 and d_2. If a decision is made based on d_1, then the expected payoff (i.e., U) of outcome states s_1 and s_2 for B is quantified with the value of $U(d_1,s_1)$ and $U(d_1,s_2)$ respectively. However, if a decision is made based on d_2, then U of outcome states s_1 and s_2 for B is quantified with the value of $U(d_2,s_1)$ and $U(d_2,s_2)$ respectively. The EU (i.e., the sum of the weighted payoffs for the decision alternative) for both alternatives can thus be calculated as:

$$EU(d_1) = P(s_1|d_1)U(d_1,s_1) + P(s_2|d_1)U(d_1,s_2)$$
$$EU(d_2) = P(s_1|d_2)U(d_2,s_1) + P(s_2|d_2)U(d_2,s_2)$$

When the values of the variables that are parents of the first decision node in the ID have been observed, one expects to know the MEUs for the alternatives of this decision. The decision alternative d that provides the MEU is given by:

$$MEU(d) = \max_{EU}\{EU(d_1), EU(d_2)\}$$

The utility figures are usually given in terms of property, health, finances, liability, people, environment, departmental image, public confidence, etc. as applicable to the analytical domain. Utility theory can be used in both *decision-making under risk* (where the probabilities are explicitly given) and in *decision-making under uncertainty* (where the probabilities are not explicitly given). The theory can be expanded to

application for safety-based marine and offshore decisions through *cost-benefit evaluation*, whereby utmost considerations, for cost-effectiveness, are given to both *cost* and *safety* (i.e., *risk-reduction*). In such a case, evaluation of RCOs according to its values of *Implied Cost of Averting a Fatality (ICAF)*, rather than the utility figures of an outcome state, may enable initial comparing and ranking these options. The more attractive options for realisation would be those with the lower ICAFs. The ability to map preferences (e.g., RCOs) into a single numerical value for ranking follows from the axioms of utility.

6.5 Proposed Bayesian Network Methodology

A BN reasoning process has been developed to provide a natural framework for maritime risk assessment and decision support. A flow chart of the approach is shown in Figure 6.11, and this format ensures that the BN analysis is conducted in a disciplined, well managed, and consistent manner that promotes the delivery of quality maritime decision-making results. The depth or extent of application of the methodology should be commensurate with the nature and significance of the problem. Nonetheless, the entire methodology consists of nine key steps that have been encapsulated within the following three modules:

- Module 1: Visual Bayesian Network Modelling (i.e., Steps 1 and 2).
- Module 2: Inference Algorithm of Bayesian Analysis (i.e., Steps 3 to 7).
- Module 3: Reasoning Evaluation via an Influence Diagram (i.e., Steps 8 and 9).

In building a BN model, one can first focus on specifying the qualitative structure of the domain (Module 1) and then on quantifying the influences. When finished, one is guaranteed to have a complete specification of the probability distributions. Then following evidence propagation (Module 2), an intuitive evaluation for decision-making is enabled through added nodes of decisions and utilities (Module 3). *Hugin* is used as the robust BN programming environment for the risk modelling and its probability calculations.

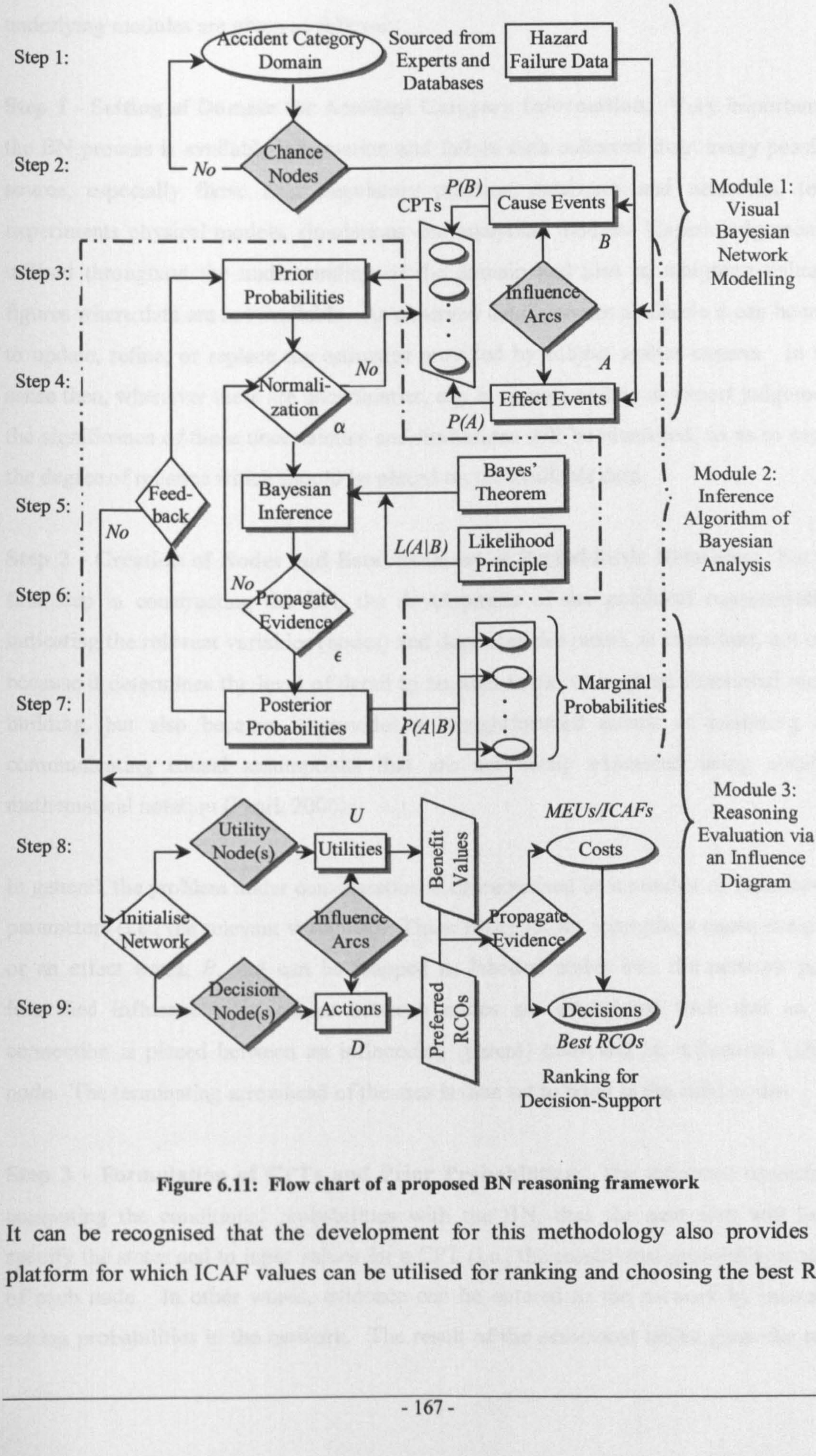


Figure 6.11: Flow chart of a proposed BN reasoning framework

It can be recognised that the development for this methodology also provides the platform for which ICAF values can be utilised for ranking and choosing the best RCO

for a safety-critical maritime system. Explanations for each of the steps in these underlying modules are given as follows:

Step 1 - Setting of Domain for Accident Category Information: Very important to the BN process is available information and failure data collected from every possible source, especially those from regulatory practice, databases and networks, tests, experiments physical models, simulations and analytical models. Expert judgement is utilised throughout the understanding of the domain and also in assigning valuable figures where data are not available. As observed data becomes available it can be used to update, refine, or replace the estimates provided by subject matter experts. In this sense then, whenever there are uncertainties, e.g. in respect of data or expert judgement, the significance of these uncertainties and limitations will be identified, so as to assess the degree of reliance which should be placed on the available data.

Step 2 - Creation of Nodes and Establishment of Probabilistic Relations: For the first step in constructing the BN, the development of the graphical representation, indicating the relevant variables (nodes) and dependencies (arcs), is important, not only because it determines the level of detail to be used in the subsequent functional model building, but also because it provides a straightforward means of analysing and communicating causal assumptions that are not easily expressed using standard mathematical notation (Pearl, 2000).

In general, the problem under consideration is characterised by a number of functions or parameters (i.e., the relevant variables). These relate to, for example, a cause event, *A*, or an effect event, *B*, and can be mapped as labelled nodes into the network pane. Identified influence relationships between nodes are established such that an arc connection is placed between an influencing (parent) node and an influenced (child) node. The terminating arrowhead of the arcs is then set to point at the child nodes.

Step 3 - Formulation of CPTs and Prior Probabilities: The inference consists of computing the conditional probabilities with the BN, thus the next step will be to specify the states and to input values for a CPT (i.e., the conditional probability matrix) of each node. In other words, evidence can be entered to the network by manually setting probabilities in the network. The result of the associated tables gives the prior

probabilities, such as *P(A)* and *P(B)*, for the nodes. However, nodes without any parents give probabilities that are marginal instead of the conditional ones.

Step 4 - Normalization of Probability Values in the CPT: The probability of marginal and conditional terms being true is non-zero and becomes 1 after normalization (i.e., The belief values are normalized on a scale from zero to one). Thus, the process in this step is to normalize the probability values in every column of CPTs. This normalizing (with an encoded inverse value that gives the normalizing constant, $\propto$) has to be done independently for each state of each manifestation across the set of effects.

Step 5 - Processing of Data via Bayesian Inference Induction: The Bayesian inference is enabled via the formula: $P(A|B) = \propto L(A|B)\ P(A)$, which indicates that the likelihood function, $L(A|B)$, is the instrument to pass from prior probability distribution, $P(A)$, to posterior probability distribution, $P(A|B)$, via Bayes' theory. $L(A|B)$ is induced via LP.

Step 6 - Propagation of Evidence: One has to keep in mind that entered evidence propagates in both directions, even though the graph is directed.

Step 7 - Generation of Posterior Probabilities: The beliefs computed after evidence is entered to improve the state of knowledge and thus the prior probability values are updated by calculating revised/updated probabilities, referred to as the *posterior probabilities*, $P(A|B)$. Posterior marginal probabilities, $P(A)$ and $P(B)$ can be obtained via the marginalization process.

If feedback is required due to availability of new data, then the calculated posterior probabilities may become the new prior probabilities for future risk assessment. However, they proceed forward to provide basis for action.

Step 8 - Creation of Decision Node(s) for Preferred RCOs: Initialising the network retracts all findings entered in the risk analysis domain. An ID should be constructed so that one can see exactly which variables (represented by discrete chance nodes) are known at the point of deciding for each decision node. Where the state of a chance

node is known at the time of making a decision, one must add a link from the chance node to the decision node. Where the state of a chance node is known before some given decision, and this chance node has impact on another chance node which is also known before the decision, only the last chance node needs to have a link to the decision node. This means that their only need to be a directed path from a chance node to a decision node if the chance node is known before the decision is made.

Evaluation of the ID is done by setting the value of the decision node to a particular choice of action (i.e., best RCO), and treating the node just as a nature node with a known value that can further influence the values of other nodes.

Step 9 - Creation of Utility Node(s) for Values of Achievable Benefits: The action's utility is calculated, first by calculating the conditional probabilities for the parents of the utility node using the standard inference algorithm, and then feeding the results to the utility function. The utility figures can be given in terms of property, health, finances, liability, people, environment, public confidence, etc. When propagating, one can follow the expected utility of choosing each decision in the next decision node in the decision sequence in the node list pane. The best of the RCOs provides the MEU or lowest ICAF value. Hence, the ranking of the RCOs resulting from the domain case study can be used by decision-makers at all levels and in a variety of contexts without a requirement of specialist expertise.

6.6 Maritime Application of Reasoning in Bayesian Models

To illustrate the universal applicability of BNs and IDs to decision problems, it is best to imagine trying to model a situation in which causality plays a role but where an understanding of what is actually going on is incomplete. Thus things need to be described probabilistically and by inference. Therefore, the demonstration of the modelling and reasoning perspective of this powerful tool is given in the following settings:

- A typical ship evacuation scenario (a marine case study).

- Authorised vessels to floating, production, storage and offloading (FPSO) installation collision scenario (an offshore case study).

6.6.1 Case Study of an Typical Evacuation Scenario

The safety of people onboard a ship in distress is very much dependent on effective emergency *escape, evacuation and rescue (EER)* operational system (final barrier to avoid fatalities) being in place and being enabled in due time. As the EER system in place would have to be activated due to the occurrence of some major accident situations, a *risk contribution tree (RCT)* of the underlying situations may well provide a suitable platform for putting out a BN evacuation model. The RCT of Figure 4.10 in Chapter 4, Section 4.7.1 provides such a modelling platform. However, conditional probabilities where not deduced during the trial FSA study, which makes it difficult to model this RCT scenario with confidence. Besides, eliciting conditional probabilities can be quite problematic without expert being available to provide such inputs and sound logic or techniques. As such, a generic solution is being modelled to provide an insight of BN modelling to the marine and offshore industry.

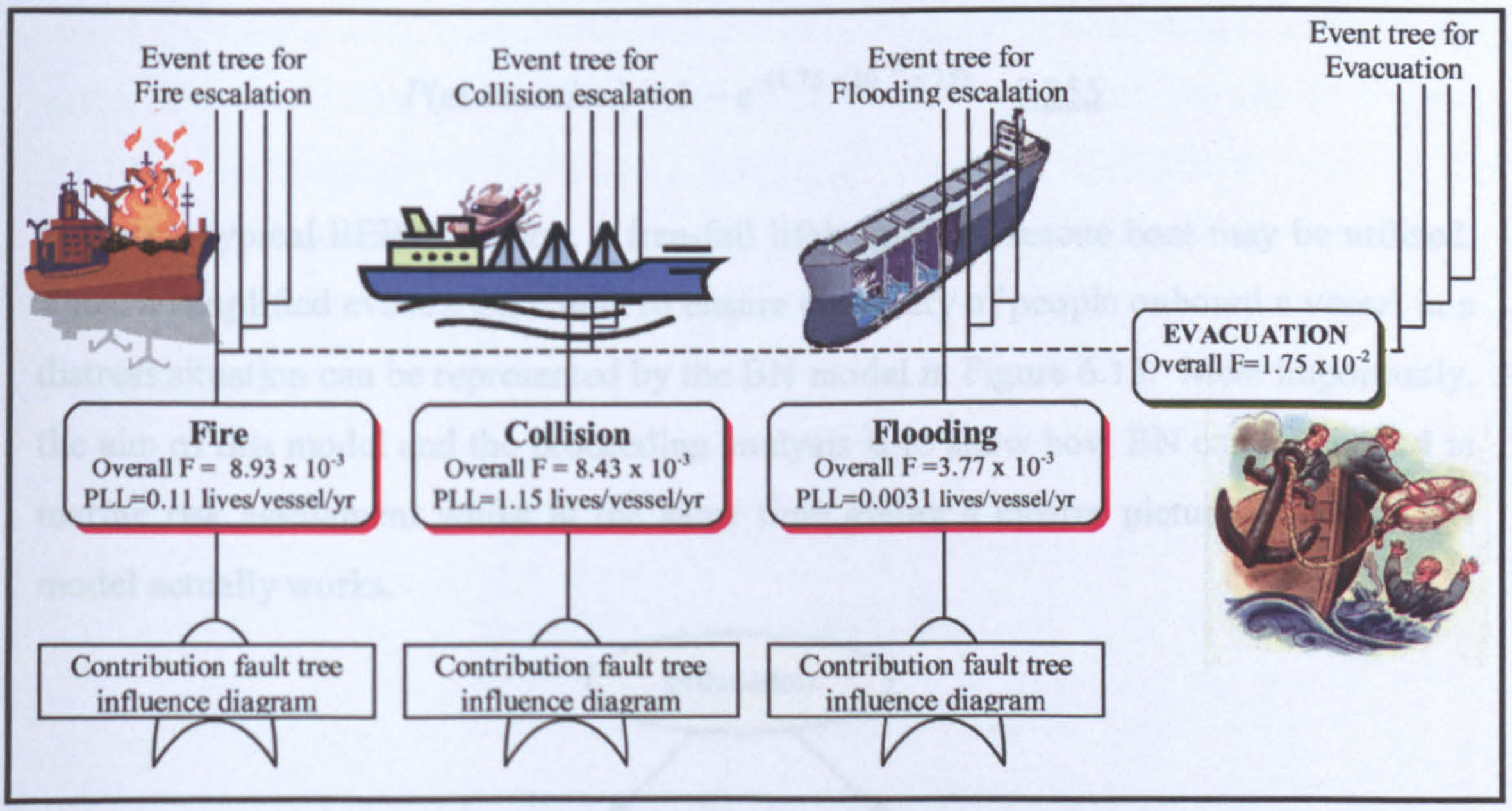


Figure 6.12: Risk contribution from major hazards leading to a marine evacuation scenario

A generic RCT for effecting the evacuation modelling is shown in Figure 6.12. It comprises a contribution fault tree and an escalation event tree for the accident category of fire, collision and flooding events, together with an evacuation event tree relevant to the accident categories. Each contribution fault tree of the RCT also has the integration of influencing factors (e.g., technical, organisational and human factors (See Chapter 1, Section 1.2.2)).

The *frequency (F)* and the *potential loss of life (PLL)* values shown in Figure 6.12 represent some generic data that may be derived for these critical events from an incident database. Frequency distributions need to be converted into probability distributions for use in BN, while the PLLs can be applied in cost effectiveness calculations for use in ID. Since a *failure frequency*, F, in marine assessments is well expressed in terms of per vessel operating year, the overall F values in the RCT can be considered as their *failure rate,* λ, value. If the failure were to follow an exponential distribution, then Equation 2.4 in Chapter 2, Section 2.5.3 can be applied to obtain the equivalent probability values for the failure states. This distribution may be used in this case study RCT since it is similar to the discrete Poisson distribution when the occurrence of the event is zero. So for example, given that a ship has an operational life expectancy of 25 years, evacuation being necessary can be calculated as:

$$P(evacuation) = 1 - e^{-(1.75 \times 10^{-2} \times 25)} = \underline{0.355}$$

For some typical EER operation, a free-fall lifeboat and a rescue boat may be utilised. Thus, a simplified evacuation model to ensure the safety of people onboard a vessel in a distress situation can be represented by the BN model in Figure 6.13. Most importantly, the aim of this model and the proceeding analysis is to show how BN can be applied in marine risk assessment whilst at the same time giving a clearer picture of how a BN model actually works.

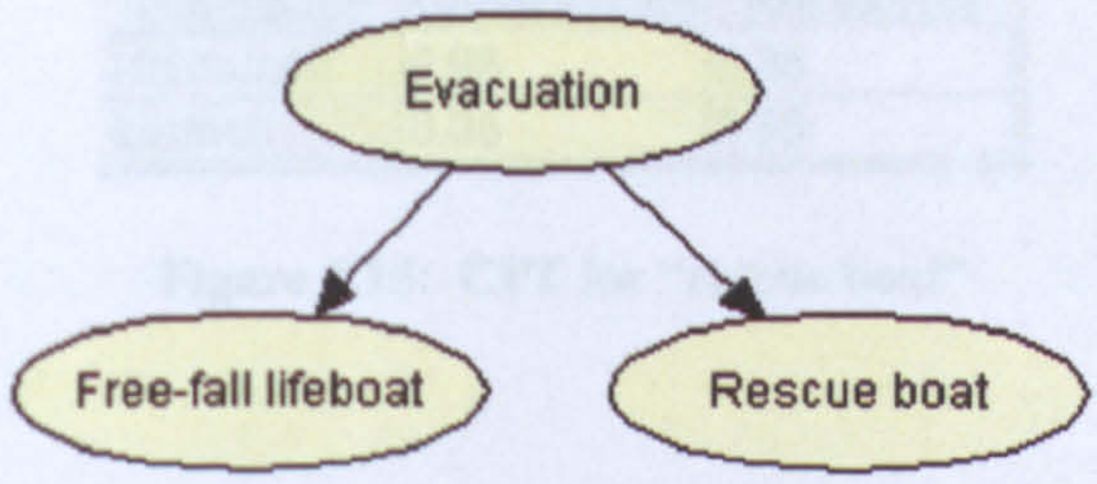


Figure 6.13: Simplified BN showing a marine evacuation scenario

To start with, this case study setting has been modelled in a perspective such that, "*evacuation being necessary*" does not imply that free-fall lifeboat will not be launched, but that there is a high probability on their launch (or usage). This is modelled in the BN by filling in a CPT for the "*free-fall lifeboat*" node (Figure 6.14).

Free-fall lifeboat

Edit Functions View

Evacuation	Unnecessary	Necessary
No launch	0.92	0.04
Launch	0.08	0.96

Figure 6.14: CPT for "free-fall lifeboat"

This CPT is actually the *conditional probability* of the variable "*free-fall lifeboat*" given the variable "*evacuation*". The possible values (launch or no launch) for "*free-fall lifeboat*" are shown in the first column. Note that a probability is provided for each combination of events (four in this case). The particular values in this table suggest that the use/launch of free-fall lifeboat(s) is unlikely to increase (8% chance), but once evacuations are necessary, their use is very likely to increase (96% chance). Now let the use/launch of rescue boat(s) be considered. To model the uncertainty about whether or not the use of rescue boat(s) will increase when evacuation is necessary, added to the graph is a new node "*rescue boat*" and an arc from "*evacuation*" to the new node. Although there might not be a great chance that the free-fall lifeboats will not be launched, the rescue boats may not respond quickly in this setting of the evacuation. Therefore, the CPT for "*rescue boat*" (Figure 6.15) is different from the one for "*free-fall lifeboat*".

Resue boat

Edit Functions View

Evacuation	Unnecessary	Necessary
No launch	0.95	0.35
Launch	0.05	0.65

Figure 6.15: CPT for "rescue boat"

The CPT associated with the node "*evacuation*" is somewhat different in nature. This node has no "parent" node in this example, and consequently, only needs to be assigned a CPT without conditions (Figure 6.16).

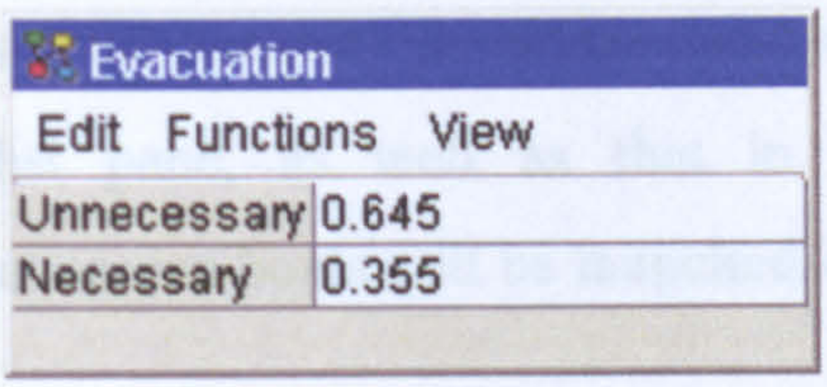


Figure 6.16: CPT for "evacuation"

Determining the probabilities of CPTs is done in several ways. In an instance as this example, it might be a simple case of assigning the probabilities based on the statistical data obtained from a marine incident database, or from experts with good experience to predict the subjective probabilities.

Having entered the probabilities, the BN can now be used to do various types of analysis. The most important use of BN in this case study is in revising probabilities in the light of actual observations of events (in BN modelling, these are called *evidences* for the maritime BN).

The values of these conditional probabilities can be used to obtain the unconditional probabilities. For example, the unconditional probability that free-fall lifeboats will be launched can be calculated as follows:

$$P(\text{'free-fall lifeboat' launch}) = (P(\text{'free-fall lifeboat' launch} \mid \text{no-evacuation}) \times P(\text{no-evacuation})) + (P(\text{'free-fall lifeboat' launch} \mid \text{evacuation}) \times P(\text{evacuation}))$$

$$= (0.08 \times 0.645) + (0.96 \times 0.355) = \underline{0.392}$$

The rule used here to compute the unconditional probability is called *marginal probability*. Now the unconditional probability that free-fall lifeboats will be launched is known to be 0.392 (i.e., 39.2%).

By running the BN for this evacuation scenario, as can be seen in Figure 6.17, *Hugin* gives to the left its the *node list pane* and to the right the *modelled network pane*. The *monitor window* placed near corresponding node in the network pane gives exactly the same as those in the node list pane, thus they are not always necessary (as they can take up too much space). They are used mainly for nodes that have special interest. As can be seen from the node list pane, as well as that in the monitor window, the unconditional probability that rescue boats will be launched is 26.3%.

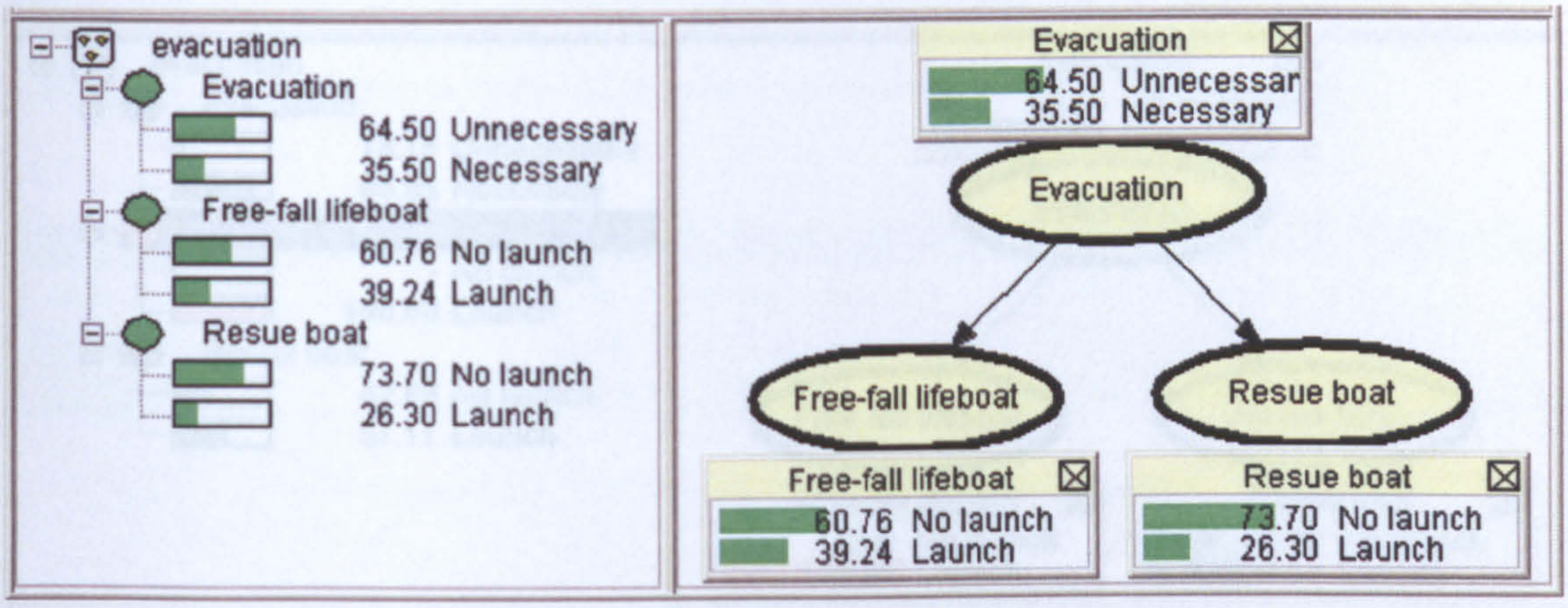


Figure 6.17: BN showing results for unconditional probabilities in evacuation scenario

Here comes the reasoning exquisiteness of BNs. Suppose the launching of free-fall lifeboat is known to increase. In this case the evidence that "*free-fall lifeboat = launch*" is entered, and then this evidence can be used to determine:

- The *updated probability* of evacuation taking place.
- The *updated probability* that the use of rescue boat also increases.

Using Bayes' rule, the probability of evacuation taking place can be calculated as:

$$P(evacuation \mid \text{'free-fall lifeboat' launch})$$

$$= \frac{P(\text{'free-fall lifeboat' launch} \mid evacuation) \times P(evacuation)}{P(\text{'free-fall lifeboat' launch})}$$

$$= 0.96 \times 0.355/0.392 = \underline{0.869}$$

Using *marginal probability*, the probability that there will be rescue boat launch (see Figure 6.18) can be calculated as:

$$P(\text{'rescue boat' launch}) = (P(\text{'rescue boat' launch} \mid \text{no-evacuation}) \times P(\text{no-evacuation})) + (P(\text{'rescue boat' launch} \mid \text{evacuation}) \times P(\text{evacuation}))$$

$$= (0.05 \times 0.131) + (0.65 \times 0.869) = \underline{0.571}$$

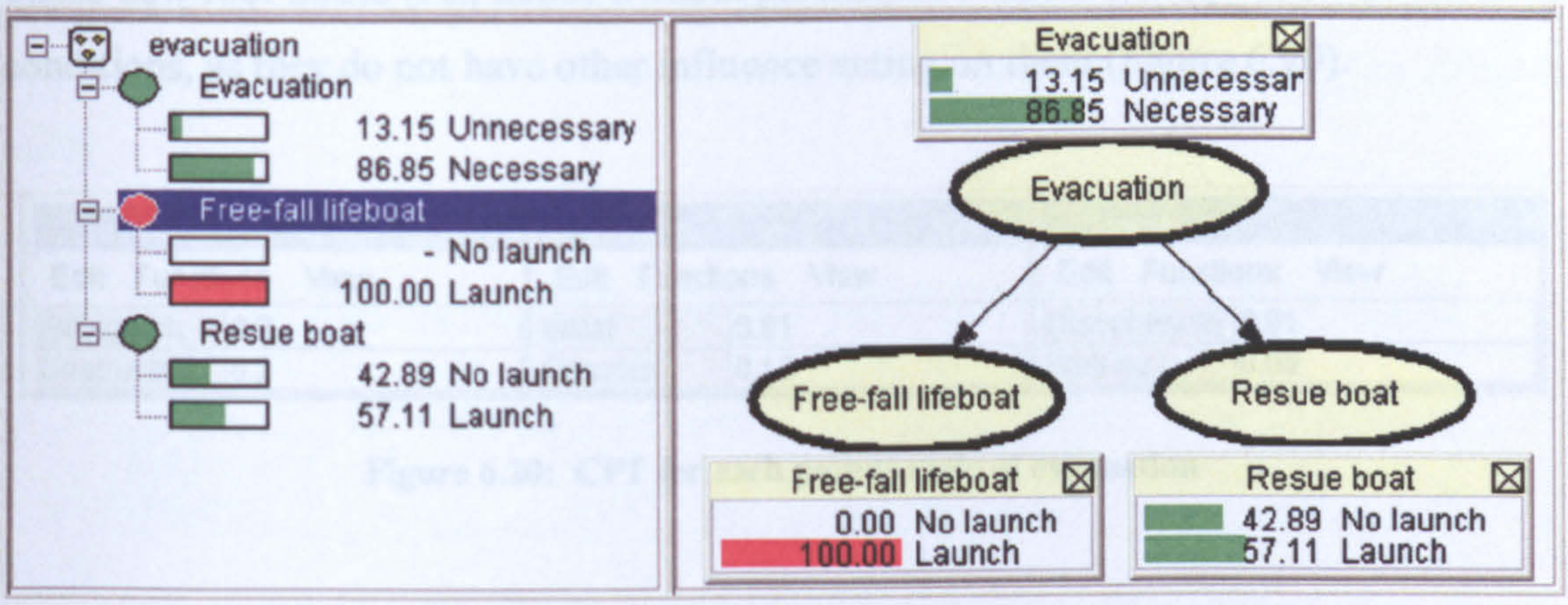


Figure 6.18: BN showing propagated results when free-fall lifeboat is launched

Entering pieces of evidence and using them to update the probabilities in this way is called *propagation*. Figure 6.18 shows the results with "*evidence*" node for free-fall lifeboats being launched represented by an *evidence bar* in both the node list pane and in its monitor window in *Hugin*. As would be expected, the probability of evacuation taking place increases dramatically to 86.9%, when the launch of free-fall lifeboats has been observed. This update is due to *diagnosis* (i.e., *bottom-up*) *inference* from the "*free-fall lifeboats*" node to the "*evidence*" node. Furthermore, the updated probability of evacuation taking place results in bringing up the probability for launching of rescue boats to 57.1%, by way of *causal* (i.e., *top-down*) *inference*.

Now, there lies the provision that the major marine accident of *fire*, *collision* and *flooding*, which are often variables for external factors, may lead to evacuation. The use of such information has to imply that a *new node* is created and added as *parents* to the evacuation node, for each of these accident categories (Figure 6.19).

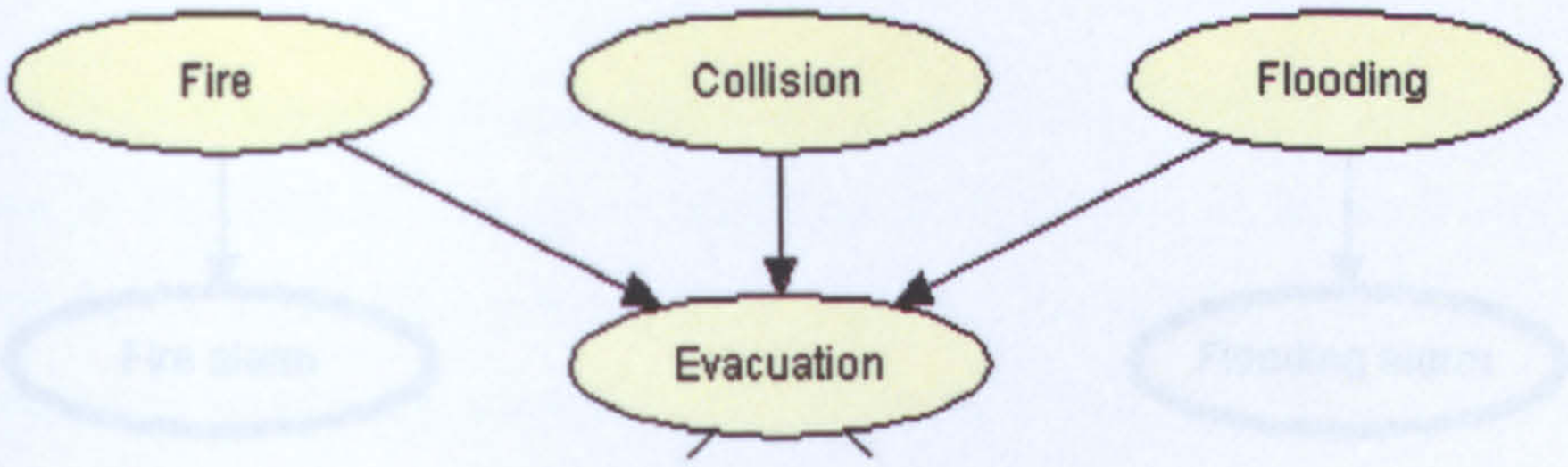


Figure 6.19: Fire, collision and flooding added as parent nodes of evacuation

These new root nodes (i.e., nodes without parents) of evacuation require a CPT without conditions, as they do not have other influence acting on them (Figure 6.20).

Fire

Edit Functions View

Extinguish...	0.8
Destructive	0.2

Collision

Edit Functions View

Intact	0.81
Capsize	0.19

Flooding

Edit Functions View

Discontinuity	0.91
Sinking	0.09

Figure 6.20: CPT for each parent node of evacuation

For the evacuation node, on the other hand, an expanded new CPT is used to reflect the fact that it is now conditional on its three parent nodes (i.e., "*fire*", "*collision*" and "*flooding*"). In other words, the evacuation CPT provides "*P(evacuation | fire, collision, flooding)*" (See Figure 6.21).

Evacuation

Edit Functions View

Flooding	Discontinuity				Sinking			
Collision	Intact		Capsize		Intact		Capsize	
Fire	Extinguish...	Destructive	Extinguish...	Destructive	Extinguish...	Destructive	Extinguish...	Destructive
Unnecess...	0.89	0.35	0.34	0.24	0.16	0.13	0.12	0.01
Necessary	0.11	0.65	0.66	0.76	0.84	0.87	0.88	0.99

Figure 6.21: New evacuation CPT reflecting conditional probabilities due to parent nodes

Given that in the event of fire or/and flooding *an alarm* will be triggered, a suitable alarm node as *child node* (shown as the highlighted nodes in Figure 6.22) can each be linked from the nodes of "*fire*" and "*flooding*" respectively.

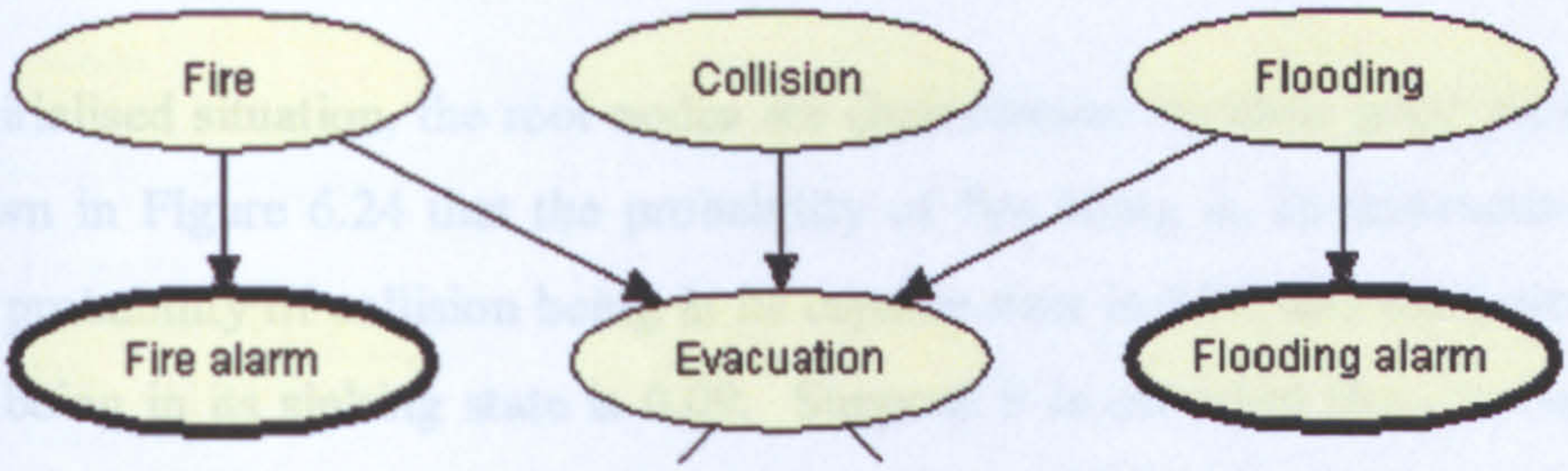


Figure 6.22: A suitable alarm added as individual child node to fire and flooding

Since each of the new alarm node acts on entirely different accident events, their respective CPT provides input values of different conditional probabilities (Figure 6.23).

Fire alarm

Edit Functions View

Fire	Extinquishable	Destructive
Not Activated	0.87	0.001
Activated	0.13	0.999

Flooding alarm

Edit Functions View

Flooding	Discontinuity	Sinking
Not Activated	0.89	0.001
Activated	0.11	0.999

Figure 6.23: CPT for individual alarm nodes of fire and flooding

Analysing from the fact that the JPD "*P(evacuation, fire, collision, flooding)*" is known, the unconditional probability that evacuation is necessary, "*P(evacuation)*" can be given by marginalizing out the "*fire*", "*collision*" and "*flooding*" variables. *Hugin* computes the marginal probability as 35.54% or 0.355 (Figure 6.24). Note that *Hugin* also gives the values of 0.304 and 0.19 as the marginal probability of the "*fire alarm*" and "*flooding alarm*" respectively.

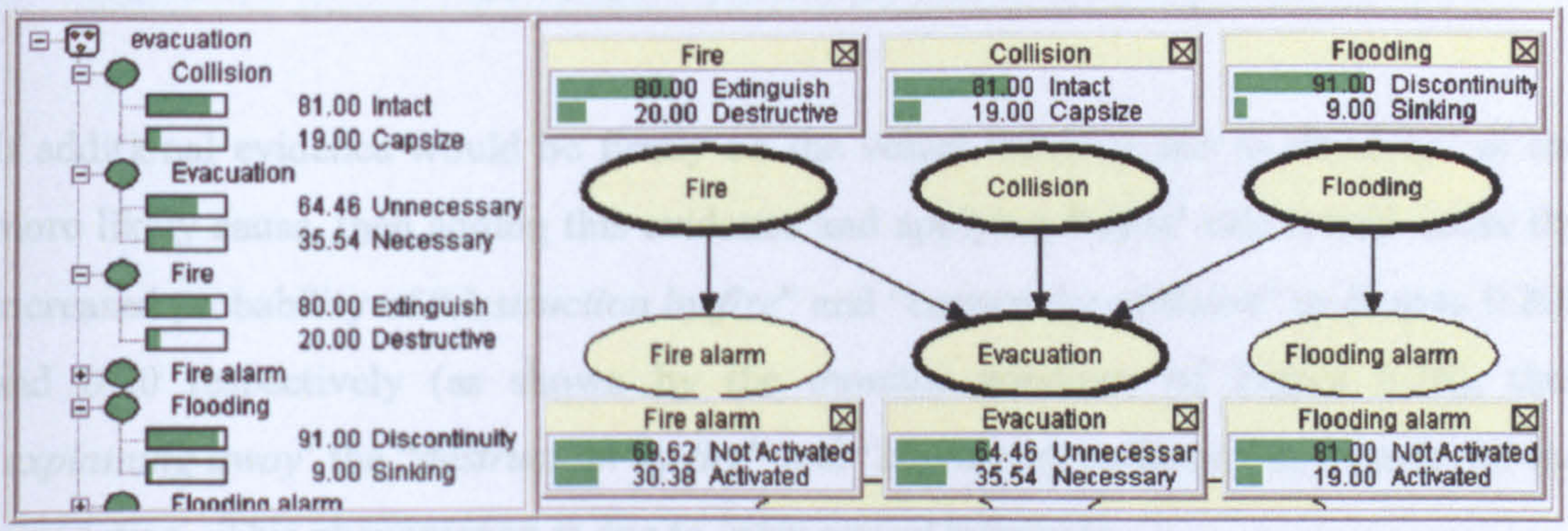


Figure 6.24: BN showing marginalised probabilities of evacuation node and its parents

In this initialised situation, the root nodes are characterised by their prior probabilities. It is shown in Figure 6.24 that the probability of fire being in its destructive state is 0.20, the probability of collision being in its capsize state is 0.19, and the probability of flooding being in its sinking state is 0.09. Suppose it is observed that, "*evacuation is necessary*", then this entered evidence increases the belief in all of the possible causes (namely "*destructive*" for fire, "*capsize*" for collision, and "*sinking*" for flooding) based on *diagnostic inference*. Specifically, applying Bayes theorem yields a revised probability for fire in destructive state of 0.388 (up from the prior probability of 0.20), a revised probability for collision in capsize state of 0.374 (up from the prior probability of 0.19), and a revised probability for flooding in sinking state of 0.217 (up from the prior probability of 0.09) (Figure 6.25). Nonetheless, these revised probabilities are subject to change by the provision of some *additional* observation(s), for example:

- The *additional evidence* firmly on the vessel sinking due to flooding; or
- The *additional evidence* that the fire alarm is activated.

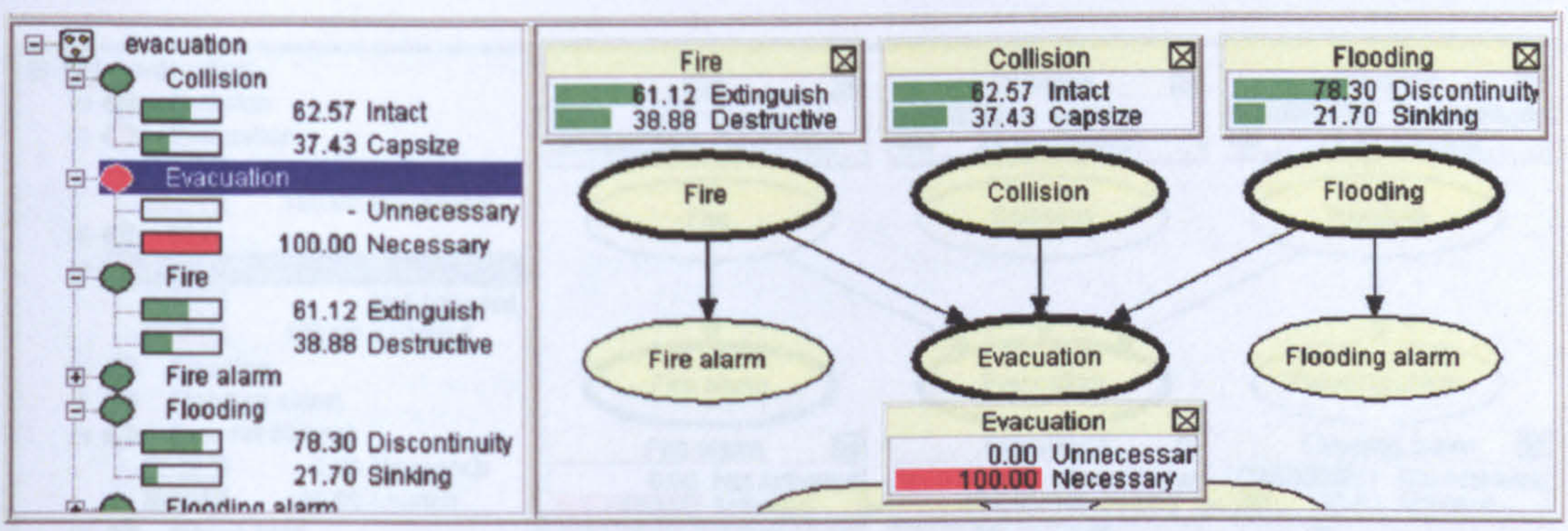


Figure 6.25: BN showing propagated results of evacuation evidence to its parent nodes

If additional evidence would be firmly on the vessel "*sinking due to flooding*" as the more likely cause, then adding this evidence and applying Bayes' rule would cause the increased probability of "*destruction by fire*" and "*capsize by collision*" to drop to 0.208 and 0.20 respectively (as shown by the monitor windows of Figure 6.26), thus '*explaining away*' the "*destruction by fire*" and "*capsize by collision*" as a cause for the evacuation. This phenomenon is due to *inter-causal* inference.

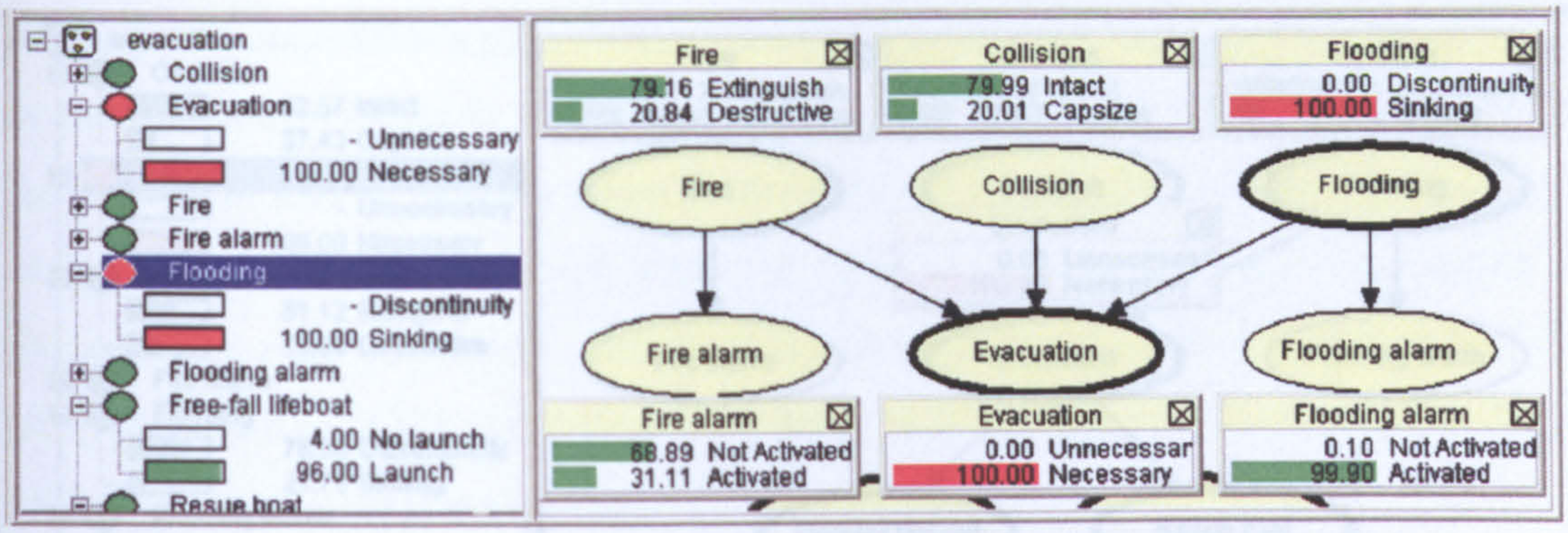


Figure 6.26: BN showing propagated results of both evacuation and flooding evidence

Conversely, if it is discovered that the fire alarm is activated, then entering this evidence and applying Bayes' rule would yield the revised probabilities of 0.83 for destruction by fire, 0.259 for capsize by collision and 0.144 for sinking by flooding (as shown by the monitor windows of Figure 6.27). Thus the odds are that the destructive fire, rather than capsize due to collision and sinking due to flooding, has caused the evacuation to be necessary. Once again, it is said that the necessary evacuation has been '*explained away*'.

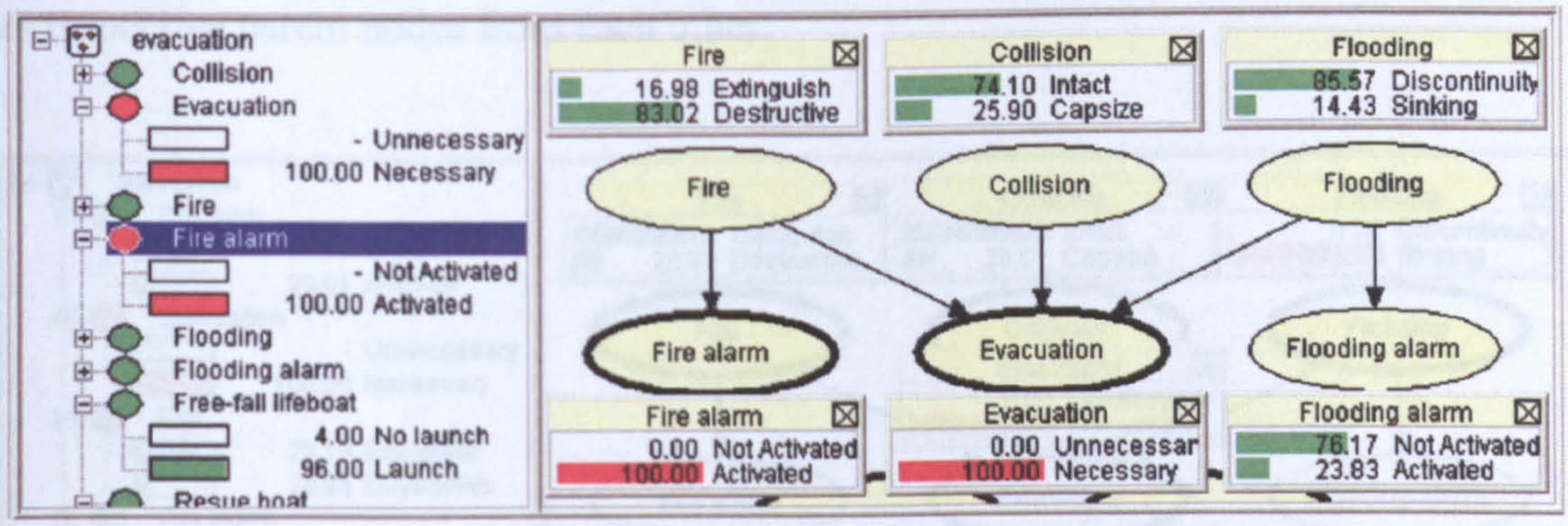


Figure 6.27: BN showing propagated results of both evacuation and fire alarm evidence

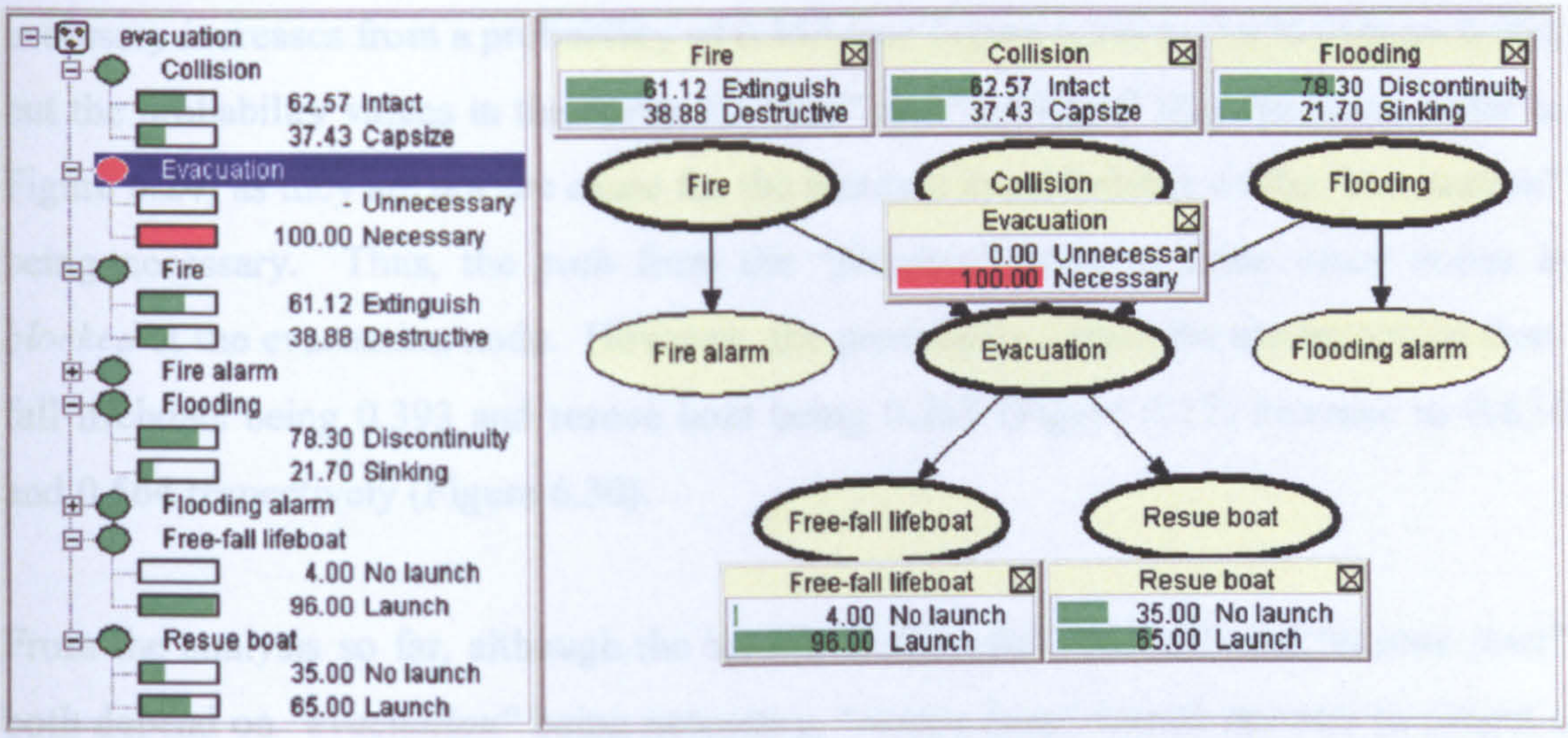


Figure 6.28: BN showing evacuation evidence propagation to free-fall lifeboats and rescue boats

Now, going back to when only evacuation being necessary is observed, the launch of the free-fall lifeboats and rescue boat are seen to have a probability of 0.96 and 0.65 respectively (Figure 6.28) as induced by *causal inference*. However, when the additional evidence of "*flooding by sinking*" is entered, these respective probabilities remain unchanged (Figure 6.29). It is said that the "*evacuation*" node *d-separates* all of its respective parent nodes from each other.

