RISK ASSESSMENT AND DECISION MAKING OF CONTAINER SUPPLY CHAINS

A Thesis Submitted to Liverpool John Moores University
for the Degree of Doctor of Philosophy

ZAILI YANG

Marine Offshore and Transportation Research Group
School of Engineering
Faculty of Technology and Environment

September 2006

Table of Contents

Abstract

Container shipping lines are exposed to various risks in their internal operations and external interactions with the upstream transportation suppliers and downstream demanders, whether these risks are recognised, managed and addressed in a cursory manner, or altogether ignored. In order to allow better understanding and control of the risks that exist in container supply chains (*CSCs*, the chain aggregations of the lines and their suppliers/demanders), the stakeholders/organisations can proactively assess their reliability and robustness in advance, or reactively discover risks after a detrimental event occurs.

The purpose of this study is to explore and analyse various *CSC* risks, derive their common themes, deal with the corresponding uncertainties and develop a proactive and advanced risk assessment methodology with novel and flexible modelling techniques. However, the literature review in the context of *CSC* risk research has indicated that such a task is not straightforward considering the facts that *a)* the chains are characterised as having the nature of complexity, uncertainty and dependence, which may constrain the applicability and practicability of traditional risk assessment methods in the chains and *b)* compared to the nuclear, chemistry, aerospace and marine (including shipping and offshore) industries, there is a significant gap between academic research and industrial safety and reliability demand in the logistic field, particularly in the post-9/11 era.

Starting with the development of a conceptual risk assessment model based on a modified Formal Safety Assessment (*FSA*) methodology, this study focuses on the research of novel and effective risk analysis and risk based decision making techniques using various uncertainty treatment theories and methods. They include:

- A discrete fuzzy set technique.
- A continuous fuzzy set technique.
- An evidential reasoning (*ER*) approach.
- A belief fuzzy rule-based approach.
- A fuzzy link-based approach.
- A Bayesian network (*BN*) model.
- An *ER* based Bayesian probability distribution model.
- A hybrid decision making method of combining fuzzy logic, *BN*, *ER* and multiple attribute utility theory (*MAUT*).

A considerable body of high quality publications and reference materials is produced to support the methods and techniques developed.

The methodological view to the risk assessment adopted in the thesis is based on a requisite logical modelling, where risk and decision models are first generated to support risk assessment and decision making under uncertainty in a specific analysis constraint, and then refined when more generic and wider analysis contexts are provided and incorporated. Such a process keeps being conducted until the risk assessors and decision makers have confidence and satisfaction with the results and prescriptions obtained from the modified and upgraded models. Consequently, the models developed can be well suited to dealing with different risk assessment and decision making problems, generic or special and objective or subjective, in *CSCs*.

Findings from this research imply that the conceptual risk assessment methodology and its attached unique risk analysis and decision making techniques have provided a way of presenting the organisations in *CSCs* with a consistent way of making a comprehensive assessment of the factors associated with complex risk and decision modelling. The approaches described will, based on a thorough and detailed analysis of the possible uncertain contexts, present the results of the analysis in a simple, transparent and justifiable way that could be understandable by the assessors or decision makers not versed in dealing with the complexities and uncertainties of the chain systems involved. Although the risk assessment and decision making approaches are presented on the basis of the specific context in *CSCs*, they can also, with domain-specific knowledge, be tailored to facilitate risk and decision modelling in other application areas where a high level of uncertainty is involved.

Acknowledgements

This thesis is the result of three-year work whereby I have been accompanied and supported by many people and organisations. It is a pleasant aspect that I have now the opportunity to express my sincere gratitude for all of them.

The first person I would like to thank is my principal supervisor Professor Jin Wang. I thank Professor Wang not only because of his patience, encouragement, great direction and advices provided in completing this thesis. More importantly, his overly enthusiasm and integral view on research and his mission for providing 'only high-quality work and not less', have made a deep impression on me. I owe him lots of gratitude for having shown me this way of conducting research. He could not even realise how much I have learned from him. I am really glad that I have known Professor Wang in my life.

In those excellent tutors who provided me great help in my study, if I forget to thank Dr Steve Bonsall and Professor Quangen Fang, I would be too careless to be unforgiving. I would like to express my gratitude to both of them who always monitored the progress of my work and were available when I needed their advices. I would also like to thank Dr Alan Wall and Professor Jianbo Yang who took effort in reading and providing me with valuable comments on the earlier work of this thesis. My colleagues of the MORG group all gave me the feeling of being at home at work. They also substantially contributed to the development of this thesis. I thank them all.

This research has been supported and funded by various organisations including the Institute of Marine Engineering, Science and Technology, the International Maritime Organisation and the UK Health and Safety Executive. I thank them for their confidence and assistance in me. I am also deeply grateful for the School of Engineering at LJMU for providing me an excellent working environment during the past three years.

I feel a deep sense of gratitude for my father and mother for their great material and spiritual support. I am very grateful for my wife, Zhuohua, for her love, trust and patience during the PhD period. Without their love, care and understanding, I would not have delivered the thesis like this.

The chain of my gratitude would be definitely incomplete. Many persons have helped me and many good friends have shared experiences and thoughts with me throughout the past years. For all of them, if their names do not appear in the first course of the chain, I would like to express my heartfelt gratitude here.

List of Figures

List of Tables

Abbreviations

AHP	Analytic Hierarchy Process
AI	Artificial Intelligent
AIS	Automatic identification systems
ALARP	As Low As Reasonably Practicable
ANN	Artificial Neural Network
API	Applicable Programmer's Interface
BBN	Bayesian Belief Networks
BDD	Binary Decision Diagrams
BDMP	Boolean logic Driven Markov Processes
BDT	British Department of Transport
BFRB	Belief Fuzzy Rule Base
BN	Bayesian Network
BRB	Belief Rule Base
CBA	Cost Benefit Analysis
CBP	Customs and Border Protection
CP	Contingency Planning
CPT	Conditional Probability Table
CSC	Container Supply Chain
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DA	Diagraph based Analysis
DAG	Directed Acyclic Graphs
DBN	Dynamic Bayesian Network
D-S	Dempster-Shafer
ECR	Efficient Customer Response
EP	Extension Principle
ER	Evidential Reasoning
ETA	Event Tree Analysis
FBCP	Formal Business Continuity Planning
FBN	Fuzzy Bayesian Network
FCBA	Fuzzy Cost and Benefit Analysis
FCL	Full Container Loads
FER	Fuzzy Evidential Reasoning
FLB-ER	Fuzzy Link Based Evidential Reasoning
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FRB-ER	Fuzzy Rule Based Evidential Reasoning
FSA	Formal Safety Assessment
FSI	Flag State Implementation
FST	Fuzzy Set Theory
FTA	Fault Tree Analysis
GQM	Goal Question Metric
GUI	Graphical User Interface
HAZOP	HAZard and OPerability studies
HBN	Hierarchical Bayesian Network
HSE	Health and Safety Executive
ID	Influence Diagram
IDS	Intelligent Decision System via evidential reasoning
IMB	International Maritime Bureau
IMO	International Maritime Organisation
ISL	Institute of Shipping and Logistics
ISPS	International Ship and Port facility Security code
JIT	Just-In-Time