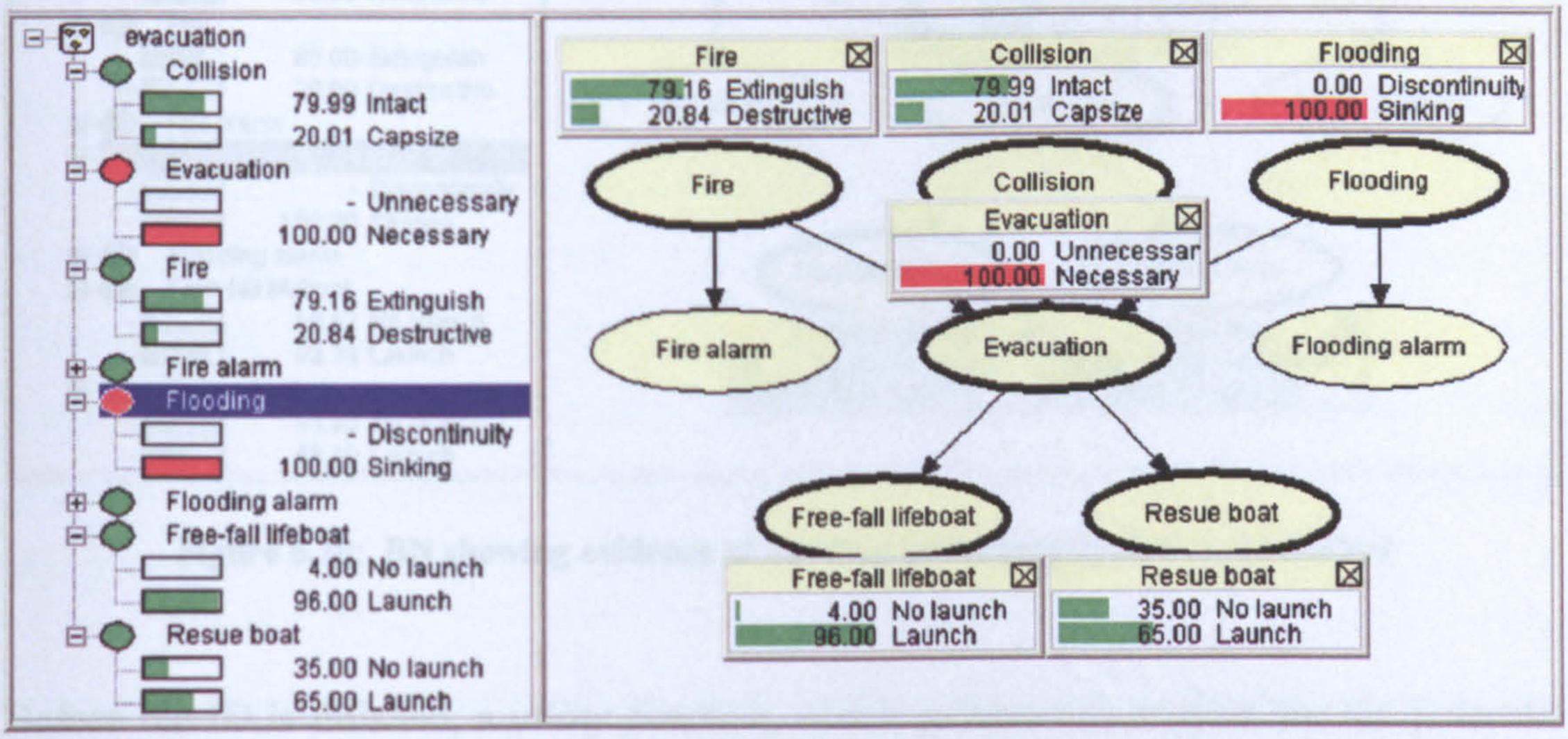


Figure 6.29: Flooding and evacuation evidence propagation to lifeboats and rescue boats

The notion of d-separation (which follows from *human perception*) can also be noticed where only evidence is given for "*flooding by sinking*". In this case, evacuation being

necessary increases from a probability of 0.355 (see Figure 6.24) to 0.856 (Figure 6.30), but the probability values in the nodes for "*fire*" and "*collision*" stay the same (refer to Figure 6.24) as they are not the cause for the increase in probability of the "*evacuation*" being necessary. Thus, the *path* from the "*flooding*" node to these other nodes is *blocked* at the evacuation node. However, the probability values for the launch of free-fall lifeboats being 0.393 and rescue boat being 0.263 (Figure 6.17) increase to 0.834 and 0.564 respectively (Figure 6.30).

From the analysis so far, although the launch of "*free-fall lifeboat*" and "*rescue boat*" both depend on "*evacuation*" being necessary, "*rescue boat*" launch appears to output a probability value that is less than that of the "*free-fall lifeboat*" launch. The risk analyst has the opportunity to do something about this outcome situation. Thus, a *decision node* that depends upon the rescue boat is added into the model, thereby converting the network into an ID. This new type of node will permit the modelling of an effective decision-support solution that outputs *optimal survival* for those onboard the vessel.

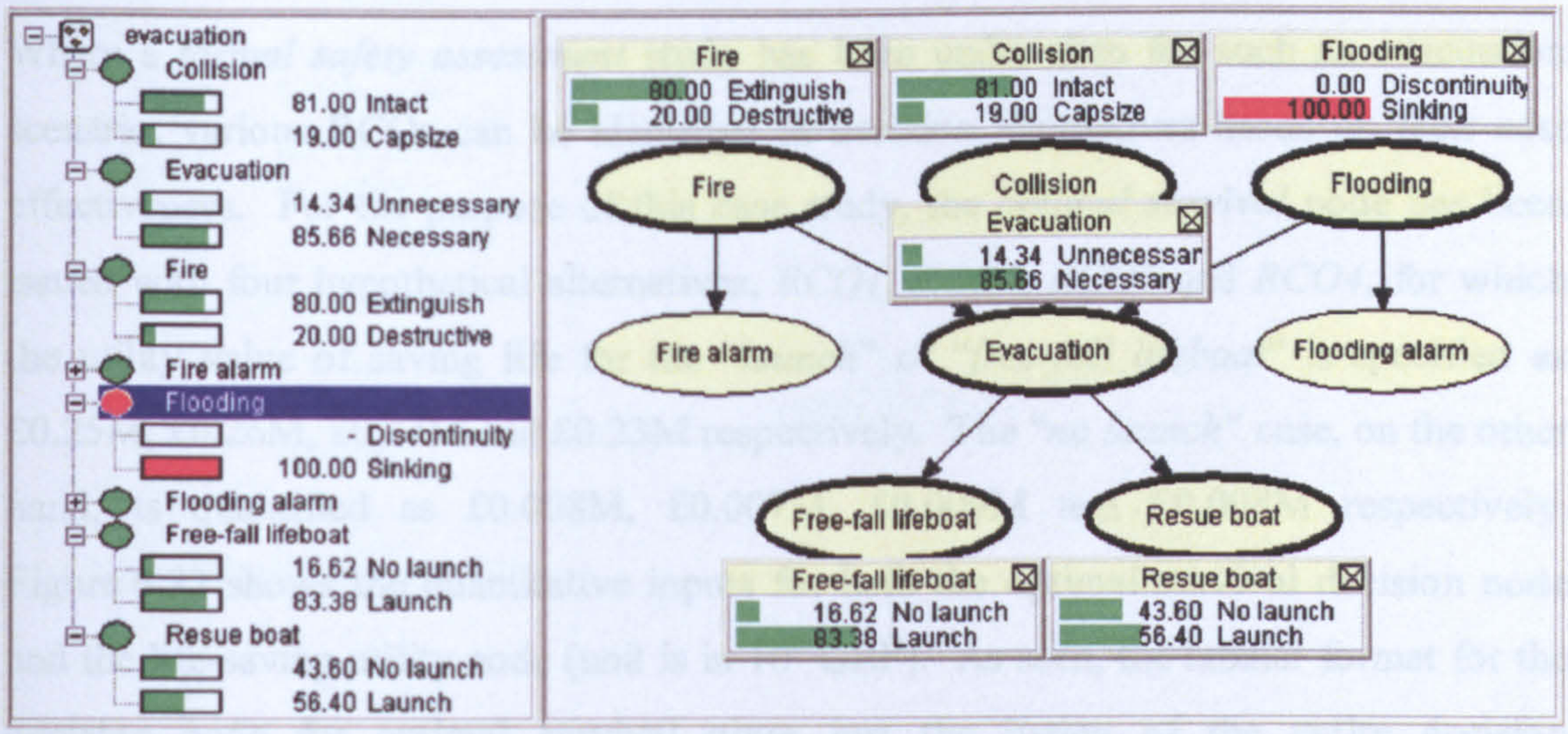


Figure 6.30: BN showing evidence of flooding being propagated to evacuation

Before the ID is finished, a *utility function*, which gathers information for the potential benefits that come with the different implementation options, and as well, enabling the risk analyst to calculate the *expected utility* of the optimal survival, needs to be specified. Given the *outcome state* of "*free-fall lifeboat*", a *value node* of *life-saving*, based on the value of lives saved, is created for specifying these quantitative benefits as

a function of the decision. Figure 6.31 presents the overall view of this evacuation domain ID.

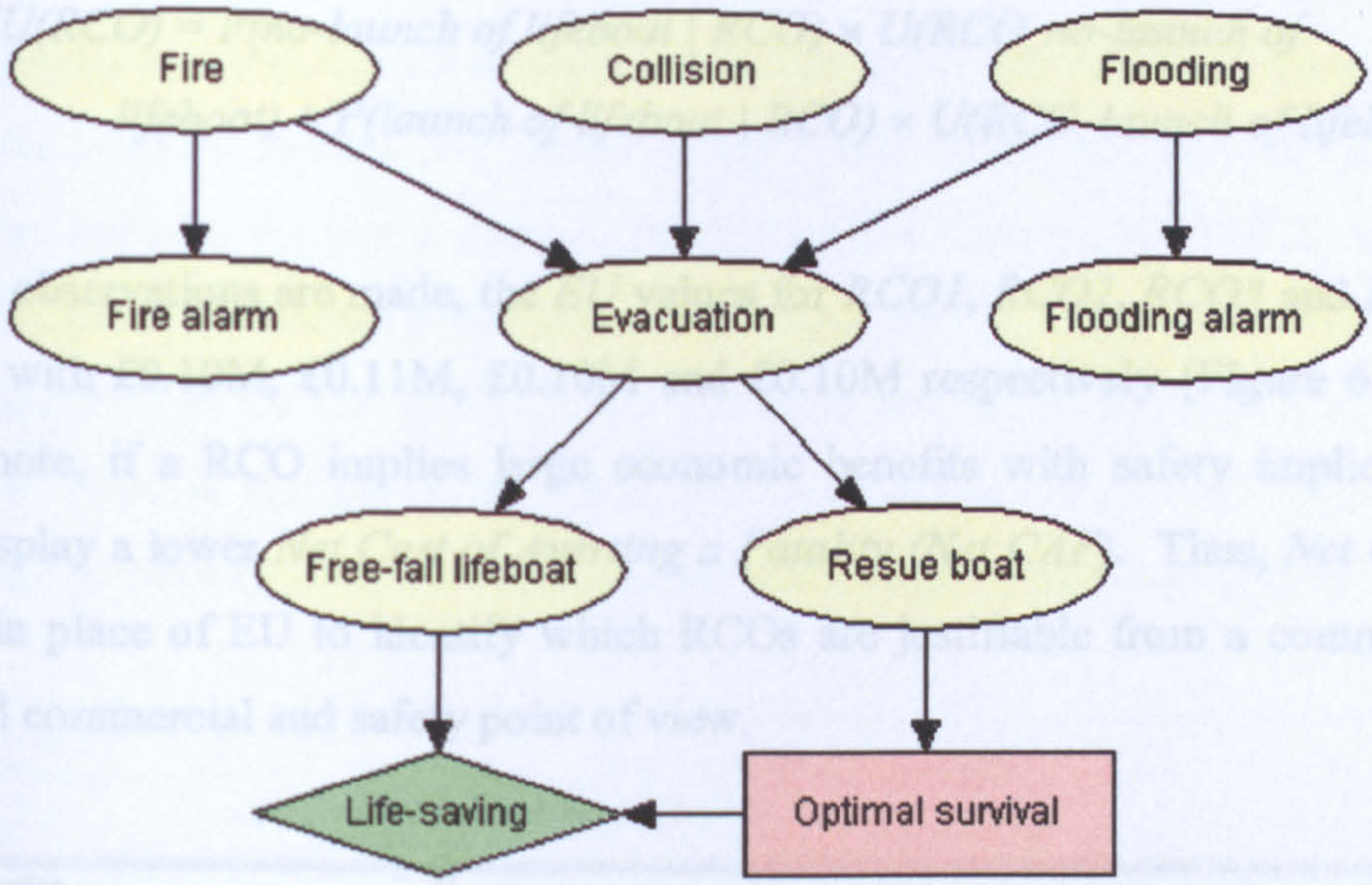


Figure 6.31: Simplified ID showing a marine evacuation domain

Where a *formal safety assessment* study has been undertaken for such an evacuation scenario, various RCOs can be identified as decision alternatives based on their cost effectiveness. For the purpose of this case study, the *optimal survival* node has been issued with four hypothetical alternatives, *RCO1*, *RCO2*, *RCO3* and *RCO4*, for which the utility value of saving life for the "*launch*" of "*free-fall lifeboat*" is specified as £0.25M, £0.26M, £0.24M and £0.23M respectively. The "*no launch*" case, on the other hand, is quantified as £0.008M, £0.007M, £0.009M and £0.008M respectively. Figure 6.32 shows the quantitative inputs for both the optimal survival decision node and the life-saving utility node (unit is in 10^6 GBP). As seen, the tabular format for the decision node for optimal survival gives just the listing of the entire decision alternatives.

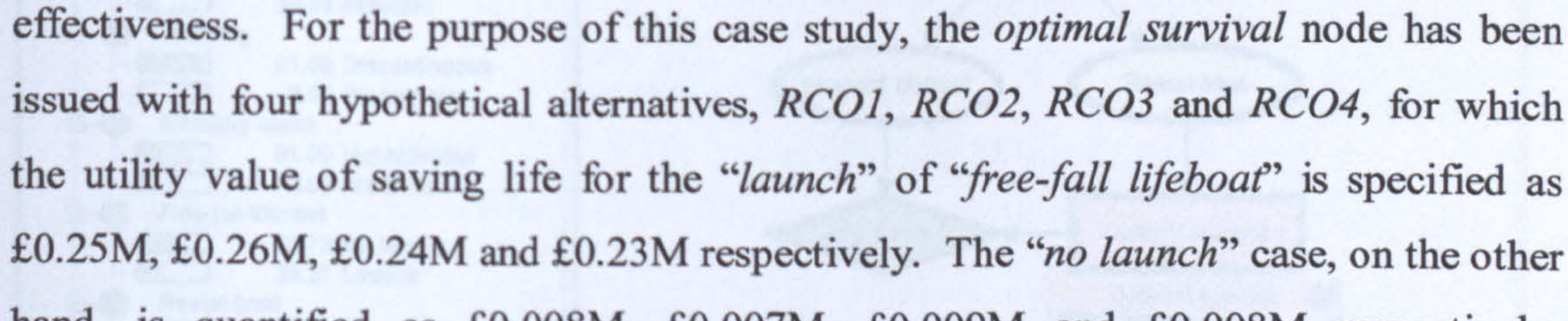


Figure 6.32: Encoded inputs in both the node of optimal survival and life-saving

Hugin can then calculate the *expected utility (EU)* for all of the RCOs as follows:

$$EU(RCO) = P(\text{no-launch of lifeboat} \mid RCO) \times U(RCO, \text{no-launch of lifeboat}) + P(\text{launch of lifeboat} \mid RCO) \times U(RCO, \text{launch of lifeboat})$$

When no observations are made, the *EU* values for *RCO1*, *RCO2*, *RCO3* and *RCO4* are assigned with £0.10M, £0.11M, £0.10M and £0.10M respectively (Figure 6.33). On another note, if a RCO implies large economic benefits with safety implications, it would display a lower *Net Cost of Averting a Fatality (Net CAF)*. Thus, *Net CAF* may be used in place of EU to identify which RCOs are justifiable from a commercial or combined commercial and safety point of view.

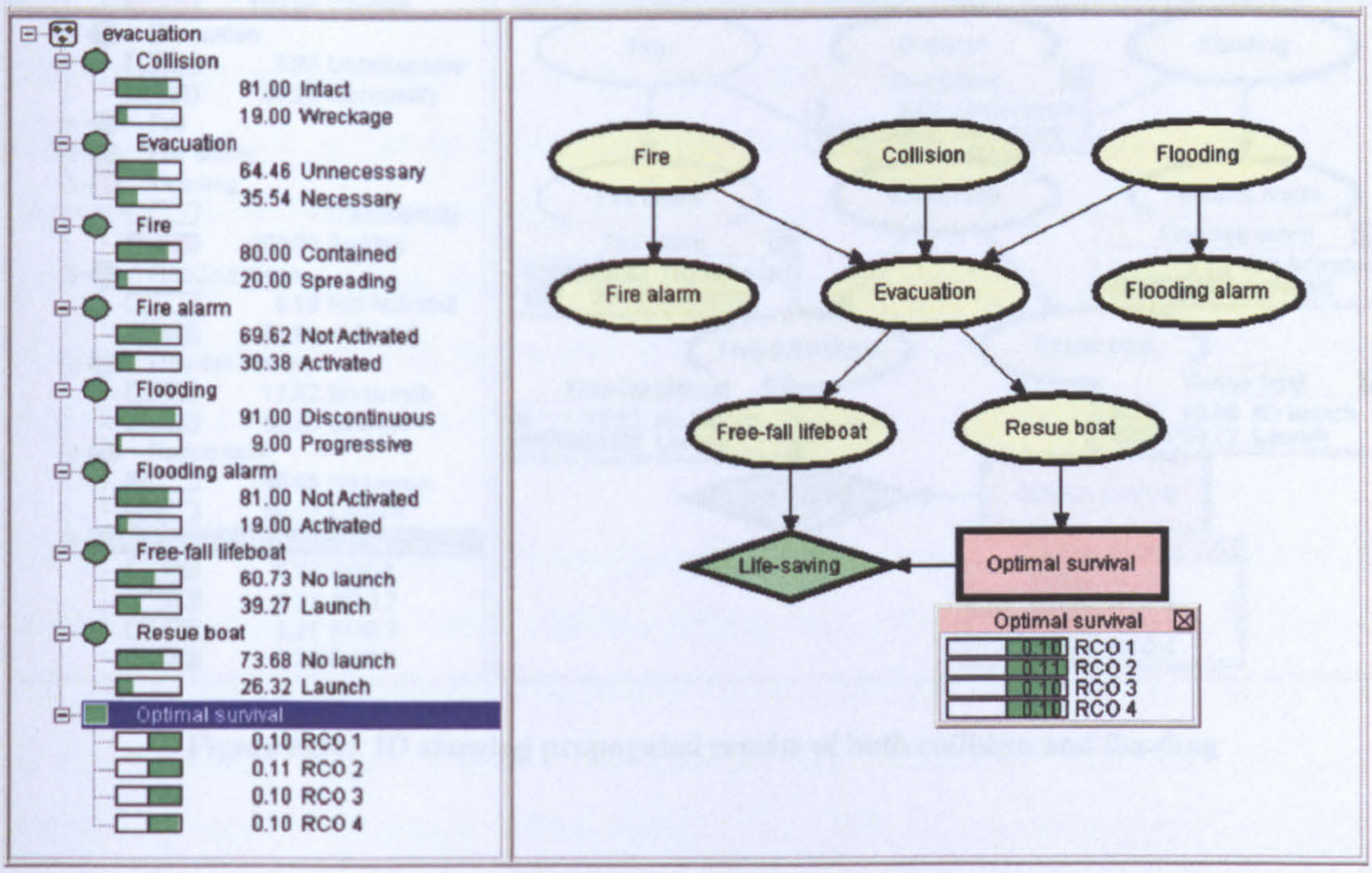


Figure 6.33: ID showing initialised values for optimal survival EU

Once any observation is made, it propagates the evidence by *message passing* and therefore updates the free-fall lifeboat probability. This, in turn, recalculates the EU values for the four decision alternatives. As the best RCOs are those that give the MEUs of optimal survival decision, the RCOs can be ranked accordingly for use in the decision-making process. The MEU is calculated as:

$$MEU(RCO) = \max_{RCO}\{EU(RCO1), EU(RCO2), EU(RCO3), EU(RCO4)\}$$

In a worst-case scenario, collision might cause damage to the structural integrity of the vessel. As a result, capsize and flooding might upshot into the sinking of the ship. Since those onboard the vessel need to survive such a disaster, the RCOs for optimal survival are given a *ranking profile* according to their MEU. The MEU order ranking is *RCO2* (£0.23M), *RCO1* (£0.22M), *RCO3* (£0.21M) and *RCO4* (£0.20M), as shown in the monitor window in Figure 6.34. Thus, the recommendation is for *RCO2* and *RCO1* to be given top priority with respect to implementation of the optimal survival strategy.

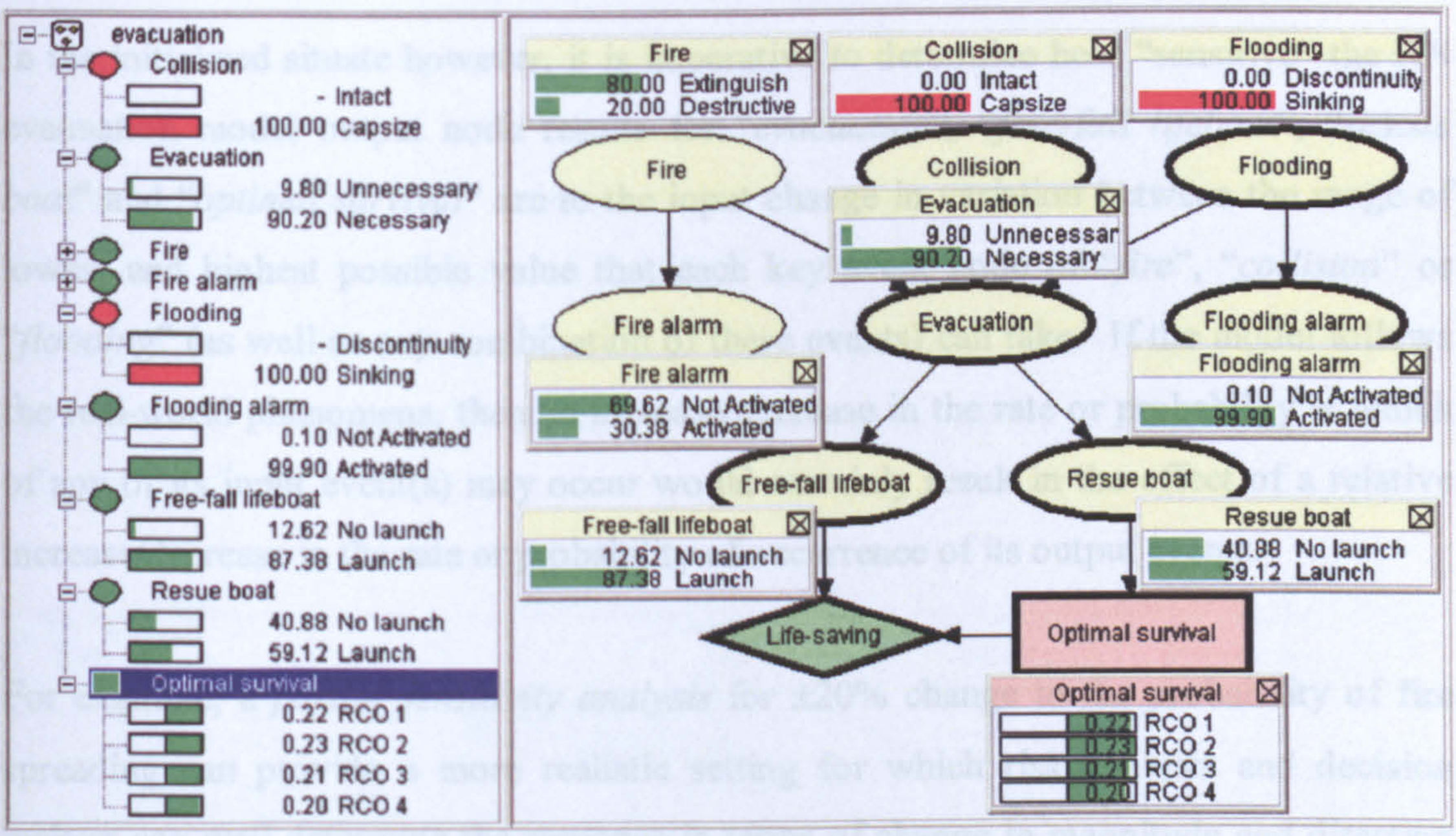


Figure 6.34: ID showing propagated results of both collision and flooding

A number of entered evidence circumstances for this model can be investigated. For example, even with the accidental evidence of all root nodes entered, the calculated MEU emerges again with a ranking order of the RCOs as *RCO2*, *RCO1*, *RCO3* and *RCO4*, although higher MEU values are reached in this setting (as displayed in the node list pane of Figure 6.35).

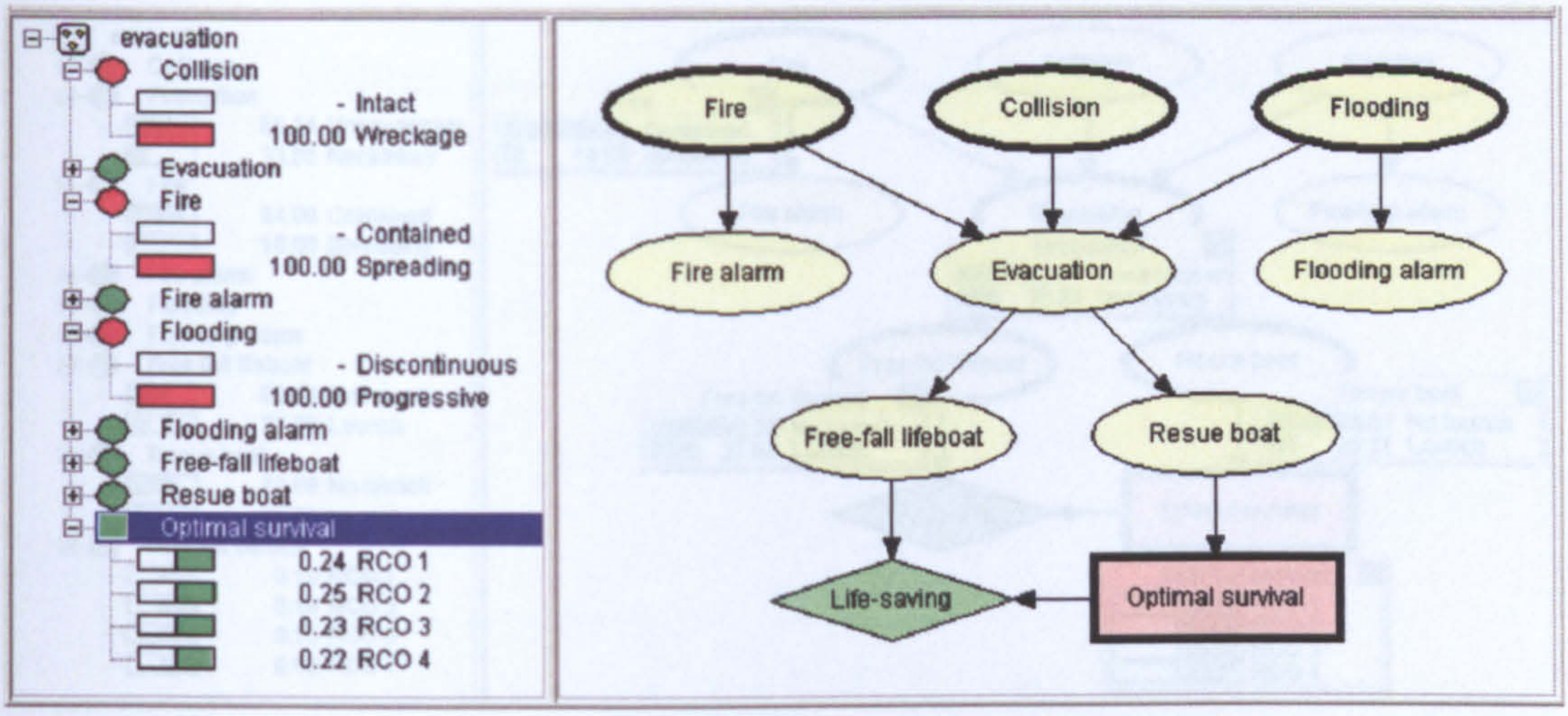


Figure 6.35: ID showing optimal survival MEU after entered evidence on all key root nodes

In the initialised situate however, it is imperative to determine how "sensitive" the BN evacuation model output node results for "*evacuation*", "*free-fall lifeboat*", "*rescue boat*" and "*optimal survival*" are to the input change in variation between the range of lowest and highest possible value that each key event node of "*fire*", "*collision*" or "*flooding*" (as well as any combination of these events) can take. If the model follows the real-world phenomena, then an increase/decrease in the rate or probability at which of any of its input event(s) may occur would certainly result in the effect of a relative increase/decrease in the rate or probability of occurrence of its output events.

For example, a *partial sensitivity analysis* for ±20% change to the probability of fire spreading can provide a more realistic setting for which risk analysts and decision makers can well determine the response in terms of change in magnitude and direction of the resulting output events. To conduct this sensitivity analysis, the lowest probability value in the range, which is 0.16 (i.e., –20% of the initial probability of fire spreading value), replaces the initial input value of 0.20 and then using marginal probability, the probability of evacuation being necessary, free-fall lifeboat launch and rescue boat launch is calculated as 0.339 (≈ –4.7% change), 0.378 (≈ –3.7% change) and 0.253 (≈ –3.8% change) respectively (See Figure 6.36). Likewise, the MEU for optimal survival becomes £0.10M for *RCO1*, £0.10M for *RCO2*, £0.10M for *RCO3* and £0.09M for *RCO4*.

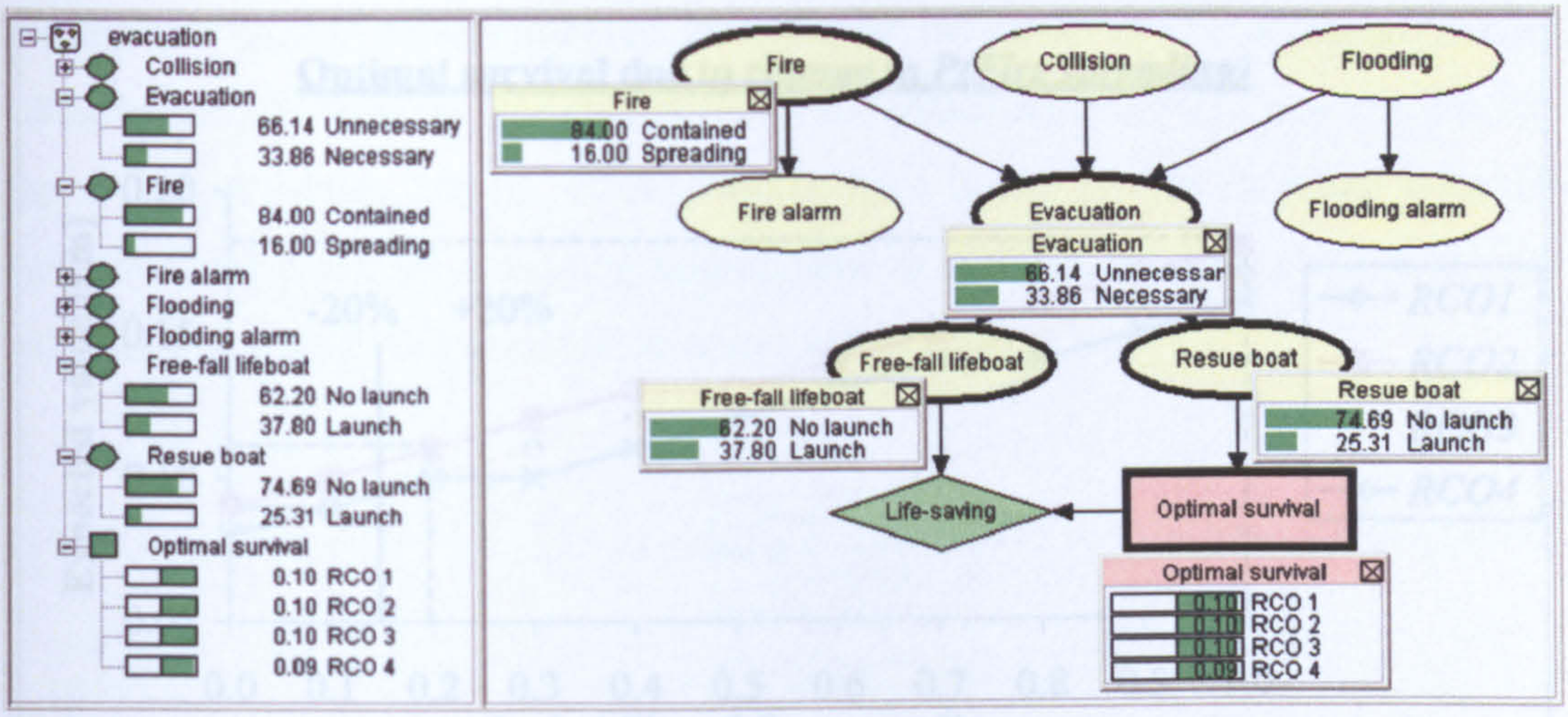


Figure 6.36: ID showing model output values for an initialised –20% of *P*(*fire spreading*)

In repeating the sensitivity analysis calculation after substituting the highest probability value in the range, which is 0.24 (i.e., +20% of the initial probability of fire spreading value), the probability of evacuation being necessary, free-fall lifeboat launch and rescue boat launch is calculated as 0.372 (≈ +4.7% change), 0.406 (≈ +3.7% change) and 0.273 (≈ +3.8% change) respectively (See Figure 6.37). Similarly, the MEU for optimal survival becomes £0.11M for *RCO1*, £0.11M for *RCO2*, £0.10M for *RCO3* and £0.10M for *RCO4*.

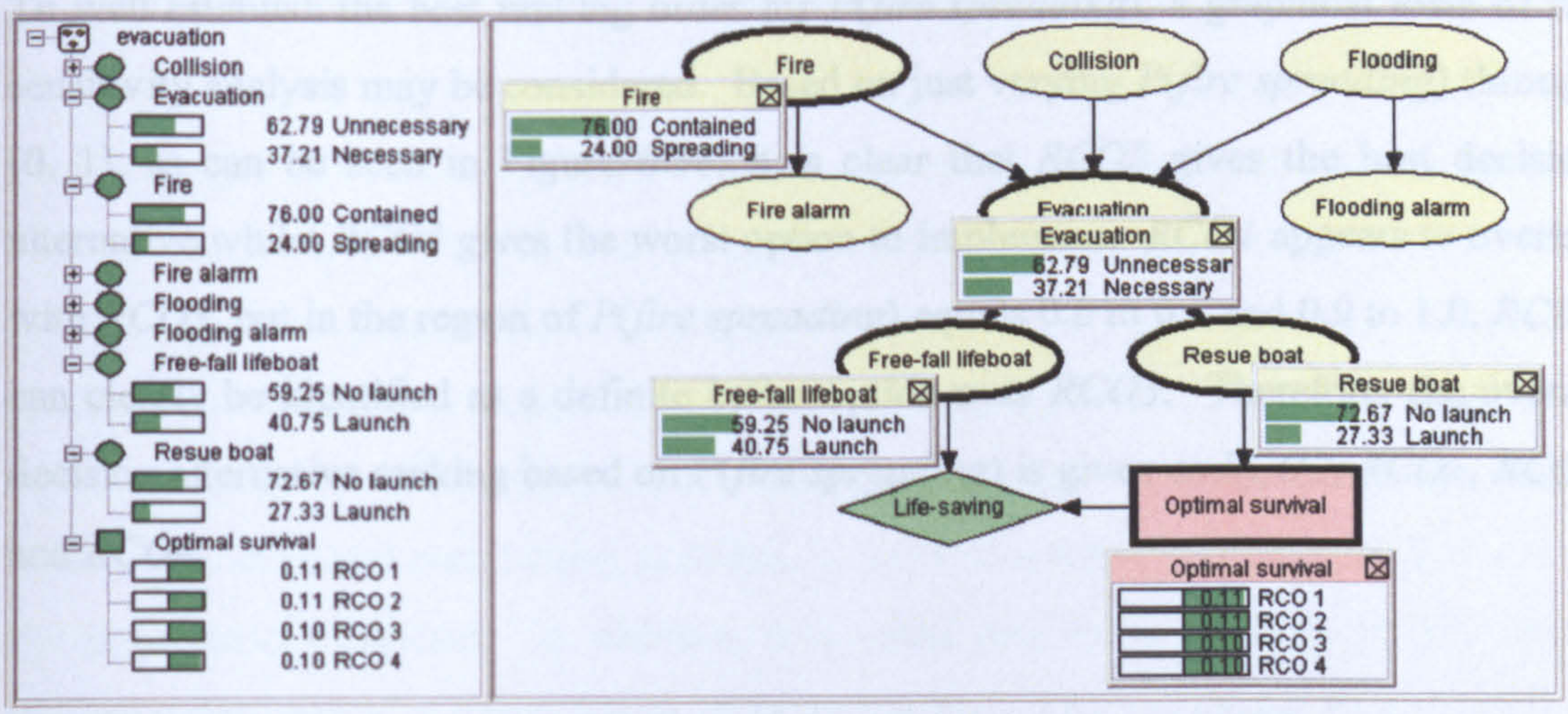


Figure 6.37: ID showing model output values for an initialised +20% of *P*(*fire spreading*)

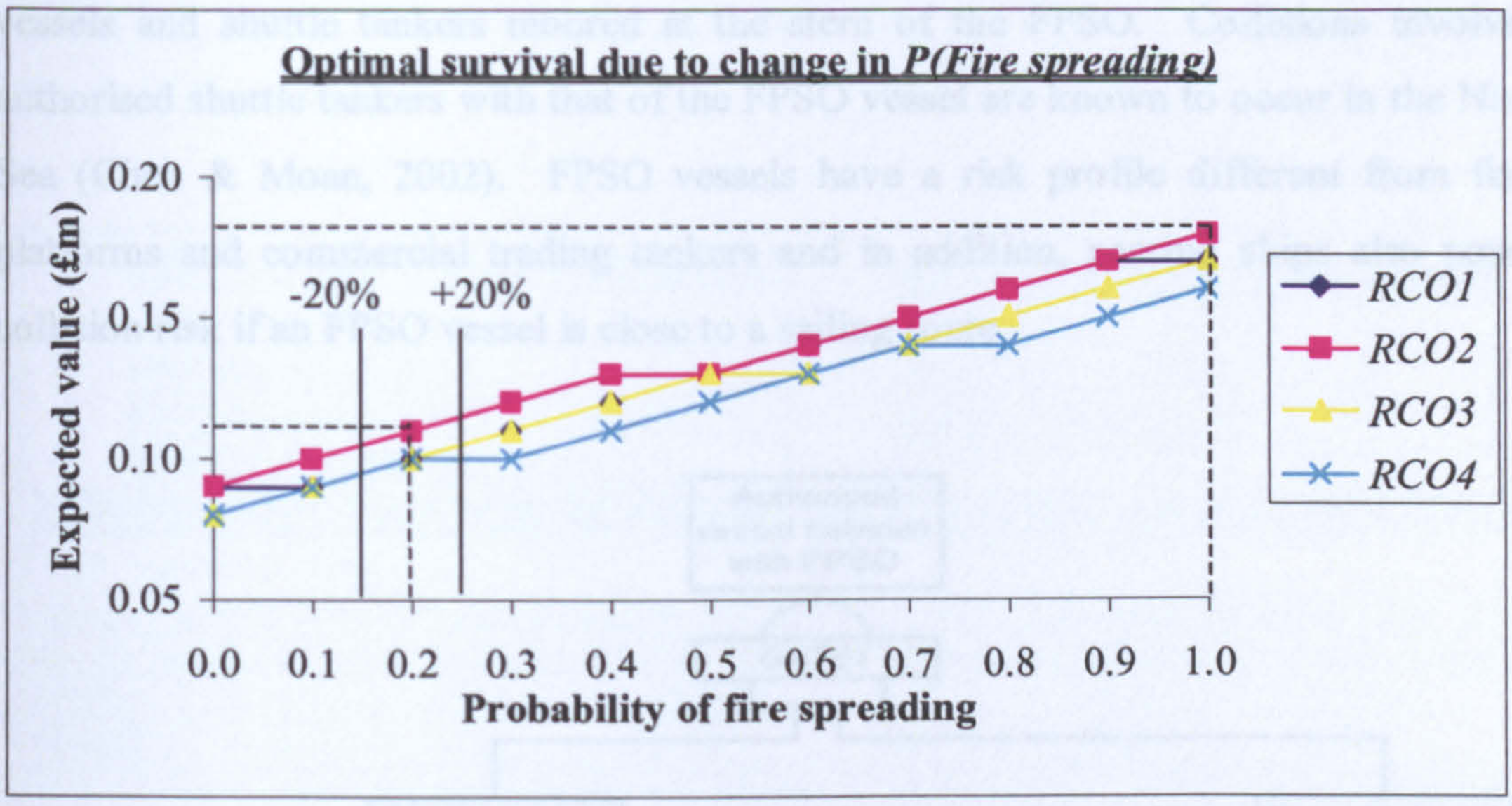


Figure 6.38: Effect of varying *P(fire spreading)* for optimal survival ranking

From the sensitivity study, the effects of the ±20% variation in *P(fire spreading)* reveal that this input parameter is a *linear function* with respect to the probability of the evacuation model outputs. Although the decision for optimal survival is sensitive to the state value of *P(fire spreading)*, it does not quite reveal the ranking order in the ±20% variation setting.

To well establish the best ranking order for *P(fire spreading)*, a graphical form of the sensitivity analysis may be considered. Based on just varying *P(fire spreading)* through [0, 1], as can be seen in Figure 6.38, it is clear that *RCO2* gives the best decision alternative whilst *RCO4* gives the worst option to implement. *RCO1* appears to overlap with *RCO3*, but in the region of *P(fire spreading)* equals 0.0 to 0.1 and 0.9 to 1.0, *RCO1* can clearly be identified as a definite better option over *RCO3*. Therefore, the overall decision alternative ranking based on *P(fire spreading)* is given as *RCO2*, *RCO1*, *RCO3* and *RCO4*.

6.6.2 Case Study of Authorised Vessels to FPSO Collision Scenario

To offload oil for shipment to market, a ship-shaped FPSO vessel that is being stationed in one location, will typically be routinely serviced by authorised supply/standby

vessels and shuttle tankers moored at the stern of the FPSO. Collisions involving authorised shuttle tankers with that of the FPSO vessel are known to occur in the North Sea (Chen & Moan, 2002). FPSO vessels have a risk profile different from fixed platforms and commercial trading tankers and in addition, passing ships also pose a collision risk if an FPSO vessel is close to a sailing route.

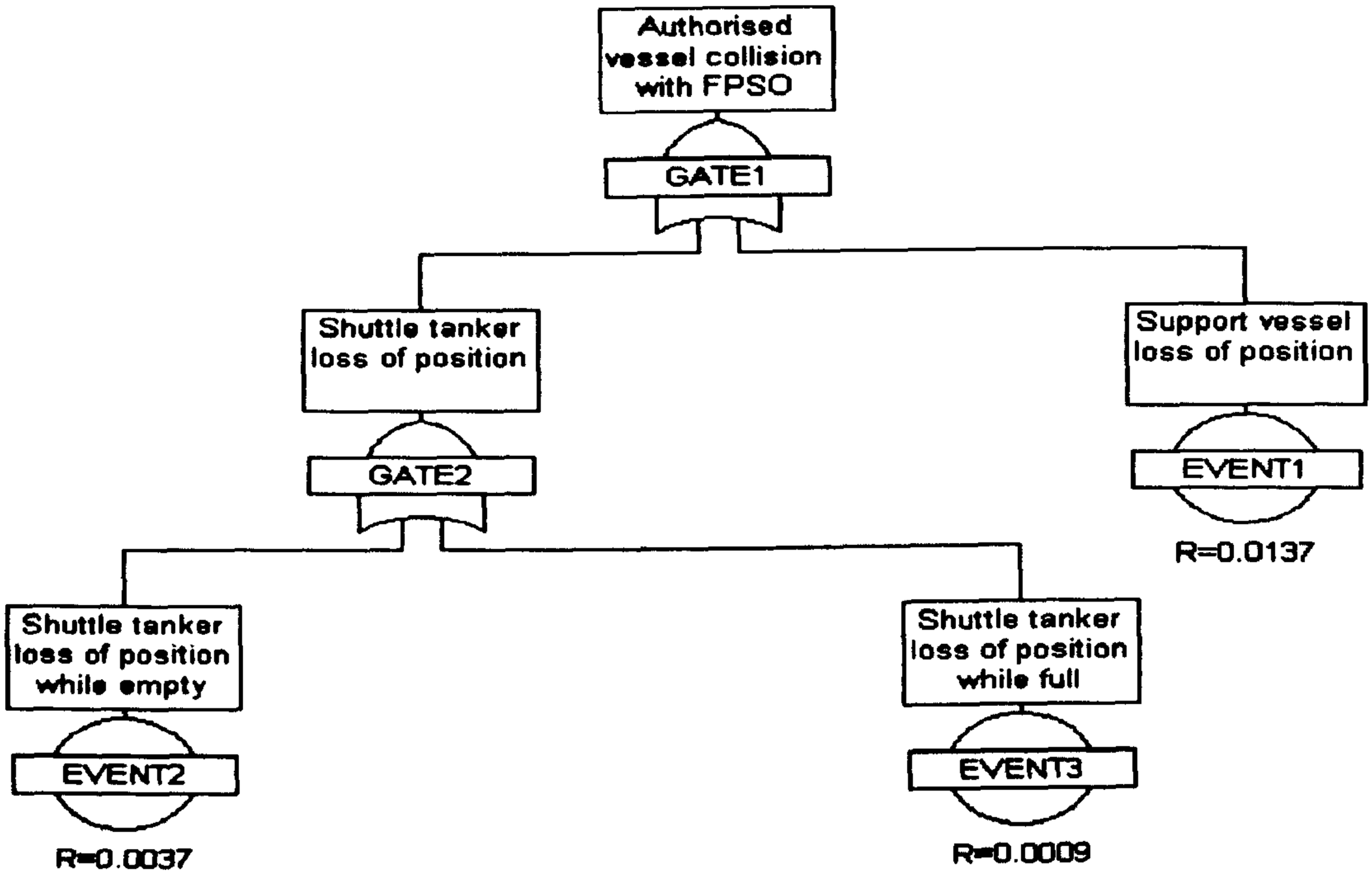


Figure 6.39: Fault tree to estimate frequency of collisions of an FPSO by authorised vessels

The frequency of collision between a shuttle tanker and an installation, or storage unit, is estimated to be 0.0046/year due to failure of the dynamic positioning system. It is assumed that 20 percent (i.e., 0.0009/year) of shuttle tanker collisions occur after loading operations are complete and the fully loaded vessel is leaving the field (Husky Oil, 2000). This relatively low percentage is due to the fact that the shuttle tanker is holding and maintaining position, in order to achieve loading, and is aware of the installation's location. In addition, it is usual practice to perform shuttle tanker loading operations at a safe distance from the facility. The remaining 80 percent (i.e., 0.0037/year) of shuttle tanker collisions are assumed to occur while the tanker is empty and on approach to the facility. The failure of the dynamic positioning system on a maintenance support vessel, causing a collision, is estimated to be 0.0137/year

(Husky Oil, 2000). Figure 6.39 gives the fault tree to estimate frequency of collisions of an FPSO by authorised vessels.