JPD	Joint Probability Distribution
LCL	Less than Container Load
LMIS	Lloyds Maritime Information Services
MAUT	Multiple Attribute Utility Theory
MADM	Multiple Attribute Decision Making
MC	Markov Chains
MCDM	Multiple Criteria Decision Making
MEU	Maximum Expected Utility
MHIDS	Major Hazard Incident Data Service
MSA	Maritime Safety Agency
MTBN	Modifiable Temporal Bayesian Network
NIEDT	Net of Irreversible Events in Discrete Time
PHA	Preliminary Hazard Analysis
PLL	Potential Loss of Life
PRA	Probabilistic Risk Assessment
QR	Quick Response
QRA	Quantitative Risk Analysis
RCC	Rescue Co-ordination Centre
RCM	Risk Control Measure
RCO	Risk Control Option
RPN	Risk Priority Numbers
RRN	Risk Ranking Numbers
RV	Random Variables
SA	Sensitivity Analysis
SCM	Supply Chain Management
SMED	Single-Minute Exchange of Die
SOLAS	Convention on the Safety of Life at Sea
TBN	Temporal Bayesian Network
TNBN	Temporal Node Bayesian Network
TOPSIS	Technique for Order Preference by Similarity to an Ideal Solution
TPM	Total Productive Maintenance
UTA	Utility Additive
WMoM	Weighted Mean of Maximums

Chapter 1 – Introduction

SUMMARY

This chapter gives a brief introduction and essentially "sets the scene" for the thesis by: making key definitions used in the study; giving a background analysis (understanding research necessity from a practical viewpoint); demonstrating the challenges of conducting the research by following the explanation of the research objectives, either primary or subsidiary; presenting and justifying the methodology employed; stating the hypothesis and discussing how it is to be examined, tested or addressed and where this appears in the thesis; describing the layout and scope of the thesis and summarising the deliverables, contributions to knowledge and achievements against objectives.*

1.1 Definitions for Typical Terms Used in *CSC* Risk Assessment

Accident: An unintended event involving fatality, injury, property loss or damage, and/or environmental damage (Wang and Trbojevic, 2006).

Container Supply Chains (CSCs): A natural process of evolution of liner shipping services in the era of containerisation. *CSCs* can be defined as one logistics distribution service that extends liner shipping services, which are provided on a regularly scheduled basis to the pre-determined ports, to inland transport services to complete efficient flow and storage of container cargoes, information and related value added services from point of origin to point of consumption for the purpose of conforming to customers' requirements.

Decision Making: The process of sufficiently reducing uncertainty and doubt about alternatives to allow a reasonable choice to be made from among them (Harris, 1998).

Formal Safety Assessment (FSA): *FSA* is based on the principles of identifying hazards, evaluating risks and cost benefit analysis (*CBA*), and has as its objective the development of a framework of safety requirements for shipping in which risks are addressed in a comprehensive and cost effective manner (*MSA*, 1993; *MCA*, 1996). The *FSA* methodology comprises five inter-related steps as follows (*MSA*, 1993):

1. Identification and ranking of hazards.
2. Quantified assessment of the risks arising from the hazards identified in Step 1.
3. Identification of regulatory options for controlling the risks defined in Step 2.
4. *CBA* of the risk control options (*RCOs*) identified in Step 3.
5. Recommendation for decision making, based upon the information derived in the preceding steps.

---

* The research necessity from an academic viewpoint is illustrated in Chapter 2.

Judgement: In the context of risk assessment, judgement is not simply the final decision but is an integral part of the whole risk assessment progress with the essential nature as the ability to make a critical assessment of evidence (Chicken and Posner, 1998).

Hazard: A physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these (Henley and Kumamoto, 1992).

Probability distribution: The characteristic of an item expressed by the probability that it will perform a required function under stated conditions for a stated period of time (Henley and Kumamoto, 1992).

Reliability: Reliability can be defined either as the probability that a system or a component performs its specified function as intended within a given time horizon and environment, or in other words as the probability of the absence of failures affecting the performance of the system over a given time interval and under given environmental conditions (Kuo and Zuo, 2003; Andrew and Moss, 2002).

Risk: A combination of the probability of occurrence of an undesired event and the degree of its possible consequences (Wang and Trbojevic, 2006).

Risk assessment: A comprehensive estimation of the probability and the degree of the possible consequences in a hazardous situation in order to select appropriate safety measures (BS 4778, 1986; Wang and Trbojevic, 2006).

Robustness: Robustness can be defined as the extent to which a system is able to perform its intended function relatively well in the presence of failures of components or subsystems (Santa-Fe institute, 2001).

Safety: Freedom from unacceptable risk or personal harm (Wang and Trbojevic, 2006).

Threat: An action or a potential action likely to cause damage, harm or loss (Burns *et al.*, 2003).

Uncertainty: A situation in which a person does not have the quantitatively and qualitatively appropriate information to describe, prescribe or predict deterministically and numerically a system, its behaviour or other characteristics (Zimmermann, 2000).

Vulnerability: In a *CSC* context, vulnerability can be defined as an exposure to serious disturbances, arising from a hazard or a threat (Also see Section 3.2.2).

1.2 Background Analysis

Globalization and containerization processes have been the impetus behind the significant advances in the world prosperity and economic development experienced in the last twenty years of the 20th century. They have caused many transformations within

the world economy and their consequences are extending to all sectors of commercial and industrial activities, including the liner shipping environment. Responding to the new trends and increasingly considering the requirements of commercial partners, suppliers and customers throughout the globe, liner container shipping is undergoing an evolution from an original transport service of shipping lines to an advanced *CSC* system. The *CSC* system integrates the services of shipping lines, ports and inland transport, and consequently extends from port-to-port to door-to-door services. One most obvious property of this evolution is that the port and inland transport services are effectively integrated rather than simply physically combined with the shipping lines by many value added services and exchange of information. The integration provides the ability of a "one stop shop" service for the chains. The emerging paradigm for the "one stop shop" service has been predicated on a near-frictionless international transport process. The paradigm has allowed, however, the *CSCs* to contribute to economic prosperity and also rendered them uniquely vulnerable to many risks, which range from the possibility of physical breaches in the integrity of shipments to the interruption of information communication. The stakes of these risks are extremely high, as any important breakdown in the chains would fundamentally cripple the world and/or regional economy.

Modern *CSCs* are very complex, with many parallel physical and information flows occurring in order to ensure that products are delivered at the right time, in the right place, at the right cost and at the right quality (Rushton *et al.*, 2000). Thus, supply networks may be a more accurate term than supply chains (Chapman *et al.*, 2002). The cooperation and dependence among the entities in the container supply networks increase their interdependent and cooperating risks. Furthermore, the other drives towards more vulnerable supply chains mainly include many uncertainty related factors (i.e. the unavailability or incompleteness of historical failure data) resulting from more volatile markets and less predictable economic operating rules, the widespread adoption of Just-in-Time (*JIT*) rather than just-in-case practices, and the physical extension of supply chains originating from a global sourcing strategy, etc.