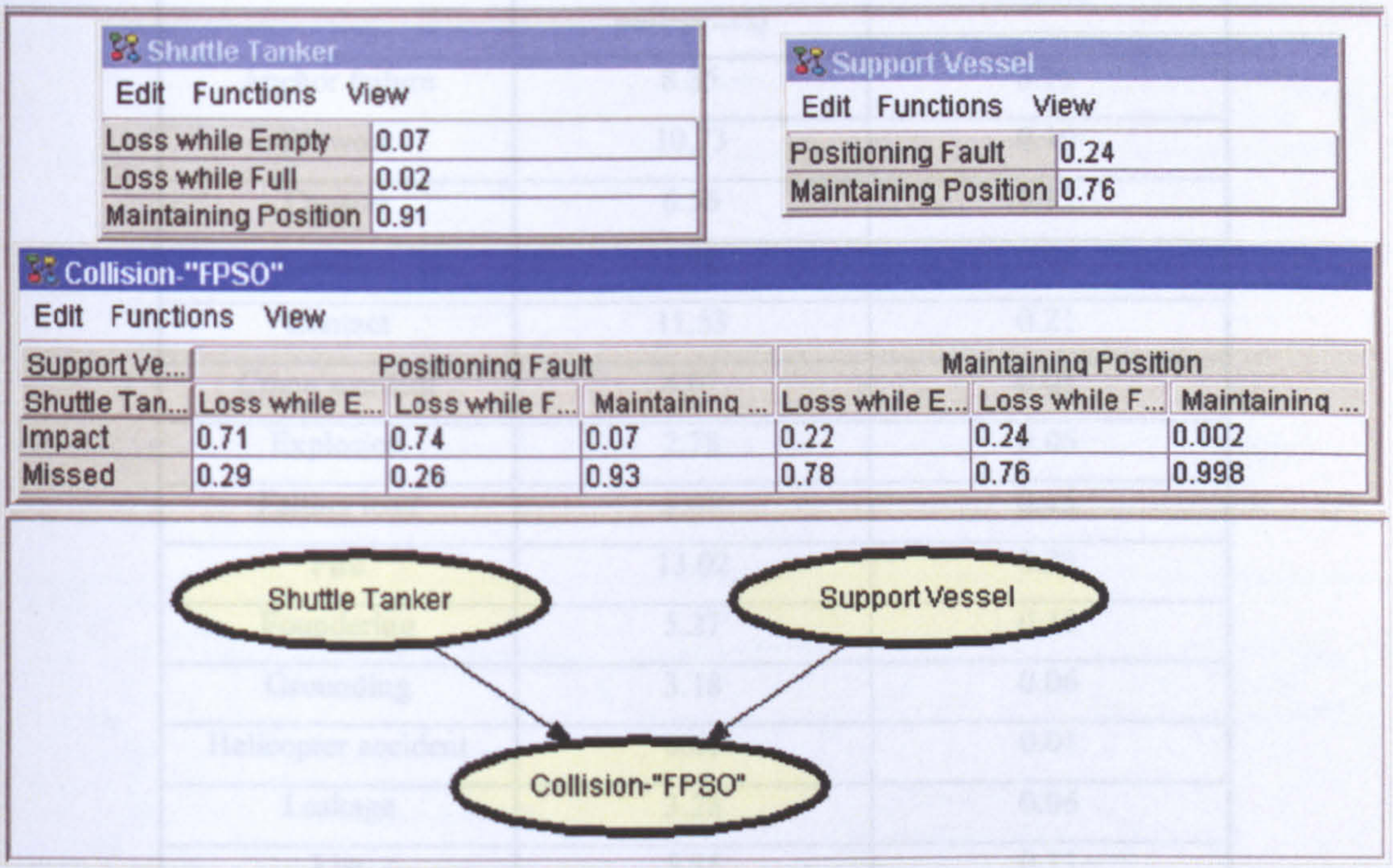


Figure 6.40: BN of authorised vessels-FPSO collision scenario with conditional probability tables

The evaluation of an FPSO's collision and contact damage risks needs some special technique(s), thus a BN, as shown in Figure 6.40, is created in *Hugin* to model this scenario for the FPSO not being able to take measures in avoiding a collision by the authorised vessels manoeuvring within close proximity of it. With the ship lifetime and overall production system very conservatively set to 20 years of operation for a lifetime probability in the Bayesian analysis, appropriate probabilities were assigned into the conditional probability tables (CPT) of each node in the model domain. These were based on the failure rates derived from WOAD Statistical Report (1998) (see Table 6.1) and from the assessments carried out in Husky Oil (2000).

Table 6.1: Probability values from failure frequency for offshore mobile units during 1980-97

Type of Accident	Failure frequency of mobile units (1000 unit-years)	Probability (at t = 20yrs)
Anchor failure	8.35	0.15
Blowout	10.73	0.19
Capsize	6.56	0.12
Collision	2.78	0.05
Contact	11.53	0.21
Crane accident	4.07	0.08
Explosion	2.78	0.05
Falling load	8.05	0.15
Fire	13.02	0.23
Foundering	5.27	0.10
Grounding	3.18	0.06
Helicopter accident	0.60	0.01
Leakage	3.28	0.06
List	5.86	0.11
Machinery failure	1.39	0.03
Off position	11.53	0.21
Spill/release	9.44	0.17
Structural damage	17.09	0.29
Towing accident	5.86	0.11
Well problem	14.01	0.24
Other	2.48	0.05

When the net is compiled in "run" mode (Figure 6.41), the ship-FPSO collision network window is split into two by a vertical separation and this gives the initial situation to the left with the node list pane and to the right with the network pane. The probabilities of a node in a certain state are viewed double clicking it in the node list pane.

Given the information that collision with the FPSO takes place, the probability of the shuttle tanker and the support vessel being in a loss of position failure state can be found. This fact is entered by double clicking the state "impact" of the Collision-"FPSO" node (Figure 6.42). The figure shows the probability of the shuttle tanker being lost while empty to be most disturbing quantity of the "Shuttle Tanker" node (i.e.,

49.75%). Likewise, the "Support Vessel" node now indicates an increase in failure probability to 64.77%.

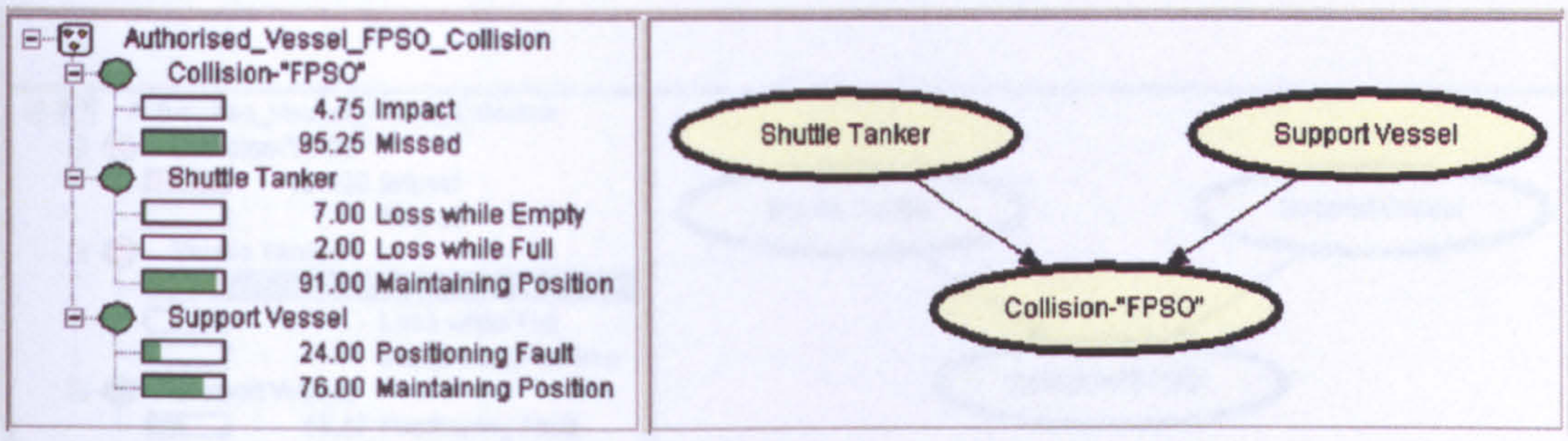


Figure 6.41: Initial Situation in the BN of authorised vessels-FPSO collision scenario

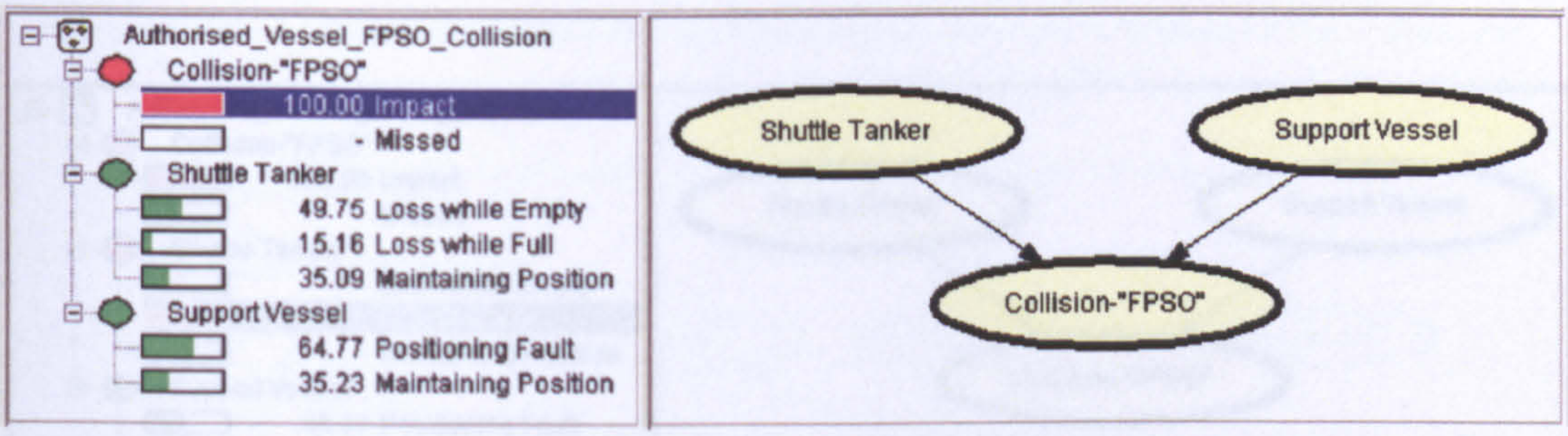


Figure 6.42: Probability of impact for Collision-"FPSO" set to 100%

If it is taken that the shuttle tanker completely (100%) maintains its position, then it can be seen as in Figure 6.43 that the support vessel would have failed drastically in positioning fault (i.e. 91.70%) for there to be a 100% collision impact on the FPSO.

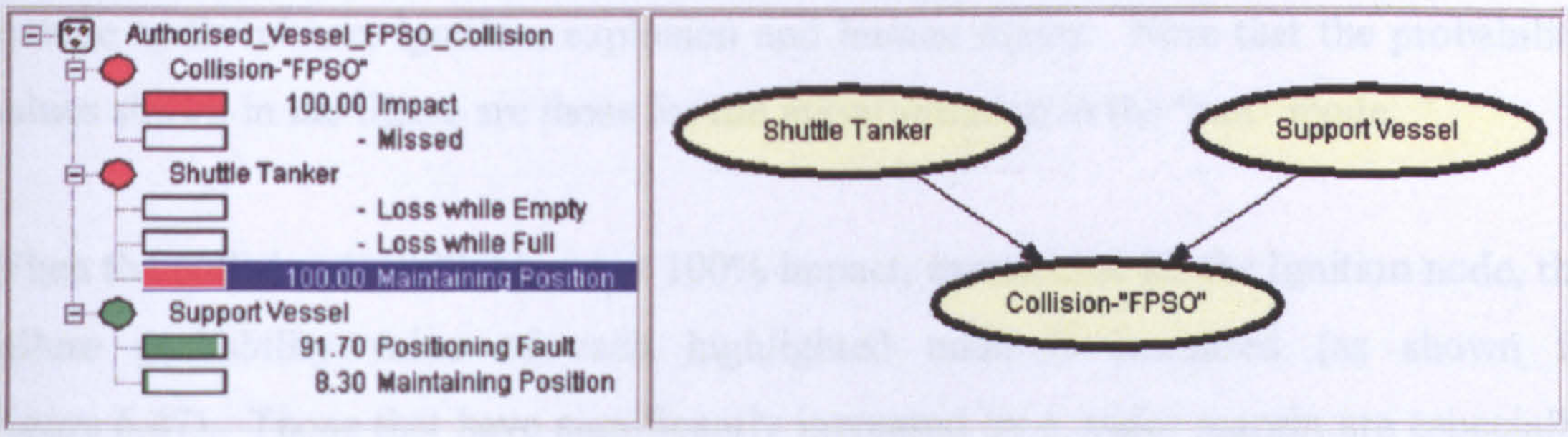


Figure 6.43: Collision-"FPSO" impact probability set to 100% in Shuttle Tank maintained position

On another note, where collision on the FPSO occurs at either the shuttle tanker being lost while empty (Figure 6.44) or whilst full (Figure 6.45), then the Support Vessel node indicates a 50:50 chance of having a positioning fault or maintaining its position.

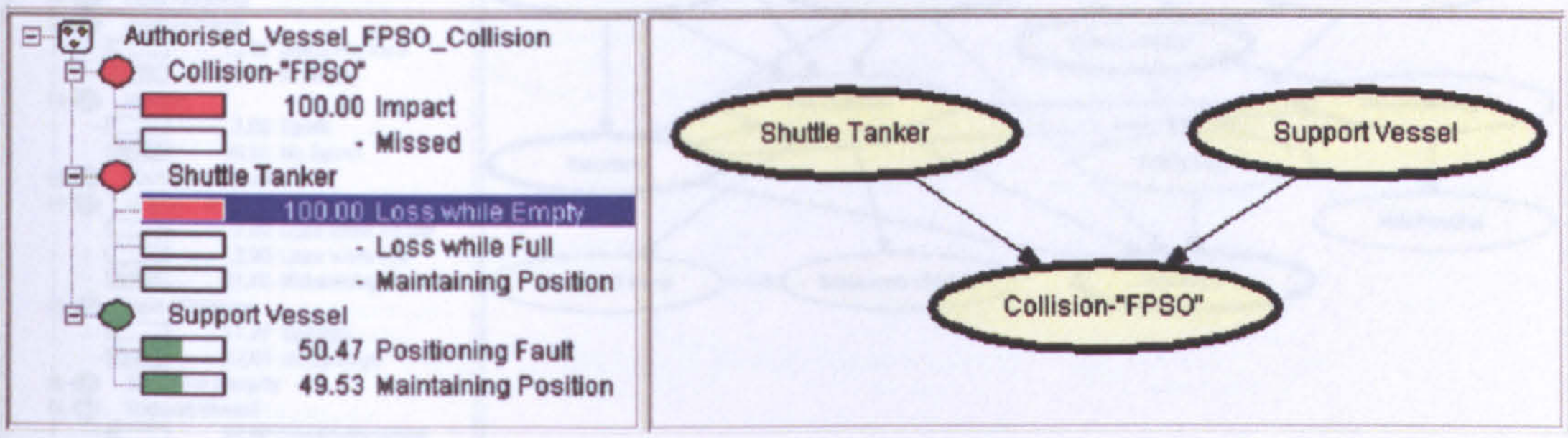


Figure 6.44: Collision-"FPSO" impact probability set to 100% in Shuttle Tank loss while empty

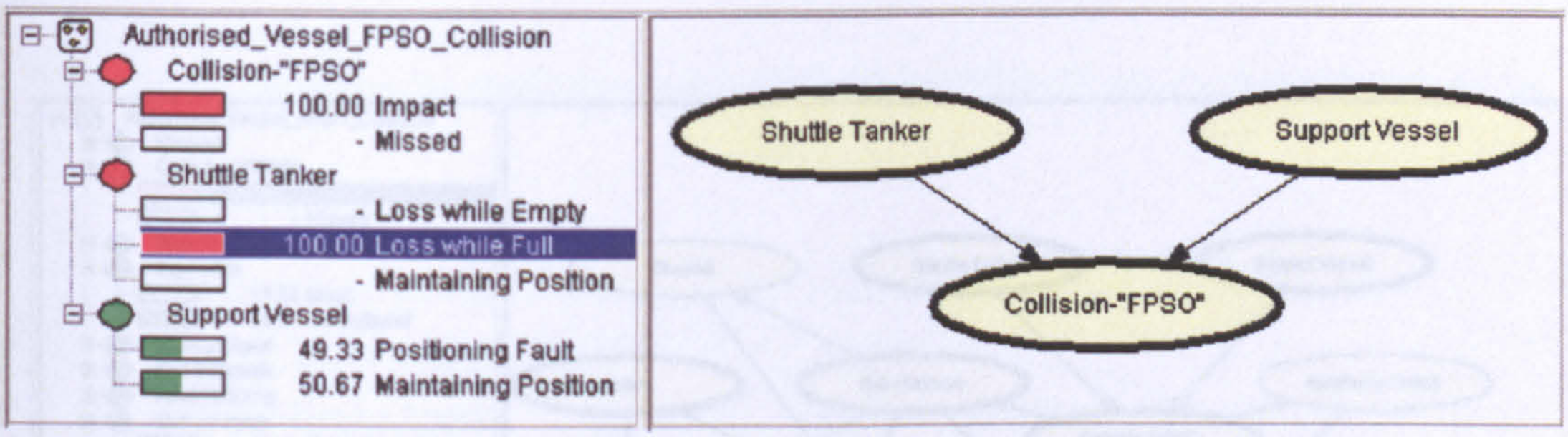


Figure 6.45: Collision-"FPSO" impact probability set to 100% in Shuttle Tank loss while full

Evidence identified for nodes being in any state can be added as a node with the links attached from it to these nodes. Some resulting events known to occur due to collision with an FPSO have been identified herein. Some of these, as highlighted in Figure 6.46, include spills/release, ignition, explosion and human injury. Note that the probability values shown in the figure are those for the initial situation in the "run" mode.

When the collision-to-FPSO is set at 100% impact, except that for the Ignition node, the failure probability value of each highlighted node is increased (as shown in Figure 6.47). Those that have significantly increased by a wider margin are especially the Spill/Release node and the Human Injury node. The Ignition node has remained the same in probability value, since it is only a piece of evidence for explosion and fire outbreak and not a resulting incident of the collision to the FPSO in this scenario.

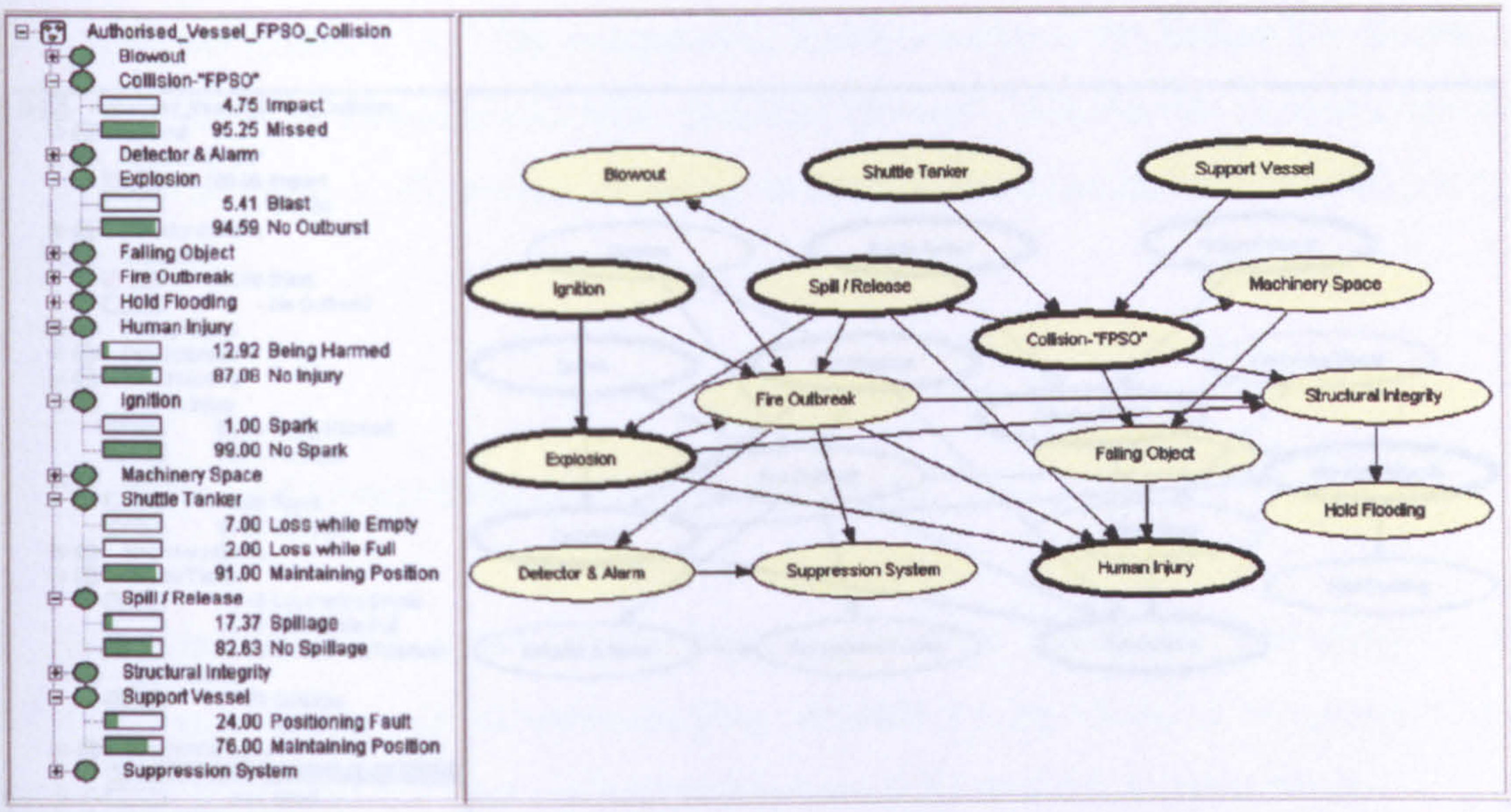


Figure 6.46: Addition of evidence and resulting events from the Collision-"FPSO" situation

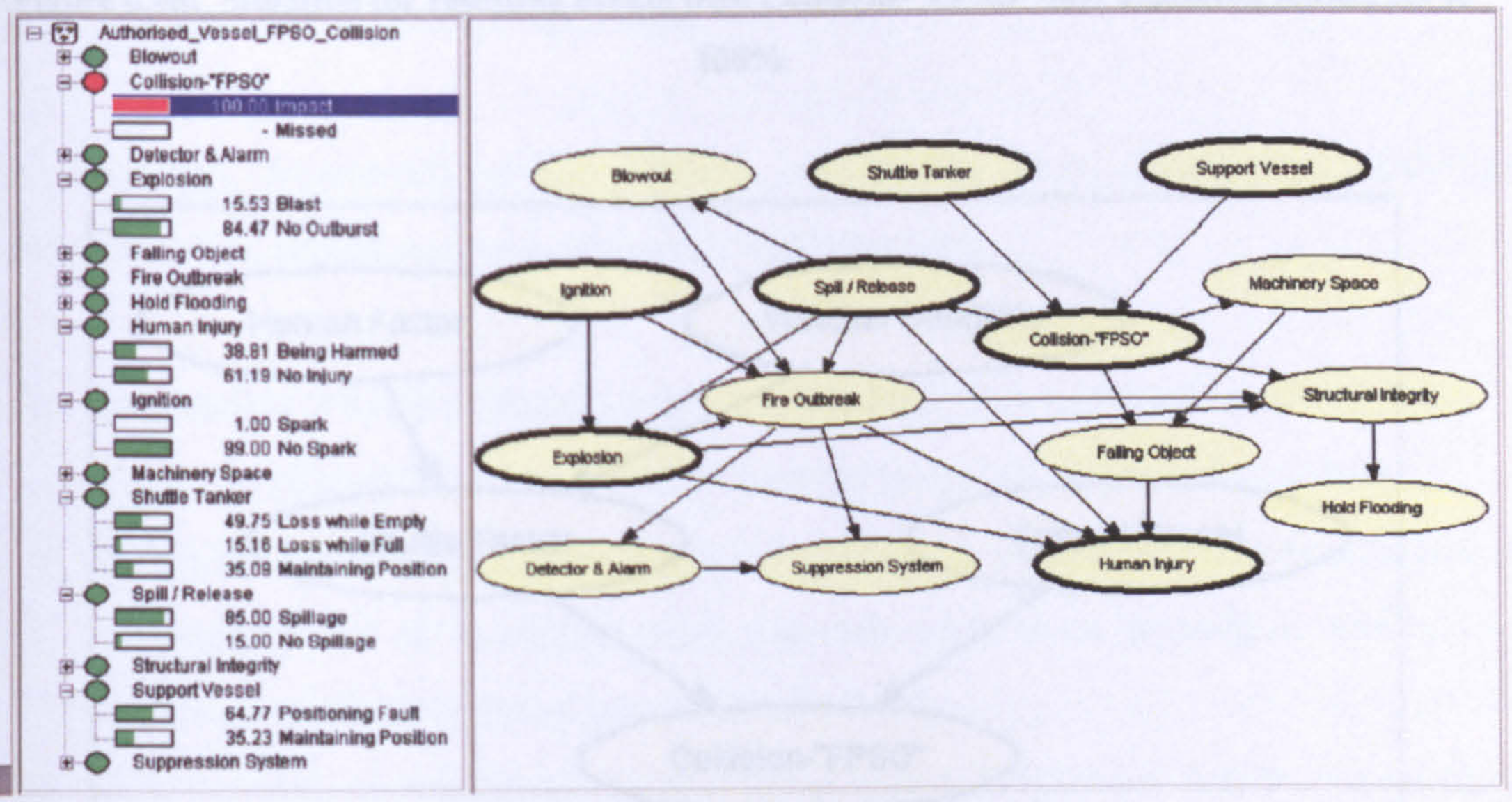


Figure 6.47: Situation for resulting events from Collision-"FPSO" impact probability set to 100%

With the Explosion node set to a failure of 100% blast during a 100% impact on collision with the FPSO, the probability of 96.66% indicates a high amount in certainty for a structural damage to happen (Figure 6.48). The same can be said for the Human Injury node, which now has a probability value of 84.26% for being harmed. As such a great deal of attention will have to be paid to increasing safety for these represented nodes. Thus, the risk analyst and decision makers might find it appropriate to consider modelling out an ID for explosion.

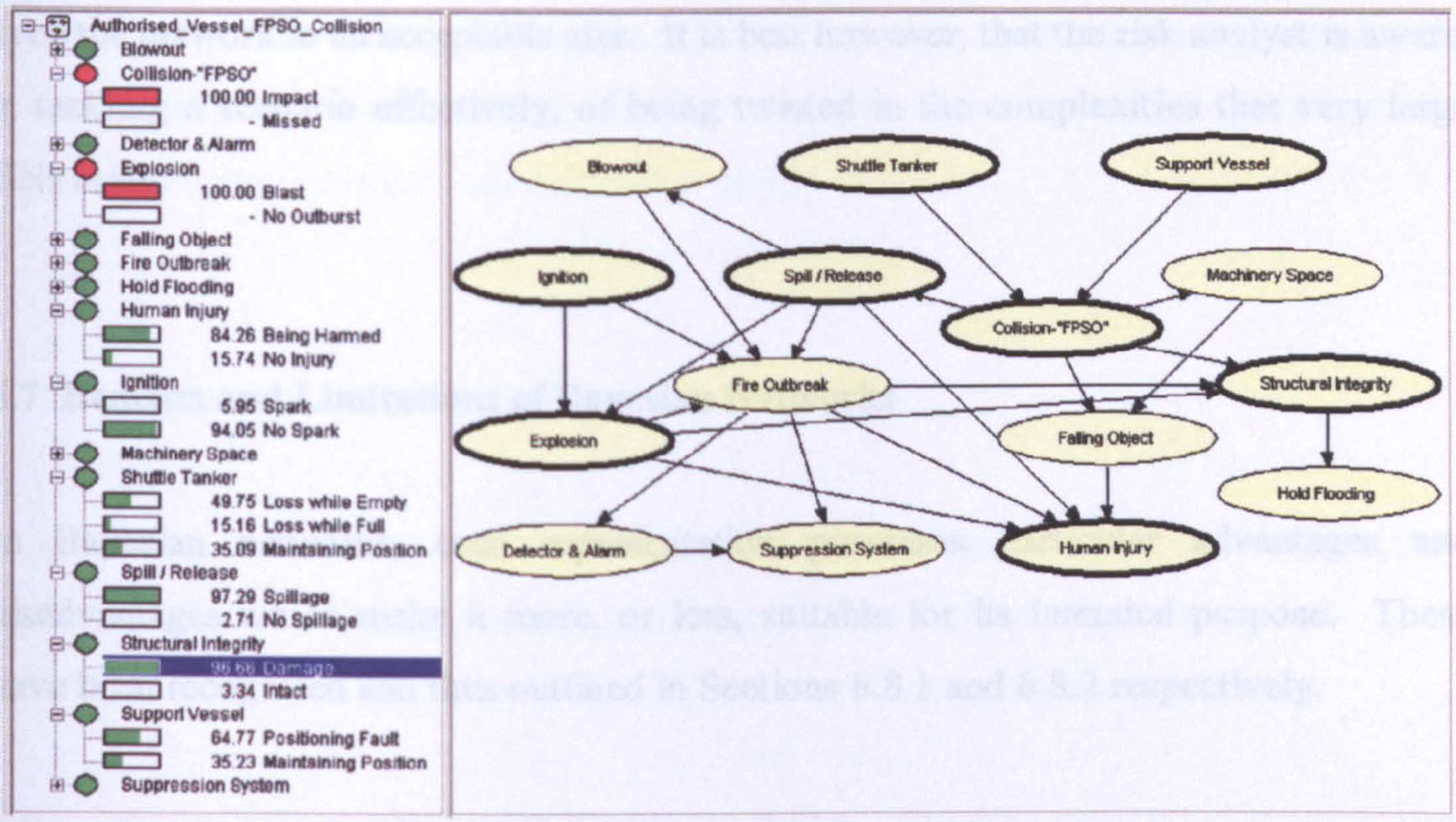


Figure 6.48: Situation for resulting events with Collision-"FPSO" and explosion failure set to 100%

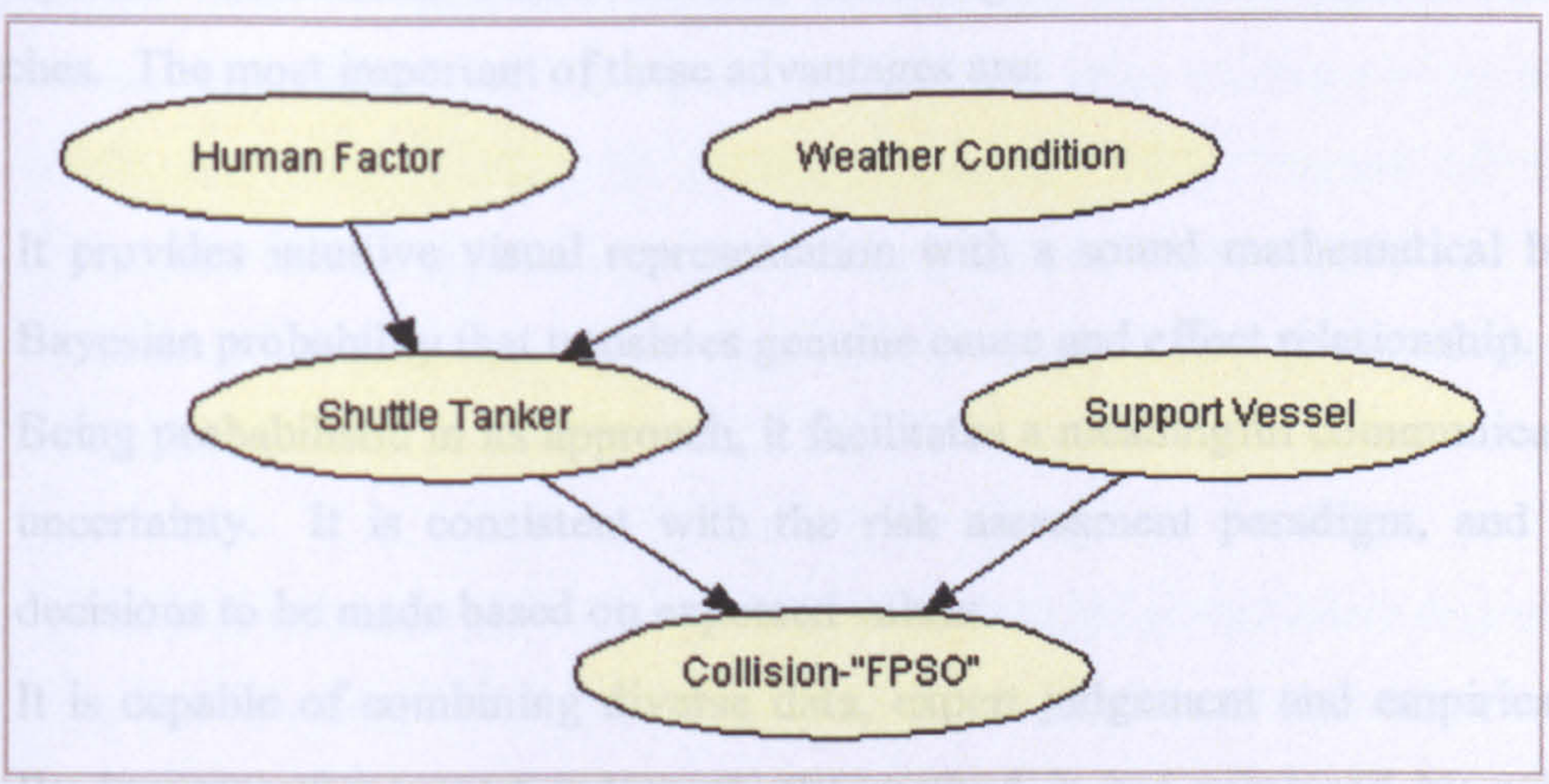


Figure 6.49: Some added typical evidence for a shuttle tanker loss of position

Other such pieces of typical evidence as the human element (with states such as "error" and "intervention"), weather condition (with sea states of "calm", "harsh" "adverse" and "severe") (see Figure 6.49), electrical/electronic aspects, etc., can be made into new nodes and added to diversify the range of the BN applicability in this scenario.

The scenario settings for this case study can enable a dominant decision in a marine and offshore risk assessment study. Nonetheless, as extensions to the scenario network may

lie in the discrepancy of the risk analyst and decision makers, the author has chosen to keep the network to an acceptable size. It is best however, that the risk analyst is aware, in tackling a scenario effectively, of being twisted in the complexities that very large BNs bring.

6.7 Benefits and Limitations of Bayesian Networks

In Bayesian networks, each representation possesses particular advantages and disadvantages which make it more, or less, suitable for its intended purpose. These have been recognised and thus outlined in Sections 6.8.1 and 6.8.2 respectively.

6.7.1 Strengths of Bayesian Networks

The Bayesian framework offers several advantages over alternative modelling approaches. The most important of these advantages are:

- It provides intuitive visual representation with a sound mathematical basis in Bayesian probability that translates genuine cause and effect relationship.
- Being probabilistic in its approach, it facilitates a meaningful communication of uncertainty. It is consistent with the risk assessment paradigm, and allows decisions to be made based on expected values.
- It is capable of combining diverse data, expert judgement and empirical data. By incorporating expert judgment, the method is not paralysed by a lack of observational data.
- It allows easy updating of prediction and inference in a statistically rigorous manner when observations of model variables are made. Deleting or adding new information does not also require the whole network to be revised.
- The assessment endpoints are chosen so that they are of vital interest to stakeholders and decision-makers and can be easily conceived in terms of utility for use in formal decision analysis.

These particular advantages offered by BNs make it very useful in situations where uncertainty is unavoidable – Bayesian methods provide a mechanism to model the uncertainty. Thus, such methods can also be used where normal optimisation and decision-making techniques are difficult to apply.

6.7.2 Difficulties of Using Bayesian Networks

In spite of their remarkable power and potential to address inferential processes, there are some inherent limitations and liabilities to BNs. These drawbacks include the following:

- They cannot easily incorporate unobserved variables, owing to the fact that the size of the internal CPT for a child node can very quickly become quite large.
- There is computational complexity/difficulty (filling in of details of numerical recipe, computer time, convergence monitoring), which is exponential in the number of nodes. These complex models with large numbers of parameters, which are often referred to as *non-parametric (NP)*, become NP-hard in complexity as they approach general multiply-connected networks.
- Likelihood functions are not always solvable analytically (Rather, heuristics are extensively used in practice).

The complexity of inference is usually associated with large probabilistic dependencies recorded during inference. However, a large model is preferable to a smaller one only if it provides a sufficiently large improvement of fit to offset the penalty for its additional complexity.

6.8 Concluding Remarks

A BN could be used to model the components that affect risk and how they interact. Besides, its graphical nature makes the assessment model intuitive for users to understand. The process of performing Bayesian updating involves selecting a prior probability distribution, calculating the normalizing constant, formulating the likelihood function, and then calculating the posterior probability distribution. The likelihood

function incorporates the objective information whilst the prior distribution can include subjective information known about the distributions of the model parameters. Therefore, the posterior distribution incorporates both the *objective* and *subjective* information into the distributions of the model parameters. Hence, BNs are well suited for modelling maritime safety-critical systems prediction and risk analysis.

The proposed BN methodology has been used to combine evidence from different information sources for the quantitative assessment of a generic ship evacuation scenario and that of authorised vessels to FPSO installation collision via the *Hugin* program tool. This program software allowed for the probabilities of states of nodes based on observed information to be adjusted and it propagated such changes through the network to update the conditional probabilities at each node. It was also possible to show all the implications and results of a complex Bayesian argument based on the underlying Bayes' theorem. This theorem is the fundamental principle governing the process of logical Bayesian inference that determined what conclusions can be made with a degree of confidence based on the totality of relevant evidence available. The probabilistic predictions of the case studies can be used to give stakeholders and decision-makers a realistic appraisal of the chances of achieving desired outcomes. The results also indicate that BNs give a sound and transparent approach modelling marine operational risk. Thus, BN is an integrative model that can be used effectively within the existing decision-making process. The evacuation study BN was further expanded with life-saving utility and optimal survival decision nodes that permitted the rapid development of a practical maritime decision model, and one in which the value of IDs as a highly intuitive communication tool has been confirmed. IDs provide a compact alternative to decision trees such that, during review, persons who are not risk analysts are able to interpret the diagrams and propose improvements to the decision model.

Chapter 7: Fuzzy Logic Modelling

Chapter Summary

In dealing with complex and ill-defined systems of a maritime application, modelling to support human reasoning for the purpose of risk assessment requires the effectiveness of a systematic logic-based approach. Floating production, storage and offloading (FPSO) installations, for example, combine traditional process technology with marine technology, and thus are quite dependent on technical design and operational safety control. Such safety-critical dependencies require novel approaches to properly analyse the risk involved. Hence, a proposed framework utilising fuzzy logic, as the mathematical tool for approximate reasoning, and evidential reasoning approaches is provided for modelling the assessment task.

As based on fuzzy set theory, the model enables subjective uncertainties to be described mathematically and further processed in the analysis of the structures. The forms of membership functions that could be used in representing fuzzy linguistic variables to quantify risk levels are presented. A case study of collision risk between FPSO and shuttle tanker due to technical failure during tandem offloading operation is used in this chapter to illustrate the application of the proposed model. Furthermore, the obtained results from the case study provide confirmation that at various stages of offshore engineering systems design process, the framework of incorporated approximate reasoning is a well-suited and convenient tool for attaining reliable risk analysis.

7.1 Introduction

The safety of a large maritime engineering system is relatively affected by the growing technical complexity regarding its design to operation phase, and even in its maintenance. Thus, an ample amount of reliable data needs to be provided in order to

determine a probabilistic value of all the failure mode variables that are necessary for conducting its safety analysis. Realistically, not all the variables may have the necessary numerical data and those available may be somewhat imprecise that there may be no simple mathematical model to implement them. Such variables might have to be supported immensely by the knowledge of experts (such as marine engineers and safety analysts), which means that the obscure nature in their knowledge representation will have to be analytically taken into account. For example, the field experts may precisely describe the occurrence of a specified failure mode for the system as 'reasonable frequent' or 'highly unlikely', for which the possible value falls within an accepted interval of a scale.

The incorporation of subjective terms leads to both the uncertainty that can be attributed to vagueness of the system's ill-defined boundaries and that of ambiguity where there are several choices associated with a given condition. The employment of fuzzy logic (FL) is a powerful and versatile tool tolerant of imprecise, ambiguous and vague data/information, and one for which its reasoning builds this understanding into the process rather than just tacking it onto the end. It utilises the concept of a linguistic variable, that is a variable whose values are not numbers but words or sentences in a natural or synthetic language (as built from the system's qualitative assessment), and provides a framework for dealing with such variables in a systematic way. Its rule-base would naturally allow for the linguistic attributes to be specifically guided towards a justified output result. Thus, FL opens the door to the application of the linguistic approach in a wide variety of problem areas, which do not lend themselves to precise analysis in the classical spirit.

In FL, one can apply the input parameters from a hazard identification worksheet. In the typical case, a defuzzification process is used to obtain a crisp output result brought about my aggregating the degree to which all the rules are activated. For example, a risk priority number or a criticality number could be the defuzzied result of a fuzzified input that combines failure mode occurrence, severity and detectability (as taken from a failure mode, effect and criticality analysis (FMECA) worksheet) in its rule-base. As weighted ranking may better be utilised from analysis having multiple experts and attributes, instead of a crisp output, an evidential reasoning process may be used to synthesis the aggregation. A multiple experts and attributes scenario of the collision

risk between an FPSO and a shuttle tanker due to technical failure during tandem offloading operation can utilise this approach for its maritime safety analysis.

7.2 Logic Approach of Approximate Reasoning

Approximate reasoning (AR) uses fuzzy sets and FL to model human reasoning (Zadeh, 1975). It lacks the precision of the exact reasoning in classical logic but it may be more effective in dealing with complex and ill-defined systems. Its max-min composition (Mamdani, 1974) plays an important role in inferential rules based on generalised modus ponens.

7.2.1 Basis of Fuzzy Set Theory

Fuzzy theory holds that all things are matters of degree, and also reduces black-white logic and mathematics to special limiting cases of grey relationships. Mathematically fuzziness means multivalence so that multivalued fuzziness corresponds to degrees of indeterminacy or ambiguity, partial occurrence of events or relations. Introduced by Zadeh (1965), as a modest extension of the classical notion of set, the notion of fuzzy set proved to have far-reaching, unexpected impact. The idea is that unlike crisp set, which is completely determined by an indicator function taking values in {0, 1}, a fuzzy set is characterised by a membership function taking values in [0, 1].

7.2.1.1 Fuzzy Set

A fuzzy set is represented by a membership function defined on the universe of discourse. The universe of discourse is the space where the fuzzy variables are defined. Formally, a fuzzy set A in a universe of discourse U is expressed as a set of ordered pairs:

$$A = \{(x, \mu_A(x) \mid x \text{ in } U\} \tag{7.1}$$

where $\mu_A(x)$ is the membership function that gives the degree of membership of x in the fuzzy set A. This indicates the degree to which x belongs in set A.

A fuzzy set A is said to be normal if there exists $x \in X$ such that $\mu_A(x) = 1$ (It is said to be subnormal otherwise).

7.2.1.2 Membership Function

A membership function (MF) is a curve/shape that defines how each point within the set of any element in the universe of discourse is mapped to a value between 0 and 1. This value is called membership value or grade/degree of membership. A MF value of zero implies that the corresponding element is definitely not an element of the fuzzy set, while a value of unity means that the element fully belongs to the set. A fuzzy set whose MF only takes on the values zero or one is called crisp.

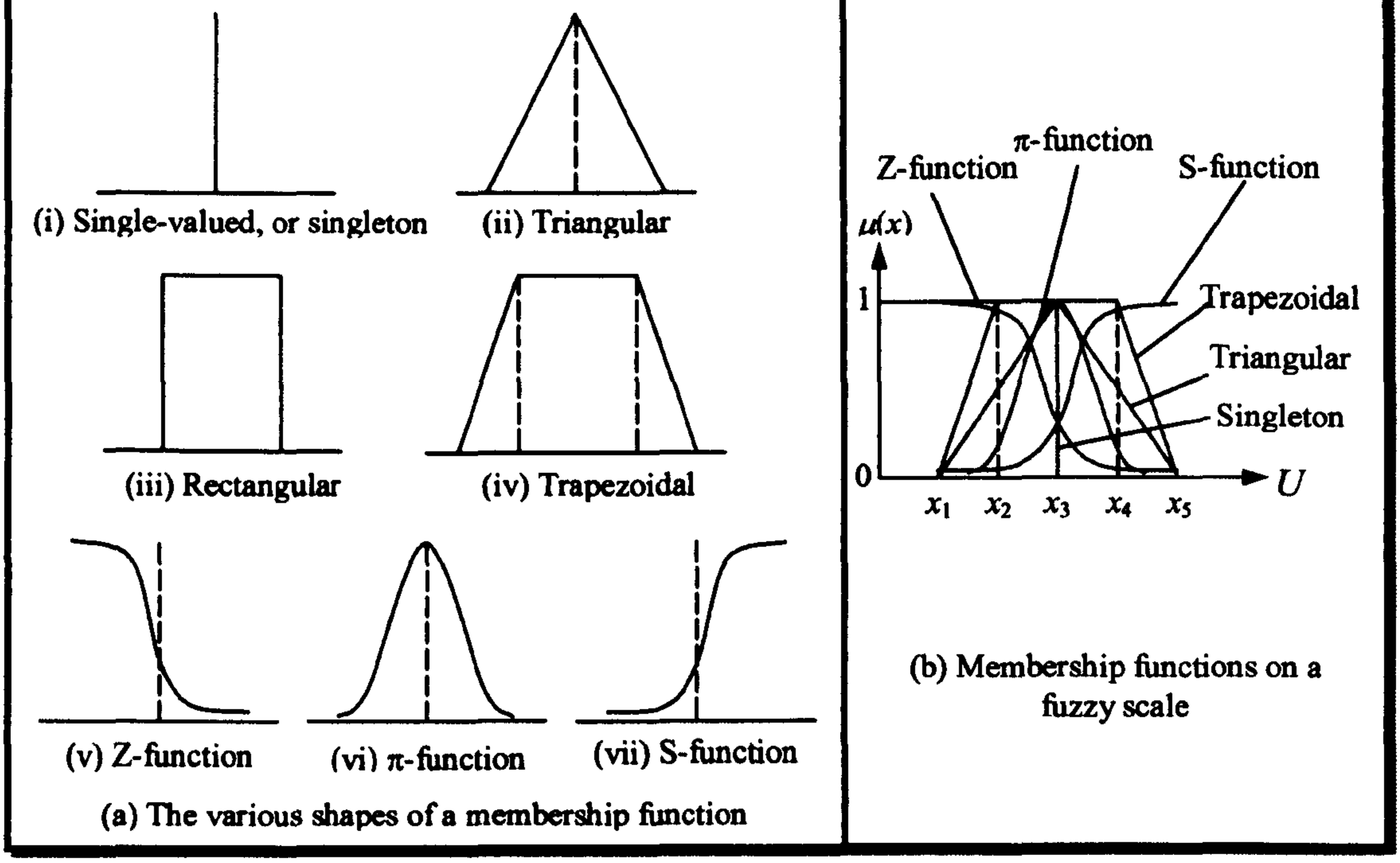


Figure 7.1: Various forms of fuzzy membership function

MFs can provide graphical representation of the magnitude of participation for each expert knowledge input. It can associate a weighting with each of the inputs that are processed, define functional overlap between inputs, and ultimately determines an output response. The feasible shapes of the parameters' membership functions are defined only in the application context and as perceived by expert. Figure 7.1(a) shows the various forms in which a typical MF may take. In safety modelling, those of Figure 7.1(a) (i) to (iv) (i.e., *singleton*, *triangular*, *rectangular* and *trapezoidal* MFs) are perceived to be appropriate in the representation of expert knowledge. As used on a fuzzy scale (Figure 7.1(b)), these are described as follows:

- *Singleton* MF: A single deterministic value, x_3, with 100 % certainty.
- *Triangular* MF: A triangular distribution defined by a most likely value, x_3, with a lower least likely value, x_1, and an upper least likely value, x_5.
- *Rectangular* MF: A closed interval defined by an equally likely range between x_2 and x_4.
- *Trapezoidal* MF: A trapezoidal distribution defined by a most likely range between x_2 and x_4, with a lower least likely value, x_1, and upper least likely value, x_5.

The idea of using fuzzy membership function is to map the parameter constraint to membership grade between the scaled intervals. The closer the membership is to one the better the solution is for that constraint. The rules use the input membership values as weighting factors to determine their influence on the fuzzy output sets of the final output conclusion.

7.2.1.3 Operations With Fuzzy Sets

The basic connectivity operations in fuzzy set theory include union, intersection, complement, Cartesian product and composition. These operations are given for two fuzzy sets A and B with membership value at x, denoted by $\mu_A(x)$ and $\mu_B(x)$ respectively as follows:

- *Union* of A and B: $\mu_{A \cup B} = max\{\mu_A(x), \mu_B(x)\}$. The union of A and B produces fuzzy set C with membership values that are the maximum of the component values.

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

- *Complementation* of A: $\mu_{\bar{A}}(x) = 1 - \mu_A(x)$. The membership values of the complementary set $\bar{A}$ are just 1 – the corresponding membership values of A.

- *Cartesian product* of A and B: $\mu_{A \times B}(x) = (\mu^{ij}{}_{A \times B}(x))_{m \times n}$, where $\mu^{ij}{}_{A \times B}(x) = min\{\mu^{i}{}_{A}(x), \mu^{j}{}_{B}(x)\}$ for the Cartesian space $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

- *Composition*: $\mu_{C \circ A \times B}(x) = max(min\{\mu_C(x), \mu^{ij}{}_{A \times B}(x)\})$. The composition of the membership functions for the fuzzy subset C and the Cartesian product of the subsets A and B, is the maximum membership value obtained from the minimum membership values of all subset.

Furthermore, Boolean algebra rules, which are common in classical set theory, also apply to fuzzy set theory.

7.2.2 Composition of a Fuzzy Variable

A fuzzy number is a quantity whose value is imprecise, rather than exact as is the case with "ordinary" (single-valued) numbers. The concept of a fuzzy number plays a fundamental role in formulating *quantitative fuzzy variables*. These are variables whose states are fuzzy numbers. When, in addition, the fuzzy numbers represent linguistic terms that are interpreted for a particular context, the resulting constructs are usually called linguistic variables.

7.2.2.1 Linguistic Variable

A linguistic variable differs from a numerical one in that its values are not numbers, but words or sentences in a natural or artificial language. Since words, in general, are less precise than numbers, the concept of a linguistic variable serves the purpose of providing a means of approximated characterization of phenomena, which are too complex, or too ill-defined, to be amenable to their description in conventional quantitative terms (Zadeh, 1975).

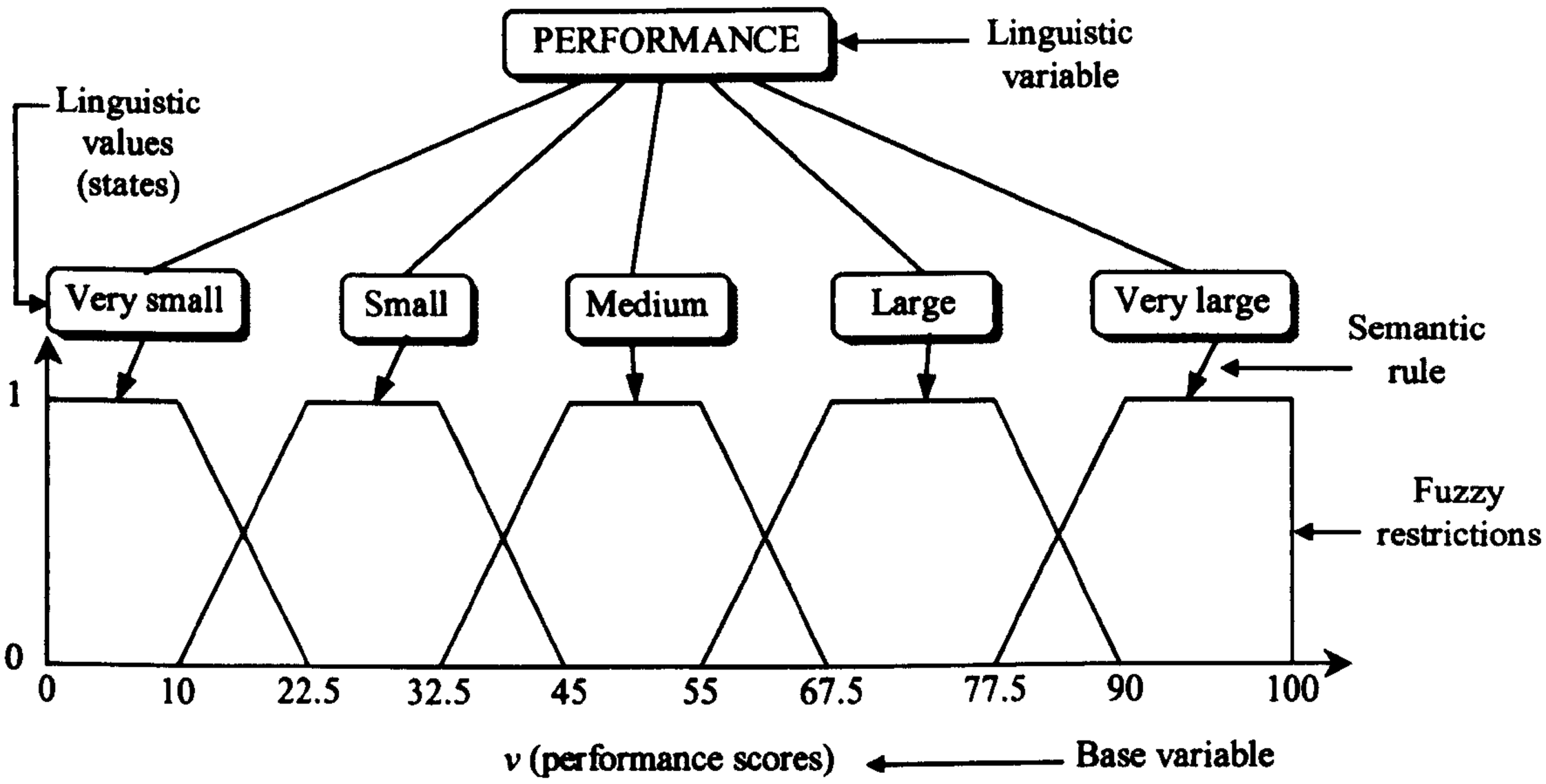


Figure 7.2: An example of a linguistic variable

Every linguistic variable is characterised by the *name* of the variable, the set of names of *linguistic terms* that refer to a base variable ranging across a universe of discourse, *U*, a *syntactic rule* (which usually takes the form of a grammar) for generating the linguistic terms and a *semantic rule* that assigns each linguistic term its meaning, which is a fuzzy set on *U*. Figure 7.2 shows an example of a linguistic variable that represents a system performance (Klir & Yuan, 1995). The fuzzy numbers, whose MFs have the usual trapezoidal shapes, are defined on the interval [0, 100], which is the range of the base variable. Each of them expresses a fuzzy restriction on this range.