1.3 Research Objectives and Their Hypothesis

The primary purpose of this research is to generate a conceptual risk assessment methodology for *CSCs* based on a modified *FSA* framework that takes risks from vulnerability (fuzziness and incompleteness) rather than hazards into account and considers the relationships between risk factors as networking instead of hierarchical structures (randomness). Providing such a methodology for the companies involved in *CSCs* enables them to identify, manage and control the vulnerability of the chains and to support the safety planning for both mitigating and continuity actions.

In order to achieve this aim, some subsidiary objectives need to be carefully addressed. They are:

- Developing novel fuzzy based models to analyse and rank the threat-based risks.
- Generating a non-linear and non-additive utility synthesising function using an evidential reasoning (*ER*) algorithm to make the risk-based decisions with a dynamic nature.
- Producing an advanced dynamic risk assessment technique using Bayesian Networks (*BNs*) to deal with the dependence between risk factors.
- Using fuzzy logic and *ER* to assist in the appropriate distribution of Bayesian prior probabilities.
- Creating a new hybrid decision-making approach to carry out the risk-based decision analysis based on multiple uncertain attributes.

The hypothesis that the objectives depend on is that the most widely used uncertainty treatment theories such as fuzzy logic, Bayesian probability and Dempster-Shafer (*D-S*) can be the foundation of and have significant contribution in developing novel and advanced risk assessment and decision making models in the context of *CSCs*.

1.4 The Challenges of Conducting the Research (The Statement of Problem)

Modern *CSCs* are complex. The complex *CSCs* are closely associated with the complexity of their risks, but this is absolutely not one single contributing factor. The complexity of the risks can also be observed by investigating many different risk forms, which can be defined using diverse categorising methods. Cavinato (2004) categorised the risks and vulnerability in supply chains into five different networks – *physical, financial, informational, relational and innovational. LCP* consulting and the Center for Logistics and Supply Chain Management (*CLSCM*) (2003) analysed the risks in supply chains through investigating their six drivers – *demand, supply, environmental, process, control and the lack of mitigation/contingency.* Still being the study of *CLSCM* (2003), the risks of supply chains have been further investigated from four interlocking levels – *process/value stream, assets and infrastructure dependencies, organisations and inter-organisational networks as well as the environment.* Chapman *et al.* (2002) defined the vulnerability of supply chains and differentiated their risks into two types – *the ones within supply chains and external to supply chains*. Yang *et al.* (2005a) discussed the risks in *CSCs* from four aspects – *process, person, organization and environment.* The work by Christopher and Lee (2004) hinted that the risks could be classified to be *expected and non-expected.*

Furthermore, the complexity of *CSCs'* risks arises when it messes with the other two risk characteristics – uncertainty and dependence. This fact can be explained through constructing a risk spiral, which is developed on the basis of the risk spiral model of Christopher and Lee (2004) and shown in Figure 1.1. The above analysis has shown that *CSC* structures contribute to the complexity of the *CSCs'* risks. Such complexity immediately leads to the lack of visibility to monitor the safety performance of *CSCs*. It is often the case that one member of a supply chain has no detailed knowledge of what goes on in other parts of the chain, e.g. adopting or not adequate risk mitigation/control measures for keeping the reliability and continuity of the chain. Because there is no visibility of upstream and downstream flows and stocks, confidence declines and decisions are made to apply safety control measures to the individual sections/sub-chains of the supply chain for preventing/mitigating risks. The lack of confidence also means that it is difficult to make optimal safety control measures at each stage of the *CSCs*. The risks of making wrong or ineffective decisions become an inevitable consequence. Thus, it will be possible to produce overreactions, unnecessary interventions, second guessing, mistrust and distorted information throughout the supply chain. These overreactions are time-consuming and then serve to further obscure supply chain visibility because *CSCs* are now more complex as a result of the build up of the longer end-to-end chains involving many unnecessary interventions. Consequently, an internal self-perpetuating risk spiral is formed and a new intangible risk is produced due to the lack of confidence.

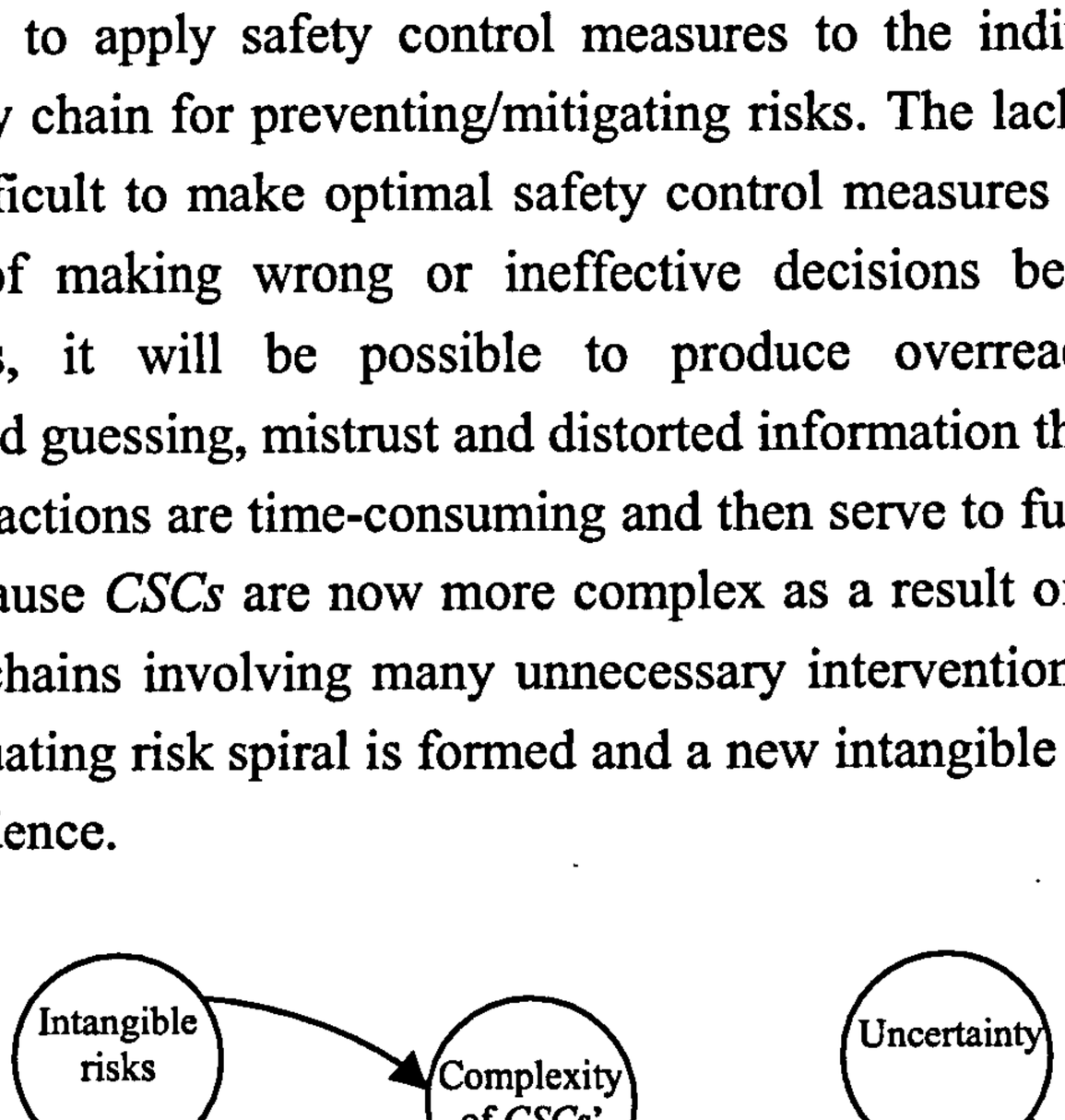


Figure 1.1.The risk spiral of *CSCs*

Such an internal risk spiral is still quite frail and easily broken by the improved confidence, given some effective countermeasures, such as the introduction of shared information. However, the entry of uncertainty and interactive dependence makes the spiral stronger and its running speed faster, an external risk spiral comes into shape to

support the internal one. Obviously, uncertainty makes it nearly impossible to clearly identify the vulnerability of *CSCs* and assess their risks. Interactive dependence significantly discounts the effectiveness of risk control. This risk spiral exists everywhere and the only way to break the spiral is to understand and appropriately deal with the uncertainty and interactive dependence in the *CSCs*.

The uncertainties associated with the *CSCs*' risks have different sources and diverse forms. Figure 1.2 summarises the types of such uncertainties. Not all of them are reducible or equally amenable to analysis. Therefore, only three principal types of uncertainties are explained and analysed. They are related to epistemic domains, measurement parameters and risk factor relationships.

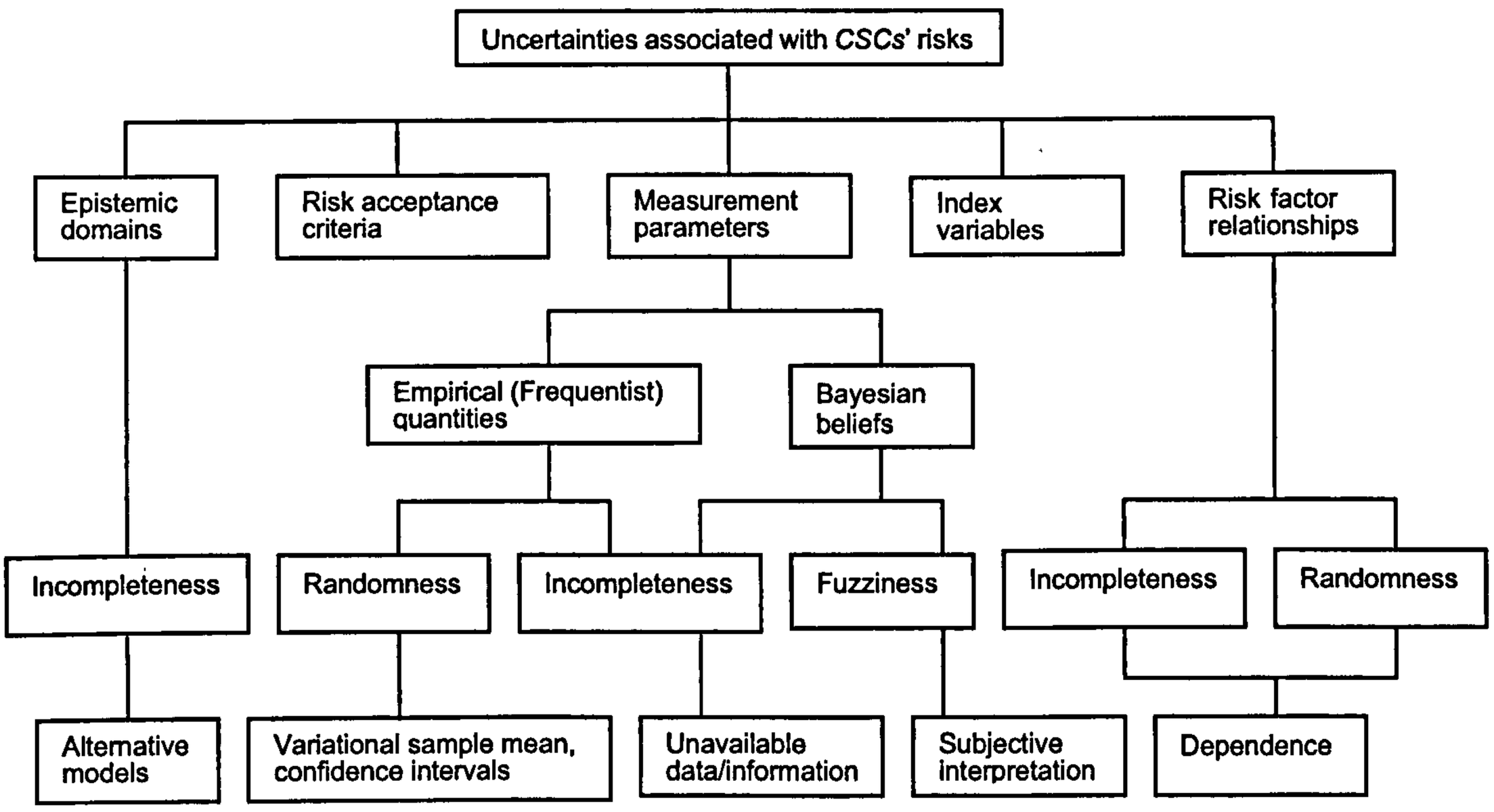


Figure 1.2. Uncertainties associated with *CSCs'* risks

An important source of uncertainty in *CSCs'* risks is our incomplete understanding of *CSC* systems that are being modelled from the viewpoint of safety. This has been termed fundamental or epistemic uncertainty (Pate-Cornell, 1996). Epistemic uncertainty expresses itself as model error, which occurs in the boundaries, structure and components of a system safety model (Hayes, 1998). Model error can also be affected by the complex risk classifications and interactive dependent relationships in *CSC* systems and be further complicated by contradictory data sets. The best way to reduce such epistemic uncertainty is to compare the model's predictions with reality. However, analysts are generally aware, before the fact, that models are maximal approximations of reality. This error is only apparent after the fact and cannot usually be addressed in a proactive manner. Hence, either comparing the results of multiple models that use different methods and assumptions, or constructing a self-promoting mechanism that has

the capability of automatically checking and modifying the model to maximally simulate reality enables the selection of a suitable model alternatively.