7.2.2.2 Linguistic Terms

A linguistic term is characterized by its term set. The linguistic term for system performance in Figure 7.2 can be defined by the term set *T*, the set of names of linguistic values of performance, in the following way: *T*(*performance*) = {*very small*, *small*, *medium*, *large*, *very large*}.

Three to seven terms are often appropriate to cover a linguistic term. Rarely, one uses less than three terms, since most concepts in human language consider at least the two extremes and the middle in between them. On the other side, one rarely uses more than seven terms because humans interpret technical figures using their short-term memory. The human short-term memory can only compute up to seven symbols at a time (Broadbent, 1975 and Miller, 1956). Another observation is that most (definitely not all) linguistic variables have an odd number of terms. This is due to the fact that most linguistic terms are defined symmetrically, and one term describes the middle between the extremes. Hence, most fuzzy logic systems use 3, 5, or 7 terms.

Fuzzy linguistic terms can be of several types (Turksen, 1992):

- Fuzzy predicates, such as *heavy*, *large*, *old*, *small*, *medium*, *normal*, *expensive*, *near*, *smart*, and the like.
- Fuzzy truth-values, such as *true*, *false*, *fairly true*, or *somewhat true*.
- Fuzzy probabilities, such as *likely*, *unlikely*, *very likely*, or *extremely unlikely*.
- Fuzzy quantifiers, such as *many*, few, *most*, or *all*.

Usually, depending on the problem domain, an appropriate linguistic term set is chosen and used to describe the vague or imprecise knowledge. The elements in the term set will determine the granularity of the uncertainty, that is the level of distinction among different sizes of uncertainty (Delgado, *et. al*, 1998).

7.2.3 Background of a Fuzzy Logic System

FL 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. For example, the following is a fuzzy *IF-THEN* rule:

> *IF* ***likelihood*** of a hazard is *frequent AND* ***severity of occurrence*** is *catastrophic, THEN* ***risk level*** is *high.*

The *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.

7.2.4 Components of a Fuzzy Logic System

A FLS consists of four components: *fuzzifier, fuzzy rule base, fuzzy inference engine,* and *defuzzifier.* Since a multi-output system can always be decomposed into a collection of single-output systems, a FLS is considered for a *multi-input-single output (MISO)* case, where $U = U_1 \times U_2 \times \ ... \times U_p \subset R^p$ is the input space and $V \subset R$ is the output space. A *fuzzy relation R(U, V)* is a set in the product space $U \times V$ and is characterized by the membership function $\mu_R(x, y)$, where $x \in U$, and $y \in V$, and $\mu_R(x, y) \in [0, 1]$.

7.2.4.1 Fuzzifier

The *fuzzifier* converts each piece of input data to degrees of membership by using one or several membership functions. It is defined as a mapping from a crisp (real-valued) point $x^* \in U \subset R^p$ to a fuzzy set A' in U. The *fuzzifier* thus matches the input data with the conditions of the rules to determine how well the condition of each rule matches that particular input instance. There is a degree of membership for each linguistic term that applies to that input variable.

7.2.4.2 Fuzzy knowledge/Rule Base

A *fuzzy knowledge/rule base* consists of a set of fuzzy *IF-THEN* rules. It is the core of a FLS in the sense that all other components are used to implement these rules in a reasonable and efficient manner. Basically, the representation of imprecise knowledge can be collected and delivered by a human expert (e.g., decision-maker, designer, process planner, machine operator). This knowledge, expressed by (k = 1, 2, ..., K) finite heuristic fuzzy rules of the type MISO, may be written in the form:

$$R^k_{MISO}: \; IF\ x_1 \text{ is } A^k_1 \text{ and } x_2 \text{ is } A^k_2 \text{ and } \ldots \text{and } x_N \text{ is } A^k_N, \; THEN\ y \text{ is } B^k \quad (7.2)$$

where $\{A^k_i\}^N_{i=1}$ (fuzzy sets in $U_i \subset R$) denotes the values of input linguistic variables $\{x_i\}^N_{i=1}$ (conditions) and B^k (fuzzy sets in $V \subset R$) stands for the value of the independent output variable linguistic variable y (conclusion).

In a FLS framework, there are three major properties of fuzzy rules (Wang, 1997). These are outlined as follows:

1. A set of fuzzy *IF-THEN* rules is complete if for any $x \subset U$, there exists at least one rule in the fuzzy rule base, say rule R^k in the form of Equation 7.2, such that

$$\mu_{A^k}(x_i) \neq 0 \qquad \text{for all } i = 1, 2, \ldots, n \qquad (7.3)$$

where $\mu_{A_i^k}(x_i)$ is the membership value associated with x_i is A_i^k.

Intuitively, the completeness of a set of rules means that at any point in the input space there is at least one rule that "fires", that is, the membership value of the *IF* part of the rule at this point is non-zero.

2. A set of fuzzy *IF-THEN* rules is consistent if there are no rules with the same *IF* parts but different *THEN* parts.

3. A set of fuzzy *IF-THEN* rules is continuous if there do not exist such neighbouring rules whose *THEN* part fuzzy sets have empty intersection.

7.2.4.3 Fuzzy Inference Engine

In fuzzy inference, all rules are fired. It carries out a mapping from fuzzy set A' in U to fuzzy set B' in V and consequently determines how the system interprets the fuzzy linguistics. It stores the rules as fuzzy associations in a matrix that maps fuzzy set A to fuzzy set B. Such a matrix forms the *fuzzy associative memory (FAM)* for the system (Kosko, 1992).

To arrive at conclusions for inference systems, the FAM matrix has to be computed such that the k^{th} *IF-THEN* rule is interpreted as an *implication* R: $A \rightarrow B$ or $R = A \times B$ and when a set of fuzzy inputs $\{A_i'\}_{i=1}^{N}$ (or observations) are given to the inference system, the fuzzy output B' (or conclusion) may be symbolically expressed as:

$$B' = (A_1', A_2', \ldots, A_N') \circ R \qquad (7.4)$$

where symbol '$\circ$' denotes the *composition rule of inference* (CRI), e.g., the *sup*-^ or *sup-prod* (*sup*-•) of fuzzy relations. Alternatively, the CRI of Equation 7.4 is easily computed as:

$$B' = (A'_N \circ \ldots \circ (A'_2 \circ (A'_1 \circ R)) \tag{7.5}$$

Thus, given fuzzy set A' (which represents the premise x in A') and fuzzy relation $A \rightarrow B$ in $U \times V$ (which represents the *IF* x is A *THEN* y is B), a fuzzy set B' in V (which represents the conclusion y is B') is inferred as (Wang, 1997):

$$\mu_{B'}(y) = \sup_{x \in U} \; t[\mu_{A'}(x), \mu_{A \rightarrow B}(x, y)] \tag{7.6}$$

where the *sup* represents the *sup*-$*$ composition.

The inference mechanism that produces the output from a collection of rules is determined by two factors (Mamdani, 1974 and Larsen, 1980):

1. '*min*' or '*algebraic product*' implication operators, and
2. '*max-min*' or '*max product*' composition operators.

The global relation aggregating all rules from $k = 1$ to K is given as:

$$\mathrm{R} = \mathit{also}_{k=1}^{K} (R_{MISO}^{k}) \tag{7.7}$$

where the sentence connective *also* denotes any t- or s-norm, e.g., min ($\wedge$) or max ($\vee$) operators) or averages.

Since any practical fuzzy rule base constitutes more than one rule, the key question here is how to infer with a set of rules. In composition-based inference, all rules in the fuzzy rule base are combined into a single fuzzy relation in $U \times V$, which is then viewed as a single fuzzy *IF-THEN* rule. There are two views for what a set of rules should mean. The first one views the rules as independent conditional statements and the reasonable operator for combining the rules is union. The second one views rules as strongly coupled conditional statements such that the conditions of all rules must be satisfied in

order for the whole set of rules to have an impact. In this case the operator intersection should be used to combine the rules.

7.2.4.4 Defuzzification

At the *defuzzifier*, the input is a fuzzy set (i.e., the aggregated output fuzzy set), and the output is a crisp value obtained by using some defuzzification method such as the *centroid*, *height*, or *maximum*.

In maritime assessment work, this processing is a computational simplicity that can be used when to the output required is a risk priority number, a criticality number or to automate a controller. It is however unsuitable to derive the risk control measures or options for which the level of risk or safety has to be known. Therefore, the aggregated fuzzy conclusion for a risk modelling output is best processed by synthesis.

7.3 Evidential Reasoning Synthesising Approach

The *evidential reasoning* (ER) approach provides a more versatile way in which a multiple criteria decision analysis (MCDA) problem with uncertainties can be modelled. It uses evidence-based reasoning processes to reach a decision and its evaluation process is based on the *Dempster-Shafer* (DS) theory, which is well suited for handling incomplete assessment of uncertainty. The DS theory can model the narrowing of the hypothesis set with the accumulation of evidence. In other words, it will become more likely that a given hypothesis is true if more pieces of evidence support that hypothesis.

The ER criteria aggregation process is in general a non-linear process and, compared to the traditional weighting MCDA methods, the non-linearity is decided by the weights of criteria and the way each criterion is assessed (Yang and Xu, 2002a). Furthermore, the ER framework not only provides flexibility in describing a MCDA problem, it also prevents any loss of information due to the conversion from a distribution to a single value in the modelling process.

7.3.1 Safety Analysis Synthesis

To express the subjective safety more explicitly, linguistic variables such as "*poor*", "*average*", "*fair*" and "*good*" can be used. For instance, it may be quite clear to state that the safety of a failure mode is to a large extent "*good*". Such linguistic variables ("*poor*", "*average*", "*fair*" and "*good*") are referred to as *safety expressions*. The safety expressions may also be characterized by membership degrees to each element in U.

The fuzzy safety description of an event can then be mapped back onto the defined safety expressions. The safety, S, can then be obtained as follows:

$$S(S) = \{(\beta_1, \text{'}poor\text{'}), (\beta_2, \text{'}fair\text{'}), (\beta_3, \text{'}average\text{'}), (\beta_4, \text{'good'})\}$$

where β_m (m = 1, 2, 3 or 4) represents the extent to which the safety of the event belongs to the m^{th} safety expression.

A safety model or an operation process is usually a hierarchical structure with multiple layers where:

- Judgments on an event at the bottom level of the hierarchy made by multiple experts need to be synthesized.
- Safety synthesis needs to be carried out at the next level.
- Safety synthesis is progressed up to the top level where the safety estimation of the system can be obtained.

The hierarchical structure of a safety model can be formulated by studying the system under investigation. The system is composed of its constituent subsystems, which can be further broken down to the component level. Each component is associated with certain failure modes. The subsystems, components and failure modes may carry different weights when synthesizing the safety of the system in such a hierarchy.

The weight of an element in a synthesis level may be judged on a subjective basis in terms of its contribution to the safety of the associated element in the upper level. The technique that is used to carry out the synthesis is the *evidential reasoning* approach,

which is based on the principle that if more pieces of evidence (each may carry different weight) support a hypothesis then it is more likely that the hypothesis is true (Yang & Sen, 1994; Yang & Singh, 1994; Yang, 2001; Yang & Xu, 2002b). The evidential reasoning approach has the advantage of synthesizing safety estimates without loss of any data and also that uncertainties in safety estimates are handled in a rational manner.

Suppose M_n^m (m = 1, 2, 3 or 4; n = 1, …, or N) is a degree to which $S(S_n)$ (safety judged by expert n) supports the hypothesis that the safety evaluation associated with a failure event is H_m (H_1 = "*poor*"; H_2 = "*fair*"; H_3 = "*average*"; or H_4 = "good"). Then, M_n^m can be obtained as follows:

$$M_n^m = \lambda_n \times \beta_n \tag{7.8}$$

where λ_n is the normalized relative weight of expert n in the safety estimation process.

Suppose M_n^H (n = 1, …, or N) is the remaining belief unassigned after commitment of belief to all H_m (m = 1, 2, 3 and 4) for $S(S_n)$. M_n^H can be obtained as follows:

$$M_n^H = 1 - \sum_{m=1}^{4} M_n^m \tag{7.9}$$

Suppose MM_n^H (m = 1, 2, 3 or 4; n = 1, . . ., or N) represents the degree to which the safety associated with the event belongs to H_m as a result of the synthesis of the judgments produced by safety analysts 1, . . . , and n. Suppose MM_n^H represents the remaining belief unassigned after commitment of belief to all H_m (m = 1, 2, 3 and 4) as a result of the synthesis of the judgments produced by safety analysts 1, . . . , and n. The algorithm for synthesizing the analysts' judgments to obtain the safety evaluation associated with the event can be stated as follows (Yang & Singh, 1994; Yang & Sen, 1994):

Initial conditions: $MM_1^m = M_1^m$ $\qquad$ $MM_1^H = M_1^H$

$$\{H_m\} \quad MM_{n+1}^{m} = K_{n+1}(MM_n^m\, M_{n+1}^m + MM_n^m\, M_{n+1}^H + MM_n^H\, M_{n+1}^m)$$

$$m = 1, 2, 3, 4$$

$$\{H\} \quad MM_{n+1}^{H} = K_{n+1}\, MM_n^H\, M_{n+1}^H$$

$$K_{n+1} = \left[1 - \sum_{T=1}^{4} \sum_{R=1 R \neq T}^{4} MM_n^T M_{n+1}^R\right]^{-1}$$

$$n = 1, \ldots, N-1$$

$N-1$ iterations of the above algorithm are required to obtain the degree (i.e., MM_n^H) to which the safety evaluation associated with the event belongs to H_m (m = 1, 2, 3 and 4). The safety evaluation associated with the failure event can then be presented in the following form:

$$S(S_{the\ event}) = \{(\beta^1, \text{“}poor\text{”}), (\beta^2, \text{“}fair\text{”}), (\beta^3, \text{“}average\text{”}), (\beta^4, \text{“}good\text{”})\} \tag{7.10}$$

where β^m (m = 1, 2, 3 and 4) is equal to MM_N^H.

It is worth mentioning that the order in which safety estimates are combined does not make any difference in terms of the final synthesis using the above algorithm. It is also worth mentioning that the sum of β^m (m = 1, 2, 3 and 4) may not be equal to 1 at the end of synthesis using the above algorithm. This is because there may be still some unassigned belief to $S(S_{the\ event})$ due to the incompleteness of the safety estimates that are combined. The evidential reasoning algorithm has the advantage that in theory the total unassigned belief decreases as more safety estimates are synthesized.

In a hierarchical structure with multiple layers, the above synthesis can be used to obtain the safety estimate for an event at the bottom level. Then the evidential reasoning algorithm can be used again to obtain safety synthesis at the next level in the hierarchy. Such a synthesis can be eventually progressed up to the top level where the safety associated with the system can be obtained as follows:

$$S(S) = \{(\beta^1, \text{“}poor\text{”}), (\beta^2, \text{“}fair\text{”}), (\beta^3, \text{“}average\text{”}), (\beta^4, \text{“}good\text{”})\} \qquad (7.11)$$

where β^m (m = 1, 2, 3 or 4) represents the extent to which the safety of the system belongs to the m^{th} safety expression.

7.3.2 Utility Based Synthesis

Cost can also be modeled in a similar manner. Given the relative importance of cost against safety, the safety and cost estimates can be synthesized, using the evidential reasoning approach, to obtain the preference estimate $U(i)$ associated with design/operation option i as follows:

$$U(i) = \{(\mu_{Ui}^1, \text{“}slightly\ preferred\text{”}), (\mu_{Ui}^2, \text{“}moderately\ preferred\text{”}), (\mu_{Ui}^3, \text{“preferred”}), (\mu_{Ui}^4, \text{“}greatly\ preferred\text{”}) \qquad (7.12)$$

where each μ_{Ui}^m (m = 1, 2, 3, 4) represents an extent to which the utility associated with design/operation option i belongs to the m^{th} utility expression (“*slightly preferred*,” “*moderately preferred*,” “*preferred*,” or “*greatly preferred*”).

7.3.3 Decision Preference Synthesis

Preference degree P_i associated with design/operation option i is obtained by (Wang et al., 1996):

$$P_i = \sum_{j=1}^{4} \mu_{Ui}^j \times K_j + \left(1 - \sum_{j=1}^{4} \mu_{Ui}^j\right) \times ¼ \times \sum_{j=1}^{4} K_j \qquad (7.13)$$

where K_1, K_2, K_3, K_4 are the utility degrees associated with the four utility expressions, respectively; $(1 - \sum_{j=1}^{4} \mu_{Ui}^j)$ describes the remaining belief unassigned after commitment of belief in the synthesis of cost and safety descriptions; and ¼ ×

$\sum_{j=1}^{4} K_j$ is the average value of the K_js. It is worth mentioning that K_1, K_2, K_3, K_4 may not be fixed for different applications and they may be determined by appropriate expert judgments.

Obviously, the larger P_i is the more desirable design/operation option i. The best design/operation option with the largest preference degree can be selected on the basis of the magnitudes of P_i (i = 1, 2, ..., D) if there are several design options available in the design process. Furthermore, If more design objectives such as reliability are dealt with, this method can be easily extended to carry multiple objective decision-making. This method may be more appropriate for use in situations where a design of a maritime engineering product is at the initial stages or there is a lack of adequate data for use in quantitative risk assessment.

7.4 Proposed Fuzzy Logic Safety Modelling Methodology

A generic framework for modelling system safety using an integrated approximate reasoning (AR) and evidential reasoning (ER) approach as depicted in Figure 7.3, consists of seven major steps. It emulates the reasoning process for synthesising human expert judgements within a specific domain of knowledge, codes and standards based on the guidelines and company policy using an AR approach, which is FL-based. In addition, an ER approach is used in the later stage of the framework to handle the safety synthesis of the system with complexity involving multi-experts, or multi-attributes, or a combination of both.

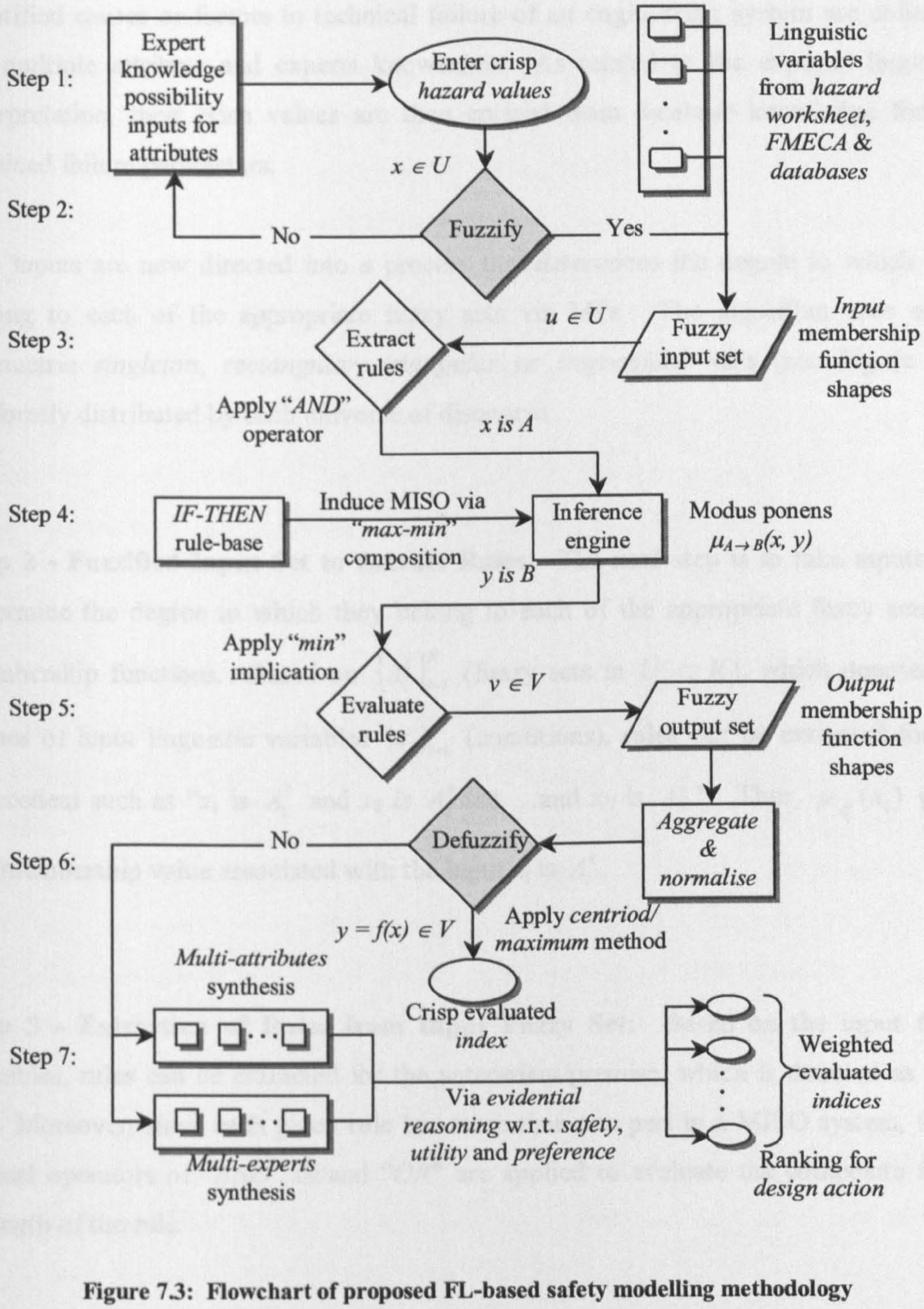


Figure 7.3: Flowchart of proposed FL-based safety modelling methodology

The proposed framework for modelling system safety for risk analysis, as shown in Figure 7.3, consists of seven major steps as follows:

Step 1 - Establishment of Experts Real-Valued Hazard Data: Anticipated and identified causes or factors to technical failure of an engineering system are collected for multiple attribute and experts knowledge. As related to the experts' linguistic interpretation, their crisp values are then entered from database knowledge for the obtained failure parameters.

The inputs are now directed into a process that determines the degree to which they belong to each of the appropriate fuzzy sets via MFs. The algorithm uses either symmetric *singleton*, *rectangular*, *triangular* or *trapezoidal* MFs (see Figure 7.1) uniformly distributed by each universe of discourse.

Step 2 - Fuzzified Input Set to Extract Rules: The next step is to take inputs and determine the degree to which they belong to each of the appropriate fuzzy sets via membership functions. Based on $\{A_i^k\}_{i=1}^N$ (fuzzy sets in $U_i \subset R$), which denotes the values of input linguistic variables $\{x_i\}_{i=1}^N$ (conditions), rules can be extracted for the antecedent such as "x_1 is A_1^k and x_2 *is* A_2^k and ...and x_N is A_N^k". Thus, $\mu_{A_i^k}(x_i)$ gives the membership value associated with the input x_i is A_i^k.

Step 3 - Extraction of Rules from Input Fuzzy Set: Based on the input fuzzy variables, rules can be extracted for the antecedent/premise, which is denoted as "*x is A*". Moreover, since each given rule has more than one part in a MISO system, fuzzy logical operators of "*AND*" or/and "*OR*" are applied to evaluate the composite firing strength of the rule.

Step 4 - Formulation of IF-THEN Rule-Base: Once the inputs have been fuzzified, the degree to which each part of the antecedent has been satisfied for each rule is recognised. If a given rule has more than one part, the fuzzy logical operators are applied to evaluate the composite firing strength of the rule.

A fuzzy relation $R(U, V)$ is a set in the product space $U \times V$ and is characterized by the membership function $\mu_R(x, y)$, where $x \in U$, and $y \in V$, and $\mu_R(x, y) \in [0, 1]$. Fuzzy relations play an important role in fuzzy inference systems. FL uses notions from crisp logic. Concepts in crisp logic can be extended to FL by replacing 0 or 1 values with fuzzy membership values. A singleton fuzzy rule assumes the form "if x *is* A, then y *is* B," where $x \in U$ and $y \in V$, and has a membership function $\mu_R(x, y)$, where $\mu_{A \to B}(x, y) \in [0, 1]$. The IF part of the rule, "x *is* A" is called the antecedent or premise, while the THEN part of the rule, "y *is* B", is called the consequent or conclusion. Interpreting an IF–THEN rule involves two distinct steps. The first step is to evaluate the antecedent, which involves fuzzifying the input and applying any necessary fuzzy operators. The second step is implication, or applying the result of the antecedent to the consequent, which essentially evaluates the membership function $\mu_{A \to B}(x, y)$.

Step 5 - Evaluation of Rules for Output Fuzzy Set: To produce safety evaluation for each cause to a technical failure at the bottom level of a hierarchical system, the consequent/conclusion as denoted by "y *is* B" is formed for the output fuzzy variable of the MISO system. Its output set can be defined using fuzzy safety estimate sets in the same way as the fuzzy inputs. The implication method of the *minimum* or the *product* then shapes the output MFs on the basis of the firing strength of the rule. This input for the implication process is a single number given by the antecedent, and its output is a fuzzy set.

Step 6 - Aggregation and Normalisation: Aggregation is a process whereby the outputs of each rule are unified. Aggregation occurs only once for each output variable. The input to the aggregation process is the truncated output fuzzy sets returned by the implication process for each rule. The output of the aggregation process is the combined output fuzzy set.

The input of the aggregation process is the list of truncated output functions returned by the implication process for each rule. The output of the aggregation process is one fuzzy set for each output variable. As this method is always commutative, the order in

which the rules are executed is not important. The *max* (maximum) method is applied to the aggregation of consequent, "*y is B*", across the rules.

The normalization is required to make the sum of weights equal to 1. This is achieved by dividing each membership value in the fuzzy conclusion set by the sum total of all membership values in the set.

Where defuzzification is used for obtaining a single number output, the input for the process is a fuzzy set (the aggregated output fuzzy set), and the output of the defuzzification process is a crisp value obtained by using some defuzzification method such as the centroid, height, or maximum.

Step 7 - ER Synthesis of Weighted Indices for Ranking: For the ER synthesis, it is highly unlikely for selected experts to have the same importance, as the weights of importance need to be utilised. The assessment of weight for each expert is an important decision for the analyst to make in view of the safety of the system under scrutiny. Each expert is assigned with a weight to indicate the relative importance of his or her judgment in contributing towards the overall safety evaluation process. The analyst must decide which experts are more authoritative. Weights are then assigned accordingly.

The final component describes the calculation of overall risk level ranking index. Then the identified potential causes are ranked on the basis of their ranking index values, or multi-attribute-multi-expert safety synthesis as performed.

7.5 Case Study of Collision Risk for Shuttle Tanker to FPSO Unit

The collision cases that have occurred between FPSO and shuttle tanker in tandem offloading operation has caused a growing concern in the North Sea as well as the rest of the world. Several recent incidents between FPSO and shuttle tanker have clearly witnessed a high likelihood of contact between vessels in tandem offloading. The large masses involved make the collision risk significance.

Tandem offloading from a spread moored FPSO is a high-risk operation, especially as the DP shuttle tanker can pose a threat of collision to the FPSO with potential serious consequences. Moreover, several recent collisions have caused a growing concern that leaves the operation deserving proactive safety scrutiny. Therefore, a novel safety model for collision risk analysis of FPSO and tanker offloading operation is being presented in this case study. The collision risk caused by various technical malfunctions is modelled by using an approximate reasoning approach. This model further provides guides to identify and assess the failure prone situations where man machine interaction happened and resulted in most collision incidents.

7.5.1 FPSO/Shuttle Tanker in Tandem Operation

FPSO (Floating production, storage and offloading) vessels are the state-of-the-art platforms utilised in the process for production, treatment and delivery of crude oil at offshore oil and gas fields worldwide. These vessels tend to be of ship-shape hulls, and therefore they are maintained on station by anchors and mooring lines. Shuttle tankers can be used to export processed oil from these vessels via 'tandem' mooring configuration and this is very popular in the North Sea.

A shuttle tanker in its tandem operational phases (i.e. approach, connection, off-loading, disconnection and departure) off-takes the processed oil from the FPSO with utmost safety precautions. During tandem offloading, the shuttle tanker must stay connected and keep on maintaining its separation proximity to the FPSO, e.g. 80m behind, by use of a DP system. The frequency of offloading operation may range from once every 3 to 5 days, depending on the production likelihood, storage capacity of FPSO, and shuttle tanker size. Normal duration of operation is in the order of 20 hours based on FPSO storage and oil transfer likelihood, though suitable environmental conditions are required. The FPSO is continuously weathering around its turret located either internally or externally. In harsh environments, due to waves and wind, it is also subject to significant low frequency motions in horizontal plane (surge, sway and yaw) (Chen & Moan, 2002). Since tankers with a DP system have greater uptime in harsh environments and are also more practical, they have become widely applied.

7.5.2 Collision Risk Experiences

Before the turn of the millennium, some 500 ships were reported to have collided with offshore installations in the UK sector for the last 25 years duration (HSE, 1999). Over 96% of the collisions have involved attendant vessels such as shuttle tankers other authorised vessels. Among these have been recent impact cases in the North Sea involving FPSO and shuttle tanker incidents (Leonhardsen et. al, 2001) as follows:

- Shuttle tanker Futura collided with Gryphon FPSO on 26th July 1997.
- Shuttle tanker Aberdeen collided with Captain FPSO on 12th August 1997.
- Shuttle tanker Nordic Savonita collided with Schiehallion FPSO on 25th September 1998.
- Shuttle tanker Knock Sallie collided with Norne FPSO on 5th March 2000.

The later of these FPSO-shuttle tanker collision cases, a 154,000 dwt shuttle tanker at 0.6 m/s impact velocity, had its impact energy as high as 31 MJ (Helgøy, 2002). Recognising the large masses and subsequently the large impact energy involved in such incidents, the damaging potential can relatively be intensified and thus the risk associated is significant. In the worst-case scenario, catastrophic consequences in terms of loss of life, environmental impact and business risk are reasonably foreseeable.

Furthermore, stern damage on the FPSO may cause penetration and flooding in the machine room. Moreover, with the widely adopted FPSO design, e.g. Gryphon, Captain, Norne, Åsgard and etc. (Kerr-McGee Oil, 1995 and Statoil, 1995), the living quarters are located in the bow area, thus the flare towers, which have to be located in the stern area, are vulnerable to tanker impact. The worst scenario could therefore be a major tanker collision that topples down FPSO's flare tower on stern. This can initiate a chain of events with severe fire and explosion on both vessels. The majority of reported incidents are caused by station-keeping related technical failure such as propulsion (thrusters, propeller, engine, generator, pitch-control device), DP, position reference sensor, and operation or maintenance of these systems.

7.5.3 A Fuzzy Rule-Based Evidential Reasoning Safety Modelling

In this section, safety assessment is carried out on risk introduced by the collision of FPSO and shuttle tanker during tandem offloading operation. It is based on risk caused by technical failures, although it should be noted that operational failures are recognised as one of the major causes of collision.

7.5.3.1 Linguistic Expression of Collision Risk Input Parameters

One realistic way to deal with imprecision is to use linguistic assessments. The main artificial intelligence mechanism behind a typical fuzzy safety model is its fuzzy inference engine. A fuzzy inference engine comprises the selection or development of the type/types of fuzzy membership function used to represent risk levels and fuzzy rule bases to generate fuzzy safety estimates. The linguistic variables are employed in the development of fuzzy membership function for each input parameter. The goal of fuzzy linguistic variables is to represent the condition of an attribute/parameter at a given interval.

Based on experience and judgment combined with grading evaluation guidelines, the assessment team assigns numeric values to each attribute/parameter for fuzzy set input. These numeric values are based on a ten-point scale as anchored by linguistic variable and descriptors provided by evaluation. The ten-point scale is indicative of performance in regards to industry standard, minimum Code requirements, and good marine practice.

The three attributes/parameters for fuzzy set input, which can be considered for modelling failure modes, are *failure likelihood, consequence severity* and *failure consequence probability* (Sii, *et. al*, 2005). These can be combined via a rule-base to find degree of failure, or degree to which safety level can be achieved.

Failure likelihood, L, describes the failure frequencies in a certain time, which directly represents the numbers of failures anticipated during the design life span of a particular

system or an item. Table 7.1 describes the range of the frequencies of the failure occurrence and defines the fuzzy set of *L*. To estimate *L*, one may choose to use such linguistic variables as "*very low* (L_1)", "*low* (L_2)", "*Reasonably low* (L_3)", "*average* (L_4)", "*Reasonably Frequent* (L_5)", "*frequent* (L_6)" and "*highly frequent* (L_7)".

It is noted that the evaluation criteria for *failure likelihood* can be modified according to different requirements in codes and standards and different aspects of platforms such as fire, explosions, structure, safety system, etc.

Table 7.1: Failure likelihood

Rank	*Failure likelihood, L*	Meaning (general interpretation)	Failure likelihood (1/year)
1,2,3	Very low, L_1	Failure is unlikely but possible during lifetime	$< 10^{-5}$
4	Low, L_2	Likely to happen once during lifetime	0.25×10^{-5}
5	Reasonably low, L_3	Between low and average	0.25×10^{-4}
6	Average, L_4	Occasional failure	10^{-3}
7	Reasonably Frequent, L_5	Likely to occur from time to time	0.25×10^{-2}
8, 9	Frequent, L_6	Repeated failure	0.125×10^{-1}
9,10	Highly frequent, L_7	Failure is almost inevitable or likely to exist repeatedly	$> 0.25 \times 10^{-1}$

Consequence severity, *C*, describes the magnitude of possible consequences, which is ranked according to the severity of the failure effects. One may choose to use such linguistic variables as "*negligible* (C_1)", "*marginal* (C_2)", "*moderate* (C_3)", "*critical* (C_4)" and "*catastrophic* (C_5)". Table 7.2 shows the criteria used to rank the *consequence severity* of failure effects.

Table 7.2: Consequence severity

Rank	*Consequence severity, C*	Meaning (generic marine and offshore structure/system interpretation)
1	Negligible, C_1	At most a single minor injury or unscheduled maintenance required (service and operations can continue).
2, 3	Marginal, C_2	Possible single or multiple minor injuries or/and minor system damage. Operations interrupted slightly, and resumed to its normal operational mode within a short period of time (say less than 2 hours).
4, 5, 6	Moderate, C_3	Possible multiple minor injuries or a single severe injury, moderate system damage. Operations and production interrupted marginally, and resumed to its normal operational mode within, say no more than 4 hours.
7, 8	Critical, C_4	Possible single death, probable multiple severe injuries or major system damage. Operations stopped, platform closed, shuttle tanker's failure to function. High degree of operational interruption due to the nature of the failure such as an inoperable platform (e.g. drilling engine fails to start, power system failure, turret mooring system failure) or an inoperable convenience subsystem (e.g. DP, PRS).
9, 10	Catastrophic, C_5	Possible multiple deaths, probable single death or total system loss. Very high severity ranking when a potential failure mode (e.g. collision between FPSO and shuttle tanker, blow-out, fire and explosion) affects safe platform operation and/or involves non-compliance with government regulations.

Failure consequence probability, E, defines the probability that ensued consequences gives the occurrence of the event. For E, one may choose to use such linguistic terms as "*highly unlikely* (E_1)", "*unlikely* (E_2)", "*reasonably unlikely* (E_3)", "*likely* (E_4)", "*reasonably likely* (E_5)", "*highly likely* (E_6)" and "*definite* (E_7)". Table 7.3 shows the possible criteria used to definite the linguistic terms for describing and ranking E of failure effects.

Table 7.3: Failure consequence probability

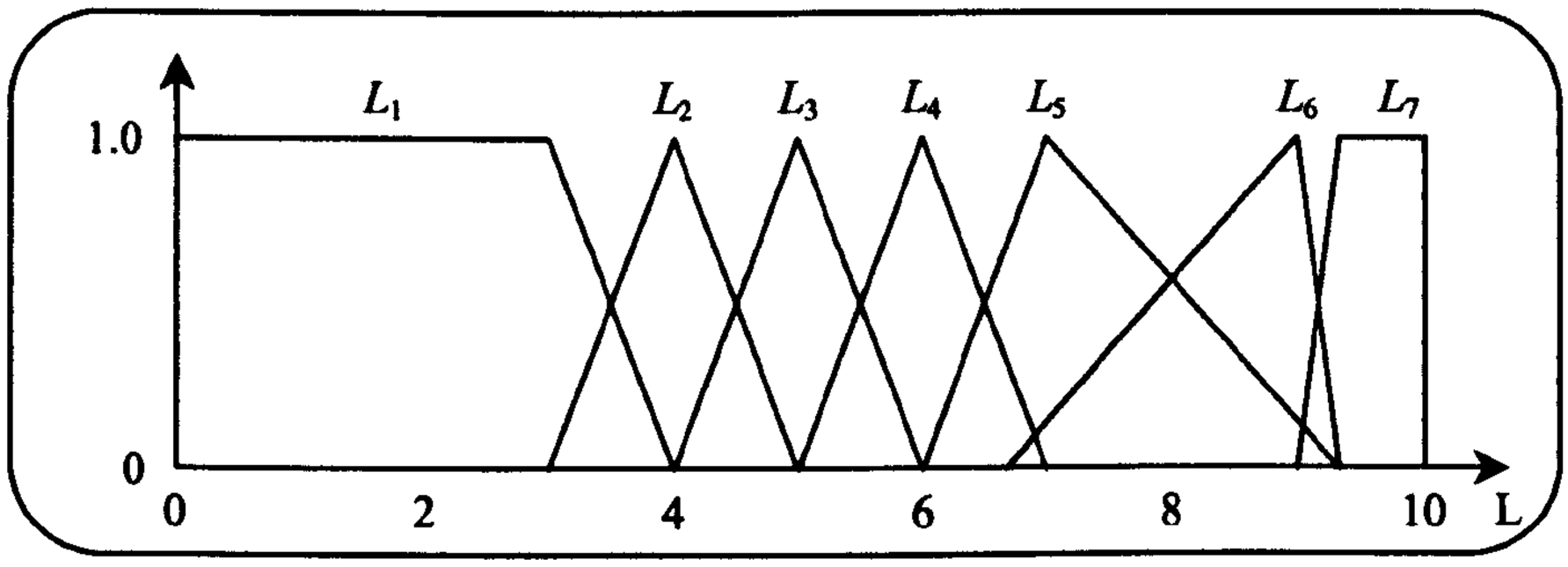
Rank	*Failure consequence probability, E*	Meaning
1	Highly unlikely, E_1	The occurrence likelihood of possible consequence is highly unlikely given the occurrence of the failure event (extremely unlikely to exist on the system or during operations).
2,3	Unlikely, E_2	The occurrence likelihood of possible consequences is unlikely but possible given that the failure event happens (improbable to exist even on rare occasions on the system or during operations).
4	Reasonably unlikely, E_3	The occurrence likelihood of possible consequences is reasonably unlikely given the occurrence of the failure event (likely to exist on rare occasions on the system or during operations).
5	Likely, E_4	It is likely that consequences happen given that the failure event occurs (a programme is not likely to detect a potential design or operations procedural weakness).
6,7	Reasonably likely, E_5	It is reasonably likely that consequences occur given the occurrence of the failure event (i.e. exist from time to time on the system or during operations, possibly caused by a potential design or operations procedural weakness).
8	Highly likely, E_6	It is highly likely that consequences occur given the occurrence of the failure event (i.e. often exist somewhere on the system or during operations due to a highly likely potential hazardous situation or design and/or operations procedural drawback).
9,10	Definite, E_7	Possible consequences happen given the occurrence of a failure event (i.e. likely to exist repeatedly during operations due to a anticipated potential design and operations procedural drawback).

With reference to the above fuzzy descriptions of *L*, *C* and *E*, it may be observed that the linguistic variables are not exclusive, as there are intersections among the defined linguistic variables describing *L*, *C* and *E*. Inclusive expressions may make it more convenient for the safety analysts to judge a safety level.

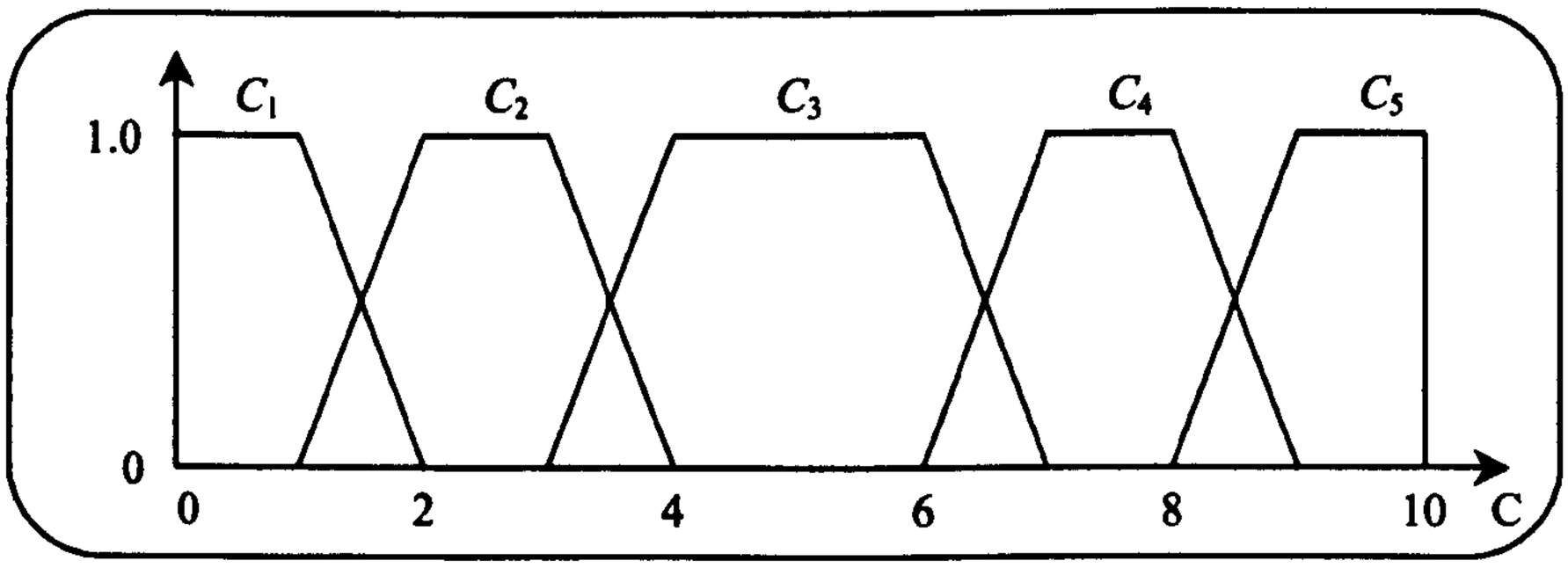
7.5.3.2 Input Fuzzy Variable Semantics for Collision Risk

In taking the form of the defined MFs, the three attributes/parameters for fuzzy set input are expresses by the following sets:

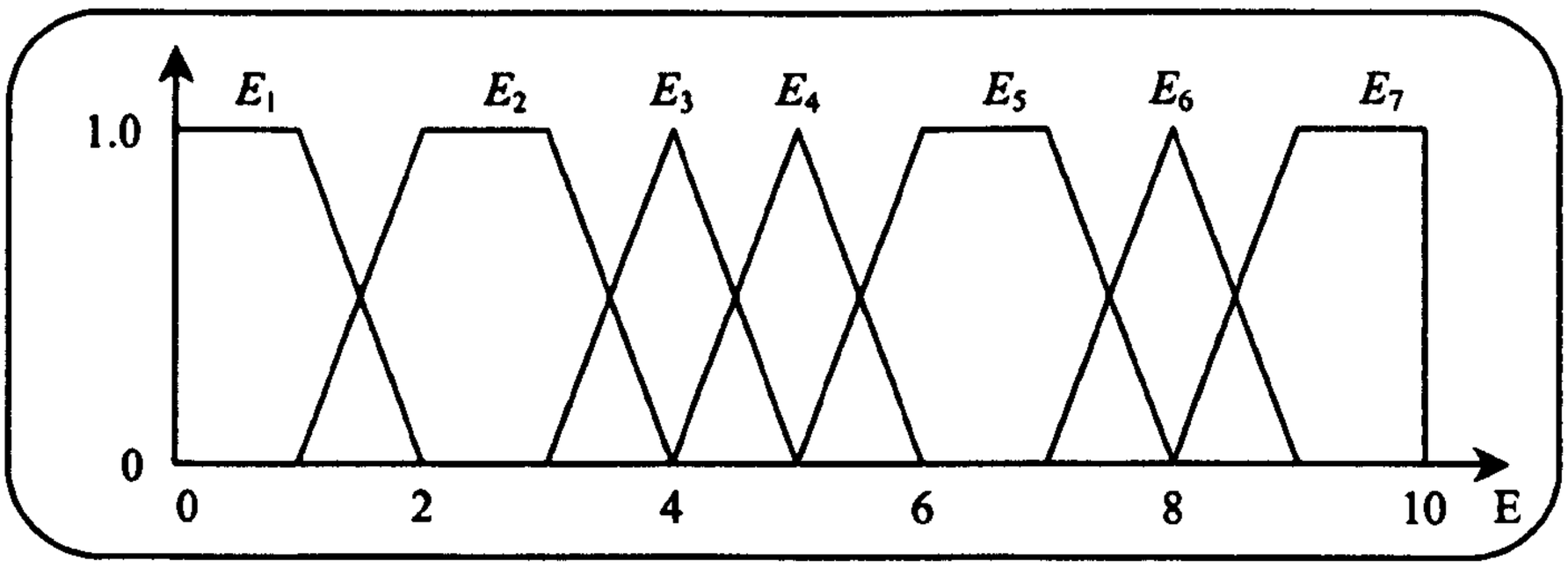
$$L = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7\}$$
$$C = \{C_1, C_2, C_3, C_4, C_5\}$$
$$E = \{E_1, E_2, E_3, E_4, E_5, E_6, E_7\}$$



(a) Fuzzy set definition for failure likelihood, L



(b) Fuzzy set definition for consequence severity, C



(c) Fuzzy set definition for failure consequence probability, E

Figure 7.4: Fuzzy input set definition for risk-based analytical modelling

Overlapping functions, as shown in Figure 7.4, are used to represent various linguistic variables for all attributes because the experts and the literature concurred that in the analysis of the risks associated with a failure event/mode, the risk levels may have "gray" or ill-defined boundaries (Bell & Badiru, 1996).

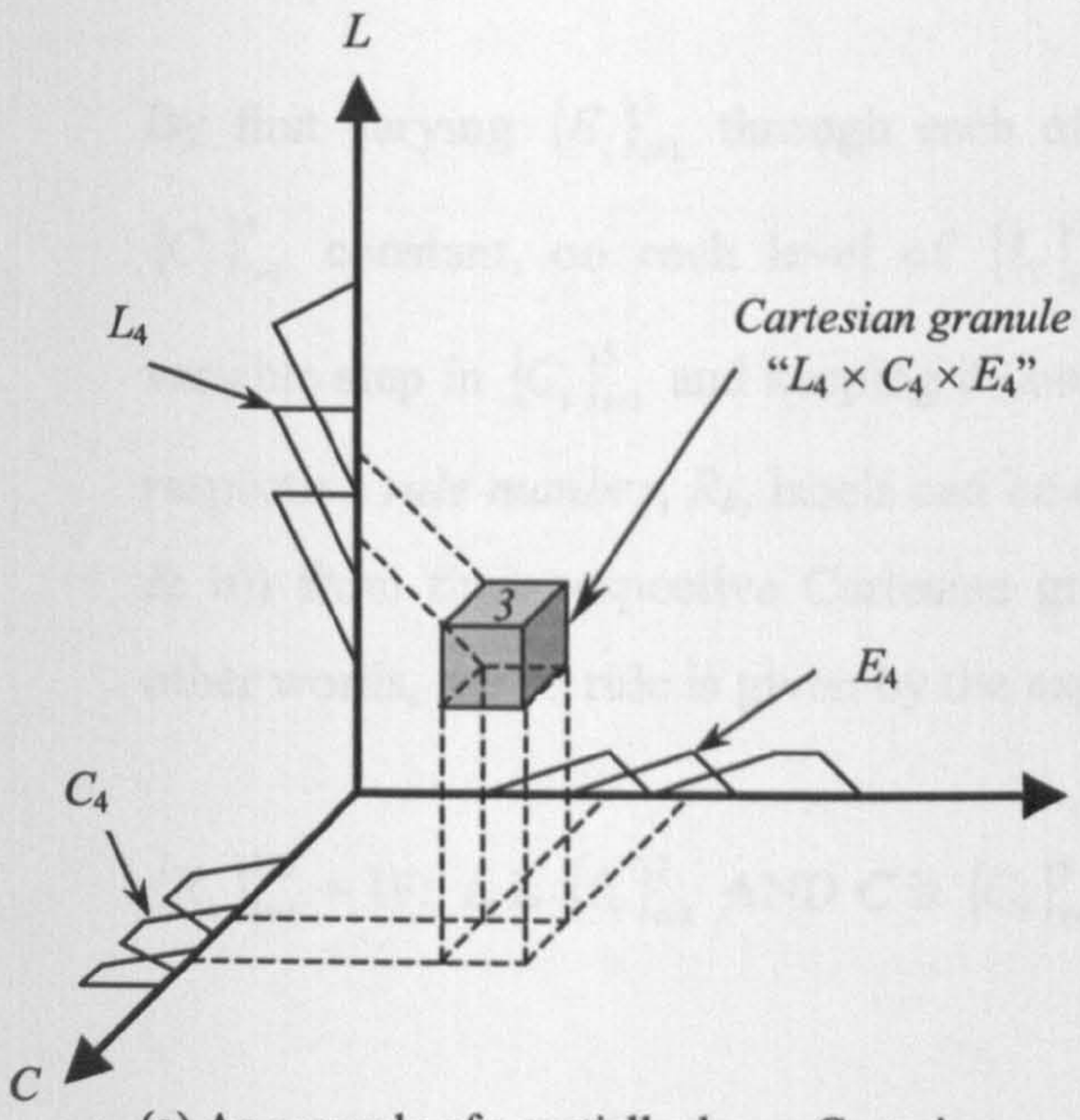
7.5.3.3 Fuzzy Associative Matrix of Collision Risk Fuzzy Conclusion

Safety estimate, *S*, is the only output fuzzy variable used in this study to produce safety evaluation for each cause to a technical failure at the bottom level of a hierarchical system. It is described linguistically by the variables "*poor*", "*fair*", "*average*", and "*good*".