Although the epistemic uncertainty is considered to be fundamental, this research is primarily concerned with the uncertainties regarding the measurement parameters of *CSCs*' risks and their factor relationships. This is because they are concerned with the types of uncertainties that can be expressed in probabilistic/possibilistic terms, and only probability and possibility are appropriate mediums to the effective risk assessment of *CSCs*. In many typical risk analysis approaches, risk measurement parameters are represented by empirical quantities. To be empirical, these quantities must be measurable, at least in principle. In other words, they must have a correct value, as opposed to an appropriate or good value (Morgan and Henrion, 1990). This is, however, not straightforward, and frequentists recognise that empirical quantities may be random and incomplete in some conditions and thus, require disparate data sources to be incorporated. The randomness depends on the variations between observations and the number of observations, and is usually expressed in terms of a sample variance or confidence intervals around the sample mean. The incompleteness indicates the unavailability of historical data. Consequently, subjective interpretations are incorporated using linguistic assessments. However, such linguistic descriptions define risk measurement parameters to a discrete extent so that fuzziness can at times be produced.

The factors/components of the *CSCs*' risks being considered are exhibiting dynamic behaviour and interactive dependence that lead to the high level uncertainty involved. The complex dynamic behaviour of the risk factors significantly increases the randomness of risk probability distributions. Any spatial or temporal component may result in the change of the risk probability distribution of one risk factor, and further lead to the alteration of other relevant risk factors and the whole system in terms of safety levels. Additionally, the risk factor relationships are also incomplete. They may be fully dependent, partially dependent or independent. The uncertainty of the dependence degree between risk factors will be reduced with the entry of more and more evidence. This will be given more explanation in the following context.

There are two other potential sources of uncertainty associated with the risks of *CSCs*:

- Risk acceptance criteria – used to represent the preferences of decision makers, stakeholders or the general public. For example, the risk preferences to different chains or even the different sections in the same chain are changeable according to their individual circumstances.
- Index variables – used to describe spatial or temporal components of a risk, such as a particular location, voyage, month or year.

None of these, however, are amenable to analysis using either probability or possibility.

At first sight, *CSC* risks can be considered to arise from a series of adverse events along the chain between point of origin and point of destination. The raw materials contained in containers may be hazardous or special attention needs to be paid to items such as frozen cargoes, the handling and treatment of the containers during transportation may be inaccurate, the transfer between different transport modes may not be smooth and connected closely, and finally the consignees may be unaware of a potential informational or financial problem and miss the collections. This scheme, whilst over simplified, can illustrate the complexity of inferring quantitative assessment of the *CSC* risks, because it is clear that, even in this case, a simple product

$$p(\text{raw material}) \times p(\text{transportation}) \times p(\text{transfer}) \times p(\text{collection})$$

is not a useful quantitative representation of the risks because the individual probabilities, p, are not independent. In this expression several of the component probabilities may change in response to a single alteration in operating conditions and therefore, the terms in the product cannot be evaluated in isolation. For example, using reefers may reduce the value of *p(raw material)* when they carry frozen foods. However, they require careful electric supply and may affect other factors (possibly increase the value of *p(transportation)* and *p(transfer)*). Equally, this representation of the risk strength does not allow for a straightforward expression of uncertainty because the direction associated with the evaluation of the produce cannot be simply responded by the trend associated with the evaluation of each component probability. Contrarily, computing the risk strength and capturing the conditional uncertainty requires using causal inference.

CSC systems suffer from high levels of dependence between their risk factors/ components. In order to stay competitive, maintain cost-effectiveness, and achieve reasonable safety and reliability, the systems have to take into account such risk dependence. Recently, the popularity of researching risk dependence as a concept has been increasingly growing (Vaidya and Kumar, 2003; Boudali and Dugan, 2005). Many of the discrepancies in the classifications of dependence, however, arise from different epistemological orientations. This point can be verified by the analysis and explanation in Table 1.1. In a *CSC* context, risk dependence can be studied from two aspects – dependence degrees (full or partial) and dependence characteristics (time, functional or relational).

Most of available methods in system reliability analysis, for example, series/parallel configurations, cut-set, tie-set and Fault Tree Analysis (*FTA*), etc., only consider independence and full dependence (Shrinath, 1991) and assume that partial failures of the components do not affect the performance of other components though it is often not the realistic case (Vaidya and Kumar, 2003). Moreover, the techniques, which do not consider the partial dependence, are approximate methods. For safety critical *CSC* systems, the risks with the nature of dependence may become more inaccurate or even

conflicting with the reality as the approximation at a microscopic concern is accumulated and magnified to a macroscopic level.

Table 1.1. Classifications of dependence

Vaidya and Kumar, 2003	
Extrovert dependence	If one or many components depend on the host component then it is termed as extrovert dependence.
Introvert dependence	If the host component depends on one or many components then it is termed as introvert dependence.
Self dependence	The dependence of the host component on itself is termed as self dependence.
Vaidya and Kumar, 2003	
Functional dependence	If component "A" depends on component "B" or vice-versa in order to fulfil its task or a function to be executed, then the dependence is termed as functional dependence.
Design dependence	If component "A" depends on component "B" or vice-versa for its design (estimation of shape and size, and material selection) then it is termed as design dependence.
Performance dependence	If the performance of component "A" is affected by the variations caused in the performance of component "B" or vice-versa, then it is termed as performance dependence.
Shrinath, 1991	
Full dependence	If the conditional probability value between components "A" and "B" is equal to "1", then it is termed as full dependence.
Partial dependence	If the conditional probability value between components "A" and "B" lies between "0" and "1", then it is termed as partial dependence.
Independence	If the conditional probability value between components "A" and "B" is equal to "0", then it is termed as independence.
Boudali and Dugan 2005; Svensson, 2004	
Time dependence	A category, which comprises explicit reference to time plans, delays, lead time, delivery schedules and prognoses in the companies' upstream and downstream supply chains.
Functional dependence	A category which comprises corporate functions, such as upstream and downstream inventories, production, products, transport, third party logistics, maintenance, capacity and preventive activities.
Relational dependence	A category which comprises issues of contingency plan such as economics, legal aspects, technology, knowledge, social aspects, the market, IT, information, communication, variability and planning. Suppliers and customers, as well as staff issues, belong to this category.
Svensson, 2002	
Vertical dependence	The vertical dependence refers to the incorporation between companies' business activities in marketing channels.
Horizontal dependence	The horizontal dependence refers to the competition between marketing channels.
Direct dependence	If business activities affect each other directly, then the dependence is direct.
Indirect dependence	If business activities affect each other through the changes of other middle activities, then the dependence is indirect.
Unidirectional dependence	All upstream components in supply chains will affect the host component, since the host component is unidirectionally dependent on its upstream components.
Bi-directional dependence	The interpretation of unidirectional dependence is reversed, running from the point of consumption to the point of origin. Supply chains have emphasized bi-directionality, taking into account both supply and demand chains in marketing channels.
Hammarkvist et, al., 1982	
Technical dependence	This refers to the instance when two companies use compatible equipment and adapt their mutual business activities to each other in a technical sense.
Time dependence	This refers to the instance when two companies have a time-based need or synchronization of their mutual business activities.
Knowledge dependence	This refers to the interaction processes between two companies, learning from each other's strengths and weaknesses. The interaction creates knowledge about each other's ability to solve problems.
Social dependence	This refers to the interaction between two companies, which is often based upon personal relationships. This means that the social atmosphere and the personal chemistry between the involved executives affect the business activities in the relationship between two companies.
Economical/judicial dependence	This refers mostly to the formal dependence that may exist between two companies, such as written agreements. These strengthen the dependence between the business activities of two companies in an economic and judicial sense.
Mattsson, 2000	
Market dependence	This refers to a company's image and status that may positively influence another company's image and status. It may also improve the other company's goodwill in the marketplace.
IT dependence	This refers to two companies that may invest in a common IT standard, e.g. in terms of EDI (Electronic Data Interchange). This means that the hardware and software to communicate between the two companies are compatible.