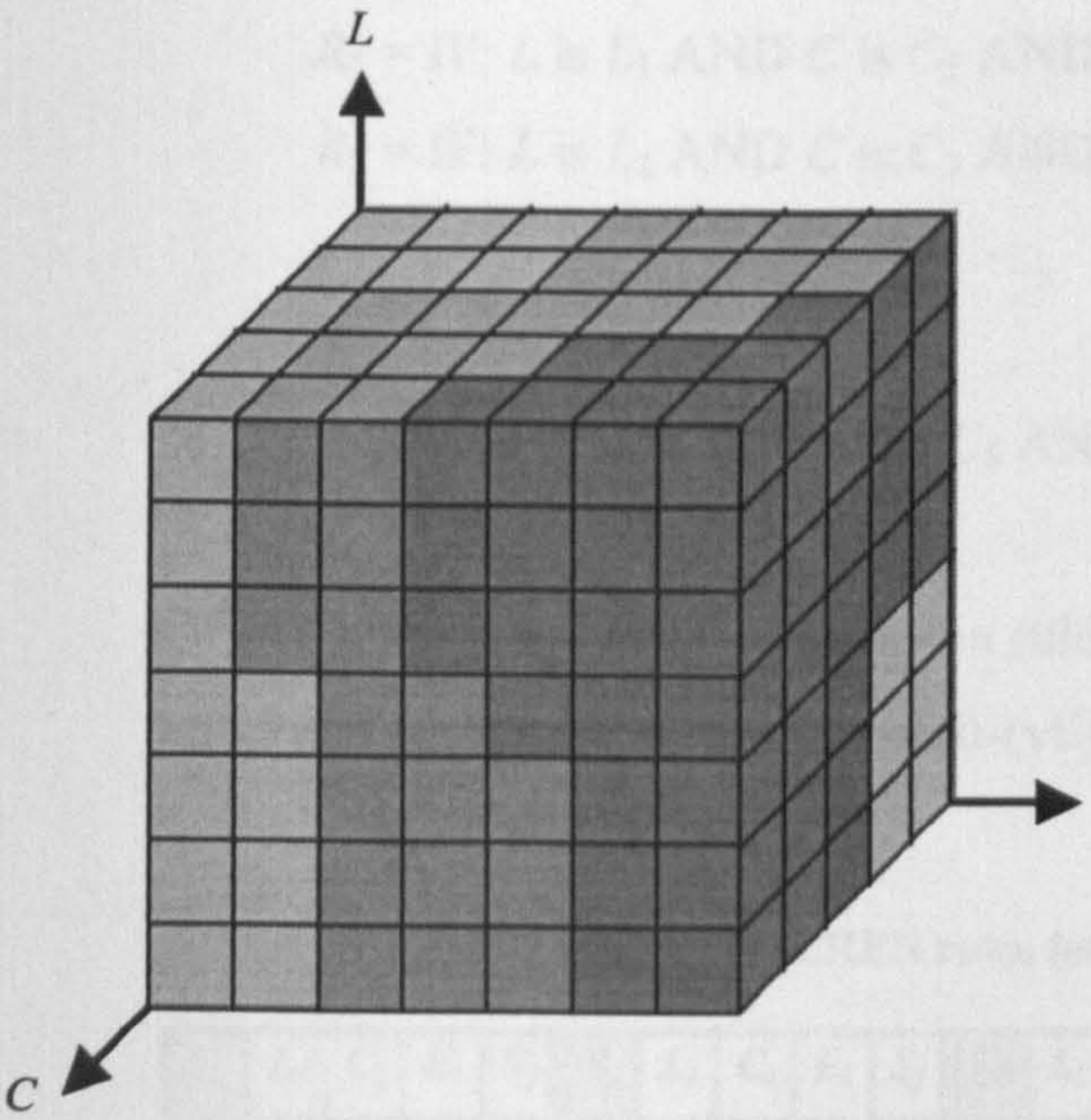
For an independent fuzzy variable, such as *S*, the rule size grows geometrically according to:

$$R_{MISO} = 7_L \times 5_C \times 7_E = 245_S \qquad (7.14)$$

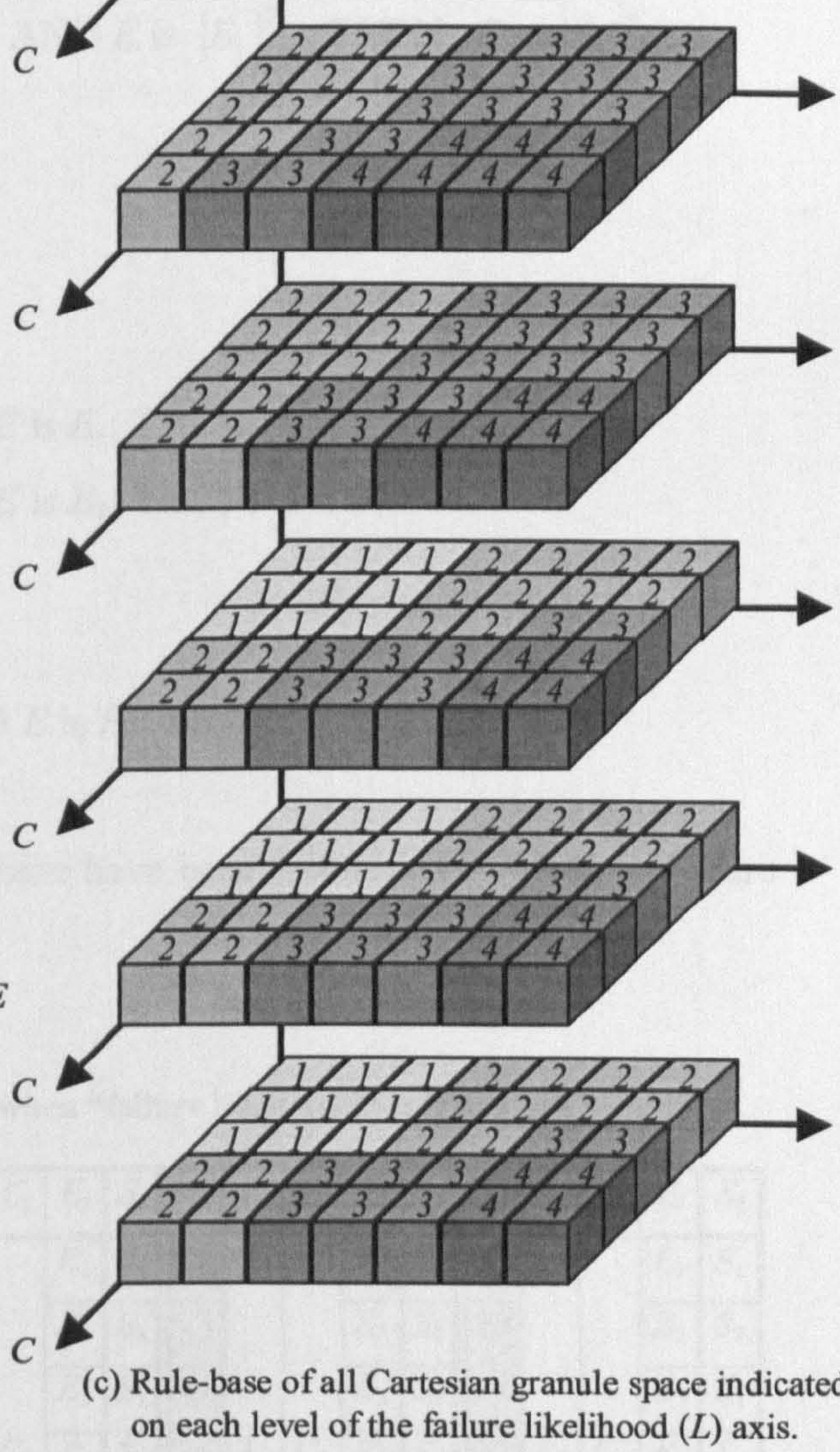
The relationship between fuzzy sets and rules is normally shown in a *fuzzy associative memory/matrix (FAM)* (i.e., the overall risk matrix for the variables). A FAM encodes the fuzzy rules. Each dimension of the matrix represents the fuzzy sets assigned to an independent variable. The cubic FAM of Figure 7.5 shows the 245 rules in its Cartesian product space format as obtained from the $7L \times 5C \times 7E$ input combinations.



(a) An example of a partially drawn Cartesian granule space build on 3 features. The Cartesian granule "$L_4 \times C_4 \times E_4$" is outlined.



(b) Assembled unit of all the Cartesian granule space in the safety expression rule-base.



(c) Rule-base of all Cartesian granule space indicated on each level of the failure likelihood (L) axis.

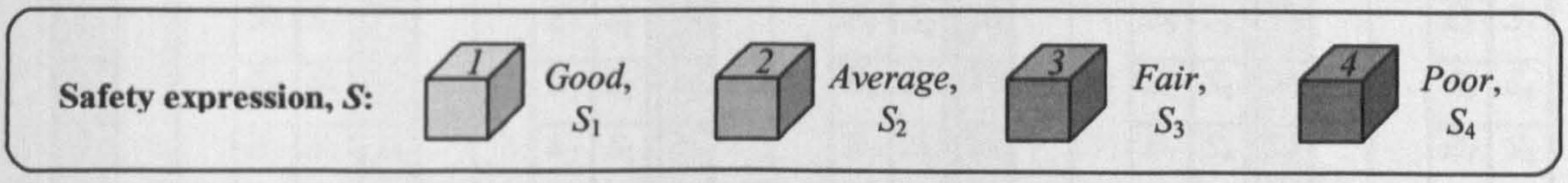


Figure 7.5: Cube FAM matrix for safety expression rule-base

By first varying $\{E_i\}_{i=1}^{7}$ through each of its linguistic variable steps, whilst keeping $\{C_i\}_{i=1}^{5}$ constant, on each level of $\{L_i\}_{i=1}^{7}$, then going next through each linguistic variable step in $\{C_i\}_{i=1}^{5}$ and keeping it constant whilst varying $\{E_i\}_{i=1}^{7}$, all rules and their respective *rule number*, R_k, labels can be obtained for $k = 1$ to $k = 245$ (see Figure 7.5(a & b)) from their respective Cartesian granule in the safety expression rule-base. In other words, the k^{th} rule is given by the expression:

$$\{R_k\}_{k=1}^{245} = \text{IF: } L \text{ is } \{L_i\}_{i=1}^{7} \text{ AND } C \text{ is } \{C_i\}_{i=1}^{5} \text{ AND } E \text{ is } \{E_i\}_{i=1}^{7}; \text{ THEN: } S \text{ is } \{S_j\}_{j=1}^{4} \tag{7.15}$$

Therefore:

$R_1 =$ IF: L is L_1 AND C is C_1 AND E is E_1; THEN: S is S_1

$R_2 =$ IF: L is L_1 AND C is C_1 AND E is E_2; THEN: S is S_1

-

-

$R_{245} =$ IF: L is L_7 AND C is C_5 AND E is E_7; THEN: S is S_4

All 245 rules in the safety expression rule base have been assembled as given in Figure 7.5(c) and as detailed in Tables 7.4(i)-(vii).

Table 7.4(i): All IF-THEN rules for when "failure likelihood" is "very low"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
1			E_1	S_1	8			E_1	S_1	15			E_1	S_1	22			E_1	S_2	29			E_1	S_2
2			E_2	S_1	9			E_2	S_1	16			E_2	S_1	23			E_2	S_2	30			E_2	S_2
3			E_3	S_1	10			E_3	S_1	17			E_3	S_1	24			E_3	S_3	31			E_3	S_3
4	L_1	C_1	E_4	S_2	11	L_1	C_2	E_4	S_2	18	L_1	C_3	E_4	S_2	25	L_1	C_4	E_4	S_3	32	L_1	C_5	E_4	S_3
5			E_5	S_2	12			E_5	S_2	19			E_5	S_2	26			E_5	S_3	33			E_5	S_3
6			E_6	S_2	13			E_6	S_2	20			E_6	S_3	27			E_6	S_4	34			E_6	S_4
7			E_7	S_2	14			E_7	S_2	21			E_7	S_3	28			E_7	S_4	35			E_7	S_4

Table 7.4(ii): All IF-THEN rules for when "failure likelihood" is "low"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
36			E_1	S_1	43			E_1	S_1	50			E_1	S_1	57			E_1	S_2	64			E_1	S_2
37			E_2	S_1	44			E_2	S_1	51			E_2	S_1	58			E_2	S_2	65			E_2	S_2
38			E_3	S_1	45			E_3	S_1	52			E_3	S_1	59			E_3	S_3	66			E_3	S_3
39	L_2	C_1	E_4	S_2	46	L_2	C_2	E_4	S_2	53	L_2	C_3	E_4	S_2	60	L_2	C_4	E_4	S_3	67	L_2	C_5	E_4	S_3
40			E_5	S_2	47			E_5	S_2	54			E_5	S_2	61			E_5	S_3	68			E_5	S_3
41			E_6	S_2	48			E_6	S_2	55			E_6	S_3	62			E_6	S_4	69			E_6	S_4
42			E_7	S_2	49			E_7	S_2	56			E_7	S_3	63			E_7	S_4	70			E_7	S_4

Table 7.4(iii): All IF-THEN rules for when "failure likelihood" is "reasonably low"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
71			E_1	S_1	78			E_1	S_1	85			E_1	S_1	92			E_1	S_2	99			E_1	S_2
72			E_2	S_1	79			E_2	S_1	86			E_2	S_1	93			E_2	S_2	100			E_2	S_2
73			E_3	S_1	80			E_3	S_1	87			E_3	S_1	94			E_3	S_3	101			E_3	S_3
74	L_3	C_1	E_4	S_2	81	L_3	C_2	E_4	S_2	88	L_3	C_3	E_4	S_2	95	L_3	C_4	E_4	S_3	102	L_3	C_5	E_4	S_3
75			E_5	S_2	82			E_5	S_2	89			E_5	S_2	96			E_5	S_3	103			E_5	S_3
76			E_6	S_2	83			E_6	S_2	90			E_6	S_3	97			E_6	S_4	104			E_6	S_4
77			E_7	S_2	84			E_7	S_2	91			E_7	S_3	98			E_7	S_4	105			E_7	S_4

Table 7.4(iv): All IF-THEN rules for when "failure likelihood" is "average"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
106			E_1	S_2	113			E_1	S_2	120			E_1	S_2	127			E_1	S_2	134			E_1	S_2
107			E_2	S_2	114			E_2	S_2	121			E_2	S_2	128			E_2	S_2	135			E_2	S_2
108			E_3	S_2	115			E_3	S_2	122			E_3	S_2	129			E_3	S_3	136			E_3	S_3
109	L_4	C_1	E_4	S_3	116	L_4	C_2	E_4	S_3	123	L_4	C_3	E_4	S_3	130	L_4	C_4	E_4	S_3	137	L_4	C_5	E_4	S_3
110			E_5	S_3	117			E_5	S_3	124			E_5	S_3	131			E_5	S_3	138			E_5	S_4
111			E_6	S_3	118			E_6	S_3	125			E_6	S_3	132			E_6	S_4	139			E_6	S_4
112			E_7	S_3	119			E_7	S_3	126			E_7	S_3	133			E_7	S_4	140			E_7	S_4

Table 7.4(v): All IF-THEN rules for when "failure likelihood" is "reasonably frequent"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
141			E_1	S_2	148			E_1	S_2	155			E_1	S_2	162			E_1	S_2	169			E_1	S_2
142			E_2	S_2	149			E_2	S_2	156			E_2	S_2	163			E_2	S_2	170			E_2	S_3
143			E_3	S_2	150			E_3	S_2	157			E_3	S_2	164			E_3	S_3	171			E_3	S_3
144	L_5	C_1	E_4	S_3	151	L_5	C_2	E_4	S_3	158	L_5	C_3	E_4	S_3	165	L_5	C_4	E_4	S_3	172	L_5	C_5	E_4	S_4
145			E_5	S_3	152			E_5	S_3	159			E_5	S_3	166			E_5	S_4	173			E_5	S_4
146			E_6	S_3	153			E_6	S_3	160			E_6	S_3	167			E_6	S_4	174			E_6	S_4
147			E_7	S_3	154			E_7	S_3	161			E_7	S_3	168			E_7	S_4	175			E_7	S_4

Table 7.4(vi): All IF-THEN rules for when "failure likelihood" is "frequent"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
176			E_1	S_2	183			E_1	S_2	190			E_1	S_2	197			E_1	S_2	204			E_1	S_2
177			E_2	S_2	184			E_2	S_2	191			E_2	S_2	198			E_2	S_3	205			E_2	S_3
178			E_3	S_2	185			E_3	S_2	192			E_3	S_2	199			E_3	S_3	206			E_3	S_3
179	L_6	C_1	E_4	S_3	186	L_6	C_2	E_4	S_3	193	L_6	C_3	E_4	S_3	200	L_6	C_4	E_4	S_3	207	L_6	C_5	E_4	S_4
180			E_5	S_3	187			E_5	S_3	194			E_5	S_3	201			E_5	S_4	208			E_5	S_4
181			E_6	S_3	188			E_6	S_3	195			E_6	S_3	202			E_6	S_4	209			E_6	S_4
182			E_7	S_3	189			E_7	S_3	196			E_7	S_4	203			E_7	S_4	210			E_7	S_4

Table 7.4(vii): All IF-THEN rules for when "failure likelihood" is "highly frequent"

R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j	R_k	L_i	C_i	E_i	S_j
211			E_1	S_2	218			E_1	S_2	225			E_1	S_2	232			E_1	S_2	239			E_1	S_2
212			E_2	S_2	219			E_2	S_2	226			E_2	S_2	233			E_2	S_3	240			E_2	S_3
213			E_3	S_2	220			E_3	S_2	227			E_3	S_2	234			E_3	S_3	241			E_3	S_3
214	L_7	C_1	E_4	S_3	221	L_7	C_2	E_4	S_3	228	L_7	C_3	E_4	S_3	235	L_7	C_4	E_4	S_3	242	L_7	C_5	E_4	S_4
215			E_5	S_3	222			E_5	S_3	229			E_5	S_3	236			E_5	S_4	243			E_5	S_4
216			E_6	S_3	223			E_6	S_3	230			E_6	S_3	237			E_6	S_4	244			E_6	S_4
217			E_7	S_3	224			E_7	S_3	231			E_7	S_4	238			E_7	S_4	245			E_7	S_4

7.5.4 Potential Causes of Collision Risk Technical Failures

Collision of an FPSO and a shuttle tanker scenario can largely be initiated by technical failures and escalated through operational failures (or visa versa). These technical

failures, such as in malfunction of propulsion system, can occur owing to the following four major causes (Chen & Moan, 2002):

- Cause 1 (a_1): *Controllable pitch propeller* (CPP) failure.
- Cause 2 (a_2): *Thruster* failure.
- Cause 3 (a_3): *Position reference system* (PRS) failure.
- Cause 4 (a_4): *Dynamic positioning system* (DPS) failure.

These causes can be modelled for risk analysis to be performed through the proposed integrated AR and ER methodology in Section 7.5. There are *five experts* (i.e., e_1, e_2, e_3, e_4, e_5,) taking part in the safety assessment. For the purpose of safety modelling, the input parameters of L, C and E, will be fed to the proposed safety model in terms of $\mu_F(x)$ in any one of the four forms in Figure 7.1(a) (i) to (iv). Pertaining to the level of ambiguity and uncertainty associated with the case as perceived by a particular expert, the selection of forms of membership function by each expert is dependent upon subjective judgment made.

7.5.5 Expert Judgment Input Membership for Potential Causes

On the basis of the qualitative assessment made by each expert, the safety estimate, S, of each technical failure for each cause can be assessed. Therefore, upon their subjective judgment, the assessment made by each expert, $\{e_i\}_{i=1}^{5}$, due to each potential cause, $\{a_l\}_{l=1}^{4}$, is as provided in Table 7.5.

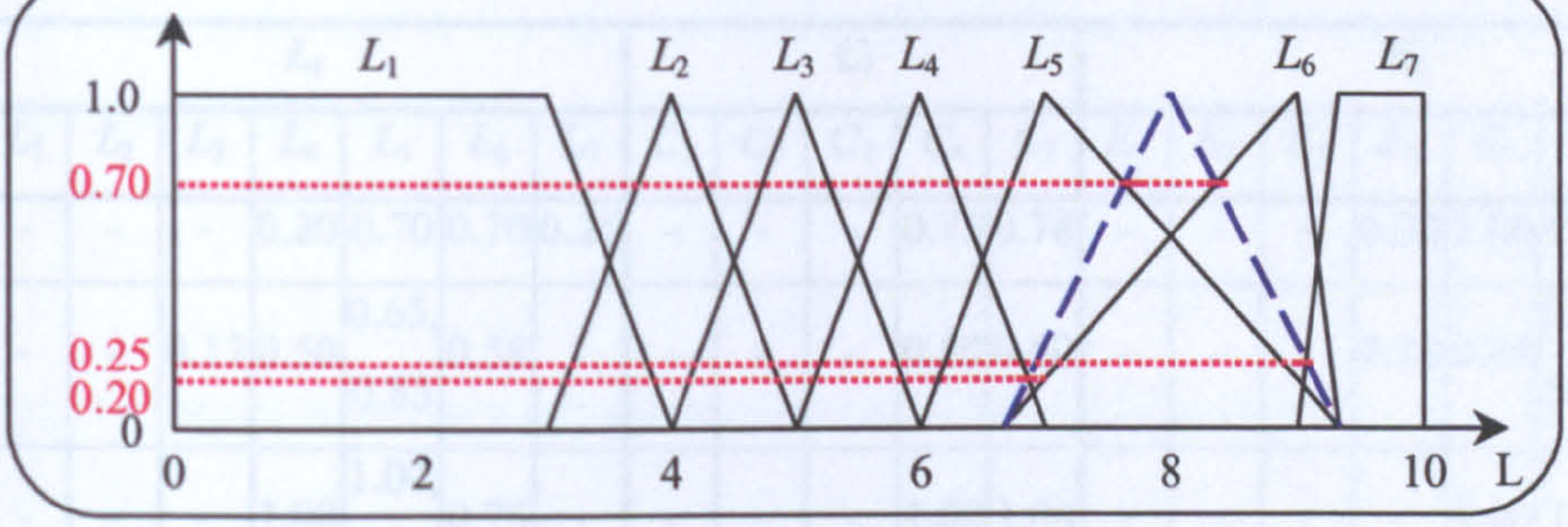
All of these subjective judgment made can be expressed diagrammatically. For example, the input membership judgement made for potential cause a_1 by expert e_1 is as shown diagrammatically in Figure 7.6.

Expert #1 used triangular form of membership function to address the inherent uncertainty associated with the data and information available while carrying out assessment on the three input parameters. L is described triangularly as (6.5, 8.0, 9.5) on the fuzzy scale as shown in Figure 7.6(a). The most likely value is 8.0, 6.5 and 9.5

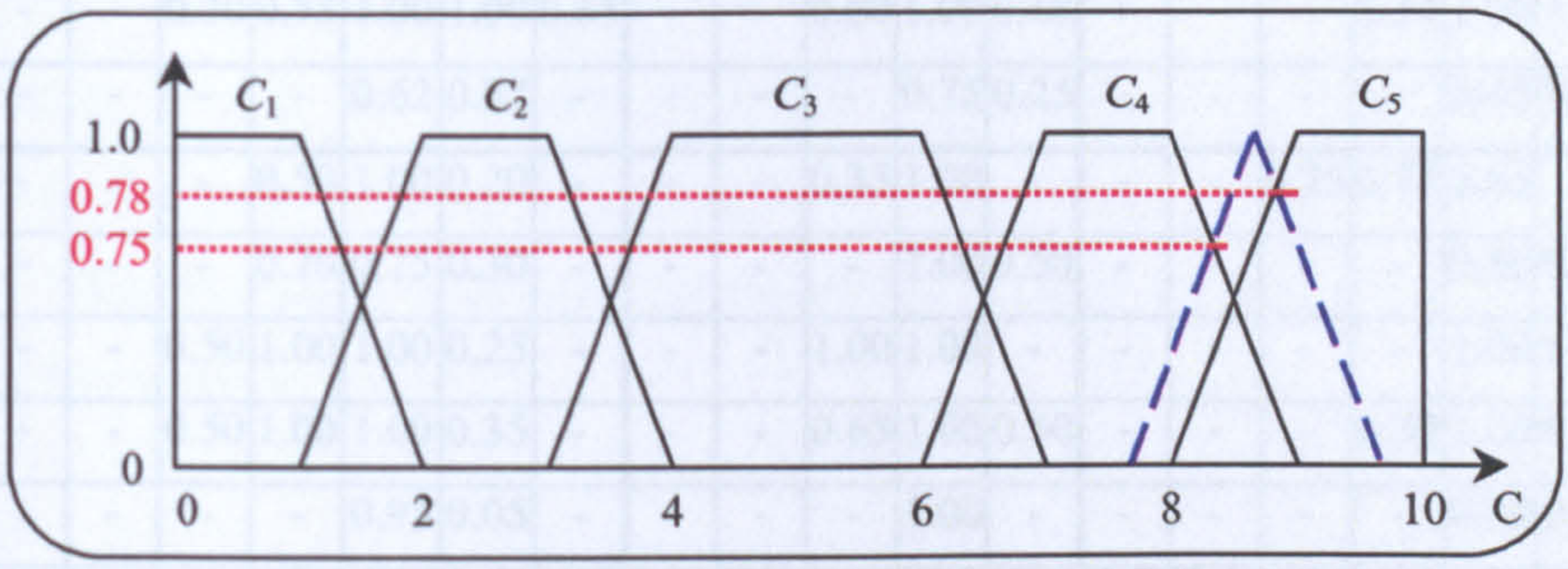
are the lower and upper least likely values, respectively. It has membership degrees of 0.2 in the "*Average*", 0.7 in the *"Reasonably frequent"*, 0.7 in the *"Frequent"*, and 0.25 in the "*Highly frequent*", respectively. As for *C* (see Figure 7.6(b)), it is described triangularly as (7.5, 8.5, 9.5). 8.5 is the most likely value, 7.5 and 9.5 are the lower and upper least likely values used to represent *C*. It has membership degree of 0.75 in the "*Critical*" and 0.78 in the "*Catastrophic*". *E* is triangularly represented as (5.5, 7.0, 8.5), with 7.0 as its most likely value, 5.5 and 8.5 as its lower and upper least likely values (see Figure 7.6(c)). It has its membership degrees of 0.2 in the "*Likely*", 1.0 in the *"Reasonably likely"*, 0.6 in the *"Highly likely"* and 0.2 in the "*Definite*", respectively.

Table 7.5: Expert judgment input membership values for each potential malfunctioned cause

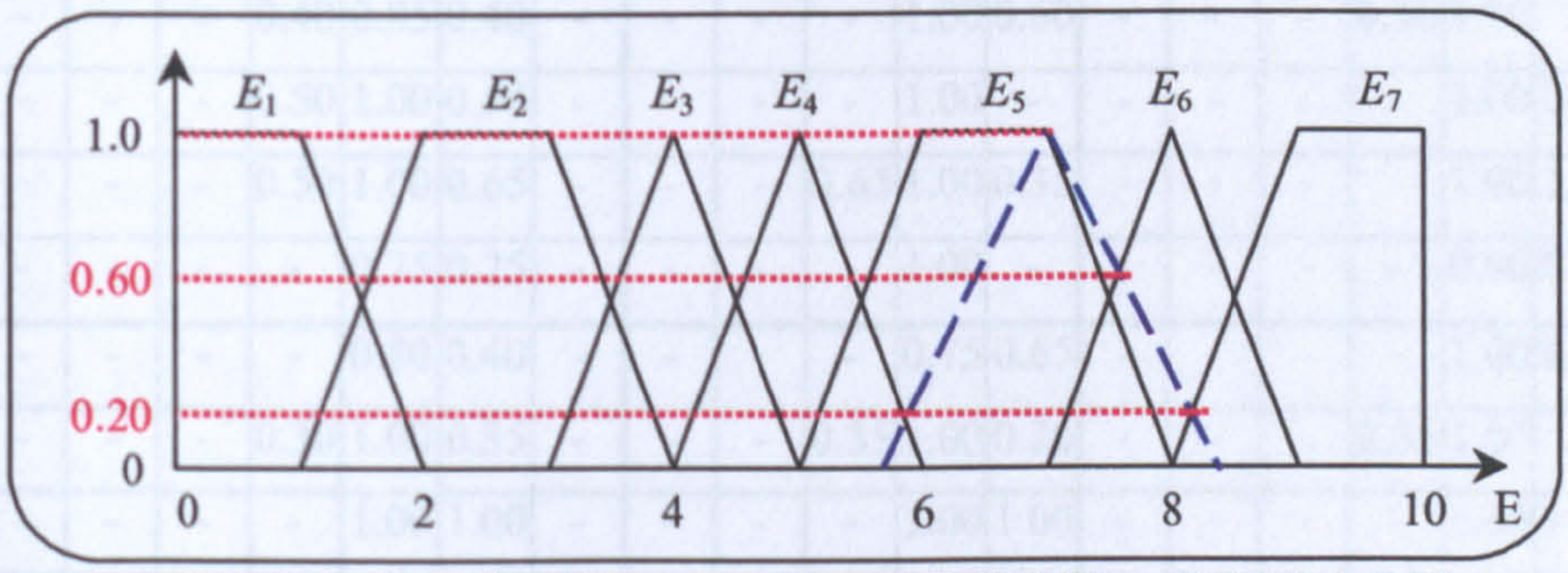
a_l	e_l	$\mu_F(x)$	*L*	*C*	*E*
1	1	Triangular	{6.5, 8, 9.5}	{7.5, 8.5, 9.5}	{5.5, 7, 8.5}
	2	Triangular	{5.5, 7.5, 9}	{7, 8.5, 10}	{5, 7.5, 9.5}
	3	Closed interval	{6, 8}	{7, 9}	{6.5, 9}
	4	Trapezoidal	{5.5, 6.5, 9, 10}	{5.5, 7, 8, 10}	{5, 7, 8, 8.5}
	5	Single deterministic	{7.75}	{8.25}	{7.6}
2	1	Triangular	{6, 7, 7.5}	{6.5, 7, 8}	{4.5, 5.5, 6}
	2	Triangular	{6, 6.5, 8}	{7, 8, 9}	{6, 7.5, 8}
	3	Closed interval	{5.5, 5.5, 7.5, 7.5}	{6, 6, 8, 8}	{6, 6, 8, 8}
	4	Trapezoidal	{5, 6, 7, 8}	{5, 7, 8, 9}	{5, 6, 7, 9}
	5	Single deterministic	{7.15}	{7.95}	{7.25}
3	1	Triangular	{6.5, 7, 7.5}	{8, 8.5, 9}	{5.5, 7, 8}
	2	Triangular	{6, 7.5, 8}	{7.5, 8, 9.5}	{5, 6, 7}
	3	Closed interval	{6.5, 6.5, 8, 8}	{7, 7, 7.5, 7.5}	{6.5, 6.5, 7.5, 7.5}
	4	Trapezoidal	{6, 7, 8, 9}	{5, 7, 8, 8.5}	{6, 7, 8, 9}
	5	Single deterministic	{7.5}	{7.2}	{7.1}
4	1	Triangular	{7, 7.5, 8}	{7.5, 8.5, 9}	{6, 7, 7.5}
	2	Triangular	{6.5, 7, 8}	{6.5, 7, 8.5}	{5.5, 6, 7}
	3	Closed interval	{7, 7, 9, 9}	{7.5, 7.5, 9.5, 9.5}	{7, 7, 8, 8}
	4	Trapezoidal	{6.5, 7, 7.5, 8}	{6, 6.5, 7, 8}	{6.5, 7, 7.5, 9}
	5	Single deterministic	{7.95}	{8.25}	{7.9}



(a) Fuzzy input for failure likelihood, L (6.5, 8.0, 9.5)



(b) Fuzzy input for consequence severity, C (7.5, 8.5, 9.5)



(c) Fuzzy input for failure consequence probability, E (5.5, 7.0, 8.5)

Figure 7.6: Expert #1 fuzzy input set definition for CPP failure

7.5.6 Risk assessment of the Input Membership for Potential Causes

The risk assessment carried out by each expert on each collision risk potential cause is depicted in Table 7.6, as given for each $\{L_i\}_{i=1}^{7}$, $\{C_i\}_{i=1}^{5}$ and $\{E_i\}_{i=1}^{7}$.

Table 7.6: Risk assessment made by each expert for each potential malfunctioned cause

a_i	e_i	L_i							C_i					E_i						
		L_1	L_2	L_3	L_4	L_5	L_6	L_7	C_1	C_2	C_3	C_4	C_5	E_1	E_2	E_3	E_4	E_5	E_6	E_7
a_1	e_1	-	-	-	0.20	0.70	0.70	0.25	-	-	-	0.75	0.78	-	-	-	0.20	1.00	0.60	0.20
	e_2	-	-	0.17	0.50	0.65, 0.85	0.58	-	-	-	-	0.80	0.80	-	-	-	0.28	0.86	0.85, 0.50	0.50
	e_3	-	-	-	1.00	1.00, 0.25	0.75	-	-	-	-	1.00	1.00	-	-	-	-	1.00	1.00	1.00
	e_4	-	-	0.30	0.75	1.00	1.00	0.65	-	-	0.60	1.00	0.68	-	-	-	0.34	1.00	1.00	0.30
	e_5	-	-	-	-	0.62	0.37	-	-	-	-	0.75	0.25	-	-	-	-	0.45	0.60	-
a_2	e_1	-	-	-	0.50	1.00	0.20	-	-	-	0.35	1.00	-	-	-	0.25	0.75	0.65	-	-
	e_2	-	-	-	0.70	0.75	0.30	-	-	-	-	1.00	0.50	-	-	-	-	0.80	0.70	-
	e_3	-	-	0.50	1.00	1.00	0.25	-	-	-	1.00	1.00	-	-	-	-	-	1.00	1.00	-
	e_4	-	-	0.50	1.00	1.00	0.35	-	-	-	0.65	1.00	0.50	-	-	-	0.50	1.00	0.65	0.32
	e_5	-	-	-	-	0.95	0.05	-	-	-	-	1.00	-	-	-	-	-	0.80	0.20	-
a_3	e_1	-	-	-	0.35	1.00	0.20	-	-	-	-	0.70	0.70	-	-	-	0.20	1.00	0.50	-
	e_2	-	-	-	0.40	0.85	0.40	-	-	-	-	1.00	0.60	-	-	-	0.50	1.00	-	-
	e_3	-	-	-	0.50	1.00	0.50	-	-	-	-	1.00	-	-	-	-	-	1.00	0.50	-
	e_4	-	-	-	0.50	1.00	0.65	-	-	-	0.65	1.00	0.35	-	-	-	-	1.00	1.00	0.50
	e_5	-	-	-	-	0.75	0.25	-	-	-	-	1.00	-	-	-	-	-	0.90	0.10	-
a_4	e_1	-	-	-	-	0.80	0.40	-	-	-	-	0.75	0.65	-	-	-	-	1.00	0.35	-
	e_2	-	-	-	0.30	1.00	0.35	-	-	-	0.35	1.00	0.20	-	-	-	0.35	1.00	-	-
	e_3	-	-	-	-	1.00	1.00	-	-	-	-	1.00	1.00	-	-	-	-	1.00	1.00	-
	e_4	-	-	-	0.35	1.00	0.40	-	-	-	0.70	1.00	-	-	-	-	-	1.00	0.80	0.40
	e_5	-	-	-	-	0.52	0.48	-	-	-	-	0.75	0.25	-	-	-	-	0.15	0.85	-

An example is used to demonstrate the rule evaluation processes in the fuzzy inference engine of the proposed safety model for risk analysis. The evaluation made by expert #1, e_1, on collision risk caused by the CPP failure, a_1, is used here to demonstrate the procedure involved in fuzzy inference engine. The "truth value" of a rule is determined from the conjunction of the rule antecedents. With conjunction defined as 'minimum', rule evaluation then consists of determining the smallest (minimum) rule antecedent, which is taken to be the truth value of the rule. This truth value is then applied to all consequents of the rule. If any fuzzy output is a consequent of more than one rule corresponding to a particular safety expression, then that output is set to the highest (maximum) truth value of all the rules.

The 245 rules in the rule base that are used in this study are listed in Table 7.4(i)-(vii) of this report. The risk matrix for this study is given Figure 7.5(b) and provided in an exploded format as shown in Figure 7.5(c).

7.5.7 Approximate Reasoning Evaluation of Safety Estimate

The evaluation of S made by five experts, $\{e_i\}_{i=1}^{5}$, for collision risk between FPSO and shuttle tanker due to CCP caused technical failure, a_1, are performed separately according to the general safety modelling framework using the approximate reasoning approach. The evaluation of S made by expert #1, e_1, with the following parameters is performed as shown in Table 7.7.

7.5.7.1 Fuzzify Inputs

In this evaluation, 245 rules are considered; however, only 32 rules are fired contributing to the actual evaluation process in this particular case. These 32 rules are rule numbers 130, 131, 132, 133, 137, 138, 139, 140, 165, 166, 167, 168, 172, 173, 174, 175, 200, 201, 202, 203, 207, 208, 209, 210, 235, 236, 237, 238, 242, 243, 244, 245. The fuzzification process results are given in Table 7.6.

In this manner, each input variable is fuzzified over all the qualifying membership functions required by the rules.

7.5.7.2 Apply Fuzzy Operator

The antecedents of the 32 rules are evaluated. For example, in applying rule #130 the three different pieces of the antecedent (L is *"average* (L_4)", C is *"critical* (C_4)" and E is "*likely* (E_4)") yield the fuzzy membership values ($\mu_{L,130}$, $\mu_{C,130}$, $\mu_{E,130}$) = (0.20, 0.75, 0.20) respectively. The fuzzy AND operator $\mu_r = min(\mu_{L,r}, \mu_{C,r}, \mu_{E,r})$ simply selects the minimum of the three values, that is, 0.20. The application of the fuzzy operator

generates the results as shown in columns 2-4 of Table 7.7 for each rule involved in the evaluation process.

Table 7.7: Safety expression results of analysis membership values from rule evaluation process

R_k	μ_L	μ_C	μ_E	S_j	μ_r (*min*)
130	0.20	0.75	0.20	*Fair*	0.20
131	0.20	0.75	1.00	*Fair*	0.20
132	0.20	0.75	0.60	*Poor*	0.20
133	0.20	0.75	0.20	*Poor*	0.20
137	0.20	0.78	0.20	*Fair*	0.20
138	0.20	0.78	1.00	*Poor*	0.20
139	0.20	0.78	0.60	*Poor*	0.20
140	0.20	0.78	0.20	*Poor*	0.20
165	0.70	0.75	0.20	*Fair*	0.20
166	0.70	0.75	1.00	*Poor*	0.70
167	0.70	0.75	0.60	*Poor*	0.60
168	0.70	0.75	0.20	*Poor*	0.20
172	0.70	0.78	0.20	*Poor*	0.20
173	0.70	0.78	1.00	*Poor*	0.70
174	0.70	0.78	0.60	*Poor*	0.60
175	0.70	0.78	0.20	*Poor*	0.20
200	0.70	0.75	0.20	*Fair*	0.20
201	0.70	0.75	1.00	*Poor*	0.70
202	0.70	0.75	0.60	*Poor*	0.60
203	0.70	0.75	0.20	*Poor*	0.20
207	0.70	0.78	0.20	*Poor*	0.20
208	0.70	0.78	1.00	*Poor*	0.70
209	0.70	0.78	0.60	*Poor*	0.60
210	0.70	0.78	0.20	*Poor*	0.20
235	0.25	0.75	0.20	*Fair*	0.20
236	0.25	0.75	1.00	*Poor*	0.25
237	0.25	0.75	0.60	*Poor*	0.25
238	0.25	0.75	0.20	*Poor*	0.20
242	0.25	0.78	0.20	*Poor*	0.20
243	0.25	0.78	1.00	*Poor*	0.25
244	0.25	0.78	0.60	*Poor*	0.25
245	0.25	0.78	0.20	*Poor*	0.20

7.5.7.3 Apply Implication Method

Implication is implemented for each rule. A consequent is a fuzzy set represented by a membership function, $\mu_{r.}$, which weights appropriately the linguistic characteristics that are attributed to it. The consequent is reshaped using a function associated with the antecedent, which is a single value. The input for the implication process is a single value given by the antecedent, μ_r, and the output is a fuzzy set. The following expression is used to generate the membership value of the consequent S for r^{th} rule:

$\mu(H_n; n = 1, 2, 3, 4)_r = \mu_r$

For rule #130, $\mu(H_2;$ '*fair* $(S_3)')_{130} = \mu_{130} = 0.20$ (i.e., membership value for the particular safety expression "*Fair* (S_3)" is 0.20 for rule #130). This result is given in column 6 of Table 7.7.

7.5.7.4 Aggregate All Outputs

In this step, the fuzzy sets that represent the outputs of each rule are combined into a single fuzzy set and this only occurs once for each output variable prior to normalisation. All 32 rules have been placed together to demonstrate how the output of each rule is combined, or aggregated, into a single fuzzy set (whose membership function assigns a weighting for every output value (S)).

The aggregation of consequents, i.e. S across the rules is expressed as follows for i^{th} expert of the l^{th} potential cause to a technical failure:

$$S(e_i(a_l)) = \{max(\beta_{1,r}, S_1); max(\beta_{2,r}, S_2); max(\beta_{3,r}, S_3); max(\beta_{4,r}, S_4)\} \quad (7.16)$$

where $r = 1,\ldots,R$ = number of rules fired in the evaluation.

S assessed by Expert #1, e_1, for potential cause #1, a_1, to a technical failure has the result as follows:

$$S(e_1(a_1)) = \{max(0, S_1); max(0, S_2); max(0.2, S_3); max(0.2, 0.25, 0.6, 0.7, S_4)\}$$

Therefore;

$$S(e_1(a_1)) = \{0, S_1; 0, S_2; 0.2, S_3; 0.7, S_4)\}$$

The output can be interpreted in such a way that *S* of the system is S_3 (i.e., *Fair*) with a belief degree of 0.20 and S_4 (i.e., *Poor*) with a belief degree of 0.70.

7.5.7.5 Normalise Safety Estimate

Since the aggregation of a fuzzy set encompasses a range of output values represented in different linguistic variables associated with varied memberships, it must be normalised before feeding *S* to the evidential reasoning framework for further evaluation in a hierarchical manner. It is worth noting that defuzzification is not required here in this study.

Then the safety estimate is normalised according to the expression given as follows:

$$S(e_i(a_i)) = \left\{ \frac{\beta_{1,i}^I}{D_i^I}, \frac{\beta_{2,i}^I}{D_i^I}, \frac{\beta_{3,i}^I}{D_i^I}, \frac{\beta_{4,i}^I}{D_i^I} \right\} \tag{7.17}$$

4

where $D_i^I = \sum_{n=1} \beta_{n,2}^I$ (i.e., the *degree of safety level* for the i^{th} *expert*).

Note that the fuzzy aggregation function is β-anonymous as this gives the same importance to the opinion of all experts. However, assessment for weight of importance is necessary for an overall safety result to be achieved.

The normalisation gives S = {0.0, S_1; 0.0, S_2; 0.2223, S_3; 0.7777, S_4}. It is obvious that the derived S belongs to S_3 (i.e., *Fair*)" and S_4 (i.e., *Poor*) with a belief of 22.23 % and 77.77%, respectively.

The similar computation is performed for safety assessment performed by the other four experts using the proposed approach for the CCP caused technical failure and the other three potential causes to technical failure. The results attained for all the caused technical failure, $\{a_l\}_{l=1}^{4}$, by five experts, $\{e_i\}_{i=1}^{5}$, are shown in Table 7.8.

Table 7.8: Safety estimate by each expert for each potential malfunctioned cause

a_l	e_i	L	C	E	S_j (normalised), β_n			
					S_1	S_2	S_3	S_4
a_1	e_1	{6.5, 8.0, 9.5}	{7.5, 8.5, 9.5}	{5.5, 7.0, 8.5}	0	0	0.2223	0.7777
	e_2	{5.5, 7.5, 9.0}	{7.0, 8.5, 10}	{5.0, 7.5, 9.5}	0	0	0.4348	0.5652
	e_3	{6.0, 8.0}	{7.0, 9.0}	{6.5, 9.0}	0	0	0.5	0.5
	e_4	{5.5, 6.5, 9.0, 10.0}	{5.5, 7.0, 8.0, 10.0}	{5.0, 7.0, 8.0, 8.5}	0	0	0.4286	0.5714
	e_5	{7.75}	{8.25}	{7.6}	0	0	0	1.00
a_2	e_1	{6.0, 7.0, 7.5}	{6.5, 7.0, 8.0}	{4.5, 5.5, 6.0}	0	0.1515	0.4545	0.3939
	e_2	{6.0, 6.5, 8.0}	{7.0, 8.0, 9.0}	{6.0, 7.5, 8.0}	0	0	0.4828	0.5172
	e_3	{5.5, 5.5, 7.5, 7.5}	{6.0, 6.0, 8.0, 8.0}	{6.0, 6.0, 8.0, 8.0}	0	0.20	0.40	0.40
	e_4	{5.0, 6.0, 7.0, 8.0}	{5.0, 7.0, 8.0, 9.0}	{5.0, 6.0, 7.0, 9.0}	0	0.20	0.40	0.40
	e_5	{7.15}	{7.95}	{7.25}	0	0	0	1.00
a_3	e_1	{6.5, 7.0, 7.5}	{8.0, 8.5, 9.0}	{5.5, 7.0, 8.0}	0	0	0.3333	0.6667
	e_2	{6.0, 7.5, 8.0}	{7.5, 8.0, 9.5}	{5.0, 6.0, 7.0}	0	0	0.3703	0.6297
	e_3	{6.5, 6.5, 8.0, 8.0}	{7, 7, 7.5, 7.5}	{6.5, 6.5, 7.5, 7.5}	0	0	0.3333	0.6667
	e_4	{6.0, 7.0, 8.0, 9}	{5.0, 7.0, 8.0, 8.5}	{6.0, 7.0, 8.0, 9.0}	0	0	0.3939	0.6061
	e_5	{7.5}	{7.2}	{7.1}	0	0	0	1.00
a_4	e_1	{7.0, 7.5.0, 8.0}	{7.5, 8.5, 9.0}	{6.0, 7.0, 7.5}	0	0	0	1.00
	e_2	{6.5, 7.0, 8.0}	{6.5, 7.0, 8.5}	{5.5, 6.0, 7.0}	0	0	0.7407	0.2593
	e_3	{7.0, 7.0, 9.0, 9.0}	{7.5, 7.5, 9.5, 9.5}	{7.0, 7.0, 8.0, 8.0}	0	0	0	1.00
	e_4	{6.5, 7.0, 7.5, 8.0}	{6.0, 6.5, 7.0, 8v}	{6.5, 7.0, 7.5, 9.0}	0	0	0.4444	0.5556
	e_5	{7.95}	{8.25}	{7.9}	0	0	0.3750	0.6250

7.5.8 Evidential Reasoning Synthesis of Safety Estimate

According to the generic framework for modelling system safety shown in Figure 7.3, the modified ER algorithm is used to synthesise the information thus produced to assess the safety of the whole system. This step is concerned with safety synthesis of a system at various configurations such as:

- Multi-attribute safety synthesis - The synthesis of safety estimates of various causes to a technical failure done by an expert, or
- Multi-expert safety synthesis - The synthesis of safety estimates of a specific cause to a technical failure done by a panel of experts, or
- Multi-attribute-multi-expert synthesis - A combination of the above two.

A window-based and graphically designed intelligent decision system (IDS) based on an ER approach is used to synthesise safety estimates.

7.5.8.1 Multi-Expert Safety Synthesis

Table 7.9 show the results of multi-expert safety synthesis on collision risk between FPSO & shutter tanker due to the CPP, thrusters, PRS and DP caused technical failure, obtained using the evidential reasoning approach. The synthesis is carried out using different relative weights of importance configurations among experts (experts with different weights).

To calculate risk ranking index values associated with various causes to technical failure, it is required to describe the four safety expressions, i.e., $\{S_1, S_2, S_3, S_4\}$ using numerical values. Experts can designate the numerical values associated with the defined safety expressions. Suppose K_1, K_2, K_3, K_4 represent the unscaled numerical values associated with S_1, S_2, S_3, S_4, respectively. Then K_1, K_2, K_3, K_4 can be represented as follows:

$$\{K_1, K_2, K_3, K_4\} = \{1, 0.8, 0.6, 0.2\}$$

Table 7.9: Safety synthesis for the different relative weights of importance among experts

a_l	Weight, λ_n of each expert, e_l					Synthesised S_j			
	e_1	e_2	e_3	e_4	e_5	S_1	S_2	S_3	S_4
a_1	1	1	1	1	1	0	0	0.2776	0.7224
	5	4	3	2	1	0	0	0.3124	0.6876
	1	2	3	4	5	0	0	0.2342	0.7658
	4	5	1	2	3	0	0	0.2557	0.7442
	3	4	5	1	2	0	0	0.3311	0.6689
a_2	1	1	1	1	1	0	0.0942	0.3333	0.5725
	5	4	3	2	1	0	0.1009	0.4205	0.4786
	1	2	3	4	5	0	0.0848	0.2433	0.6719
	4	5	1	2	3	0	0.0626	0.3520	0.5854
	3	4	5	1	2	0	0.0968	0.3772	0.5260
a_3	1	1	1	1	1	0	0	0.2438	0.7562
	5	4	3	2	1	0	0	0.2960	0.7040
	1	2	3	4	5	0	0	0.1896	0.8140
	4	5	1	2	3	0	0	0.2486	0.7514
	3	4	5	1	2	0	0	0.3334	0.6666
a_4	1	1	1	1	1	0	0	0.2699	0.7301
	5	4	3	2	1	0	0	0.2283	0.7717
	1	2	3	4	5	0	0	0.3095	0.6905
	4	5	1	2	3	0	0	0.3595	0.6405
	3	4	5	1	2	0	0	0.2235	0.7765

The risk ranking index value R_i associated with cause i to technical failure can be defined as follows:

$$R_i = \sum_{j=1}^{4} \mu_i^j \times K_i \qquad \text{for } i = 1, 2, \ldots, d \qquad (7.18)$$

where d is the number of causes to technical failure.

Obviously, the R_i values obtained using the above expression can only show the relative risk level among all potential causes identified under study. The smallest R_i is ranked first as it deserves more attention to reduce its potential risk to ALARP. The largest R_i

is ranked last to draw least attention and minimum effort for risk reduction measure consideration. A smaller R_i means that cause i is having relatively higher risk level and deserves more attention at the early design stages/or the early stages of designing operational strategies. The R_i value for each potential cause to technical failure by a panel of experts carrying different relative weights is calculated and shown in Table 7.10 (raw results) and Table 7.11 (ranking).

Table 7.10: Raw safety ranking (multi-attribute: expert with different weights)

Weight, λ_n					Ranking of a_l			
e_1	e_2	e_3	e_4	e_5	a_1	a_2	a_3	a_4
1	1	1	1	1	0.33040	0.38984	0.29752	0.30796
5	4	3	2	1	0.32496	0.42874	0.31840	0.29132
1	2	3	4	5	0.29368	0.34830	0.27584	0.32380
4	5	1	2	3	0.30226	0.37649	0.29944	0.34470
3	4	5	1	2	0.33244	0.40896	0.33336	0.28940

From Table 7.11 it can be noted that regardless of the weight difference between each expert allocated, the potential risk caused by thruster failure, a_2, is always the lowest. As the relative weights, λ_n, of the panel experts change as $\{\lambda_1; \lambda_2; \lambda_3; \lambda_4; \lambda_5\} = \{5, 4, 3, 2, 1\}$, DPS caused technical failure is ranked first, whereas the potential risk induced by PSR and DPS are ranked second and third, respectively. As the relative weights change to $\{1, 2, 3, 4, 5\}$, then PSR, a_3, is ranked first, CPP, a_1, second, DPS, a_4, third and thrusters, a_2, last. The results of other weight configurations are depicted in Table 7.10.

Table 7.11: Safety ranking (experts with different weights)

Weight, λ_n					Ranking of a_l			
e_1	e_2	e_3	e_4	e_5	a_1	a_2	a_3	a_4
1	1	1	1	1	3	4	1	2
5	4	3	2	1	3	4	2	1
1	2	3	4	5	2	4	1	3
4	5	1	2	3	2	4	1	3
3	4	5	1	2	2	4	3	1

The ranking results for risks due to various potential causes as assessed by a panel of experts may help designers understand the anticipated technical problem in question so that an improved risk reduction measure is to be incorporated in the new design or a more innovative design is to be carried out to reduce the potential risk as estimated.

7.5.8.2 Multi-Attribute Safety Synthesis

Table 7.12 shows the results of multi-attribute safety synthesis by each expert, $\{e_i\}_{i=1}^{5}$, on the four anticipated causes to the technical failure, $\{a_l\}_{l=1}^{4}$, which result in collision between FPSO and shuttle tanker. The result produced by expert #1, e_1, is as follows:

multi-attribute safety synthesis (e_1) = {0, S_1; 0.02891, S_2; 0.21430, S_3; 0.75674, S_4}

The results produced by other experts are also shown in Table 7.12.

Table 7.12: Multi-attribute safety synthesis by each expert

e_i	Synthesised S_j			
	S_1	S_2	S_3	S_4
e_1	0	0.02891	0.21430	0.75674
e_2	0	0	0.50900	0.49099
e_3	0	0.03943	0.27750	0.68304
e_4	0	0.03989	0.40832	0.55178
e_5	0	0	0.06283	0.93716

Suppose a unity of relative weight of importance is given to the panel of experts, i.e., $\{\lambda_1; \lambda_2; \lambda_3; \lambda_4; \lambda_5\} = \{1, 1, 1, 1, 1\}$. Based on the general framework, the multi-attribute-multi-expert safety synthesis = {0, S_1; 0.01660, S_2; 0.25640, S_3; 0.72697, S_4}.

7.5.8.3 Multi-Attribute Multi-Expert Safety Synthesis

The *multi-attribute-multi-expert* safety synthesis = {0, S_1; 0.01776, S_2; 0.28779, S_3; 0.69440, S_4} with a variance in weights among experts as {λ_1; λ_2; λ_3; λ_4; λ_5} = {5, 4, 3, 2, 1}. The results of multi-attribute-multi-expert safety synthesis for other weight variance configurations are depicted in Table 7.13.

Table 7.13: Multi-attribute-multi-expert safety synthesis by experts carrying different weights

Weight, λ_n					S_j (Synthesised)			
e_1	e_2	e_3	e_4	e_5	S_1	S_2	S_3	S_4
1	1	1	1	1	0	0.02891	0.21430	0.75674
5	4	3	2	1	0	0.01776	0.28779	0.69440
1	2	3	4	5	0	0.01517	0.22057	0.76423
4	5	1	2	3	0	0.01125	0.28106	0.70766
3	4	5	1	2	0	0.01721	0.27383	0.70892

Such results clearly give the estimate of the four causes leading to the technical failure in an FPSO-shuttle tanker collision risk scenario. Thus, appropriate *design action* can be taken accordingly.

7.6 Pros and Cons of Using Fuzzy Logic for Risk Analysis

Although such FL technique is possibility rather than probability based, it operates over the same numeric range. It possesses several potential benefits and limitations as have been recognised and thus outlined in Sections 7.7.1 and 7.7.2 respectively.

7.6.1 Advantages of Fuzzy Logic Risk Modelling

The main features and advantages that the proposed FL based framework offers over other alternative modelling approaches are that:

- It is conceptually easy to understand with "natural" mathematics.