Many logistics philosophies, such as supply chain management (*SCM*), *JIT*, quick response (*QR*) and efficient consumer response (*ECR*), take into consideration time, functional and relational dependence in supply chains. This also tends to happen in supply chain safety management. It has been a widely accepted fact that there is dependence between risk factors in *CSCs*. Previous studies (Svensson, 2002; 2004) hinted that time, functional and relational dependence directly results in the vulnerability in supply chains. As far as *CSCs* are concerned, time dependence means explicitly time issues. Functional dependence includes technical adoptions and coordination. Relational dependence comprises knowledge links, social bonds and economic as well as environmental ties. Nevertheless, it is noteworthy that there is implicitly an aspect of time dependence in all these other dependencies (Svensson, 2004). These dependencies can become crucial from the perspective of an overall supply chain network structure (Lambert *et al.*, 1998).

1.5 Research Methodology and Scopes of the Thesis

The methodological view to risk assessment adopted in the thesis is based on a requisite logical modelling, where risk and decision models are first generated to support risk assessment and decision-making under uncertainty in a certain analysis scope/constraint, and then refined when more and wider analysis contexts are provided and incorporated. Such a process keeps being conducted until the risk assessors and decision makers have confidence and satisfaction with the results and prescriptions obtained from the modified and upgraded models. Generally speaking, the methodology consists of six interrelated essential steps of realising the research objectives as follows:

1. Research challenge identification.
2. Critical review of the *CSC* operation, accidents and literature related to the challenges identified in Step 1.
3. The development of a conceptual framework using a modified *FSA* methodology based on the review in Step 2.
4. Fuzzy risk assessment and decision making modelling for providing a more effective technique to deal with the fuzziness and incompleteness involved in the framework developed in Step 3.
5. *BN* based risk assessment and decision making modelling for overcoming the weakness of the modelling generated in Step 4 and making the framework in Step 3 more powerful in terms of dealing with dependence between risk factors.
6. The validation of the hypothesis by comparing and analysing the modelling produced in Steps 4 and 5, particularly the consistent results obtained in risk prediction.

A graphical flowchart is presented in Figure 1.3 for clarifying the logical backbone of the complex methodology. More detailed explanations to the figure (the interrelated

relationship between the steps of the methodology) are unified together with the study of the thesis layout and given in the following.

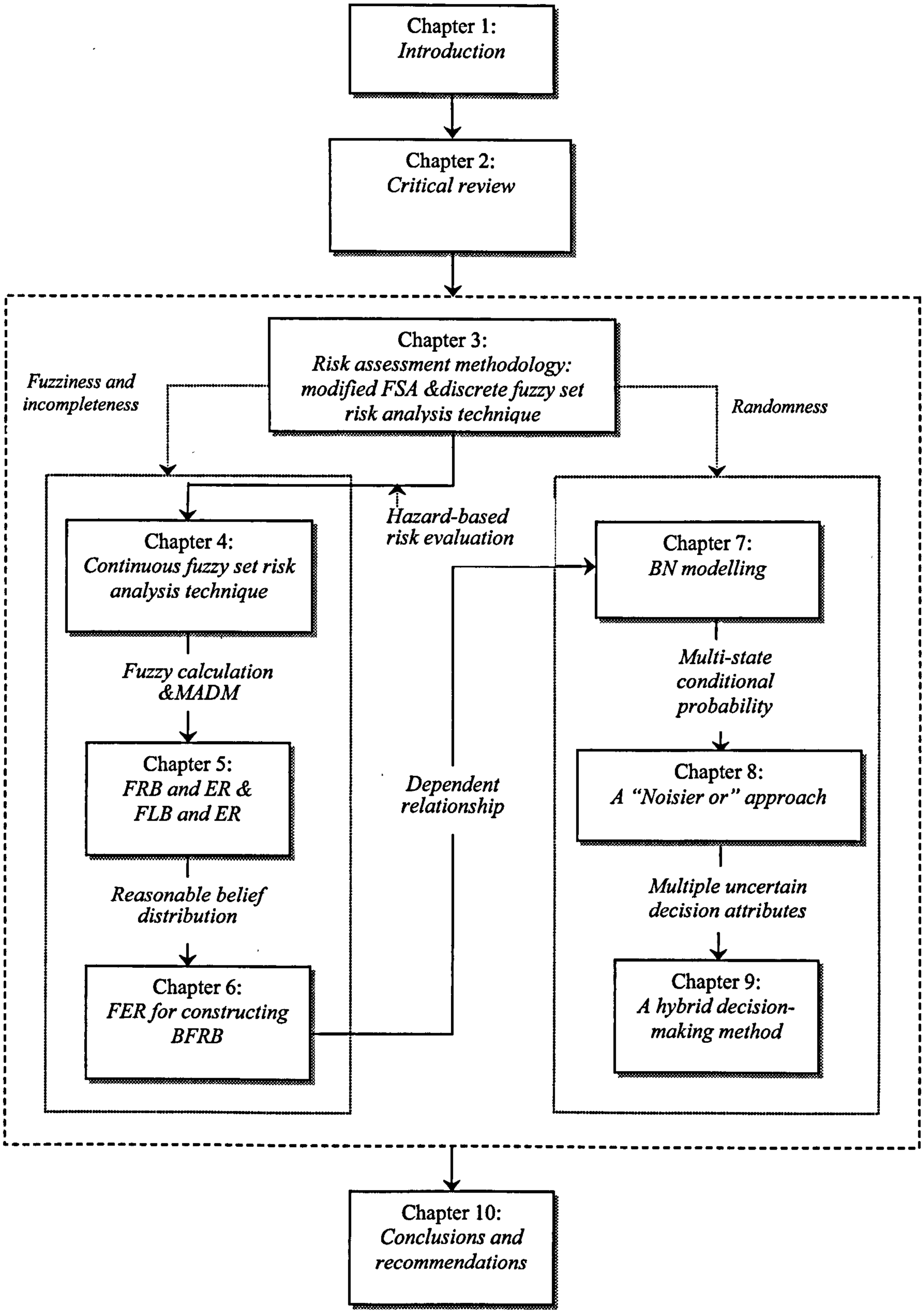


Figure 1.3. The structure of the thesis

The research scopes are set up to surround the core of the thesis, which is risk assessment and decision making of *CSCs*. The intention is to emphasize the application of some fundamental uncertainty treatment theories to the development of novel risk and decision modelling techniques and their potentialities to offer attractive features not always achievable by traditional means. The document therefore only explains the relevant theories and methods up to the level at which they are used to suit the objectives and aims clarified above instead of proving an in-depth theoretical and mathematical treatise of the theories themselves. The fundamental uncertainty theories originally step from and are mainly developed within such fields as human activity and Artificial Intelligent (*AI*) communication. This research is thus also deemed as an effort and contribution to a desirable technology transfer and communication from such areas to a modern risk assessment domain.

The thesis is complied in ten chapters. Following the description of the research scene in ***Chapter 1***, ***Chapter 2*** reviews the important literature influencing the current study. It includes the demonstration of the operation processes of *CSC* systems, the analysis of historical failure data, the review of risk assessment methodologies and approaches related to *CSCs* and the prior studies of using uncertainty treatment methods to risk assessment and decision making. The emphasis and kernel of the thesis start with Chapter 3 and end with Chapter 9. They are presented as follows in a detailed and interrelated manner.

The concept of quantitative risk analysis (*QRA*) has evolved during the last decades, starting with the safety analysis of nuclear power plants and the chemical industry and going through the risk assessment of the aerospace and marine (offshore and shipping) industries. Only quite recently, the supply chain industry has started using and further developing the methodology. In ***Chapter 3***, a conceptual methodology for *CSCs* based on a modified *FSA* framework is generated. Following the analysis of three major challenges, such a study defines an interactive five-step framework, in which some novel techniques are developed to rank risks with unavailable/incomplete historical failure data and make decisions with imprecise *CBA*.

Historical data is not always available and its collection consumes cost, time and effort and depends on many uncertainties. For example, in the process of conducting *FSA* of *CSCs*, the threat-based risks are normally ruleless and unpredictable in terms of either their risk likelihood or consequence. Also, the single consideration of historical statistics from previous cases, which may not be well suited to the current context without any adjustment, may easily cause academic bias. Under these circumstances the analysts may be able to use inductive assessment methods, in which possibilistic risk assessment is widely applied, and may also be forced to seek alternative (i.e. subjective linguistic) interpretations of probability. To deal with subjective linguistic interpretations fuzzy set

theory (*FST*) (Zadeh, 1965) can be appropriately used. The theory describes a humanistic problem mathematically (Zadeh, 1985) and therefore, can model such subjective risk linguistic variables and deal with their discrete characteristics (Wang *et, al.*, 1995; Wang *et al.*, 1996; Yang *et al.*, 2004). Unlike the risk evaluations in *QRA*, which are precisely expressed by some numerical values (i.e. potential loss of life (*PLL*)), the risk evaluations using fuzzy sets are impossibly synthesized by using normal mathematical logical operations. The *ER* approach is well suited to modelling subjective credibility induced by partial evidence. Consequently, a subjective risk assessment method based on a discrete fuzzy set technique is first developed in ***Chapter 3*** to deal with the incompleteness and unavailability of historical threat-based failure data.

The above research has greatly increased our understanding that a) the risks in *CSCs* originate from vulnerability, which can be considered as the marriage of hazards and threats; and b) the combination of the fuzzy set and *ER* approach can produce an appropriate method to deal with highly uncertain situations resulting from those threats. However, an important consideration of the effectiveness of the subjective risk assessment method is related to its capability of combining objective hazard-based risk evaluations. The risk assessment of *CSC* systems is highly possibly dependent on both hazard-based and threat-based risk implications simultaneously in a particular situation. Thus, it will be desirable that the subjective method can be used to carry out a unification of the two different risk implications in order to avoid loss of useful information. However, as the hazard-based risks may be described using objective precise quantities and the threat-based risks may be described using subjective fuzzy sets, it is not convenient to directly implement such a synthesis using either a normal mathematically logical operation or the *ER* approach. It is therefore necessary to develop a new continuous fuzzy set technique in ***Chapter 4*** to define a utility space for evaluating and synthesising objective and subjective safety expressions on the same scale.

The studies in Chapters 3 and 4 using discrete and continuous membership functions to characterise the linguistic variables to a set of categories may restrict the flexibility of experts' assessment. Furthermore, complex fuzzified and defuzzified operations are at times inadequately friendly to mathematically unsophisticated users. Consequently, more powerful possibilistic methods are incorporated into and developed to the risk assessment fields involving a high level of uncertainty. ***Chapter 5*** extends a Belief Fuzzy Rule Based (*BFRB*) expert system to risk and decision modelling with comparison of a new fuzzy link-based (*FLB*) decision modelling. A fuzzy rule-based (*FRB*) risk assessment technique (Sii *et al.* 2001; Pillay and Wang, 2003b; Liu *et al.*, 2004) unifying fuzzy logic theory and rule-based decision-making systems produces one feasible way to deal with imprecision on the basis of fuzzy production rules in fuzzy inference systems. However, in dealing with multiple hierarchical attribute decision making problems, the fuzzy rule-based method may produce an undesirable complex

calculation process, which includes the construction of multiple hierarchical fuzzy rule bases and inference between fuzzy input and output. The process can be simplified using a *FLB* method. Based on a linked belief structure between the linguistic variables expressing different level attributes, the method can unify all hierarchical fuzzy rule bases and transform the fuzzy input associated with the lowest level attributes to the corresponding fuzzy output on a common utility space constituted by the linguistic variables of the highest level attribute.

One major disadvantage of the *BFRB* approach is associated with accurately determining the parameter values (belief degrees) of the rule base entirely subjective, in particular for a large scale belief rule base with hundreds of rules. Furthermore, it is highly possible for many realistic *BFRB* systems to have different antecedent attribute weights and a change in an attribute weight may lead to significant changes in the performance of the *BFRB* systems. As such, ***Chapter 6*** presents a novel and generic fuzzy *ER* method (*FER*) for constructing *BFRB* expert systems. The new method is proposed for effectively dealing with the difference among the antecedent attribute weights and rationally producing and judging the belief degrees related to the conclusion parameters. The main feature of the new method is to consider the conditional belief degree distributions of the conclusion parameters given the individual antecedent attribute in a *BFRB* as partial conditions and then synthesise all partials using the *ER* approach to obtain comprehensive belief degree distributions.