- It is tolerant to vague or imprecise data. Its use of fuzzy set theory is particularly adapted to the representation and manipulation of imprecision and uncertainty of the linguistic labels that define the criteria of the classes.
- It presents a flexible way of dealing with different forms of uncertainty. For example, there is a lot of freedom in choosing the membership functions of fuzzy sets.
- It is more intuitive than differential equations, and enables analysts and decision-makers to capture knowledge of how the system behaves in everyday linguistic terms (i.e., based on natural language).
- Though, making use of heuristics, it still offer a convenient way to express and make the most of the experience of experts' common sense knowledge.
- It has the ability to model any very complex or highly non-linear function to any arbitrary degree of accuracy.
- It is based on rules (i.e., rule-based logic) that can be specified with a natural language. Basically, the laws are naturally broken down into individual IF-THEN statements that lend themselves to parallel processing.

When basic probability or the Bayesian concept is not considered suitable for tacking a risk-based assessment, FL techniques can be used to complement the probability concept. Nonetheless, it can also be mixed with this conventional technique, as well as others, e.g., evidential reasoning approach (as verified in the undertaken study of the framework).

7.6.2 Disadvantages of Fuzzy Logic Risk Modelling

Despite their sensational and potential ability to address risk assessment, certain drawbacks can be attributable to the FL approach. These limitations include the fact that the approach:

- Needs system/process expert to design solution.
- Needs to select balance of inputs and membership functions.

- May give combinatorial explosion as the number of fuzzy variables or fuzzy sets increase, the number of rules increases exponentially. This can quickly make the fuzzy system(s) slow, confusing, and difficult to maintain.
- Needs to choose best rule evaluation process from quite a number of possibilities.
- Is leading to relative values for comparing options at a design stage and not absolute values.

Compared to other classical risk-based techniques, FL requires higher computational effort due to the complex inference mechanisms needed. Nonetheless, utilising Fuzzy Logic Toolbox in Matlab6.5 (The MathWorks, 2005) can result in reasonable run times. Finally, FL is certainly not optimal, nor recommendable, for risk analysis when there are a lot of data that could be used to inform a probabilistic approach that can yield a satisfying result.

7.7 Concluding Remarks

The use of interval mathematics and possibility distribution such as approximate reasoning method is a departure from conventional probability-based techniques which rely rather heavily on randomness and frequency to quantify risks on engineering systems. The framework proposed in this study outlines and explains a philosophy for subjective safety modelling for offshore risk analysis using approximate reasoning and evidential reasoning approaches. Various forms of membership functions that could be used in representing fuzzy linguistic variables to qualify risk levels have been discussed. The background of approximate reasoning based on fuzzy-logic-techniques and evidential reasoning approach is outlined.

Fuzzy set theory enables uncertainties to be described mathematically and possessed in the analysis of a system. The safety assessment of systems described takes into account non-stochastic uncertainties and subjective estimates of objective values by expert judgements based on fuzzy set theory. It is possible by this means to obtain reliable safety related descriptions of the system under scrutiny for further processing with confidence.

The proposed framework offers a great potential in safety assessment and decision support of maritime systems, especially in the initial concept design stages where the related safety information is scanty or with great uncertainty involved. Safety assessment using approximate reasoning approach can formulate domain human experts' experience and safety engineering knowledge; at the same time information of difference properties from various sources can be transformed to become the knowledge base, used in the FL inference process. The results obtained from the case study on collision risk between FPSO and shuttle tanker have demonstrated that such a framework provides safety analysts and designers with a convenient tool that can be used at various stages of the design process of offshore engineering systems in performing risk analysis. The method described forms a supplement to concepts and methodologies already in use for offshore safety assessment.

The safety culture in many industries including the maritime sector in the UK has been changing over the last several years. In general, many industries are moving towards a "goal setting" risk-based regime. This gives more flexibility to safety engineers to employ the latest risk modelling techniques and decision making/optimisation tools. It may be very beneficial that many advances that have been developed and are being developed in general engineering and technology are further explored, exploited and also applied in order to facilitate risk modelling and decision-making.

Chapter 8: Fuzzy-Bayesian Network

Chapter Summary

The incorporation of the human element into a probabilistic risk-based model is one that requires a possibilistic integration of appropriate techniques and/or that of vital inputs of linguistic nature. Whilst fuzzy logic is an excellent tool for such integration, it tends not to cross its boundaries of possibility theory, except via an evidential reasoning supposition. Therefore, a fuzzy-Bayesian network (FBN) is proposed to enable a bridge to be made into a probabilistic setting of the domain. This bridge is formalised by way of the mass assignment theory. A framework is also proposed for its use in maritime safety assessment. Its implementation has been demonstrated in a maritime human performance case study that utilises performance-shaping factors as the input variables of this groundbreaking FBN risk model.

8.1 Introduction

In risk analysis, cause-effect relationships are vital for achieving the modelling process. Thus, modelling in a network format becomes useful as it also gives an intuitive vital representation that mimics the domain of the real-world. The most useful form of such a model is a casual diagram or network usual termed a directed acyclic graph (see Chapter 6), which uses nodes for representing distribution knowledge of variables and arcs for representing casual influences between nodes. If the data for a nodal variable is sufficient enough to enable the quantitative reasoning, then the form of the data (e.g. given as frequency of occurrence of the event) can be converted into a probability distribution for the analysis. The inherent uncertainty due to randomness then makes this a random node that can typically be applied in a Bayesian network (BN) (Pearl, 1988 and as given in Chapter 6). On the other hand, if information associated with a node exhibits uncertainty that is vague, ambiguous or fuzzy, then it cannot be

represented precisely by a probability distribution. Thus, fuzzy logic (FL) (Zadeh, 1975) may have to be utilised to achieve some a possibility distribution via a rule-base inference engine that permits the subjective reasoning (See Chapter 7).

When, for example, two nodes are both defined by possibilistic values, they exhibit conditional possibility and fuzzy set theory features. If they are both defined by probabilistic values, they exhibit conditional probability and Bayes' theory features. The obvious problem within the casual network arises when a fuzzy event node has a casual influence connection with that of a random event node. In this case, Bayes' theorem cannot be applied for the casual influence due to the fuzzy event present in the conditional connection. Therefore, a method of converting from possibility-to-probability distributions is most desirable. If such a method can provide bi-directional characteristics, then the fuzzy nature of variable can always be recouped. The theory of mass assignment (Baldwin, *et al.*, 1996) has been proven to offer one such feature. Hence, the causal formalism of using a combined fuzzy and Bayesian approach can be made possible. The resulting proposed route is given by the model name - "fuzzy Bayesian network". In recent research, developments and applications, FL and BN have both emerged as powerful and effective tools for reasoning under conditions of uncertainty. Thus, it is certainly quite appropriate to investigate the amalgamation of both techniques.

The amalgamation of FL and BN may well prove to provide the pioneering means of incorporating human factors/elements in a probabilistic risk analysis model domain. Obviously, such an accomplishment is bound to be a key improvement to the safety in the marine and offshore industry especially as human error has a substantial impact on the reliability of complex systems. While much attention has been placed on improving the design, construction, and operations of maritime operating equipment based on casualties, the human factor element remains the predominate contributing cause of accidents (The Nautical Institute, 2003) within each phase. Certainly, the marine and offshore industry cannot afford to simply accept that this situation is inevitable.

8.2 Fuzziness and Probability

Probability and fuzziness are related but different concepts. Fuzziness is a type of deterministic uncertainty, which describes the event class ambiguity. Fuzziness measures the degree to which an event occurs, not whether it occurs. An issue is whether the event class can be unambiguously distinguished from its opposite. Probability arouses from the question of whether or not an event occurs. Moreover, it assumes that the event class is crisply defined and that the law of non-contradiction (i.e., $A \cap \bar{A} = \emptyset$, where A is a set in the finite space) holds. Kosko (1990) shows that fuzziness occurs when the law of non-contradiction (and equivalently the law of excluded middle, i.e., $A \cup \bar{A} = X$, where X is the universe of discourse) is violated. However, it seems more appropriate to investigate the fuzzy probability for the latter case (Dubois & Prade, 1993), than to completely dismiss probability as a special case of fuzziness (Kosko, 1990).

A fuzzy probability extends the traditional notion of a probability when there are the outcomes that belong to several event classes at the same time but to different degrees. It is important to note that neither fuzziness nor probability governs the physical processes in nature, though they are orthogonal concepts that characterize different aspects of human experience (Dubois & Prade, 1993).

8.3 Comparison of Axioms of Probabilistic and Possibility-Based Methods

The objective of this section is to identify the differences in the axioms of probability and possibility and the impact of these differences on how probabilistic and fuzzy set methods model uncertainties and assess the reliability of a system.

Fuzzy set methods use possibility, which measures the degree to which an event is feasible, to quantify the likelihood this event will occur. One can think of possibility as complementary to the degree of surprise if an event occurs (Chen, *et al.*, 1999). Possibility ranges from zero to one, like probability.

A key axiomatic difference between possibility and probability is that the possibility of a union of events (disjoint or overlapping) is equal to the maximum of the possibilities of the individual events, whereas the probability of a union of disjoint events is equal to the sum of the probabilities of these events. This leads to the following observations (Chen, *et al.*, 1999):

1. The possibilities of an event and its complement may add up to more than one, whereas the probabilities of an event and its complement must add up to one.

2. The possibility of failure of a system, consisting of identical, independent components connected in series, is equal to the possibility of failure of one component, whereas the probability of failure of the system increases with the number of components.

3. The possibility of failure of a system, consisting of identical, independent components connected in parallel, is equal to the possibility of failure of a single component.

4. From observation 2, it is concluded that the possibility of an event can be smaller than its probability. For example, even if the possibility of failure of each component is greater than the corresponding probability, a system with enough components will have a possibility of failure smaller than its probability of failure. This result is counterintuitive – since one may reason that the possibility of an event should be greater or equal to its probability because if an event is probable it should also be possible.

According to observation 2, a fuzzy set method is likely to underestimate the chance of failure of a system with a large number of independent failure modes. On the other hand, it can be too conservative in systems for which the failure region is very small compared to the range of the uncertain variables. Therefore, compared to fuzzy set methods, probabilistic methods may provide a more accurate estimate of the chance of failure if there is enough data to model random uncertainties accurately and modelling errors are small.

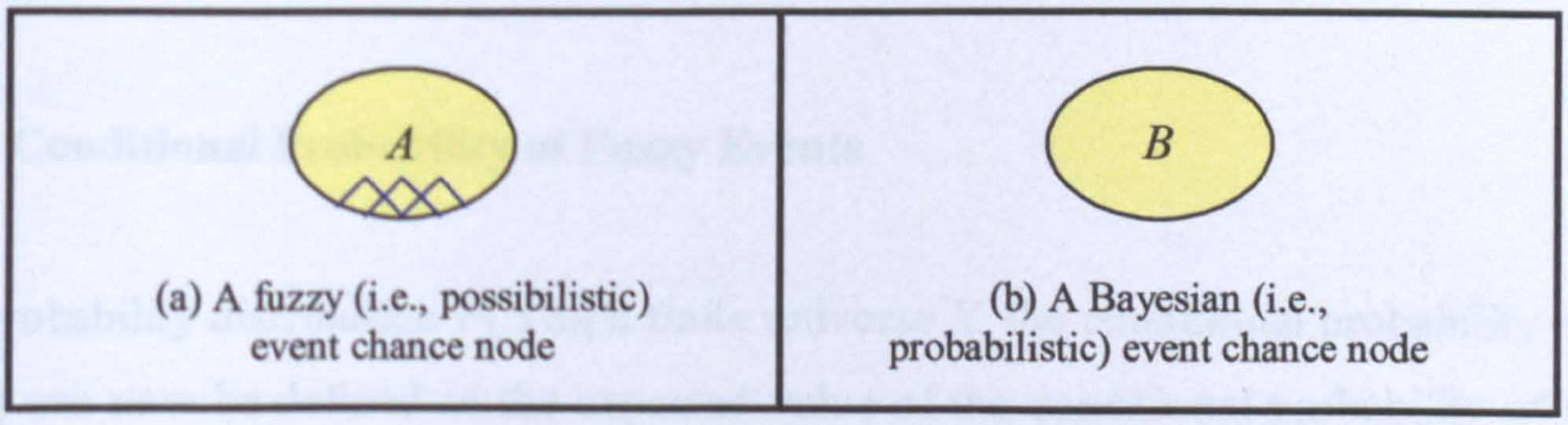
On the other hand, it is easier to determine the most conservative fuzzy set model than to determine the most conservative probabilistic model that is consistent with given information about a problem. A primary reason is that, although the area below the probability density function of a random variable must be equal to one, there is no such constraint on the possibility density function.

8.4 Proposed Semantics for a Fuzzy-Bayesian Network

The key feature of the proposed *Fuzzy-Bayesian networks (FBNs)* is that they enable modelling and reasoning about uncertainty that can be due to a combination of inherent vagueness and randomness. Hence, essential to their formalism is the idea of relating, combining and converting possibilitistic values into their probabilistic counterpart for use within the same model framework. As such, it is quite possible that the proposed FBN modelling may realise anything FL can do and also inherit the entire rigor, flexibility and other superior properties of probabilistic approaches.

8.4.1 Possibility-Probability Directed Acyclic Graph

A FBN provides factorised representation of a possibility-probability model that explicitly captures both a logical and network structure typical in human-engineered models. More generally, a FBN is a *directed acyclic graph (DAG)* of a *BN* nature that allows for the encoded *probability distribution* of a node to be derived from its *fuzzy* derivation. The fuzzy-to-probability distribution conversion is normally induced via a suitable algorithm, e.g., by *mass assignment (MA)* formalism.



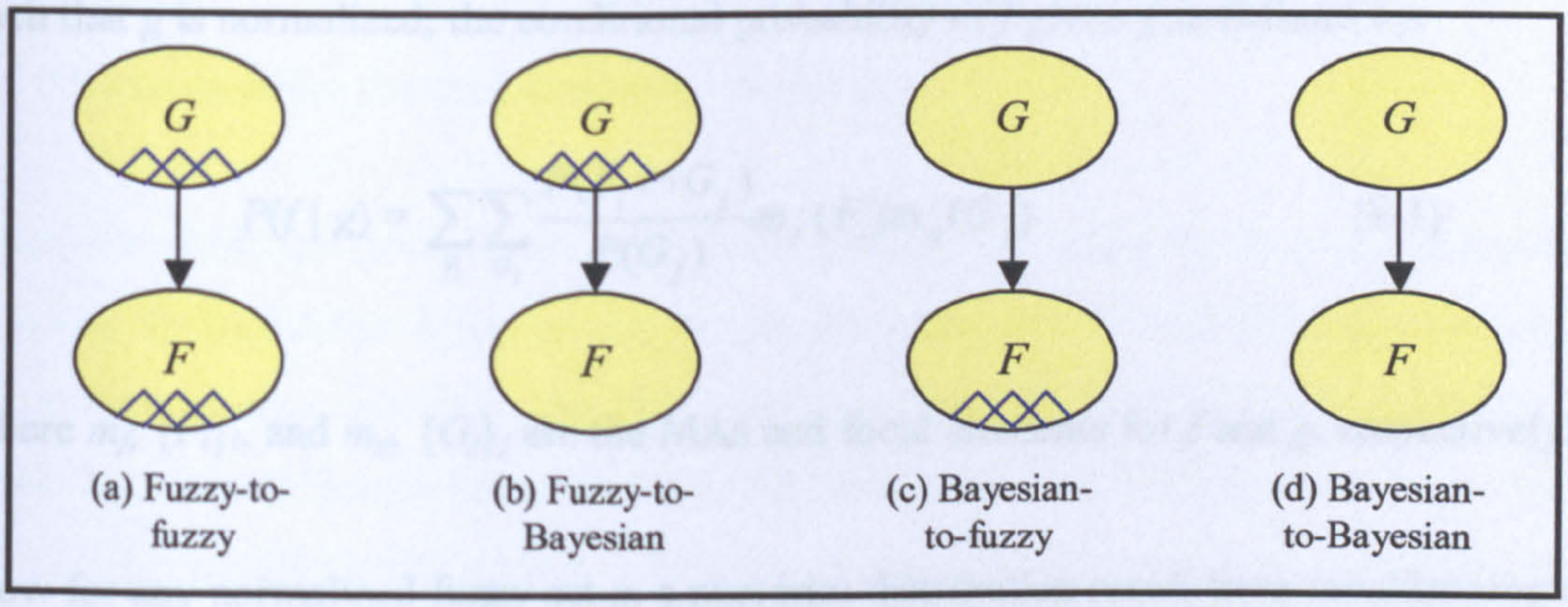
(a) A fuzzy (i.e., possibilistic) event chance node

(b) A Bayesian (i.e., probabilistic) event chance node

Figure 8.1: Proposed nodal representation for fuzzy and Bayesian chance events

Figure 8.1(a) gives a proposed nodal representation for a fuzzy event, *A*. Such a node basically obtains its prior probability input from a fuzzy set output. In order to enable this conversion of probability distribution, a conversion inference via MA is utilised. The typical representation of a random event, *B*, in a BN is as shown in Figure 8.1(b).

To understand how they are utilised in a FBN, it is worth having the most basic formats of their representation within the network. These are as given in Figure 8.2(a)-(d).



(a) Fuzzy-to-fuzzy (b) Fuzzy-to-Bayesian (c) Bayesian-to-fuzzy (d) Bayesian-to-Bayesian

Figure 8.2: Representations of proposed FBN structure for two nodal events

As expected, from a Bayesian viewpoint, a direct probabilistic inference linking from Event *G* to Event *F* is represented by a line of its terminating arrowhead resting on the later. An optional direct possibilistic inference (not shown in Figure 8.2) may be represented as a dashed terminating arrowhead line between fuzzy events. Such an optional possibilistic inference can enable a means to which a comparison study can be effected between conditional possibility and conditional probability of the fuzzy events.

8.4.2 Conditional Probability of Fuzzy Events

For a probability distribution $P(.)$ on a finite universe X, the conditional probability of f given g can now be defined as the expected value of the conditional probability of the focal elements for mass assignment of f, m_f, given the focal elements for mass

assignment of f, m_g, relative to $P(.)$ and assuming that the joint MA generated by f and g is given by $m_f \times m_g$ (Baldwin *et al.*, 1996). The idea behind this is that since the definitions for f and g are uncertain there is also uncertainty regarding to which (classical) conditional probability $P(f \mid g)$ refers. If the assumption is made that the two definitions come from different and independent sources, then $m_f \times m_g$ gives us a probability distribution across possible conditional probability values. In this case a natural estimate for $P(f \mid g)$ is to take the expected value of this distribution.

For $P(.)$, a probability distribution on a finite universe X, and f and g fuzzy subsets of X such that g is normalized, the conditional probability of f given g is defined by:

$$P(f \mid g) = \sum_{F_i} \sum_{G_j} \frac{P(F_i \cap G_j)}{P(G_j)} m_f(F_i) m_g(G_j) \qquad (8.1)$$

where m_f, $\{F_i\}_i$, and m_g, $\{G_j\}_j$ are the MAs and focal elements for f and g, respectively.

Now for any normalized fuzzy set g, a posterior distribution result from conditioning on g can be clearly defined, according to Equation 8.1. This is referred to as the least prejudiced distribution (*lpd*) of g with respect to the prior $P(x)$.

More formally:

$$\forall x \in X;\ lpd_g(x) = P(x|g) = P(x) \sum_{G_j : x \in G_j} \frac{m_g(G_j)}{P(G_j)} \qquad (8.2)$$

Indeed it can be shown (Baldwin *et al.*, 1996) that the probability of f given g as defined in Equation 8.1 is equivalent to the probability of f relative to the distribution lpd_g on X (Zadeh, 1968), that is:

$$P(f \mid g) = \sum_{x \in \Omega} \mu_f(x) lpd_g(x) \qquad (8.3)$$

where $\mu_f(x)$ is the membership function of the fuzzy subset f on X.

The notion of lpd provides a mechanism by which a fuzzy set can be converted into a probability distribution. In the absence of any prior knowledge, the lpd might be relative to the uniform prior on knowing that g naturally infers the distribution lpd_g. If, however, fuzzy sets are to serve as descriptions of probability distributions, the converse must also hold. In other words, given a probability distribution, it will be required to hold that there is a unique fuzzy set conditioning on which this distribution yields.

8.5 Mechanism for Fuzzy-Bayesian Conversion

Fuzzy-Bayesian inference is not quite direct as one would like to imagine. Instead, it relies on the use of the *theory of MAs* to play the central role. Therefore, the inferential pattern goes from a fuzzy set into MAs, and then from MAs into the prior probabilities. With Bayesian inference being enabled, the likelihood probabilities must be provided by the likes of this similar means. Likewise, the concept of conditional independence is applied to simplify the joint probability distribution of the modelling domain.

8.5.1 Basics of Mass Assignment

MA unifies probability, possibility and fuzzy sets into a single theory termed mass assignment theory (MAT). If two or more groups of MAs are necessary to provide a single MA, then operations of MAT would have to be applied.

8.5.1.1 Mass Assignment Theory

The theory of MAs has been developed by Baldwin (see Baldwin, 1992; Baldwin *et al.*, 1995) to provide a formal framework for manipulating both probabilistic and fuzzy uncertainties. Without such a theory, the construction of systems capable of handling uncertainty in a unified manner may be difficult.

The motivation for considering MAs (Baldwin, 1991; 1992; Baldwin, *et al.*, 1995) is to provide semantics for membership functions of fuzzy sets. Essentially, the idea is that a fuzzy (or vague) concept is simply a concept for which the definition is uncertain or variable (across, say, a population of voters (Williamson, 1994)). Each possible definition corresponds to a subset of the universe of discourse and a probability distribution MA across these definitions can then be defined. Given such a distribution, the focal sets are taken to be those with nonzero mass. In fact, for the above definition the added assumption is made that the uncertainty is only regarding the degree of generality or specificity of the definition so that the focal sets form a nested hierarchy. The membership value of an element is then defined as the sum of the masses for the focal sets containing that element. Given these constraints, there is a unique MA corresponding to any fuzzy set. Note that a slightly different perspective on the above is to view the definition of a vague concept as a random set into the power set of the universe and the MA as its distribution (Goodman, 1985; Kreinovich, 1997).

A MA on a finite set X is a function $m : P(X) \rightarrow [0, 1]$ such that $\Sigma_{S \subseteq X} m(S) = 1$. Note that m_f has the property that it is nonzero only on some sequence of subsets of $X\{S_i\}$ such that $S_i \subseteq S_{i+1}$. Such MAs are strongly related to consonant basic probability assignments, which in actual fact represent a family of probability distributions. Furthermore, m_f satisfies $\Sigma_{S \subseteq X} m(S) = \mu_f(x)$. Now this is a fundamental requirement of any MA corresponding to f.

8.5.1.2 Operations of Mass Assignment

One of the most attractive features of MA theory is that operations of MA are defined in a way compatible to set operations. They include the complement ( ), meet ($\cap$), and join ($\cup$). Given two MAs, $m(A) = \{M_i : m_i\}$ and $m(B) = \{M_j : m_j\}$, on universal set X, the general definitions of these operations are stated as follows:

- *Meet* of $m(A)$ and $m(B)$ is the intersection: $m(A) \cap m(B) = \{x_k : y_k\}$, where the new focal elements are given by $x_k = M_i \cap M_j$ and $y_k = \sum_{i,j;x_{ij}=x_k} y_{ij}$, respectively.

- *Join* of $m(A)$ and $m(B)$ is the union: $m(A) \cup m(B) = \{x_k : y_k\}$, where the new focal elements are given by $x_k = M_i \cup M_j$ and $y_k = \sum_{i,j;x_{ij}=x_k} y_{ij}$, respectively.

- *Complement* of $m(A)$ is the complementation: $\overline{m}(A) = m(\bar{A} = X - A)$, $\forall A \in P(X)$. Also, the focal elements of $\overline{m}(A)$ are the complements of the focal elements of $m(A)$.

$\sum_j y_{ij} = m_i \ \forall i$ and $\sum_i y_{ij} = m_j \ \forall j$ are referred to as the *row* and *column* constraints respectively. It can be noted that the complement is determined uniquely. However, the meet and the join operations are not determined uniquely because of possible combinations of redistribution of mass over new focal elements as determined by taking either intersection (meet) or union (join) of original focal elements.

8.5.2 Inferential Relationship

In order to enable inference via MA from a fuzzy set (FS) weights have to be assigned by a population of voters or a panel of experts to every fuzzy subset, μ_1, μ_2, ..., μ_n, on the universe of discourse. In this layer, each weight, w_i, by members can be either 0 or 1. This can then be transformed to the corresponding MA, i.e., m_1, m_2, ..., m_n, at the MA layer on each focal element, x_i. In contract to the basic probability assignment in Dempster-Shafer (DS) theory, $\varnothing$ can be a focal element. At the probability distribution (PD) level, $w_i \rightarrow [0,1]$ and $\Sigma w_i = 1$.

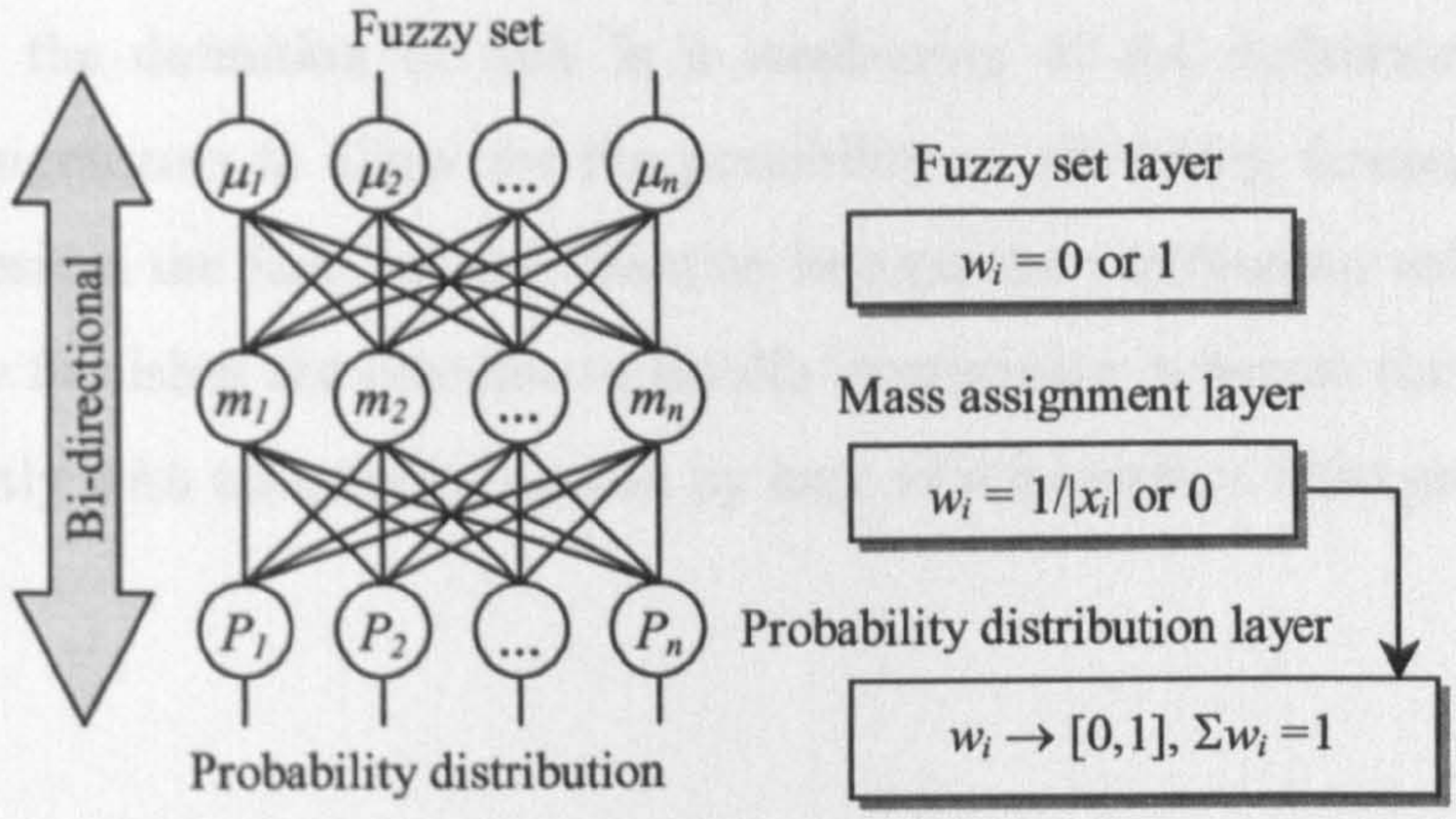


Figure 8.3: Illustrative overview of a FS-MA-PD inferential relationship

Figure 8.3 gives a mapping overview of the FS-MA-PD inferential relationship. Sections 8.5.2.1 to 8.5.2.3 provide the breakdown of this inferential process. Note that the entire inferential process is bi-directional. The key advantage offered by the bi-directional nature is that the originally normalised output fuzzy set values can be obtained from the achieved probability distribution values and vice-versa.

8.5.2.1 Fuzzy Set-Mass Assignment Relation

Let S be a sample space. Then, a mass assignment m_S associated with S is a function from the power set, $P(X)$, to an interval of real numbers such that $m_S : P(X) \rightarrow [0, 1]$ and $\Sigma_{A \subseteq S} m_S(A) = 1$. A subset $A \subseteq S$ is referred to the focal element for mass assignment m_S if $m_S(A) > 0$. Given a normalized discrete fuzzy subset $F = x_1/\mu_1 + \ldots + x_n/\mu_n$ over S, it can be denoted that $\mu_i = \mu_F(x_i)$. Without loss of generality for the normalised fuzzy subset, one can assume that:

$$1 = \mu_1 \geq \ldots \geq \mu_n \geq \mu_{n+1} = 0$$

Then a MA with nested focal elements $\{x_1, \ldots, x_i\}$ for $i = 1, \ldots, n$ can be derived as:

$$m_S(A) = \mu_i - \mu_{i+1}, \qquad \text{if } A = \{x_1, \ldots, x_i\} \tag{8.4}$$

In effect then the definition of MA is a weakening of the definition of DS basic probability assignments to allow for the possibility of allocating nonzero mass to the empty set. Besides the fact that the calculus beyond the verification role is enhanced, the MA theory furnishes the calculus to handle imprecision, whereas the theory, due to DS, deals mainly with uncertainty caused by lack of information from probability point of view.

8.5.2.2 Mass Assignment-Probabilities Relation

In MA theory, there exists the relation between a discrete probability distribution, e.g., a normalized histogram, associated to elements of a sample space, S, on the power set, $P(X)$, and a least prejudiced probability distribution, lpd_A, (i.e., a selection rule) for each $A \in P(X)$. Basically, lpd_A is the case for which the assumption is made that mass assigned to a set A is equally likely to belong to any element in A. As a result mass assigned to A is distributed equally across all elements in A. More formally, given a mass $m(A)$;

$$m_s(\{x\}) = \frac{m_s(A)}{|A|} \quad \forall x \in A \tag{8.5}$$

where 1/|A| is the lpd of A. |A| denotes the magnitude (modulus) of A, which refers to its size.

Masses assigned to singletons $\{x\}$ are now summed and assigned as probabilities for X. A probability $P_s(x)$ is therefore defined as,

$$P_s(x) = \sum_{A \subseteq S, x \in A} \frac{m_s(A)}{|A|} = \sum_{A \subseteq S, x \in A} lpd_A(x) m_s(A) \tag{8.6}$$

The main role of the selection rules is in maintaining consistency between a fuzzy set and different probability distributions that satisfy Equation 8.6.

8.5.2.3 Mapping Between Fuzzy Set and Probability

Using the relation of fuzzy set-MA and MA-probability, one can now obtain the mapping between a fuzzy set and a probability distribution as shown in Figure 8.4. Let $P_s(x_k)$ be a probability of a sample space S, and $lpd_{Ai}(x_k)$ be a selection rule for x_k from the focal element $A_i = x_1, ..., x_i$, $i = 1,..., k$ of a MA. Then:

$$P_s(x_k) = \sum_{i=k}^{n} lpd_{Ai}(x_k).(\mu_i - \mu_{i+1}) \qquad (8.7)$$

It is noted that all focal elements are nested as they correspond to the level sets (α-cuts) for $\mu_i \forall i = 1,..., n$.

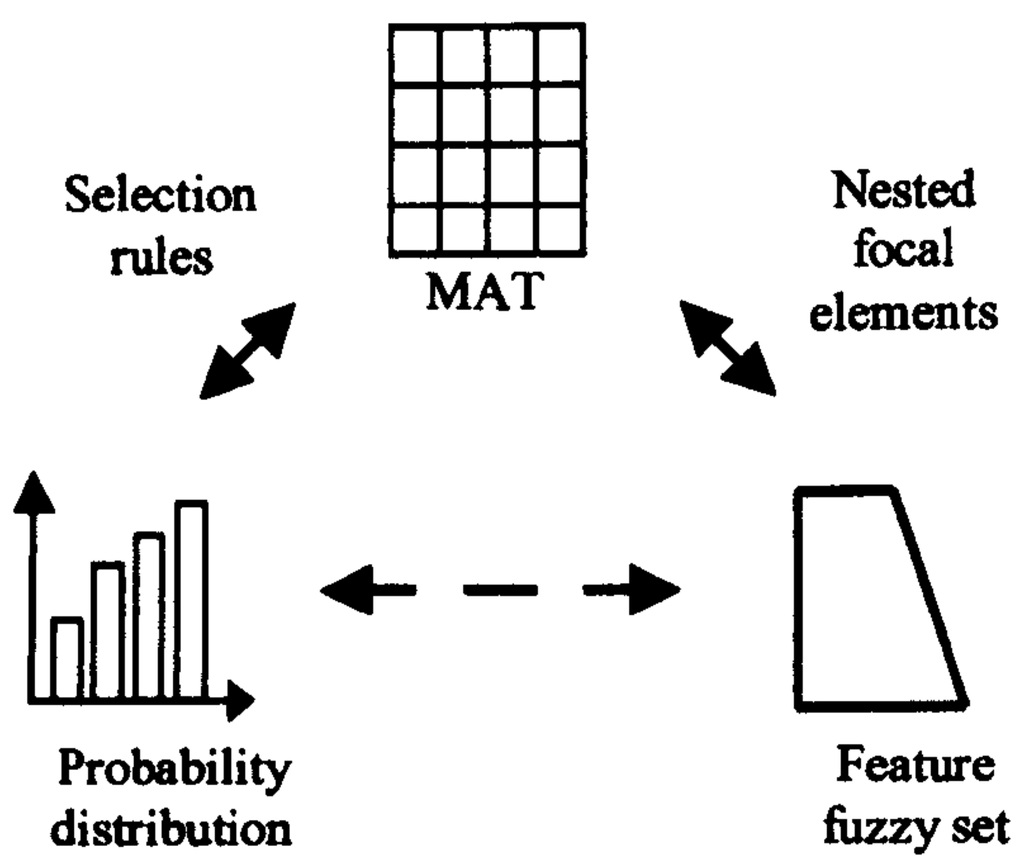


Figure 8.4: Mapping consistency between a fuzzy set and a probability distribution

The selection rules lpd_{Ai} can be tuned if the fuzzy set (i.e., the membership values μ_i's) is always manually changed in order for P_s to remain the same. This feature is important to determine the valid range of data for a given fuzzy set. Inconsistency in the data set is detected by obtaining some invalid probability in Equation 8.7. Such results are obtained when the order of membership values is not maintained. From a different angle, this can be used to determine what is lacking in order to keep the consistency.

The selection rules can also be used to establish a many-to-many relationship between probability distributions of data and its fuzzy set definition. Selection rules can also be one way of implementing experts' perception. In this case, selection rules are given arbitrarily. Then either a fuzzy set for a given data set or an ideal data set biased by experts' perception (i.e., a selection rules) for a fuzzy set representing a concept can be obtained by Equation 8.7.

8.6 Proposed Fuzzy-Bayesian Network Methodology

A FBN reasoning process has been developed to provide a natural framework for maritime risk assessment and decision support. A flow chart of the approach is shown in Figure 8.5, and this format ensures that the FBN analysis are conducted in a disciplined, well managed, and consistent manner that promotes the delivery of quality maritime decision-making results. The depth or extent of application of the methodology should be commensurate with the nature and significance of the problem. Nonetheless, the entire methodology is made up of three key modules:

- Module 1: Normalized fuzzy set from output values of FL module.
- Module 2: MA module.
- Module 3: Input values as prior probabilities of BN module.

In building a FBN model, one can first focus on specifying the qualitative structure of the domain and then focus on quantifying the influences. When finished, one is guaranteed to have a complete specification of the possibility and probability distributions. Then following evidence propagation, an intuitive evaluation for decision-making can be enabled through added nodes of decisions and utilities as in a BN. *Hugin* (Jensen, 1993) can thus be is used as the robust BN programming environment for the risk modelling and its probability calculations. Explanations for each of the underlying modules are given as follows:

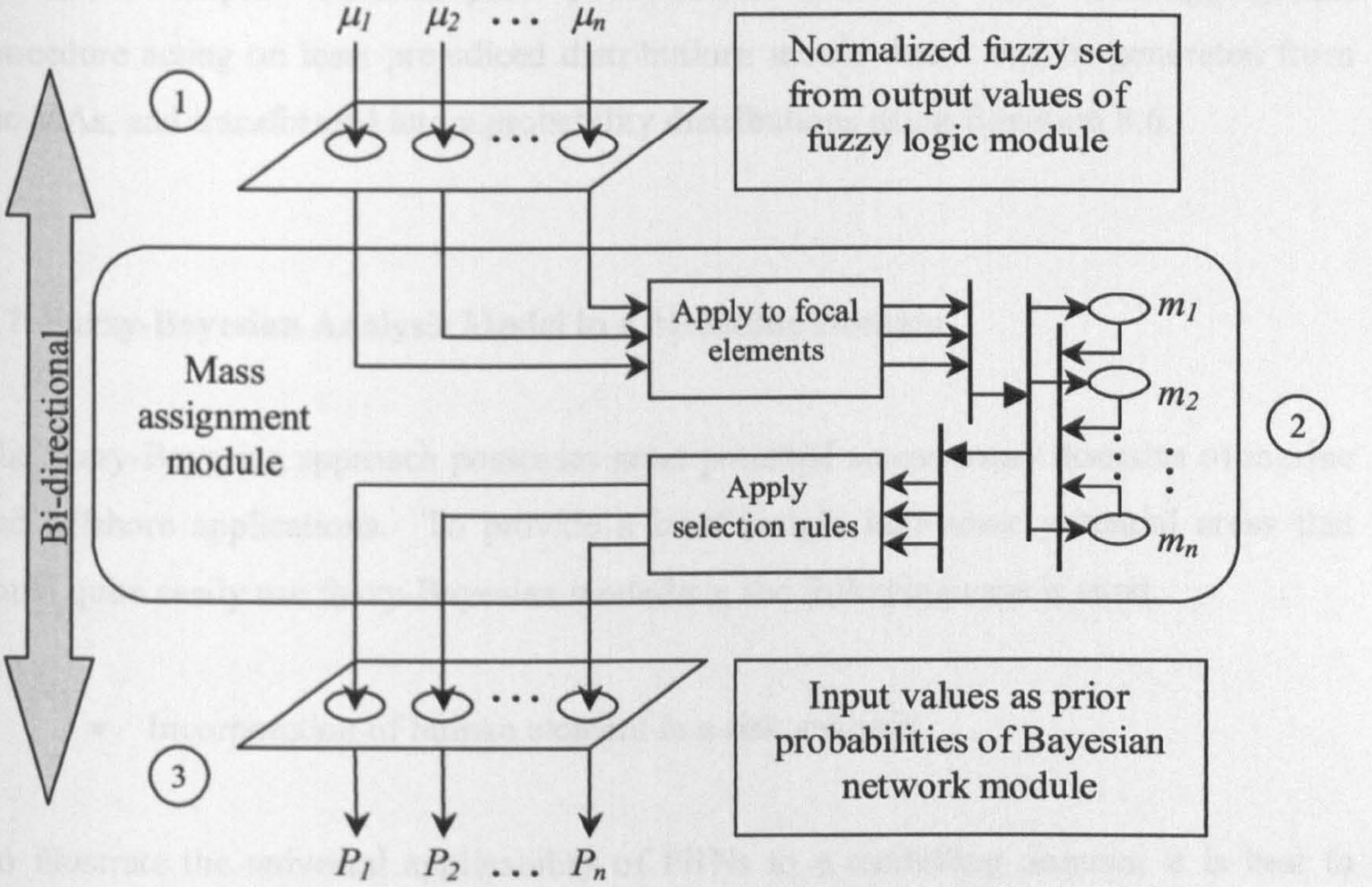


Figure 8.5: Flow chart of a proposed FBN framework of analysis

Module 1 - Normalized fuzzy set from output values of FL module: The aggregation procedure acting on fuzzy sets means that fuzzy sets are generated from data sets, and aggregated by fuzzy set operations. Therefore, the aggregated fuzzy conclusion for a risk modelling output may be processed via the assignment of weights from a panel of experts.

Module 2 - MA module: The aggregation procedure acting on MAs means applying MA theory operations such as meet and join on MA's generated least prejudiced distributions. Only then can the aggregated MA (as in Equation 8.5) be suited for its transformation into the probability distributions of its essential focal elements.

Considering the original motivation of MA theory as a treatment of evidences, it is natural to treat each data set as evidence, and thus, to treat features extracted from a single text as a focal element and sizes of features are aggregated directly as selected rules of aggregated MAs using MA theory.

Module 3 - Input values as prior probabilities of BN module: The aggregation procedure acting on least prejudiced distributions means that it can be generated from the MAs, and transformed into a probability distributions using Equation 8.6.

8.7 Fuzzy-Bayesian Analysis Model in a Maritime Domain

The fuzzy-Bayesian approach possesses great potential across many domains of marine and offshore applications. To provide a brief insight into some potential areas that could quite easily use fuzzy-Bayesian modelling, the following case is sited:

- Incorporation of human element in a risk analysis.

To illustrate the universal applicability of FBNs to a modelling domain, it is best to imagine a situation in which causality plays a role but where an understanding of what is actually going on exhibits both vague and random features. Thus, things need to be described possibilistically, probabilistically and by inference.

8.7.1 Incorporation of Human Element into Risk Analysis

Human reliability analysis (HRA) endeavours to predict the probability of human error (typically uncorrected error) against a specified base rate. Whilst it is concerned with causal analysis, it relies heavily on factors (in the operator, the environment, the equipment or the task) that affect the likelihood of error. These factors which are termed '*performance-shaping factors*' are not models in their own right, but rather, they are input attributes that have an effect on the output of human performance. In the maritime industry, the quantification of such attributes exhibits a vast amount of vagueness for which their direct input into a probabilistic model needs to allow for this uncertainty. Hence, FBN is offered as the assessment platform.

8.7.1.1 Human Errors in Maritime Operations

Human errors include (HSE, 2002):

- Slips - making an unintended action through lack of attention or skill.
- Lapses - unintended action through memory failures.
- Mistakes - an intended but incorrect action.
- Violations - a deliberate deviation from standard practice.

Human errors in marine operations, such as towing or ballast system operation, tend to have immediate effects. They may be recovered with no harm done, or they may have some direct harmful impact. This may then require some form of emergency response to mitigate the impacts. Similarly, errors may occur during evacuation, with a direct effect, e.g. incorrect release of a lifeboat.

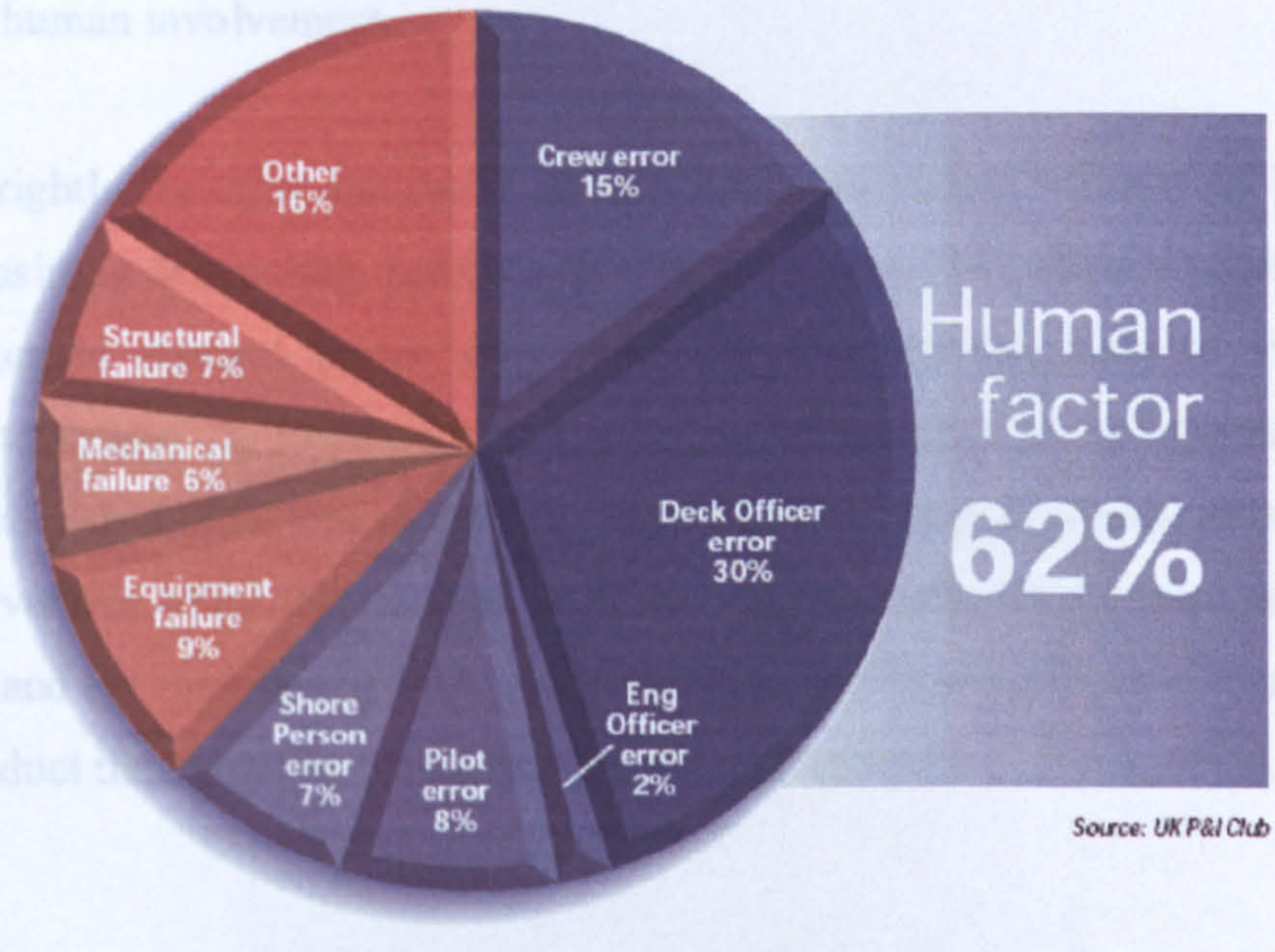


Figure 8.6: A typical UK P&I Club analysis of major claims

Errors can also occur during maintenance, and may then remain undiscovered (latent) until the equipment is required. These errors in effect cause equipment unavailability, and the significance of this depends on the system design. For example, this type of error may result in a ballast pump being unavailable when required. In fact, human error is human misery; of careers blighted, lives lost, seafarers injured and the

environment despoiled. As continually stressed by the UK P&I Club, equipment, mechanical and structural failure together is far outstripped by human error as the sole or major cause of incidents giving rise to claims. In looking at major claims, a current report (The Nautical Institute, 2003) finds that more than 62% (See Figure 8.6) are directly attributable to error by one or more individuals.

8.7.1.2 Human Factors in Maritime Risk Assessments

Wherever there is a human interacting with a system there is a human element issue. Modern technology has revolutionised the way in which a ship is operated, but lack of attention to the human-system interface, in terms of the design, layout, and integration of systems, and training in their use, is a major root cause of many accidents today. The maritime industry recognises that such accidents are the direct consequence of human failings and that in reality many of the disregarded incidents and errors have a strong element of human involvement.

Since it is rightly the crew and the shipboard management that will always be working in an increasingly demanding, technically complex system, the maritime industry needs to grasp human element issues at a higher, more integrated level to make a real difference to safety. A FBN may well prove to be adequate in an integrated task of reducing the risk due to human factor. Obviously, the key to improvement is in the close involvement of all stakeholders to ensure that a ship is 'fit for purpose', and that the master and his crew are provided with the proper tools and adequately training to be able to conduct their business in a safe and efficient manner.

8.7.1.3 Performance-shaping Factors as Model Variables

Performance-shaping factors (PSFs) are those factors that can have positive or negative influence/effect on the effectiveness of human performance and the likelihood of errors (HSE, 1999). It is essential that the proper PSFs be identified to determine the effect external influences have on the basic human error probabilities (HEPs). Examples of

PSFs in the marine and offshore industry, as well as with most other industries, include (Boring & Gertman, 2004; Brown & Amrozowicz, 1996):

- Available time.
- Stress and stressors.
- Experience and training.
- Complexity and workload.
- Ergonomics (including human-machine interaction).
- Environmental effects.
- The quality of operating procedures.
- Language and culture.
- Morale and motivation.
- Operator fitness for duty.
- Work processes.

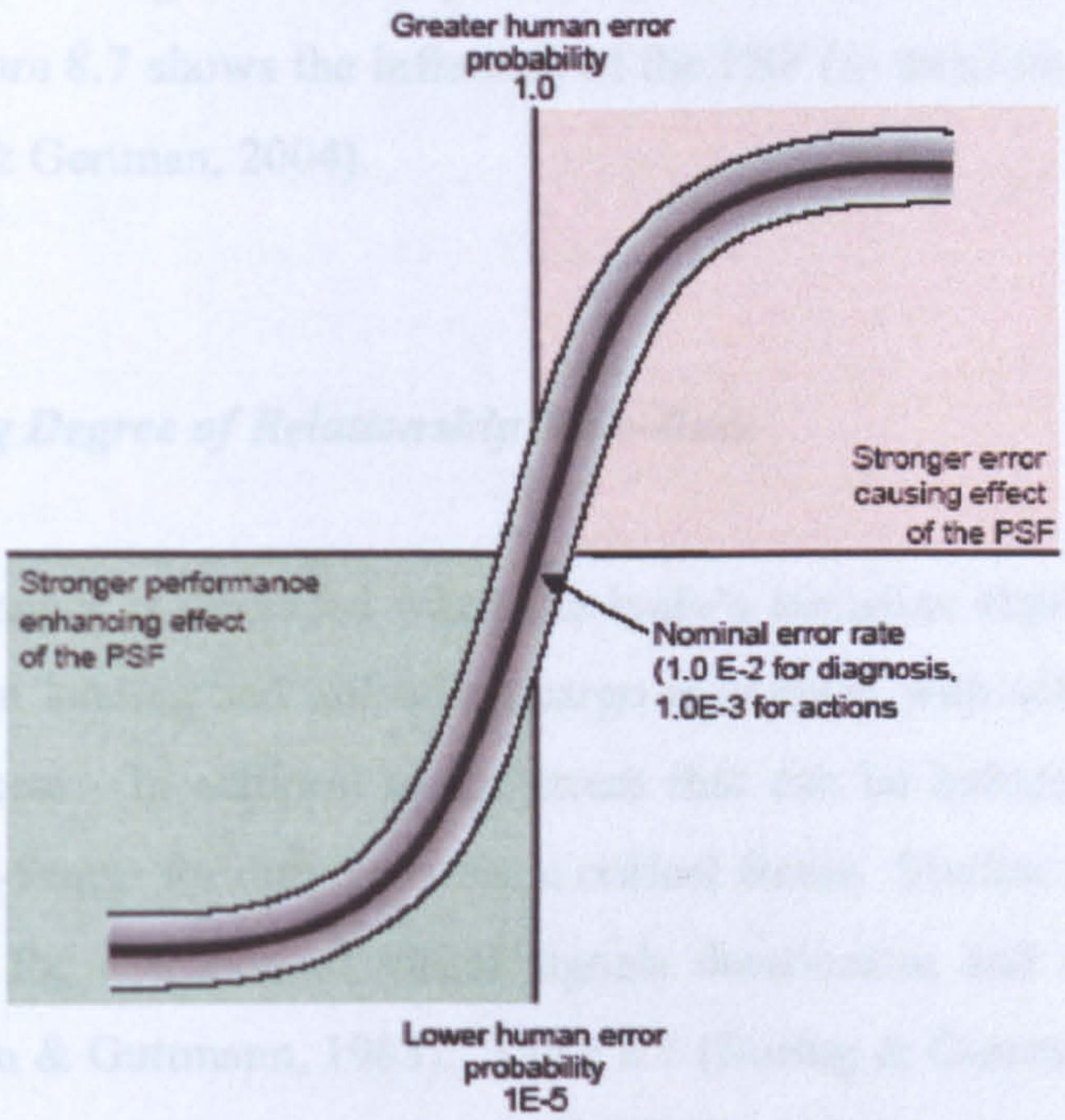


Figure 8.7: Mean human error probability as a function of PSF influence

These factors, which are "human process variables" in the operator, the environment, the equipment or the task, may be linked directly to human error through quantification.

Despite their clear importance in human error likely situations, they have been hard to implement in quantitative risk assessment. The reason for this is more or less obvious; how is it possible to estimate for example culture or self-confidence that actually does influence the safety of a system? PSFs are therefore important to take into account, but the integrating strategy is more indistinct (Kjestveit, *et al.*, 2003). Seaver & Stillwell (1983) addressed the need for approaches that explicates paired comparisons, ranking and rating, direct numerical estimation, and indirect numerical estimation techniques applied to error estimation, with a particular emphasis on aggregating the estimates from multiple experts to arrive at error probabilities. Thus, due to the qualitative characteristics of PSFs, FL approach can be utilised to allow for their input via expert judgement process.

PSFs work to increase or decrease the error rate due to situational characteristics. If, for example, the person is experiencing considerable stress, his or her task performance will decrease proportionate to the level of stress. Conversely, if a person has extensive training and practice doing a task, that person's proficiency may mitigate the chance of human error. Figure 8.7 shows the influence of the PSF (x- axis) on mean HEP values (y- axis) (Boring & Gertman, 2004).

8.7.1.4 Developing Degree of Relationship Rule-Base

Individual performance is degraded when the body's circadian rhythms are disrupted. For example, when loading and unloading cargo is coupled with scheduling pressures, time stress can occur. In addition to the stress that can be induced from long work hours, fatigue/non-fitness for duty becomes a critical factor. Studies have shown that as fatigue increases, the detection of visual signals deteriorates and individuals exhibit more errors (Swain & Guttmann, 1983). Table 8.1 (Boring & Gertman, 2004) gives the relationship on how available time as a PSF (PSF_1) is influenced by the other PSFs (PSF_i) and as well, how it affects them.

The parametric relationship between one PSF and another for a marine vessel or an offshore installation is determined by simulation and expert opinion. Figure 8.8 depicts

the interrelationship between the PSFs as well as their direct or indirect contribution to human performance.

Table 8.1: Influence of and effects on other PSFs on time availability

PSF (PSF_i)	Available time, PSF_1	
	Influence	**Effect**
Stress and stressors, PSF_2	Amount of stress does not change the available time.	Less time may increase stress.
Experience and training, PSF_3	Greater experience means that less time is required for actions and decisions.	Available time has little or no effect on experience and training.
Task complexity, PSF_4	Too much complexity and workload can make the time available insufficient.	Little time makes the task more complex for which the workload may require more hands on.
Ergonomics (including human-machine interaction), PSF_5	Poor layout can result in increased reaction time, lessening the available time to respond.	Available time has little or no effect on ergonomics and human-machine interaction.
Environmental effects, PSF_6	The likes of room temperature, vibration and sea motion can make the time available insufficient.	Available time has no effect on environmental state/condition.
The quality of operating procedures, PSF_7	Complex or poorly conceived procedures increase how much time one needs to act.	Available time has little or no effect on the quality of operating procedures.
Language and culture, PSF_8	Misunderstanding can result in increased reaction time, lessening the available time to respond.	In some cases, time may lead to misunderstanding in language and culture.
Moral and Motivation, PSF_9	Greater motivation means that less time is required for actions and decisions.	In some cases, time may have a significant effect on moral and motivation.
Operator fitness for duty, PSF_{10}	Illness or drug abuse may require increased time to decide or act.	Available time has little or no effect on the operator's fitness for duty.
Work processes, PSF_{11}	Poor shift turnover of information can reduce time available.	In some cases, time may enhance or compromise work processes.

Note that PSFs can be combined for specific rules in a FL rule-base. In the case where more than one PSF is being considered, absolute HEP values can be computed by adding individual PSF multipliers. This would be the case, for example, if available time and stress contributed to a human error (Boring & Gertman, 2004).

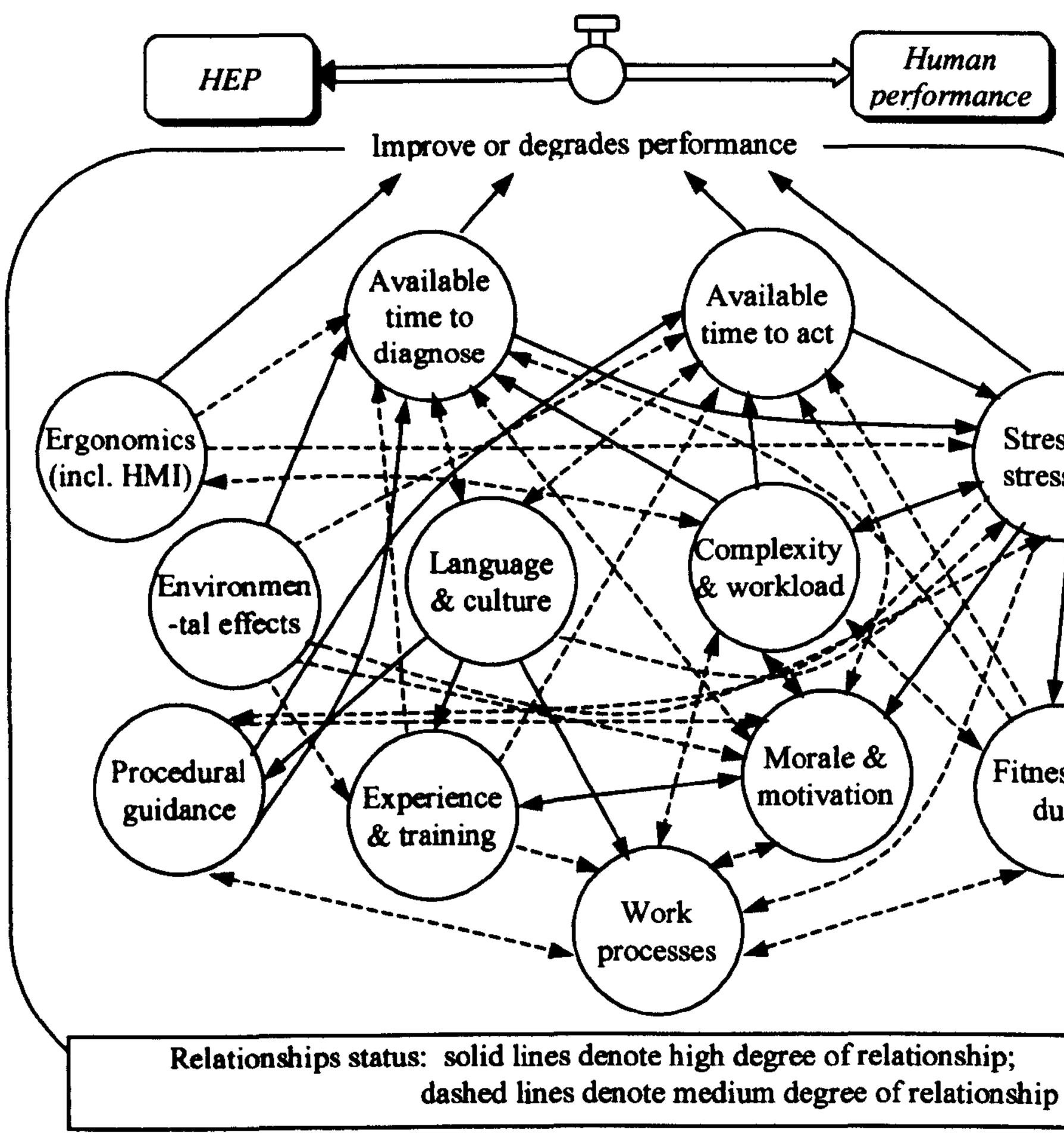


Figure 8.8: Path diagram of relationship amongst generic PSFs

In the event of multiple concurrent tasks, as is common in most real-world scenarios, Boring & Gertman (2004) state that the HEP values may also be combined. If two events must occur together for an error to occur, the HEP values are multiplied together to create a logical 'AND' relationship. For example, loosing a fresh program file that is important to the shipboard system requires the user both to fail to save the program file *and* to quit the program. If, however, errors are not in any way related to one another, the two task HEP values are added together to create a logical 'OR' relationship. For

example, a person may not be able to log in to an authorising computer either by forgetting his or her computer password *or* by failing to type the password in the correct CapsLock case. Thus, using the generic PSFs as fuzzy linguistic variables, specific IF-THEN rules can be created via such logical 'OR' and 'AND' operators for a FL rule-base.

8.7.1.5 Categorisation of Performance-shaping Factors

PSFs are characterised according to whether the task is cognitively engaging (i.e., a diagnosis task) or routinised (i.e., an action task). Operational research suggests that for cognitively engaging tasks such as diagnosis, people tend to exhibit a base human error rate equal to 1.0×10^{-2} (Boring & Gertman, 2004). This means that people have about 1 in 100 chance of making a diagnosis error. For tasks that are more action oriented, the base human error rate is equal to about 1.0×10^{-3}, suggesting about 1 in 1000 chance of making an error (Boring & Gertman, 2004). Base error rates for the two task types associated with the Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) method were calibrated against other HRA methods. The calibration revealed that the SPAR-H human error rates fall within the range of rates predicted by other methods (Gertman, *et al.*, 2004).

The PSFs are further classified according to whether they occur in a fault tolerant situation or a fault intolerant condition (Boring & Gertman, 2004). Table 8.2 (Boring & Gertman, 2004) exhibits how PSFs shape human error by using available time in a fault intolerant condition, which is the condition of occurrence during critical operation.

Now, given PSF_i as a fuzzy input of an i^{th} PSF having subset $PSF_{i,j}$ as its j^{th} category, the rule-base for a fuzzy output of human performance, H_p, with subset $H_{p,k}$ for its k^{th} category, can be represented for the l^{th} rule as:

R_l rule = IF PSF_1 is $PSF_{1,j}$ AND/OR PSF_2 is $PSF_{2,j}$ AND/OR, ..., AND/OR PSF_{11} is $PSF_{11,j}$, THEN H_p is $H_{p,k}$

Owing to the number of input PSFs in rule, R_l, a software program, such as Fuzzy Logic Toolbox 2.2.1 of Matlab 6.5 (The MathWorks, 2005), may be most essential to minimise complexity of the fuzzy mathematics.

Table 8.2: Available time in a fault intolerant condition

Available time variable, $PSF_{1,i}$	Diagnosis	HEP	Action	HEP
Inadequate time, $PSF_{1,1}$	If the operator cannot perform the task in the amount of time available, no matter what s/he does, then failure is certain.	1.0	If the operator cannot execute the appropriate action in the amount of time available, no matter what s/he does, then failure is certain.	1.0
Barely adequate time, $PSF_{1,2}$	Two-thirds of the average time required to complete the task is available.	0.1	There is just enough time to execute the appropriate action.	0.01
Nominal time, $PSF_{1,3}$	On average, there is sufficient time to diagnose the problem.	0.01	There is some extra time above what is minimally required to execute the appropriate action.	0.001
Extra time, $PSF_{1,4}$	The time available is between one to two times greater than the nominal time required.	0.001	There is an extra amount of time to execute the appropriate action (i.e., the approximate ratio of 5:1).	0.0001
Expansive time, $PSF_{1,5}$	The time available is greater than two times the nominal time required.	0.0001	There is an expansive amount of time to execute the appropriate action (i.e., the approximate ratio of 50:1).	0.00001
Insufficient information, $PSF_{1,6}$	If you do not have sufficient information to choose among the other alternatives, assign this PSF level.	0.01	If you do not have sufficient information to choose among the other alternatives, assign this PSF level.	0.001

8.7.1.6 Determination of Human Performance Output

PSFs determine whether individual performance will be very poor, excellent, or at some level in between. For this performance output, the assessment team assigns numeric values based on a 0% – 100%-fuzzy scale (Figure 8.9) as anchored by linguistic variables and descriptors provided in the evaluation layer of instrument.

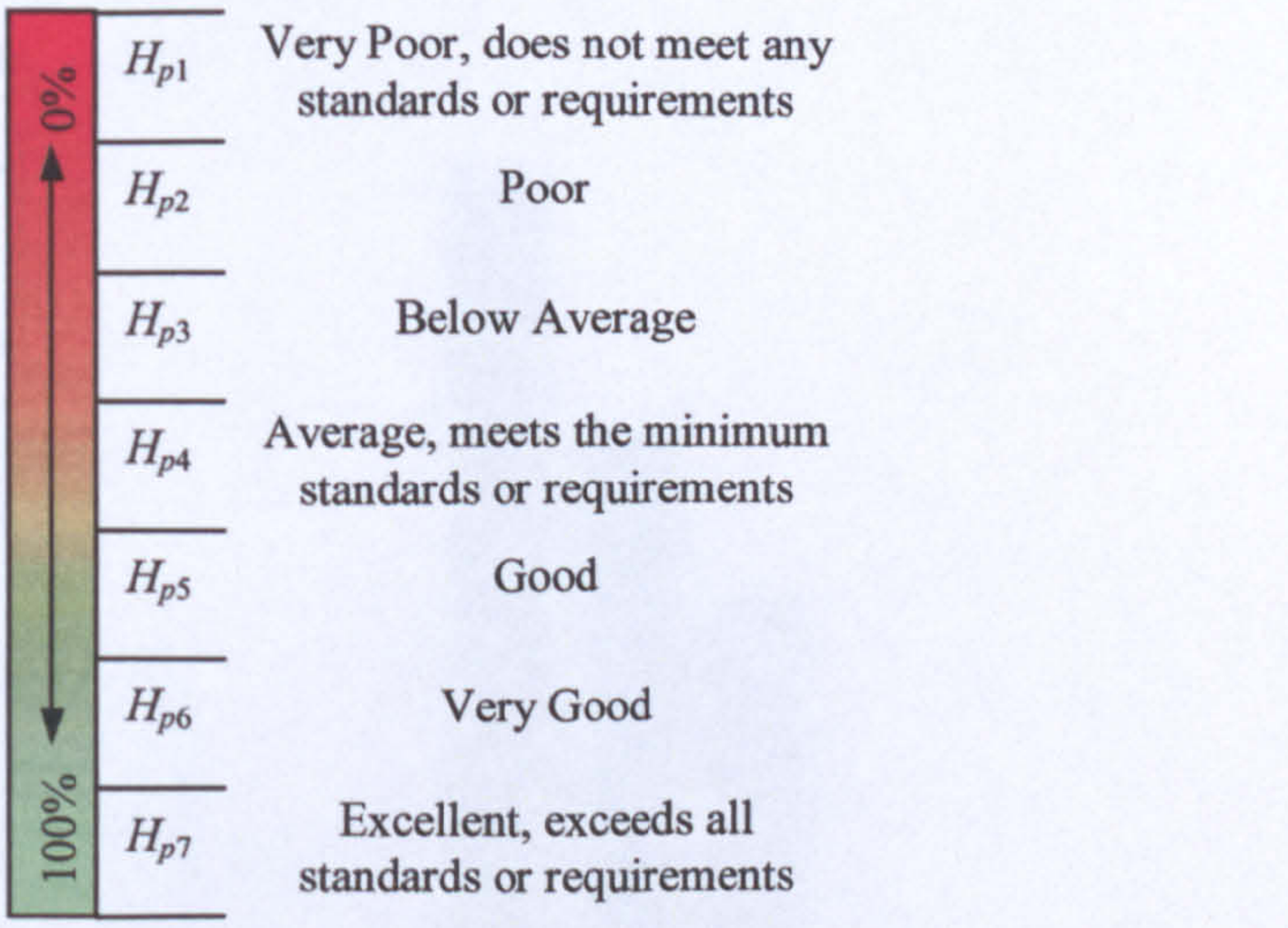


Figure 8.9: Human performance grading scale for fuzzy set definition

This process of measuring the output attribute is in a similar fashion as those undertaken for all 11 PSFs in the antecedent of the FL rule-base. The fuzzy set definition for the output attribute (i.e., human performance, H_p) is given in Figure 8.10.

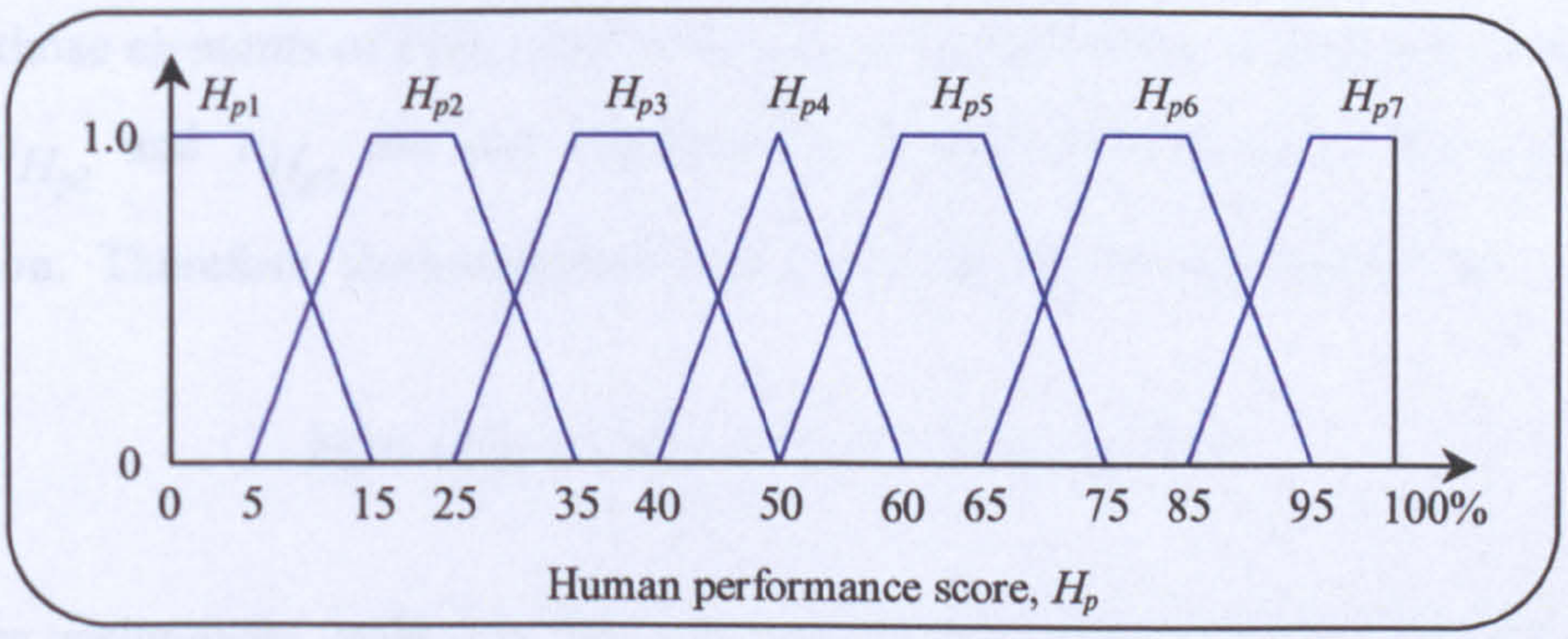


Figure 8.10: Fuzzy set definition for human performance output

In utilising expert judgment whilst executing the rule-base of the generic PSF via the FL module of the FBN methodology that has been presented in Section 8.6, the fuzzy H_p set is obtained as the fuzzy output result of the study. A hypothetical example of a normalised fuzzy set, as shown in Figure 8.11, is employed herein as the yielded discrete result for H_p to demonstrate the applicability of the FBN framework.

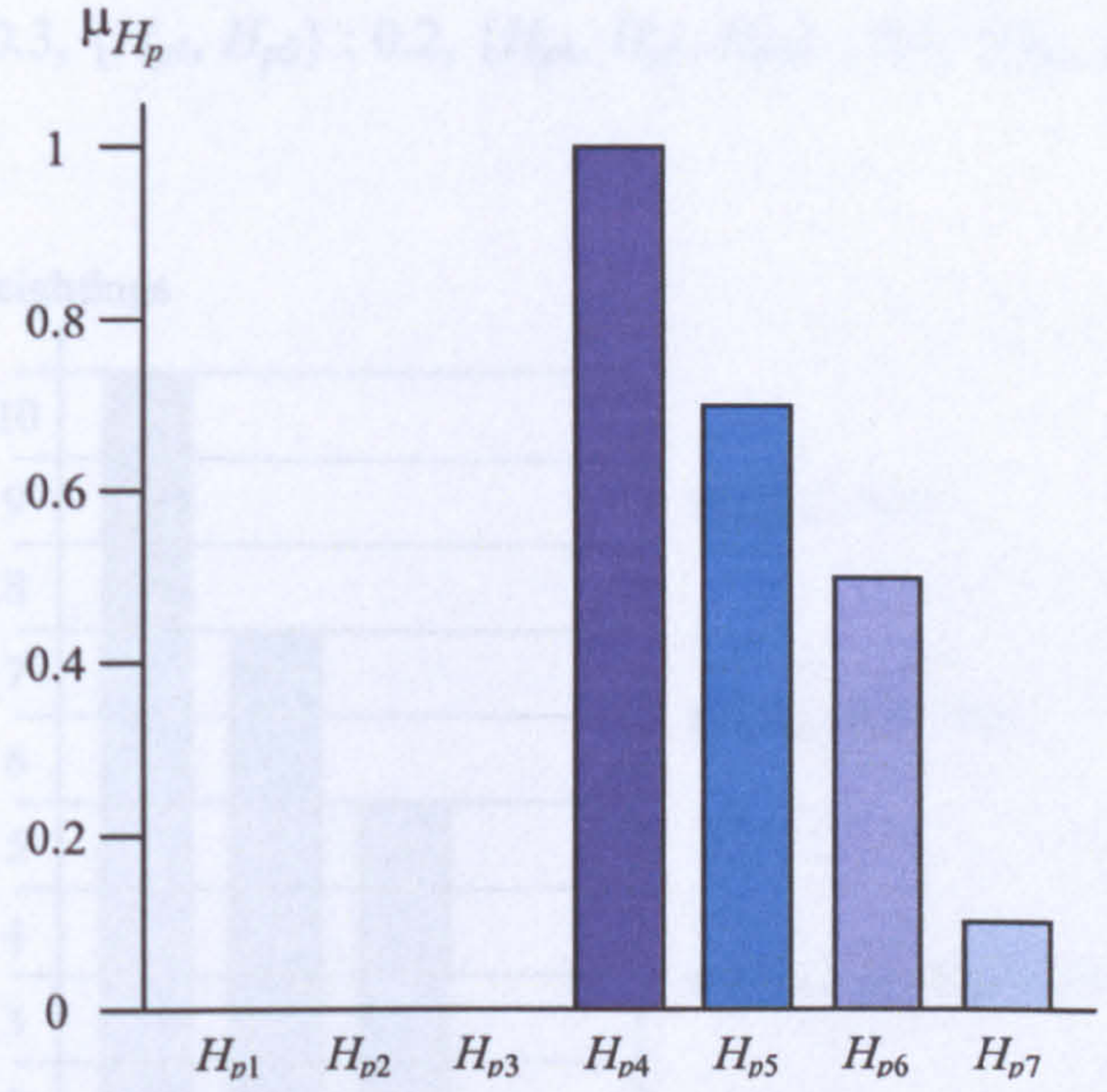


Figure 8.11: An example of a normalised fuzzy set utilised as human performance output, H_p

Membership values for each element in the H_p fuzzy set are $\mu_{H_{p1}} = 0$, $\mu_{H_{p2}} = 0$, $\mu_{H_{p3}} = 0$, $\mu_{H_{p4}} = 1$, $\mu_{H_{p5}} = 0.7$, $\mu_{H_{p6}} = 0.5$ and $\mu_{H_{p7}} = 0.1$. Since focal elements of H_p have to be only those elements of $P(H_p)$ that have non-zero probability assignment, then clearly $\mu_{H_{p1}}$ $\mu_{H_{p2}}$ and $\mu_{H_{p3}}$ are not required for further analysis into their probability conversion. Therefore, the normalised fuzzy set of H_p may be represented as:

$$H_p = \{H_{p5}/1 + H_{p5}/0.7 + H_{p5}/0.5 + H_{p5}/0.1\}$$

The mass assignment, $m(H_p)$, is derived from H_p by *weighting* the combined mass of each element in H_p. As assigned in Figure 8.12, the weighting of 10, 9 and 8 is attributable to only H_{p4}, the weighting of 7 and 6 is attributable to only H_{p4} or H_{p5}, the

weighting of 5, 4, 3 and 2 is attributable to only H_{p4} or H_{p5} or H_{p6} and the weighting of 1 is attributable to any of H_{p4}, H_{p5}, H_{p6} or H_{p7}. Normalising the number of weighting attributable to any one proposition then generates the mass assignment $m(H_p)$ for fuzzy set H_p for fuzzy set H_p as based on the use of Equation 8.4, which is given as:

$$m(H_p) = \{H_{p4}\} : \mu_{H_{p4}} - \mu_{H_{p5}}, \{H_{p4}, H_{p5}\} : \mu_{H_{p5}} - \mu_{H_{p6}}, \{H_{p4}, H_{p5}, H_{p6}\} : \mu_{H_{p6}} - \mu_{H_{p7}}, \{H_{p4}, H_{p5}, H_{p6}, H_{p7}\} : \mu_{H_{p7}}$$

$$= \{H_{p4}\} : 0.3, \{H_{p4}, H_{p5}\} : 0.2, \{H_{p4}, H_{p5}, H_{p6}\} : 0.4, \{H_{p4}, H_{p5}, H_{p6}, H_{p7}\} : 0.1$$

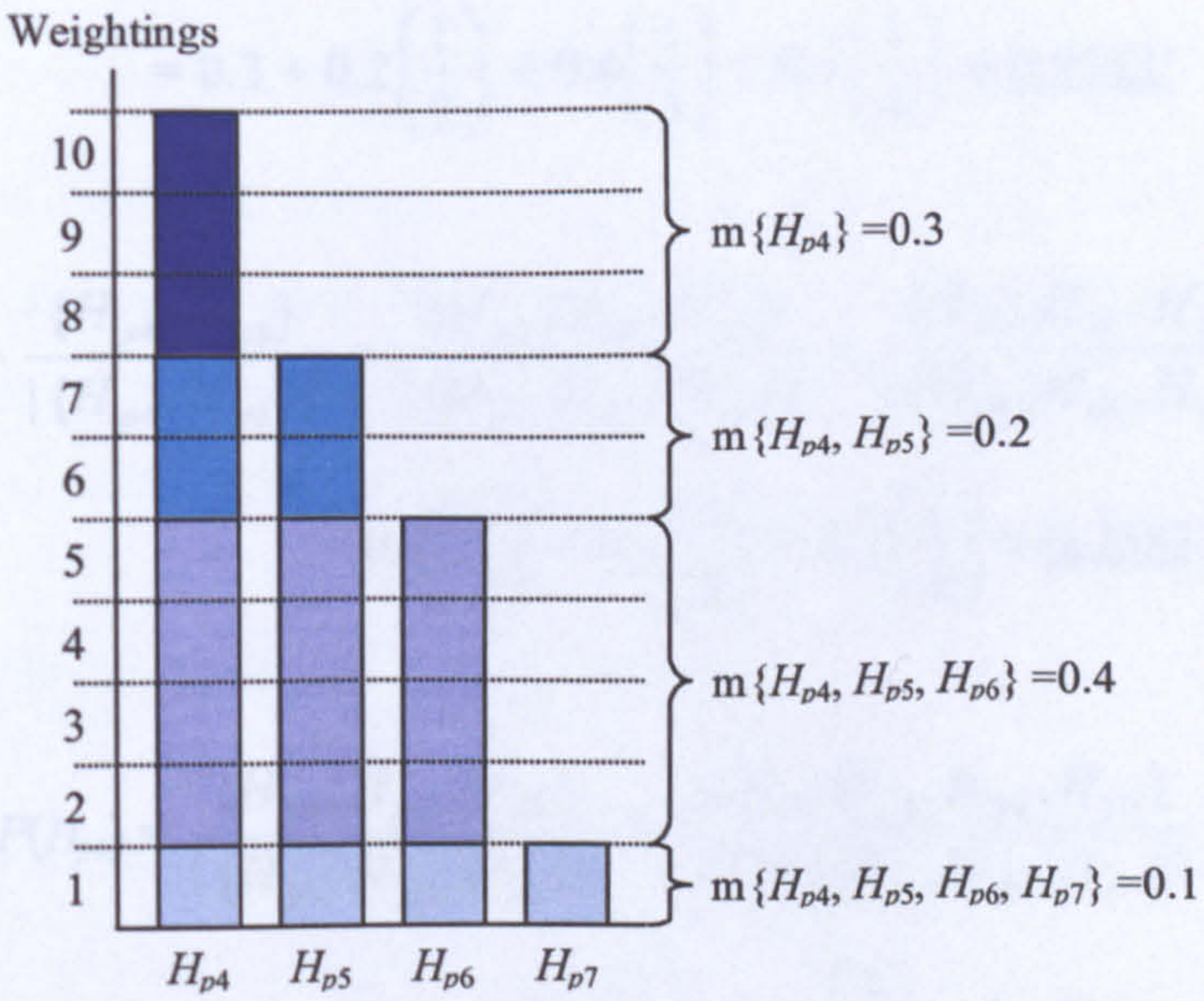


Figure 8.12: A weighting interpretation of mass assignment of human performance output, H_p

This obtained MA can be restricted using the least prejudiced distribution to give a single probability distribution. This probability distribution is defined across the human performance set H_p as is the corresponding fuzzy set. Firstly, the magnitude of masses in H_p is:

$$|\{H_p\}| = |\{H_{p4}\}| : 1, |\{H_{p4}, H_{p5}\}| : 2, |\{H_{p4}, H_{p5}, H_{p6}\}| : 3, |\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}| : 4$$

Having converted a fuzzy set into a MA, the calculus of MA can now be used to reason with fuzzy sets at the mass level. The advantage of this representation is the close

relationship between MAs and their corresponding families of probability distributions. MA therefore provides a crucial link between probability and fuzzy sets. This is a great enabler in developing maritime human element solutions based on a more unified theory than those that may be enacted by just a fully BN or FL approach.

By distributing mass across singleton subsets of the four focal elements, this now provides the probabilities from using Equation 8.6 as follows:

$$P(H_{p4}) = \frac{\{H_{p4}\}}{|\{H_{p4}\}|} + \frac{\{H_{p4}, H_{p5}\}}{|\{H_{p4}, H_{p5}\}|} + \frac{\{H_{p4}, H_{p5}, H_{p6}\}}{|\{H_{p4}, H_{p5}, H_{p6}\}|} + \frac{\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}}{|\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}|}$$

$$= 0.3 + 0.2\left(\frac{1}{2}\right) + 0.4\left(\frac{1}{3}\right) + 0.1\left(\frac{1}{4}\right) \approx \underline{\underline{0.5583'}}$$

$$P(H_{p5}) = \frac{\{H_{p4}, H_{p5}\}}{|\{H_{p4}, H_{p5}\}|} + \frac{\{H_{p4}, H_{p5}, H_{p6}\}}{|\{H_{p4}, H_{p5}, H_{p6}\}|} + \frac{\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}}{|\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}|}$$

$$= 0.2\left(\frac{1}{2}\right) + 0.4\left(\frac{1}{3}\right) + 0.1\left(\frac{1}{4}\right) \approx \underline{\underline{0.2583'}}$$

$$P(H_{p6}) = \frac{\{H_{p4}, H_{p5}, H_{p6}\}}{|\{H_{p4}, H_{p5}, H_{p6}\}|} + \frac{\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}}{|\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}|}$$

$$= 0.4\left(\frac{1}{3}\right) + 0.1\left(\frac{1}{4}\right) \approx \underline{\underline{0.1583'}}$$

$$P(H_{p7}) = \frac{\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}}{|\{H_{p4}, H_{p5}, H_{p6}, H_{p7}\}|}$$

$$= 0.1\left(\frac{1}{4}\right) = \underline{\underline{0.0250}}$$

Thus, the probability distribution achieved from the fuzzy event of human performance, H_p, is given as:

$$P(H_{p4}) = 0.5583', P(H_{p5}) = 0.2583', P(H_{p6}) = 0.1583', P(H_{p7}) = 0.0250$$

Note that ' is used after to show a recurring decimal digit, which in this case is the number 3. The reverse operation is also possible, that is, converting a probability distribution into a MA, and then into a fuzzy set. For this reverse operation some assumptions must be made to generate only one fuzzy set rather than a whole family of fuzzy sets. The problem arises since masses are assigned across members of the $P(H_p)$ while the H_p fuzzy set is defined on the universe of H_p itself.

Once again, the least prejudiced distribution approach of distributing mass across singleton subsets of the MA focal elements is favoured. This least prejudiced distribution notion relies on an assumption of an equal-likelihood prior to generate a single fuzzy set.

For a normalised fuzzy set, the membership of an element with the largest frequency is always 1. This element is also that which gives the largest probability associated with the least prejudiced distribution assumption. Since the order of frequencies in H_p is given for the probabilities as:

$$P(H_{p4}) > P(H_{p5}) > P(H_{p6}) > P(H_{p7})$$

Then, the order of frequencies in H_p is given for the elements in its fuzzy set can be given as:

$$\mu_{H_{p4}} > \mu_{H_{p5}} > \mu_{H_{p6}} > \mu_{H_{p7}}$$

Therefore, the MA for H_p is well generated, by applying Equation 8.4, as:

$$m(H_p) = \{H_{p4}\} : \mu_{H_{p4}} - \mu_{H_{p5}},\ \{H_{p4}, H_{p5}\} : \mu_{H_{p5}} - \mu_{H_{p6}},\ \{H_{p4}, H_{p5}, H_{p6}\} : \mu_{H_{p6}} - \mu_{H_{p7}},\ \{H_{p4}, H_{p5}, H_{p6}, H_{p7}\} : \mu_{H_{p7}}$$

Now, using the least prejudiced distribution assumption, a corresponding fuzzy set can be generated by assigning each element within each focal element in the probability distribution the mass assigned to that focal element can be obtained via Equation 8.7 as follows:

$$P(H_{p4}) = \mu_{H_{p4}} - \mu_{H_{p5}} + \left(\frac{1}{2}\right)(\mu_{H_{p5}} - \mu_{H_{p6}}) + \left(\frac{1}{3}\right)(\mu_{H_{p6}} - \mu_{H_{p7}}) + \left(\frac{1}{4}\right)\mu_{H_{p7}} \approx \underline{0.5583'}$$

$$P(H_{p5}) = \left(\frac{1}{2}\right)(\mu_{H_{p5}} - \mu_{H_{p6}}) + \left(\frac{1}{3}\right)(\mu_{H_{p6}} - \mu_{H_{p7}}) + \left(\frac{1}{4}\right)\mu_{H_{p7}} \approx \underline{0.2583'}$$

$$P(H_{p6}) = \left(\frac{1}{3}\right)(\mu_{H_{p6}} - \mu_{H_{p7}}) + \left(\frac{1}{4}\right)\mu_{H_{p7}} \approx \underline{0.1583'}$$

$$P(H_{p7}) = \left(\frac{1}{4}\right)\mu_{H_{p7}} = \underline{0.0250}$$

Thus, in working backwards, the focal element's membership values are obtained as:

$$\mu_{H_{p7}} = 0.1,\ \mu_{H_{p6}} = 0.5,\ \mu_{H_{p5}} = 0.7 \text{ and } \mu_{H_{p4}} = 1$$

Hence, this gives the discrete fuzzy set of H_p as:

$$H_p = \{1/_{H_{p4}} + 0.7/_{H_{p5}} + 0.5/_{H_{p6}} + 0.1/_{H_{p7}}\}$$

The bi-directional processed values for the fuzzy, mass and probability level of the H_p output set focal elements is pictorially represented as shown in Figure 8.13.

It has been well recognised that the element of human factor holds an all-essential input role into countless maritime risk investigation domains. For example, successful marine emergency *escape, evacuation, and rescue (EER)* are achieved through an effective and efficient interaction of the evacuees' human performance and the mechanical performance of the physical EER system (Bercha, *et al.*, 2003). Nonetheless, without a fit for function physical EER system, human performance becomes an act of brute survival - running, jumping, swimming, and fighting hypothermia.

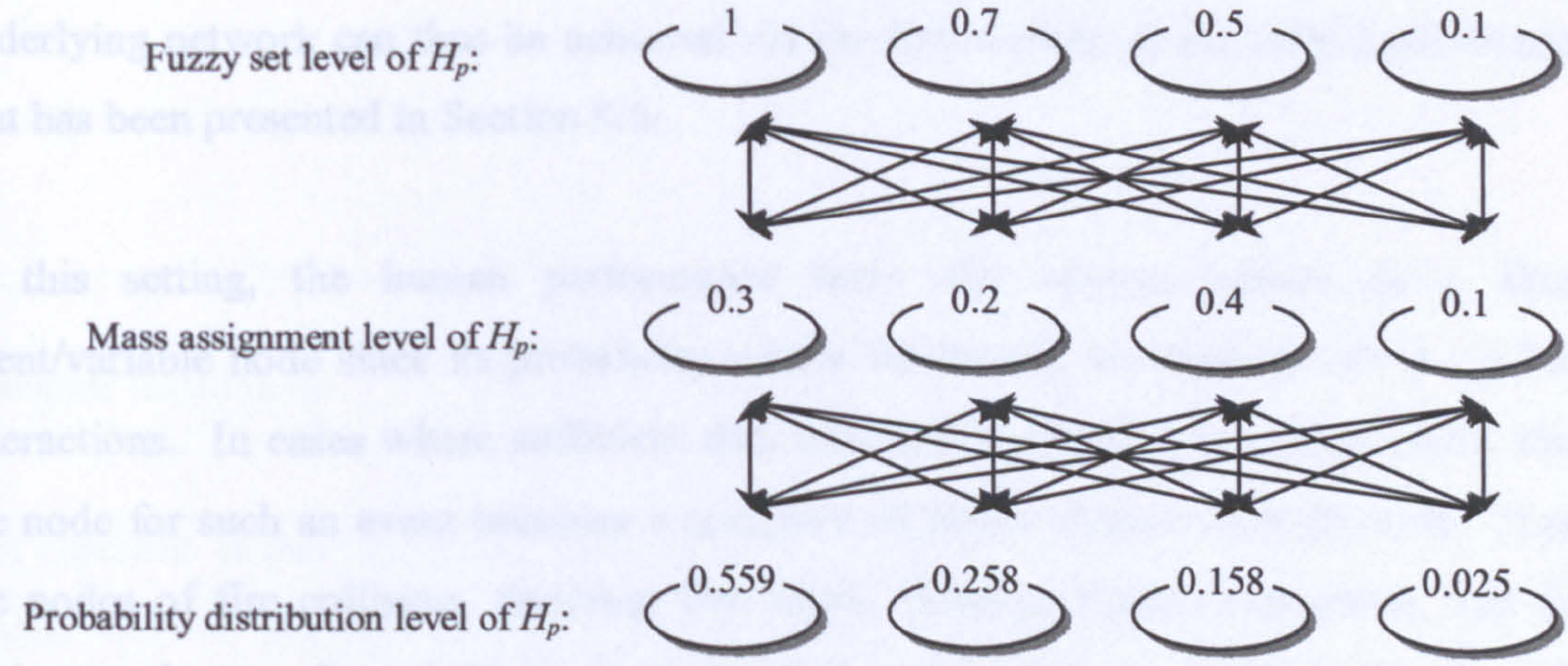


Figure 8.13: Levels and values in the bi-directional processed human performance output, H_p

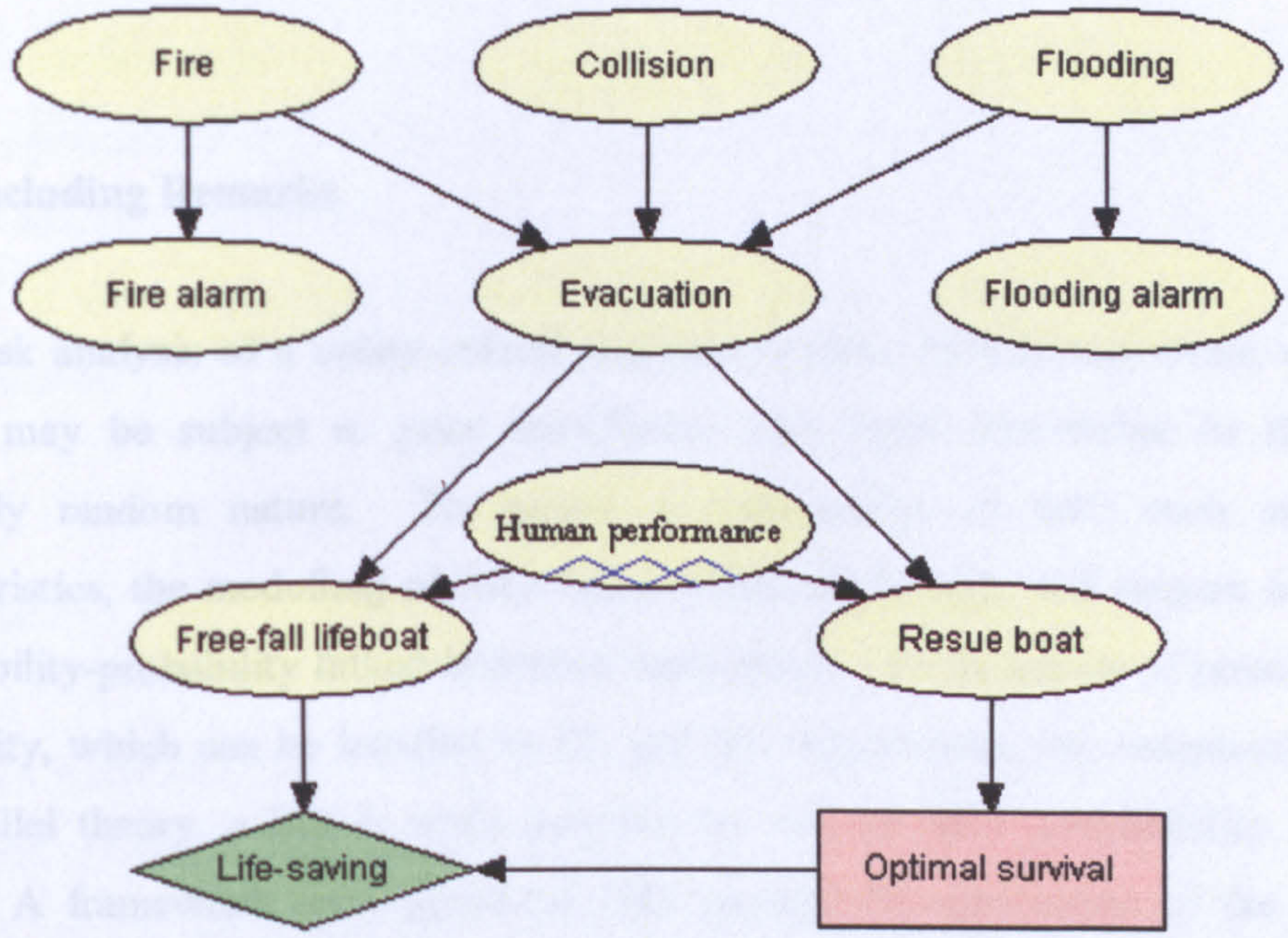


Figure 8.14: A FBN of a marine evacuation analysis domain

The subject here is not on human performance alone, but rather on the modelling of the interaction between humans and EER physical systems. As such, in following from the case study of the marine evacuation scenario as already analysed in Chapter 6, Section 6.7.1, the fuzzy event of human performance element (such as the H_p output example that has been analysed in this section) can be added and linked as a new node that has an effect on both free-fall lifeboat and rescue boat launch. In so doing, a FBN

as shown in Figure 8.14 is obtained. The probabilistic cause-effect analysis of this underlying network can thus be achieved via the BN module of the FBN methodology that has been presented in Section 8.6.

In this setting, the human performance node will always remain as a fuzzy event/variable node since its probability cannot be directly ascertained unless via PSF interactions. In cases where sufficient data becomes available for a fuzzy event, then the node for such an event becomes a complete Bayesian chance variable node. Thus, the nodes of fire collision, flooding, fire alarm, flooding alarm, evacuation, free-fall lifeboat and rescue boat in Figure 8.14 are all Bayesian chance variable node. The life-saving node and the optimal survival node represent the standard utility node and decision node respectively that aids in achieving the decision-making aspect of the model.

8.8 Concluding Remarks

In the risk analysis of a safety-critical maritime system, each hazard event within the domain may be subject to prior insufficient and vague knowledge or that of an inherently random nature. To permit a combination of both such uncertainty characteristics, the modelling of their cause-effect relationship will require some form of possibility-probability linked inference mechanism. As the theory of possibility and probability, which can be handled by FL and BN respectively, are completely distinct but parallel theory, a link is made possible by way of their compatibility with MA theory. A framework for a proposed FBN permits the application of the inference algorithm whilst, justifying for data problem cases and at the same time, aiding to provide a proficient graphical tool for risk-based decision-making of the model. Incorporation of the human element into maritime risk assessment is an area prone to benefit from the combined use of fuzzy and Bayesian principle as a causal network solution. Furthermore, the hypothetical human performance outcome case study has demonstrated how the fuzzy PSFs can be incorporated into any random processing risk-based model. Therefore, the usefulness of the FBN modelling should offer a sound means for improving safety knowledge/assessments/practices in the marine and offshore industry.

Chapter 9: Conclusion

Chapter Summary

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. Thus, this chapter revisits the goals achieved in this thesis and expresses its key findings. It also outlines those areas for further work as based on the major limitations to the research.

9.1 Review

Before the scene of this thesis was set, the background work had revealed safety in the marine and offshore industry as previously a case of being a reactive response to major accidents. A change in such culture provided for proactive approaches to be applied, and one that takes into consideration near misses and incident occurrences. These approaches, which are safety case (SC) for the offshore industry and formal safety assessment (FSA) for the marine industry, were thus reviewed. On the basis of the reviewed SC and 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 (as reported in Chapter 1). The framework incorporates risk analysis for which data were obtained from industrial databases and/or by expert

judgement (as reported in Chapter 2), and for which safety and reliability analytical tools and techniques (as reported in Chapter 3) were applied to generate domain models.

The concept of FSA was particularly examined as it provides an elegant route to the application of the well-established risk analysis methods that are already widely used in other industries within shipping activities. The developments in the risk analysis study of the FSA trial application to generic high speed passenger catamaran ferries (HSC) and bulk carrier (BC) ships were then briefly reviewed. This revealed that issues such as uncertainty treatment and the human element issue were still left unresolved in the advancement of the approach (as reported in Chapters 4 and 5). Thus, such unresolved issues were facilitated into maritime application domains of risk-based analytical reasoning. Bayesian network (BN) was adopted as the modelling that dealt with the random/inherent uncertainties and also enabled a powerful marine and offshore decision-support solution (as reported in Chapter 6). Fuzzy logic (FL) was utilised as the modelling tool that dealt with the vague/subjective uncertainties towards evidential reasoning synthesis in maritime engineering safety analysis (as reported in Chapter 7). As cases of both types of uncertainties are always recurrent in maritime human element issue, the excellent features of BN and FL modelling tools were therefore combined via the theory of mass assignment for the development of an advanced network-modelling tool. This network was given the name 'fuzzy-Bayesian network' and furthermore, a case study was demonstrated for the incorporation of human error into safety assessments (as reported in Chapter 8).

In following this 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 at the onset of the thesis and therefore, they may effectively be integrated into both the SC and the FSA approach.

9.2 Principal Findings

The undertaken research in this thesis have resulted in the following key findings that may reflect salient issues:

- The exponential distribution, which arises in the calculations of reliability, is particularly convenient for the risk-based mathematical modelling, because it implies a fixed rate of occurrence. This distribution is intimately linked with the discrete Poisson distribution. In fact, it is similar to Poisson distribution when the occurrence of the event is zero (clarify from Equations 2.3 and 2.5) and since the distribution of intervals between successive occurrences is exponential, the Poisson distribution is stationary.

- 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 offshore SC and marine FSA are appropriate proactive approaches 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. Despite the fact that they can integrate the application of both well-established and the developed (e.g., BN and FL) risk analysis methods in a transparent and justifiable manner, the trial application of FSA to HSC and BC ships have utilised just the most widely used well-established methods of mainly fault tree, event tree and RCT, and thus, have falling short of the unrivalled handling for the different types of uncertainties present in each study.

- In dealing with aleatory (i.e., random/inherent) uncertainties for safety-critical marine and offshore systems may be best handled by the probabilistic analysis of probability theory and Bayes' theory, whilst its epistemic (i.e., vague/subjective) uncertainties could best be handled by the possibilistic analysis of possibility theory and fuzzy set theory. Inference processes between both types of uncertainty in risk-based models can be enabled effectively via reasoning evidentially by way of the Dempster-Shafer theory and/or the theory of mass assignment.

- In FL risk-based analytical modelling that has been applied to offshore collision risk scenario between a floating, production, storage and offloading (FPSO) installation and a shuttle tanker, fuzzy set theory has provided a convenient framework for representing uncertainty, both in data and knowledge, in a manner that can be appreciated by the non-mathematical domain expert. However, the approach requires sufficient expert knowledge for the formulation of the rule-base, the combination of sets and the evidential reasoning approach, which emerges as a better preference to defuzzification in the safety assessment study. The input-output mappings of the FL model provided an intuitive insight that may not have been relevant from a theoretical viewpoint, but in practice have been well worth using.

- Results from the BN risk-based analytical modelling that were undertaken for both an offshore FPSO installation collision scenario and a typical ship evacuation scenario case studies do indicate that BNs are promising techniques for maritime risk analysis. These BNs can also be expanded to form influence diagrams, which permits rapid development of a practical decision model. Thus, BN is an integrative model that can be used effectively within the existing SC and FSA decision-making process. Via the theory of mass assignment, FBN (a developed combination model of BN and FL) has better still been found to intuitively and realistically integrate the human element into the decision-making process.

These findings of the research do suggest that multiple dimensions of risk-based analytical modelling can be incorporated into the safety assessment and also decision model framework for any marine and offshore safety-critical units/systems.

9.3 Major 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 ships and offshore installations. These limitations include the following:

- Eliciting conditional probabilities is more difficult, especially if the probability is conditioned on several states. Besides, many of such probabilities required to quantify a BN cannot be derived from databases and scientific literature, so they may need to be elicited 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 or FL risk-based reasoning to be enabled. All case study data 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 only to the safety of people.

- Sensitivity analysis is generally deterministic and limited to one- and two-way analyses. Thus, only a partial sensitivity analysis could be conducted for the ship evacuation scenario BN case study. The impact of uncertainty in the input parameters has somewhat been expressed in the context of variance, i.e., ±20% change.

- Reliable data for incorporating the human element performance shaping factors (PSFs) into safety assessment is scarce. For this reason, full-scale FL modelling

of human performance PSF was not feasible and therefore, it was considered viable to utilise a hypothetical example in demonstrating the practical applicability of a FBN risk-based analytical model.

These limitations did not mitigate the efficacy 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. Suggestions can be made for further research where appropriate, e.g. the incorporation of human element, but this is not often a major requirement for the other cases.

9.4 Future Work

As based on the key findings and major limitations of this research, further work required in the areas which are related to the integrative of risk-based analytical modelling developed in this thesis for application its to safety-critical marine and offshore systems is described the following subsection.

9.4.1 Formal Process for Eliciting Expert Opinion

Expert opinion/judgement has always played a large role in science and engineering. Increasingly, this opinion/judgement is recognised as just another type of analytical information, data or evidence, and expert elicitation methods are developed to treat these as such. The Delphi technique (Helmer, 1969) is one such method for combining expert opinion preferences (weights) that are obtained through anonymous questionnaires, controlled feedback, and statistical analysis. Another combination approach is to use analytic hierarchy process pairwise comparisons (Saaty, 1980) with regards to information about the experts' qualifications. Through this later technique, the relative importance, or weights, of different factors can be measured and also, tradeoffs between objectives are explicitly considered in these pairwise comparisons. Overall, these elicitation techniques may provide the formal heuristic process that can be used in the safety assessment of a maritime application domain to gather information about model input parameters, model processes and on output change impacts.

9.4.2 Development of Linguistic Database

As the application of database technology moves outside the realm of a crisp mathematical world to the realm of the real world, the need to handle imprecise information becomes important, because a database that can handle imprecise information shall store not only raw data but also related information that shall allow us to interpret the data in a much deeper context (Bedi, *et al.*, 2002), e.g. a Structured Query Language (SQL) query (Galindo, *et al.*, 1998) "Which crew is young and has sufficiently good training grades?" captures the real intention of the user's query than a crisp query as:

```
SELECT * FROM CREW
WHERE AGE < 19 AND GPA > 3.5
```

GPA is '*grade point average*'.

Such a SQL technology can have wide applications in areas such as maritime human reliability, security, FSA of ballast water management and for near misses and errors event as the industry heads in the proactive risk-based direction because in such areas subjective and uncertain information is not only common but also extremely useful by the likes of experts, risk analysts and decision-makers. The developed database of this nature can enable a justified qualitative risk assessment. It can highly promote and, at the same time, ease the use possibility theory and fuzzy linguistic knowledge, and enable its transmission into that of a probability domain.

9.4.3 Petri Net Dynamic Modelling

Petri net is well known for its capability in modelling discrete event systems in terms of cause-consequence relationships possibly extended by timing information related to the underlying dynamic system variations. A Petri net is a directed graph with two kinds of nodes, places and transitions, and with arcs that run either from places to transitions or from transitions to places. The state of the Petri net is indicated by the presence of

tokens in one or more places, and a token moves from one place to another when a transition fires (Murata, 1989). The occurrence of an event is modelled by the firing of the corresponding transition. Petri nets are capable of describing the dynamic behaviour of process systems and handle the hierarchy. A RCT can form the basis for the hierarchy and therefore its analytical process may additional be useful for inspection and ultimately for reliability-centred maintenance.

9.4.4 Environment Protection Case Study

The developed risk-based methodologies can be expanded to tackle areas of environmental concerns such as those that lead to oil spillage, e.g., via FSA study of oil tankers and ballast water risk assessment, on a large scale. Evidence of oil tanker concern can be seen in Table 1.1 in which grounding, stranding and the loss of structural integrity has caused oil spillage to the sea. Other serious consequences for due consideration in oil tanker FSA can be that of dangerous gas release. Ballast water discharge may also expose the sea and its creatures to such dangerous release.

To achieve better ship-handling characteristics, ballast is necessary for the safe operation of ships of all types. Prior to entering a port, the ballast of seawater will usually be discharged thus introducing the risk of harmful alien species invasion into that region of its discharge. With no historical database for detailing species assemblages under specific ballasting conditions, ballast water risk assessment can utilise FLs, BNs and FBNs in its application to the non-native introductions. The risk assessment should proceed in a species and site specific manner and seek to develop an in-depth understanding of the life-history of species a prior considered hazard, expressed through a series of bio-rules for these species (Hayes, 1998).

9.4.5 Multiple Sensitivity Analysis

Sensitivity analysis in BNs is broadly concerned with understanding the relationship between local network parameters and global conclusions drawn based on the network (Castillo, et al., 1997; Kaerulff & Van der Gaag, 2000; Laskey, 1995). A key aspect of

sensitivity analysis is the number of considered parameters (Chan, & Darwiche, 2004). The simplest case involves one parameter at a time, i.e., one can only be allowed to change a single parameter 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. This is significant since multiple parameter changes can be more meaningful, and may disturb the probability distribution less significantly than single parameter changes (Chan, & Darwiche, 2004).

9.5 General Industrial Application of the Developed Methodologies

When it comes to proactively ensuring maritime safety and environmental protection at the highest level, it is the practical industrial application of the developed methodologies in this thesis that matters. Any such practical application can thus be examined through the exploration of a specific case study of relevance to the safety-critical marine and offshore system/unit and via the use of the most reliable real-life data and competent expert judgment.

9.6 Concluding Remarks

Overall, the thesis have 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, FL and FBN were developed to provide powerful tools for uncertainty treatment. FBN was also utilised for demonstrating the incorporation of the human element into a safety assessment task.

The thesis has revealed six principal findings and five main limitations of the research conducted. As such recommendations for further work were made in the areas of utilising a formal process for eliciting expert opinion, developing a linguistic database,

modelling with Petri nets, ensuring safety assessments of environmental nature and conducting multiple sensitivity analysis. The practicality of the developed methodologies can be justified for the safety assessment of real-life marine and offshore applications.

References

ABS (2000), *Guidance Notes on Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries*, American Bureau of Shipping (ABS), June, Houston, USA.

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.

Andrews, J. D. & Moss, T. R. (1993), *Reliability and Risk Assessment*, ISBN: 0-582-09615-4, Longman Scientific and Technical, Harlow, UK.

Andrews, J. D. & Ridley, L. M. (2001), *Reliability of Sequential Systems Using the Cause-Consequence Diagram Method*, Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, Vol. 215, No. 3, Pp. 207-220, ISSN: 0954-4089, Professional Engineering Publishing.

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, Issue 2, Pp. 99.

Baldwin, J. F. (1991), *Symbolic and Quantitative Approaches to Uncertainty*, Kruse, R. & Siegel, P. (Eds.), Lecture Notes in Computer Science 548, Springer-Verlag: Berlin, Pp. 107-115.

Baldwin, J. F. (1992), *The Management of Fuzzy and Probabilistic Uncertainties for Knowledge Based Systems*, in: Shapiro, S. A. (Ed.), Encyclopaedia of Artificial Intelligence, Wiley, New York, Pp. 528-537.

Baldwin, J. F. (1996), *Knowledge From Data Using Fuzzy Methods*, Pattern Recognition Letters, Vol. 17, No. 6, Pp. 593-600.

Baldwin, J. F., Lawry, J. & Martin, T. P. (1996), *A Mass Assignment Theory of the Probability of Fuzzy Events*, Fuzzy Sets Systems, Vol. 83, Pp. 353-367.

Baldwin, J. F., Martin, T. P. & Pilsworth, B. W. (1995), *FRIL - Fuzzy and Evidential Reasoning in Artificial Intelligence*, Research Studies Press, Wiley, New York.

Bayes, T. (1763), *An Essay Towards Solving a Problem in the Doctrine of Chances*, Philosophical Transactions of the Royal Society of London, Vol. 53, Pp. 370-418.

Bedi, P., Kaur, H. & Malhotra, A. (2002), *Fuzzy Dimension to Databases*, Harnessing and Managing Knowledge, 37th National Convention of Computer Society of India, 26 October to 2 November, Bangalore, India.

Bell, P. M. & Badiru, A. B (1996), *Fuzzy Modelling and Analytic Hierarchy Processing to Quantify Risk Levels Associated with Occupational Injuries – Part I: The Development of Fuzzy-Linguistic Risk Levels*, IEEE Transactions on Fuzzy Systems, Vol. 4, No. 2, Pp. 124-131.

Bercha, F. G., Brooks, C. J. & Leafloor, F. (2003), *Human Performance in Arctic Offshore Escape, Evacuation and Rescue*, The Proceedings of the 13th International Offshore and Polar Engineering Conference, Volume IV, 25-30 May, Honolulu, Hawaii, USA, ISBN: 1-880653-60–5.

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

Boring, R. L. & Gertman, D. I. (2004), *Human Error and Available Time in SPAR-H*, Conference on Human Factors in Computing Systems, INEEL/CON-04-01630, 24-29 April, Vienna, Austria.

Bozzano, M. & Villafiorita, A. (2003), *Integrating Fault Tree Analysis with Event Ordering Information*, Proceedings of ESREL 2003, 15-18 June, Pp. 247-254, Maastricht, The Netherlands.

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, Larsson, T. J. & Hale, A. R. (Eds), Vol. 4, Issue 1, Article 3, ISSN: 1443-884.

Brennan, E. G. & Peachey, J. H. (1996), *Recent Research into Formal Safety Assessment For Shipping*, Lloyds Register Technical Association.

Broadbent, D. E. (1975), *The Magic Number Seven After Fifteen Years*, In. Kennedy, A and Wilkes, A. (Eds.), Studies in Long-Term Memory, New York: Wiley, Pp. 3-18.

Brown, A. J. & Amrozowicz, M. (1996), *Tanker Environmental Risk - Putting the Pieces Together*, Joint SNAME/SNAJ Conference on Designs and Methodologies for Collision and Grounding Protection of Ships, San Francisco, USA.

Cacciabue, C. (1997), *Human Reliability Assessment: Methods and Techniques*, In Redmill, F. & Rajan, J. (Eds): Human Factors in Safety-critical Systems, Pp.66-96. ISBN: 0-7506-2715-8, Butterworth-Heinemann, London, UK.

Canter, P. (1997), *Formal Safety Assessment – A Progress Report*, Seaways, September, Pp. 15-23.

Castillo, E., Gutiérrez, J. M. & Hadi, A. S. (1997), *Expert Systems and Probabilistic Network Models*, Springer-Verlag, New York, USA, ISBN 0-387-94858-9.

Castillo, E., Gutiérrez, J. M. & Hadi, A. S. (1997), *Sensitivity Analysis in Discrete Bayesian Networks*. IEEE Transactions on Systems, Man, and Cybernetics, Part A (Systems and Humans), Vol. 27, Pp. 412-423.

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

Chan, H. & Darwiche, A. (2004), *Sensitivity Analysis in Bayesian Networks: from Single to Multiple Parameters*, Proceedings of the 20th Conference on Uncertainty in Artificial Intelligence, Banff, Canada, Vol. 70, Pp. 67-75, ISBN: 0-9749039-0-6, AUAI Press, Arlington, Virginia, USA.

Chauhan, S. S. & Bowle, D. S. (2003), *Dam Safety Risk Assessment with Uncertainty Analysis*, Proceedings of the Australian Committee on Large Dams Risk Workshop, October, Launceston, Tasmania, Australia.

Chen, H. & Moan, T. (2002), *Collision Risk Analysis of FPSO-Tanker Offloading Operation*, OMAE2002-28103, Proceedings of the 21st OMAE Conference, 23-28 June 2002, Oslo, Norway.

Chen, S., Nikolaidis, E, & Cudney H. H. (1999), *Comparison of Probabilistic and Fuzzy Set Methods for Designing under Uncertainty*, In Proceedings of the 40th American Institute of Aeronautics and Astronautics (AIAA) Structures, Structural Dynamics, and Materials Conference, AIAA-1999-1579, 12-15 April, St. Louis, Missouri, USA.

Chou, K. C. & Yuan, J. (1993), *Fuzzy-Bayesian Approach to Reliability of Existing Structures*, Journal of Structural Engineering, November, Vol. 119, No. 11, Pp. 3276-3290.

CIA (1977), *A Guide to Hazard and Operability Studies*, Chemical Industry Safety, Health and Environment Council (CISHEC) CISHEC/8906/1000, Chemical Industries Association (CIA) Ltd, London, UK.

Clark, D. F. & Kandel, A. (1990), *Fuzzy Belief Networks*, Proceedings of the ACM SIGSMALL/PC Symposium on Small systems, Crystal City, Virginia, USA, Pp. 246-248, ACM Press, New York, USA, ISBN: 0-89791-347-7.

Coggin, R. (2001), *FMEA Annual Trials and Experience of the Ocean Intervention*, Dynamic Positioning Conference, 18-19 September, Houston, USA.

Corana, A., Marchesi, M., Martini, C. & Ridella, S. (1987), *Minimizing Multimodal Functions of Continuous Variables With the 'Simulated Annealing' Algorithm*, ACM Transactions Mathematical Software, Vol. 13, No. 3., Pp. 262-280.

Cortazar, G. & Schwartz, E. S. (1998), *Monte Carlo Evaluation Model of an Undeveloped Oil Field*, Journal of Energy Finance & Development, Vol. 3, Issue 1, Pp. 73-84.

Coutinho, J. S. (1964), *Failure-Effect Analysis*, Transactions of the New York Academy of Sciences, Vol. 26, Pp. 564-584.

D'Ambrosio, B. (1999), *Inference in Bayesian Networks*, Artificial Intelligence Magazine, Vol. 20. No. 2. Pp. 21-36.

Dearden, A. M. & Harrison, M. D. (1996), *Impact and the Design of the Human-Machine Interface*, In Compass 96, Proceedings of the 11th International Conference on Computer Assurance, Pp 161-170, ISBN: 0-7803-3390-X, Piscataway, New Jersey, USA.

Delgado, M., Herrera, F., Herrera-Viedma, E. & Martinez, L. (1998), *Combining Numerical and Linguistic Information in Group Decision Making*, Journal of Information Sciences, Vol. 107, Pp. 177-194.

DOE (1990), *The Public Enquiry into the Piper Alpha Disaster (Cullen Report)*, ISBN: 0-10-113102, Department of Energy (DOE), HMSO: London, UK.

Dixon, P. (1964), *Decision Tables and Their Applications*, Computer and Automation, Vol. 13, No. 4, Pp. 376-386.

DNV (1992), *OREDA - Offshore Reliability Data Handbook*, 2nd Edition, DNV Technica, Norway.

DOD (1969), *System Safety Program Requirements*, Military Standard MIL-STD-882, 15 July, Department of Defense (DOD), Washington, DC, USA.

DOD (1980), *Procedures for Performing a Failure Mode, Effects and Criticality Analysis*, Military Standard MIL-STD-1629A, 24 November, Department of Defense (DOD), Washington DC, USA.

DOD (1995), *Reliability Prediction of Electronic Equipment*, Military Handbook MIL-HDBK-217F, Notice 2, 28 February, Department of Defense (DOD), Washington DC, USA.

DOD (2000), *Standard Practice for System Safety*, Military Standard MIL-STD-882D, 10 February, Department of Defense (DOD), Washington, DC, USA.

Dougherty, E. M. Jr (1990), *Human Reliability Analysis - Where Shouldst Thou Turn?*, Journal of Reliability Engineering and System Safety, Vol. 29, Pp. 283-299.

Dubois, D. & Prade H. (1988), *Possibility Theory: An Approach to Computerized Processing of Uncertainty*, New York, ISBN: 0-306-42520-3.

Dubois, D. & Prade, H. (1993), *Fuzzy Sets and Probability: Misunderstandings, Bridges and Gaps*, In Proceedings of the 2nd EEE International Conference on Fuzzy Systems, San Francisco, CA, 28th March –1st April, Vol. 2, Pp. 1059-1068.

Dubois, D. & Prade, H. (1997), *Bayesian Conditioning in Possibility Theory*, Fuzzy Sets and Systems, 1 December, Vol. 92, Issue 2, Pp. 223-240, ISSN: 0165-0114, Elsevier North-Holland, Inc, Amsterdam, The Netherlands.

Edwards, A. W. F. (1992), *Likelihood*, ISBN: 0801844436, Johns Hopkins University Press, Baltimore, USA.

Embrey, D. E., Humphreys, P. C., Rosa, E. A., Kirwan, B. & Rea, K. (1984), *SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement*, Technical Report NUREG/CR 3518, Brookhaven National Laboratory, New York, USA.

EPA (1996), *Proposed Guidelines for Ecological Risk Assessment*, US Environmental Protection Agency (EPA) Notice, Federal Register, FRL-5605-9, Vol. 61, No. 175, Pp. 47551-47631, 9 September, Washington, DC, USA.

EPSMA (2004), *Guidelines to Understanding Reliability Prediction*, 13 October, European Power Supply Manufacturers Association (EPSMA), Northants, UK.

FAA (2005), *Guide to Reusable Launch and Reentry Vehicle Reliability Analysis*, Version 1.0, April, Federal Aviation Administration (FAA), Washington DC, USA.

Farmer, F. R. (1967), Siting *Criteria: A New Approach*, Proceedings of the International Atomic Energy Agency Symposium on the Containment and Sting of Nuclear Power Plants, 3-7 April, Paper IAEA SM-89/34, Pp. 303-329, Vienna, Austria.

Fisher, R. A. (1922), *On the Mathematical Foundations of Theoretical Statistics*, Philosophical Transactions of the Royal Society, Series A, Vol. 222, Pp. 309-368.

Frank, M. V. (2000), *Case Studies of Uncertainty Analysis in Reliability and Risk Assessment*, Tutorial Notes for the 2000 Annual Reliability and Maintainability Symposium, January, Institute of Electrical and Electronic Engineers, ISSN: 0897-5000.

French, S. (1988), *Decision Theory: An Introduction to the Mathematics of Rationality*, ISBN: 0-470-21091-5, John Wiley and Sons, New York, USA.

Frühwirth-Schnatter, S. (1993), *On Fuzzy Bayesian Inference*, Fuzzy Sets and Systems, 25 November, Vol. 60, Issue 1, Pp. 41-58.

Fussel, J. B. (1973), *Synthetic Tree Model - Formal Methodology for Fault Tree Construction*, ANCR-1098, March, Spring Field, VA, USA.

Galindo, J., Medina, J. M., Pons, O. & Cubero, J. C. (1998), *A Server for Fuzzy SQL Queries*, Proceedings of the 3rd International Conference on Flexible Query Answering Systems, Andreasen, T., Christiansen, H. & Larsen, H. L. (Eds), Lecture Notes in Computer Science, Vol. 1495, Pp. 164-174, ISBN: 3-540-65082-2, Springer-Verlag, London, UK.

Gámez, J. A., Serafin, M. & Salmerón, A. (2004), *Advances in Bayesian Networks*, Series: Studies in Fuzziness and Soft Computing, Vol. 146, ISBN: 3-540-20876-3, Springer.

Gerdes, V. G. J. (1995), *HRA Techniques: A Selection Matrix*, Journal of Microelectronics and Reliability, Vol. 35, No. 9/10, Pp.1215-1231.

Gertman, D. I. (1993), *Representing Cognitive Activities and Errors in HRA Trees*, Journal of Reliability Engineering and System Safety, Vol. 39, Pp. 25-34.

Gertman, D. I., Blackman, H. S., Haney, L. N., Seidler, K. S. & Hahn, H. A. (1992), *INTENT: A Method for Estimating Human Error Probabilities for Decision-Based Errors*, Journal of Reliability Engineering and System Safety, Vol. 35, Pp. 127-136, Elsevier Science Publishers Ltd.

Gertman, D., Blackman, H., Marble, J., Byers, J., Haney, L. & Smith, C. (2004), *The SPAR-H Human Reliability Analysis Method*, US Nuclear Regulatory Commission.

Goodman, I. R. & Nguyen, H. T. (1985), *Uncertainty Models of Knowledge Based Systems*, North-Holland: Amsterdam.

Graham I. & Jones P. L. (1988), *Expert Systems: Knowledge, Uncertainty and Decision*, Chapman and Hall, New York, ISBN: 0-412-28510-X.

Groen, F. J. & Mosleh, A. (2001), *Principles of Uncertain Evidence in the Context of a Failure Rate Assessment Problem*, University of Maryland, College Park, MD 20740, USA.

Groumpos, P. P. & Merkuryev, Y. (2002), *A Methodology of Discrete-Event Simulation of Manufacturing Systems: An Overview*, Studies in Informatics and Control, March, Vol. 11, No. 1, Pp 53-60.

Halebsky, M. (1989), *System Safety Engineering as Applied to Ship Design*, Marine Technology, Vol. 26, No. 3, Pp. 245-251.

Hall, R. E., Fragola, J. R. & Wreathall, J. (1982), *Post Event Human Decision Errors: Operator Action Tree/Time Reliability Correlation*, Technical Report NUREG/CR 3010, Nuclear Regulatory Commission (NRC), Washington DC, USA.

Halpern, J. Y. & Fagin, R. (1992), *Two Views of Belief: Belief as Generalized Probability and Belief as Evidence*, Artificial intelligence, April, Vol. 54, Issue 3, Pp. 275-317, ISSN: 0004-3702, Elsevier Science Publishers Ltd, Essex, UK.

Hannaman, G. W., Spurgin, A. J. & Lukic, Y. D. (1984), *A Model for Assessing Human Cognitive Reliability in PRA Studies*, Technical Report NUS 4531, Electrical Power Research Institute (EPRI), California, USA.

Hansen, K. K., Rogdar, S. O. & Sørby, K. (2002), *Risk Assessment of Safety Critical Systems - An Approach Using LEGO Mindstorms for Prototyping*, NTNU Technical Report, 22 November, Norwegian University of Science and Technology (NTNU), Norway.

Harms-Ringdahl, L. (2001), *Safety Analysis: Principles and Practice in Occupational Safety*, 2nd Edition, ISBN: 041523655X, Taylor & Francis, London, UK.

Hauge, H. J. (2001), *A Survey of Software Safety*, NTNU Technical Report, 23 November, Norwegian University of Science and Technology (NTNU), Norway.

Hayes, K. R. (1998), *Bayesian Statistical Inference in Ecological Risk Assessment*, Crimp Technical Report Number 17, November, Centre for Research on Introduced Marine Pests, CSIRO, Hobart, Australia.

Heckerman, D., Mamdani, A., & Wellman, M, eds. (1995), *Real-World Applications of Bayesian Networks*, Communications of the ACM, Vol. 38, No. 3, Pp. 49-57.

Heinrich, H. W. (1931), *Industrial Accident Prevention*, McGraw Hill Books, New York, USA.

Helgøy, K (Navion ASA), *Private Communication Regarding Tandem Offloading Operations in the North Sea*, February 2002, Stavanger, Norway.

Helmer, O. (1969), *Analysis of the Future: The Delphi Method*, Rand Corporation, Santa Monica, California, 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, 2-3 December, Houston, USA.

Henley, E. J. & Kumamoto, H. (1981), *Reliability Engineering and Risk Assessment*, ISBN: 0137722516, Prentice Hall, Englewood Cliffs, New Jersey, USA.

Henley, E. J. & Kumamoto, H. (1992), *Probabilistic Risk Assessment*, The Institute of Electrical and Electronics Engineers (IEEE) Press, New York, USA.

Hisdal, E. (1994), *Interpretative Versus Prescriptive Fuzzy Set Theory*, IEEE Transactions Fuzzy Systems, Vol. 2, No. 1, Pp. 22-26.

HM Treasury (1997), *The Green Book - Appraisal and Evaluation in Central Government*, HMSO London, UK.

Hollnagel, E. (1994), *Human Reliability Analysis: Context and Control*, Computers and People Series, ISBN: 0123526582, Academic Press, London, UK.

Hollnagel, E. (1996), *Reliability Analysis and Operator Modelling*, Journal of Reliability Engineering and System Safety, Vol. 52, Pp. 327-337.

Hollnagel, E. (1998), *Cognitive Reliability and Error Analysis Method: CREAM*, ISBN: 0-08042-848-7, Elsevier Science, Oxford, UK.

House of Lords (1992), *Safety Aspects of Ship Design and Technology*, Select Committee on Science and Technology, 2nd Report, HL Paper 30-1, February, HMSO, London, UK.

HSC (2004), *Consultative Document 198: Proposals to Replace the Offshore Installations (Safety Case) Regulations 1992*, C20, June.

HSE (1992), *Tolerability of Risk from Nuclear Power Stations*, HMSO, London, UK.

HSE (1998), *A guide to the Offshore Installations (Safety Case) Regulations 1992*, L30, 2nd Edition, HSE Books, ISBN: 0-7176 1165 5.

HSE (1999), *Health & Safety Executive Offshore Technology Report - OTO 1999 080: Ship/Platform Collision Incident Database (1997)*, November, UK.

HSE (2001), *Reducing Risks, Protecting People - HSE's Decision-Making Process*, HSE Books, ISBN: 0-7176-2151-0.

HSE (2002), *Marine Risk Assessment*, Offshore Technology Report 2001/063, Prepared by Det Norske Veritas (DNV), HSE Books, ISBN: 0-7176 2231-2.

HSE (2003), *Transport Fatal Accidents and FN-Curves: 1967-2001*, Research Report 073, HSE Books, ISBN: 0-7176-2623-7, HMSO.

Humphreys, P. (1995), *Human Reliability Assessor's Guide*, Human Factors in Reliability Group, Report SRDA - R11, AEA Technology, UK.

Husky Oil (2000), *White Rose Oilfield Development Application: Assessment of Ship Impact Frequencies*, Vol. 5 Part Two (Concept Safety Assessment), 31 July, Husky Oil Operations Limited, Calgary, Alberta, Canada.

IEC (2005), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - ALL PARTS*, International Standard IEC 61508-SER, Edition 1.0, 20 January, International Electrotechnical Commission (IEC), Geneva, Switzerland.

IMarE (1997), *Marine Risk Assessment – A Better Way to Manage Your Business*, The Institute of Marine Engineers (IMarE) Conference Proceedings, 8-9 May, London, UK.

IMCA (2002), *Guidelines on Failure Modes and Effects Analyses (FMEAs)*, International Marine Contractors Association (IMCA), IMCA M 166, April, London, UK.

IMO (1996), *Formal Safety Assessment*, MSC 66/INF.8, Submitted by the United Kingdom to IMO Maritime Safety Committee, London.

IMO (1997a), *Interim Guidelines for the Application of Formal Safety Assessment (FSA) to the IMO Rule-making Process*, MSC/Circ.829 and MEPC/Circ.335, 17 November.

IMO (1997b), *Formal Safety Assessment Guidelines Adopted*, Maritime Safety Committee 68th session (MSC68), 28 May to 6 June.

IMO (1997c), *Formal Safety Assessment Trial Application to High Speed Passenger Vessels*, Submitted by the United Kingdom to the FSA Working Group, MSC 68/INFORMAL PAPER, 27 May.

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 14, 12 February.

IMO (1999), *Resolution of the 1997 SOLAS Conference Relating to Bulk Carrier Safety*, Series ID: IMO-160E, ISBN: 92-801-6101-6, IMO London, UK.

IMO (2001a), *Focus on IMO: A Summary of IMO Conventions*, April, London, UK.

IMO (2001b), *Formal Safety Assessment of Bulk Carriers Fore-end Watertight Integrity*, Submitted by IACS to IMO, MSC 74/5/4, 31 May.

IMO (2002a), *Formal Safety Assessment of Bulk Carrier Safety*, Submitted by Japan to IMO Maritime Safety Committee, MSC75/5/2, 12 February.

IMO (2002b), *Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process*, MSC Circ.1023/MEPC Circ.392, 5 April.

IMO (2002c), *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, 12 March.

IMO (2004), *Formal Safety Assessment Risk Evaluation*, Submitted by the International Association of Classification Societies (IACS), MSC 78/19/2, 5 February.

INCOSE/PMI (2002), *Universal Risk Project Final Report*, the International Council on Systems Engineering (INCOSE) Risk Management Working Group (RMWG) and the Project Management Institute (PMI) Risk Significant Interest Group (SIG), Program Report Section 2-01, February.

Itoh, S. & Itagaki, H. (1989), *Applications of Fuzzy-Bayesian Analysis to Structural Reliability*, In Proceedings of ICOSSAR'89, the 5th International Conference on Structural Safety and Reliability, 7-11 August, San Francisco, CA, USA, Vol. 3, Pp. 1771-1774.

ITOPF (2005), *Oil Tanker Spill Statistics: 2004*, Oil Spill Database Information Pack, The International Tanker Owners Pollution Federation (ITOPF) Ltd, London, UK.

Jensen, F. V. (1993), *Introduction to Bayesian Networks: HUGIN*, Aalborg University Press, Denmark.

Jensen, F. V., Lauritzen, S. L. & Olesen, K. G. (1990), *Bayesian Updating in Causal Probabilistic Networks by Local Computations*, Computational Statistics Quarterly, Vol. 4, Pp. 327-352.

Jensen, F., Jensen, F. V. & Dittmer, S. L. (1994), *From Influence Diagrams to Junction Trees*, Proceedings of the 10th Conference on Uncertainty in Artificial Intelligence, Pp. 367-373, Mántaras, R. L. & Poole, D. (Eds.), Morgan Kaufmann, San Francisco, USA.

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, July, Microsoft Corporation, Redmond, USA.

Kærulff, U & Van der Gaag, L. C. (2000), *Making Sensitivity Analysis Computationally Efficient*, In Proceedings of the 16th Conference on Uncertainty in Artificial Intelligence (UAI), San Francisco, California, Pp. 317-325, Morgan
Kaufmann Publishers.

Kahn, J. M. (2004), *A Generative Bayesian Model for Aggregating Experts' Probabilities*, Proceedings of the 20th Conference on Uncertainty in Artificial Intelligence, Pp. 301-308, ISBN: 0-9749039-0-6, Banff, Canada.

Kennedy, R. & Kirwan, B. (1998), *Development of a Hazard and Operability-Based Method for Identifying Safety Management Vulnerabilities in High Risk Systems*, Safety Science, December, Vol. 30, Issue 3, Pp. 249-274.

Kerr-McGee Oil (UK) Plc (1995), *Gryphon A: The First Purpose-Built Permanently Moored FPSO in the North Sea*, OTC 7424, 26th Annual Offshore Technology Conference, 2-5 May 1995, Houston, USA, Pp. 31.

Kirwan, B. (1992), *Human Error Identification in Human Reliability Assessment, Part I: Overview of Approaches*, Journal of Applied Ergonomics, Vol. 23, No. 5, Pp. 299-318.

Kirwan, B. & Ainsworth, L. K. (1992), *A Guide to Task Analysis*, ISBN: 0-7484-0058-3, Taylor and Francis, London, UK.

Kjestveit, K., Allred, K. B. & Nesvåg, S. M. (2003), *The Concept of Human Factors - A Discussion of Risk Assessments*, Project No. 720-1918, Report RF: 2003/079, Rogaland Research, Stavanger, April 22, ISBN: 82-490-0252-0.

Kletz, T. A. (1974), HAZOP and HAZAN - *Notes on the Identification and Assessment of Hazards*, Institute of Chemical Engineers, Rugby, UK.

Kletz, T. A. (2001), *An Engineer's View of Human Error*, 3rd Edition, ISBN: 0852954301, Institution of Chemical Engineers, Rugby, UK.

Klir, G. J. (1994), *The Many Faces of Uncertainty*, In Uncertainty Modeling and Analysis: Theory and Applications, Ayyub, B. M & Gupta, M. M., (Eds), Pp. 3-19, ISBN: 0-444-81954-1, Elsevier Science.

Klir, G. J. and Yuan, B. (1995), *Fuzzy Sets and Fuzzy Logic: Theory and Applications*, ISBN: 0-13-101171-5, Prentice Hall, Upper Saddle River, New Jersey, USA.

Kosko, B. (1990), *Fuzziness vs. Probability*, International Journal of General Systems, Vol. 17, Pp. 211-240.

Kosko, B. (1992), *Neural Networks and Fuzzy Systems: A Dynamical Systems Approach to Machine Intelligence*, Prentice-Hall, Englewood Cliffs, New Jersey, USA.

Kosko, B. (1994), *The Probability Monopoly*, IEEE Transactions Fuzzy Systems, Vol. 2, No. 1, Pp. 32–33.

LIVERPOOL
JOHN MOORES UNIVERSITY

Kramer, M. A. & Palowitch, B. L. (1987), *A Rule-Based Approach to Fault Diagnosis Using the Signed Directed Graph*, American Institute of Chemical Engineers (AIChE) Journal, Vol. 33, No. 7, Pp. 1067-1077.

Kreinovich, V. (1997), *In Random Sets: Theory and Applications*, Goutsias, J., Mahler, R. P. S., Nguyen, H. T. (Eds.), Springer-Verlag: Berlin.

Kumamoto, H. & Henley, E. J. (1979), *Safety and Reliability Synthesis of Systems with Control Loops*, American Institute of Chemical Engineers (AIChE) Journal, Vol. 25, No. 1, Pp. 108-113.

Lapp, S. A. & Powers, G. J. (1977), *Computer Aided Synthesis of Fault-Trees*, IEEE Transactions on Reliability, Vol. R-26, No.1, Pp. 2-13.

Larsen, P. M. (1980), *Industrial Applications of Fuzzy Logic Control*, International Journal of Man-Machine Studies, Vol. 12, No. 1, Pp. 3-10.

Laskey, K. B. (1995), *Sensitivity Analysis for Probability Assessments in Bayesian Networks*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 25, Pp. 901-909.

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 (B), Vol. 50, Pp. 157-224.

Laviolette, M. & Seaman, J. W. (1994), *The Efficacy of Fuzzy Representations of Uncertainty*, IEEE Transactions Fuzzy Systems, Vol. 2, No. 1, Pp. 4-15.

Law, A. M. & Kelton, W. D. (1982), *Simulation Modelling and Analysis*, McGraw-Hill Book Company, Berkshire, UK.

Lawley, H. G. (1974), *Operability Studies and Hazard Analysis*, In Chemical Engineering Process, Howe, J. (Eds.), American Institute of Chemical Engineers, April, Vol. 70, Issue 4, Pp. 45-56.

Leonhardsen, R. L., Ersdal, G., Kvitrud, A. (2001), *Experience and Risk Assessment of FPSOs in Use on the Norwegian Continental Shelf: Description of Events*, Proceedings of 11th ISOPE Conference, Vol. 1 (ISBN 1-880653-52- 4), 17-22 June, Pp. 309, Stavanger, Norway.

Leveson, N. G. (1995), *Safeware: System Safety and Computers*, Addison Wesley, ISBN: 0-201-11972-2.

Lindley, D. V. (1970), *Bayesian Analysis in Regression Problems in Bayesian Statistics*, Meyer, D. L. & Collier, R. O. (Eds.), F. E. Peacock Publishers, Itasca, Illinois, USA, Pp. 38.

LMIS (1995), *Ship Editorial, Casualty System Guide*, Maritime Information Publishing Group, Stamford, Connecticut, USA.

Loughran, C. G., Pillay, A., Wang, J., Wall, A. & Ruxton, T. (2002), *A Preliminary Study of Fishing Vessel Safety*, Journal of Risk Research, 1 January, Vol. 5, No. 1.

LR (1982), *Pump System Reliability Data*, Lloyds Register (LR), London, UK.

Mamdani, E. H. (1974), *Application of Fuzzy Algorithm for Control of Simple Dynamic Plant*, Proceedings of the Institute of Electric Engineers, Vol. 121, No. 12, Pp. 1585-1588.

Mamdani, E. H. & Assilian, S. (1975), *An Experiment in Linguistic Synthesis With a Fuzzy Logic Controller*, International Journal of Man-Machine Studies, Vol. 7, No.1, Pp. 1-13.

Mannan, S. (2005), *Lees' Loss Prevention in the Process Industries*, 3rd Edition, 3-Volume Set, ISBN: 0-7506-7555-1, Butterworth Heinemann Ltd.

Mathiesen, T. C. (1997), *Cost Benefit Analysis of Existing Bulk Carriers*, DNV Paper Series No 97-P008.

McKelvey, T. C. (1988), *How to Improve the Effectiveness of Hazard and Operability Analysis*, IEEE Transaction on Reliability, June, Vol. 37, No. 1.

Mengshoel, O. J. & Wilkins, D. C. (1997), *Abstraction and Aggregation in Bayesian Networks*, Proceedings of the American Association of Artificial Intelligence (AAAI) Workshop on Abstractions, Decisions, and Uncertainty, July, Providence, USA.

Miller, G. A. (1956), *The Magical Number Seven, Plus or Minus Two: Some Limits On Our Capacity for Processing Information*, The Psychological Review, Pp. 81-97.

Misra, K. B. (1992), *Reliability Analysis and Prediction*, ISBN: 0-444-89606-6, Elsevier Science Publishers, Oxford, UK.

MOD (1996), *Safety Management Requirements for Defence Systems*, Defence Standard 00-56, Ministry of Defence (MOD), Issue 2, 13 December, Glasgow, UK.

Morgan, M. & Henrion, M. (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, Cambridge, United Kingdom.

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.

Murata, T. (1989), *Petri Nets: Properties, Analysis and Applications*, Proceedings of the IEEE, Vol. 77, No. 4, April, Pp. 541-580.

Netica (2002), *Netica-J Reference Manual - Version 2.21, Java Version of Netica API*, Norsys Software Corporation.

Nielsen, D. S. (1971), *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis*, Danish Atomic Energy Commission, RISØ-M-1374, May, ISBN: 87-550-0084-3, RISØ National Laboratories, Denmark.

Nielsen, D. S. & Runge, B. (1974), *Unreliability of a Standby System with Repair and Imperfect Switching*, IEEE Transaction on Reliability, April, Vol. 23, Pp. 17-24.

Nielsen D. S (1975), *Use of Cause-Consequence Charts in Practical Systems Analysis*, Reliability and Fault Tree Analysis, SIAM, Pp. 849-880, Philadelphia, USA.

Nielsen, D. S., Platz, O. & Runge, B. (1975), *A Cause-Consequence Chart of a Redundant Protection System*, IEEE Transactions on Reliability, April, Vol. 24, No. 1.

Nielsen D. S., Platz, O. & Kongs, H. E (1977), *Reliability Analysis of Proposed Instrument Air System*, RISØ-M-1903, April, RISØ National Laboratories, Denmark.

North. D. W. (1968), *A Tutorial Introduction to Decision Theory*, IEEE Transaction on Systems Science and Cybernetics, Vol. 4, No. 3, Pp. 105-115.

NRC (1975), *Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants*, Report WASH-1400, NUREG-75/014, October, Nuclear Regulatory Commission (NRC), Washington DC, USA.

NRC (1991), *Fault Tree Handbook*, NUREG-0492, January, Systems and Reliability Research Office of Nuclear Regulatory Commission (NRC), Washington DC, USA.

NRC (1994), *Science and Judgment in Risk Assessment*, National Research Council (NRC), National Academy Press, Washington, D. C., USA.

NRC (2000), *Risk Analysis and Uncertainty in Flood Damage Reduction Studies*, National Research Council (NRC), National Academies Press, Washington, DC, USA.

NTSB (1990), *Marine Accident Report on the Grounding of U.S. Tankship Exxon Valdez on Bligh Reef, Prince William Sound Near Valdez, AK March 24, 1989*, National

Transportation Safety Board (NTSB) Report Number: MAR-90-04, Adopted on 31 July.

O'Connor, P.D.T. (1993), *Quantifying Uncertainty in Reliability and Safety Studies*, Paper Presented to Society of Reliability Engineers' Symposium, Arnhem, The Netherlands.

Pan, H. & Liu, L. (1999), *Fuzzy Bayesian Networks - A General Formalism for Representation, Inference and Learning with Hybrid Bayesian Networks*, In Proceedings of ICONIP'99, the 6th International Conference on Neural Information Processing, November, Perth, Australia, Pp. 401-406.

Pan, H. & Liu, L. (2000), *Fuzzy Bayesian Networks - A General Formalism for Representation, Inference and Learning with Hybrid Bayesian Networks*, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 14, No. 7, Pp. 941-962.

Pan, H. & McMichael, D. (1998), *Fuzzy Causal Probabilistic Networks - A New Ideal and Practical Inference Engine*, Proceedings of IAIAF'97, the 1st International Conference on Multisource-Multisensor Information Fusion, 6-8 July, Las Vegas, USA.

Papoulis, A. & Pillai, S. U. (2002), *Probability, Random Variables and Stochastic Processes*, 4th Edition, ISBN: 0072817259, McGraw-Hill Book Company.

Parry, G. W. (1996), *The Characterization of Uncertainty in Probabilistic Risk Assessment of Complex Systems*, Journal of Reliability Engineering and System Safety, Vol. 54, No. 2-3, Pp. 119-126.

Peachey, J. (1995), *Formal Safety Assessment Seminar, Overview of the 5 Steps of FSA*, International Maritime Organisation, MSA, 18 May, Section 1, Paper 2.

Pearl, J. (1986), *Fusion, Propagation, and Structuring in Belief Networks*, Artificial Intelligence, Vol. 29, No. 3, Pp. 241-288.

Pearl, J. (1988), *Probabilistic Reasoning in Intelligent Systems*, Networks of Plausible Inference, Morgan Kaufmann, San Mateo, California, USA.

Pearl, J. (2000), *Causality: Models, Reasoning, and Inference*, Cambridge University Press, Cambridge, UK.

Pentti, H. & Atte, H. (2002), *Failure Mode and Effects Analysis of Software-Based Automation Systems*, STUK-YTO-TR 190, August, ISBN: 951-712-584-4, VTT Industrial Systems, Helsinki, Finland.

Peterman, R. M. (1990), *The Importance of Reporting Statistical Power: The Forest Decline and Acidic Deposition Example*, Ecology Vol. 71, Pp. 2024-2027.

Petersen, D. (1996), *Safety by Objectives, What Gets Measured and Rewarded Gets* Done, 2nd Edition, Van Nostrand Reinhold, New York.

Peterson, D. (1978), *Techniques of Safety Management*, 2nd Edition, McGraw Hill Books, New York.

Phillips, C. V. & LaPole, L. M. (2003), *Quantifying Errors Without Random Sampling*, Journal of BioMed Central Medical Research Methodology, Vol. 3, Issue 1, ISSN: 14712288.

Pomeroy, R. V. (1995), *The Role of Reliability in Marine Classification*, Journal of Reliability Engineering, Pergamon Press.
Pp. 107-115.

Ramer, A. (1987), *Uniqueness of Information Measure in the Theory of Evidence*, Fuzzy Sets and Systems, Special Issue: Measures of Uncertainty, November, Vol. 24, Issue 2, Pp.183-196, ISSN: 0165-0114, Elsevier North-Holland, Inc., Amsterdam, The Netherlands.

Rasmussen, J. (1983), *Skills, Rules, Knowledge: Signals, Signs and Symbols and Other Distinctions in Human Performance Models*, IEEE Transactions on Systems, Man and Cybernetics (SMC), Vol. 13, No. 3, Pp. 257-266.

Reason, J. (1990), *Human Error*, ISBN: 0-521-31419-4, Cambridge University Press.

Redmill, F. (2002), *Human Factors in Risk Analysis*, Engineering Management Journal, August, Vol. 12, Issue 4, Pp. 171-176.

Riding, J. F. (1997), *Formal Safety Assessment (FSA): Putting Risk into Marine Regulations*, Transactions of the IMarE, Vol. 109, Part 2, Pp. 185-192.

RINA (2002), *Guidance on the Safety Role of the Naval Architect*, The Royal Institution of Naval Architects (RINA), London, UK.

Rook, L.W. (1962), *Reduction of Human Error in Industrial Production*, Report No. STCM 93-62, Sandia National Laboratories, Albuquerque, New Mexico, USA.

Russell, S. & Norvig, P. (2003), *Artificial Intelligence: A Modern Approach*, 2nd Edition, Prentice Hall, New Jersey, USA.

Saaty T. L. (1980), *The Analytic Hierarchy Process*, McGraw-Hill, New York, New York, USA.

SAE (1967), *Design Analysis Procedure for Failure Modes, Effects and Criticality Analysis (FMECA)*, Aerospace Recommended Practice (ARP) 926, 15 September, Society of Automotive Engineers (SAE), Warrendale, USA.

SAE (1996), *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, ARP 4761, 6 May, Society of Automotive Engineers (SAE), Warrendale, USA.

Salski, A., Fränzle, O. & Kandzia, P. (1996), *Fuzzy Logic in Ecological Modelling*, Ecological Modelling, Special Issue, Vol. 85, No. 1.

Seaver, D. & Stillwell, W.G. (1983), *Procedures for Using Expert Judgment to Estimate HEPs in Nuclear Power Plant Operations*, NUREG/CR-2743, US Nuclear Regulatory Commission.

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, 1-3 September, Pp. 499-505.

Sentz, K. & Ferson, S. (2002), *Combination of Evidence in Dempster-Shafer Theory*, Technical Report, SAND 2002-0835, Sandia National Laboratories, April, Albuquerque, New Mexico.

SERENE Consortium (1999), *SERENE (Safety and Risk Evaluation using Bayesian Nets): Method Manual*, ESPRIT Project 22187.

Shafer, G. (1976), *A Mathematical Theory of Evidence*, Princeton University press, Princeton, New Jersey, USA.

Sherwin, E. R. (2004), *Application of the Poisson Distribution*, Selected Topics in Assurance Related Technologies (START), A Publication of the Reliability Analysis Center, Vol. 9, No. 1.

Shishko, R. (1995), *NASA Systems Engineering Handbook, SP-6105*, ISBN: 0-16-061848-7, National Aeronautics and Space Administration (NASA), Washington DC, USA.

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, No. 2, Pp. 163–177, ISSN: 1366-9877, Taylor & Francis Ltd.

Sii, H. S., Wang, J., Eleye-Datubo, A., Liu, J. & Yang J. B. (2005), *Safety Assessment Of FPSO Turret-Mooring System Using Approximate Reasoning and Evidential Reasoning*, Marine Technology, April, Vol. 5, No. 2, Pp. 88-102.

Smith, D. J. (1985), *Reliability and Maintainability in Perspective*, 2nd Edition, ISBN: 0-333-39116-0, Macmillan Publishers Ltd, London, UK.

Smith, D. J. (1992), *Reliability, Maintainability and Risk*, 4th Edition, ISBN: 07506-5168-7, Butterworths-Heinemann Ltd, Basingstoke, UK.

Smith, D. J. (1992), *Reliability, Maintainability and Risk*, 4th Edition, ISBN: 07506-5168-7, Butterworths-Heinemann Ltd, Basingstoke, UK.

Smith, E. P. & Shugart, H. H. (1994), *Issue Paper on Uncertainty in Ecological Risk Assessment*, In: Ecological Risk Assessment Issue Papers, Washington, DC: Risk Assessment Forum, U.S. Environmental Protection Agency, Pp. 8-1 to 8-53, EPA/630/R-94/009.

Spouge, J. R. (1997), *Risk Criteria for Use in Ship Safety Assessment*, Conference Proceedings on Marine Risk Assessment: A Better Way to Mange Your Business, London, 7-8 May, Part I, Vol. 109, No. 3, Paper 15, ISBN: 0907206840, Institute of Marine Engineers.

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.

Statoil (1995), *The Nome Production Ship – Design Considerations*, OTC 7926, 27th Annual Offshore Technology Conference, 1-4 May, Pp. 543, Houston, USA.

Sugeno, M. (1985), *Industrial Applications of Fuzzy Control*, ISBN:0444878297, Elsevier Science Inc., New York, New York, USA.

Swain, A. D. (1963), *A Method for Performing a Human Factors Reliability Analysis*, Monograph SCR-685, Sandia National Laboratories, Albuquerque, New Mexico, USA.

Swain, A.D. & Guttmann, H. (1983), *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, US Nuclear Regulatory Commission.

Swain, A. D. (1988), *Adapting Risk Analysis to the Needs of Risk Management*, Paper Presented at the World Bank Workshop of Risk Management and Safety Control, Washington DC, USA.

Taylor, J. R. (1977), *Interlock design using Fault Tree Analysis and Cause-Consequence Analysis*, RISØ-M-1890, RISØ National Laboratories, Denmark.

Telcordia Technologies (2001), *Reliability Prediction Procedure for Electronic Equipment*, Special Report SR-332, Issue 1, May, Piscataway, New Jersey, USA.

Terano, T., Asai, K. & Sugeno, M. (1992), *Fuzzy Systems Theory and Its Applications*, ISBN: 0-12-685245-6, Academic Press Inc., San Diego, California, USA.

The MathWorks (2005), *Fuzzy Logic Toolbox For Use with MATLAB®*, User's Guide Version 2, March, The MathWorks, Inc.

The Nautical Institute (2003), *Just Waiting To Happen ...The Work of The UK P&I Club*, Alert! - The International Maritime Human Element Bulletin, Issue No.1, Pp. 3, October, Sponsored by Lloyd's Register.

THEMES (2001), *Report on the Identified Loopholes Existing in the Current Safety Management Measures and Policies*, Thematic Network for Safety Assessment of Waterborne Transport (THEMES), Deliverable No. D6.1, June, Sweden.

Turban, E. (1992), *Expert Systems and Applied Artificial Intelligence*, Macmillan, ISBN: 0024216658.

Türksen, I. B. (1992), *Fuzzy Second-Generation Expert System Design for IE/OR/MS*, Proceedings of IEEE International Conference on Fuzzy Systems, 8-12 March, San Diego, CA, USA, Pp. 779-786.

Türksen, I. B. (2004), *Belief, Plausibility, and Probability Measures on Interval-Valued Type 2 Fuzzy Sets*, International Journal of Intelligent Systems, Special Issue: Granular Computing and Data Mining, Lin, T. Y. & Zadeh, L. A. (Eds), Vol. 19, Issue 7, Pp. 681-699.

Tweeddale, M. (2003), *Managing Risk and Reliability of Process Plants*, ISBN: 0-7506-7734-1, Butterworth-Heinemann.

Umeda, T., Kuriyama, T., O'shima, E. & Matsuyama, H. (1980), *A Graphical Approach to Cause and Effect Analysis of Chemical Processing Systems*, Journal of Chemical Engineering Science, Vol. 35, No. 12, Pp. 2379-2388.

Vaidhyanathan, R. & Venkatasubramanian, V. (1995), *Digraph-Based Models for Automated HAZOP Analysis*, Journal of Reliability, Engineering and System Safety, Vol. 50, No. 1, Pp. 33-49.

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.

Vendrig, M., Spouge, J., Bird, A., Daycock, J. & Johnsen, O. (2003), *Risk Analysis of the Geological Sequestration of Carbon Dioxide*, Report No. R246, DTI/Pub URN 03/1320, Department of Trade and Industry (DTI), London, UK.

Veseley, W. E., Goldberg, F. F., Roberts, N. H. & Haasl, D. F. (1981), *Fault Tree Handbook*, Technical Report NUREG 0492, January, Systems and Reliability Research Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission (NRC), Washington DC, USA.

Vesely, W. E., Dugan, J., Fragola, J., Minarick III, J. & Railsback, J. (2002), *Fault Tree Handbook with Aerospace Applications*, Version 1.1, August, National Aeronatics and Space Administration (NASA) Office of Safety and Mission Assurance, Washington DC, USA.

Villemeur, A. (1992a), *Reliability, Availability, Maintainability and Safety Assessment, Volume 1: Methods and Techniques*, ISBN: 0-471-93048-2, John Wiley & Sons, Chichester, UK.

Villemeur, A. (1992b), *Reliability, Availability, Maintainability and Safety Assessment, Volume 2: Assessment, Hardware, Software and Human Factors*, ISBN: 0-471-93048-2, John Wiley & Sons, Chichester, UK.

Von Neumann, J. & Morgenstern, O. (1964), *Theory of Games and Economic Behavior*, 3rd Edition, Princeton University Press, Princeton, USA.

Wang J. (2002), *A Review of Marine and Offshore Safety Assessment*, Marine Technology, SNAME, April, Vol. 39, No. 2, Pp. 77-85.

Wang, J. & Ruxton, T. (1998), *A Safety and reliability analysis Methodology of Large Engineering Systems*, Journal of Engineering Design, Vol. 9, No. 2, Pp. 159-170.

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.

Wang, J., Yang, J. B. & Sen, P. (1996), *Multi-Person and Multi-Attribute Design Evaluations Using Evidential Reasoning Based on Subjective Safety and Cost Analyses*, Reliability Engineering and System Safety, Vol. 52, No. 2, Pp. 113–129.

Wang, L. X. (1997), *A Course in Fuzzy Systems and Control*, Prentice-Hall, ISBN: 0-13-540882 2.

Wang, Y., Teague, T. L., West, H. H. & Mannan, M. S. (2000), *Use of Fault Trees for Quantitative Risk Assessment*, Proceedings of the 3rd Annual Mary Kay O'Connor Process Safety Center Symposium - Beyond Regulatory Compliance: Making Safety Second Nature, 24-25 October, Pp. 121-127, College Station, Texas, USA.

Wang, Y., Teague, T. L., West, H. H. & Mannan, M. S. (2001), *Computer-Aided Fault-Tree Synthesis for Quantitative Risk Assessments*, Proceedings of the 4th Annual Mary Kay O'Connor Process Safety Center Symposium - Beyond Regulatory Compliance: Making Safety Second Nature, 30-31 October, Pp. 574-601 College Station, Texas, USA.

Warner, F. (1992), *Risk: Analysis, Perception and Management*, Report of a Royal Society Group, Pp. 4.

Wellman, M. P. & Henrion, M. (1993), *Explaining "Explaining Away"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No. 3, pp. 287-292.

Williams, J. C. (1985), *Validation of Human Reliability Assessment Techniques*, Journal of Reliability Engineering, Vol. 11, Pp. 149-162.

Williams, J. C. (1988), *A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance*, Proceedings of the IEEE 4th Conference on Human Factors in Power Plants, Monterey, California, 6-9 June, Institute of Electronic and Electrical Engineers (IEEE), New York, USA.

Williamson, T. (1994), *Vagueness*, Routledge, London and New York.

WOAD (1998), *Worldwide Offshore Accident Databank (WOAD) Statistical Report*, Veritas Offshore Technology & Services, Høvik, Norway.

Yang, J. B. & Sen, P. (1993), *A Hierarchical Evaluation Process for Multiple Attribute Design Selection With Uncertainty*, In Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE-93), Chung, P. W. H., Lovegrove,

G. & Ali, M. (Eds.), Gordon and Breach Science Publishers, Switzerland, Pp.484-493, ISBN 2-88124-604-4.

Yang, J. B. & Sen, P. (1994), *A General Multi-Level Evaluation Process for Hybrid MADM with Uncertainty*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 24, No. 10, Pp. 1458–1473.

Yang, J. B. & Singh, M. G. (1994), *An Evidential Reasoning Approach for Multiple Attribute Decision Making with Uncertainty*, IEEE Transactions on Systems, Man, and Cybernetics, Vol. 24, No. 1, Pp. 1–18.

Yang, J. B. & Xu, D. L. (2002a), *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, No. 3, Pp. 376–393.

Yang, J. B. & Xu, D. L. (2002b), *On the Evidential Reasoning Algorithm for Multi-Attribute Decision Analysis Under Uncertainty*, IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, Vol. 32, No. 3, Pp. 289–304.

Yang, J. B. (2001), *Rule and Utility Based Evidential Reasoning Approach for Multi-Attribute Decision Analysis Under Uncertainties*, European Journal of Operational Research, Vol. 131, Pp. 31–61.

Yu, Y. (2001), *Bayesian Belief Networks and BBN Modelling*, September, Electrical and Computer Engineering Department, University of Virginia, USA.

Zadeh, L. A. (1965), *Fuzzy sets, Information and Control*, June, Vol. 8, No. 3, Pp. 338-353.

Zadeh, L. A. (1968), *Probability Measures of Fuzzy Events*, Journal of Mathematical Analysis and Applications, Vol. 23, Pp. 421-427.

Zadeh, L. A. (1973), *Outline of a New Approach to the Analysis of Complex Systems and Decision Processes*, IEEE Transactions Systems, Man, and Cybernetics, January, Vol. 3, No.1, Pp. 28-44.

Zadeh, L. A. (1975), *The Concept of a Linguistic Variable and Its Application to Approximate Reasoning - Parts 1, 2, and 3*, Information Sciences, Vol. 8, Pp. 199-249, Vol. 8, Pp. 301-357, Vol. 9, Pp. 43-80.