Despite showing much attractiveness, the *BFRB* and *FLB* method discussed still reveals some application problems. The principal limitation is that adding/removing risk factors or their linguistic variables may significantly affect a *FRB* system (i.e. its size may significantly be increased/reduced). Moreover, the method can be very difficult to address the interactive dependent features of the risks in *CSCs*, although employing *If-Then* rules is arguably able to describe the intercausal relationship between the risk factors to a certain degree. In other words, the interactive rather than intercausal risks in the chains require an effective solution to have the inherent ability to reverse inference logic, however the rule-based tool cannot realise the exchange from the output to input parts of one rule without redeveloping the rule base. ***Chapter 7***, therefore, proposes a *BN*-based risk assessment model for assisting the *CSCs*' managers to check, predict and improve the safety and reliability performance of the chains. For any *CSC* safety-critical application, the methodology demonstrates how the *BN* technique can be used in formalizing the reasoning of systematically interactive dependence and incorporating subjective expert judgements to compensate for the absence of objective statistical data.

BNs provide a unified and consistent framework for analysing and expressing risks and thus, have been broadly analysed and applied to safety studies. Yet, the research above focuses on using the advances of Bayesian theorem and posterior probabilities to risk

prediction and diagnosis (forward and backward inference) and assumes that the risk related prior probabilities could be easily obtained from subjective expert judgements if the associated objective historical failure statistics is incomplete or unavailable, although in many circumstances this is realistically not the case. ***Chapter 8***, therefore, discusses and deals with some of the practical challenges of implementing Bayesian reasoning in relative risk analysis (from the Bayesian view), which corresponds to those positivism risk analyses from a classical perspective, including the risk ranking in a networking environment using the sensitivity analysis (*SA*) of *BNs*. It emphasizes the introduction of a novel "*Noisier or*" approach on the basis of an *ER* algorithm for obtaining the Bayesian prior probability distributions conditioned on multi-state parents. Consequently, analysts can assign subjective probabilities with single condition and synthesise them using the *ER* algorithm (and its attached computing software – *IDS*) without adopting the somewhat mathematically sophisticated procedure of specifying prior distributions with multiple parents.

After the updating and modification by the approaches introduced in Chapter 8, the *BN* model of risk assessment created in Chapter 7 can provide a more powerful risk assessment support tool and be used in a range of practical applications connected with *CSC* systems. In most of these applications, the interests are, however, only focused on the single attribute of the systems, safety or reliability. Although such networks provide important support for risk based decision making, in many circumstances decisions need to be made on the basis of multiple attributes, such as safety, cost, techniques, politics and environmental factors, etc. *BNs* do not allow for the incorporation of the notation of preference, which is necessary in such cases. Because they cannot, alone, provide a complete solution for the kind of wider decision problem in which a systematic safety assessment exercise inevitably fits, the *BNs* must be complemented by other decision making techniques (Fenton and Neil, 2001) such as those associated with Multiple Attribute Utility Theory (*MAUT*) (Keeney and Raiffa, 1976). In ***Chapter 9*** a heuristic two-stage methodology that enables the quantification of the uncertainties related to the risk attributes based on *BNs* and then uses the fuzzy logic theory to generate novel utility representation functions for selecting the "optimal" safety solution is outlined as an effective and realistic alternative.

Chapter 10, the conclusion chapter of this thesis, distils the evidence and the arguments presented in the previous chapters, and from the distillate, a novel and sound risk assessment methodology with many original and advanced risk analysis and decision making methods and techniques can be clearly displayed. The hypothesis can be validated by comparing and discussing fuzzy and *BN* related modelling. The results of the study will be emphasised by demonstrating their academic and practical contributions of assessing risks and making decisions inherently having an uncertain nature as well as facilitating the recommendation of future work.

1.6 Conclusion

The basic concepts, ideas and conditions of developing a novel risk assessment methodology and the relevant risk and decision modelling to facilitate the *CSC* risk assessment in various situations have been put forward. The main problems are identified, the research objectives are targeted, the hypothesis condition is stated, a logical research structure and scope is represented and a considerable body of publications (See Appendix 1) is achieved to validate the accuracy and reliability of the deliverables against the objectives.

Chapter 2 – Critical Review

SUMMARY

The critical review of CSC systems taken in this chapter is broad, embracing all processes that are associated with container cargo flow and its value-added services. Equally wide is the range of the review associated with the risks considered which cover not only the historical failure data analysis and literature review of risk assessment methodologies and technologies related to CSCs, but also the presentation of the prior contributions of uncertainty treatment methods to risk and decision studies.

2.1. Introduction

Over the last five years there has been growing international recognition that the safety performance of *CSCs* needs to be reviewed on an urgent basis. Three serious accidents - the 9/11 terrorism attacks in 2001, the lock-out of the American West Ports in 2002 and the breakout of SARS disease in 2003, closely related to the chains in particular have prompted this urgency whilst they shocked the whole international shipping and logistics industries. Both the public and political authorities have woken up to the situation that the evolution of liner shipping from the original general-cargo liner service to the current complex *CSCs*, together with the increasing dependency of the world economy to them, has virtually increased its risk stake and categories. The risks occurring in modern *CSCs* not only range from the possibility of physical breaches in the integrity of shipments to the interruption of information communication, but also come from the vulnerability in wider levels that may be personal, managerial or environmental. Furthermore, academies and industries have initiated research and adopted more systematic and effective safety methods to assess and manage their *CSCs*. Therefore, in order to ensure the significance of this research, it is necessary to give an overall and detailed review of the operational processes, historical failure data, historical development of risk assessment research related to *CSCs* and the prior studies of using uncertainty treatment to risk assessment. This chapter just focuses on this point and demonstrates and highlights the necessity and motivation of this research.

2.2 The Operational Process of *CSCs*

Modern *CSCs* are very complex. A typical door-to-door journey using a shipping container will involve the interaction of approximately 25 different participants, generate 30-40 documents, use 2-3 different modes and be handled at as many as 12-15 physical locations (OECD, 2003). Compared to other logistics systems, *CSCs* have two

distinctive features. One is that both physical and information flows move in the same direction, although the information flow should always be ahead of the physical flow. The other is that another sub-flow - custody flow is identified under the umbrella of the physical flow in order to attempt critical assessment of the risks/vulnerability in the system as comprehensively as possible.

2.2.1 Physical Cargo Flow

A physical cargo flow means the physical movements of cargo from place to place and from mode to mode. Cargo originates from a manufacturer's place where it is palletized and/or packed into a container and transported by road/rail either directly to a port, or to an intermediary's premises. In the latter case, the shipment will be consolidated with others and transported to a multi-modal stacking area or to a port. While in transit, the container may be stationary for various periods of time as trucks are stopped on the roadside and/or container-carrying trains are being assembled in freight yards. Once in ports, the container is sent to a stacking area before it is placed immediately next to the vessel on the quay. Even within the port area, a container may be moved several times as required by port operators and/or the Customs. After being placed on board, the container can be removed and trans-shipped through another port onto another vessel before arriving at its destination port. Here again, the container may be moved several times for Customs clearance and temporary storage while waiting to be picked up. Carried by road or rail to its final destination, the shipment may again transit several intermediaries' facilities where the container is unpacked and the palletised shipments it contains are distributed to the final consignees (OECD, 2003). Such a cargo flow process can be visually presented in Figure 2.1.

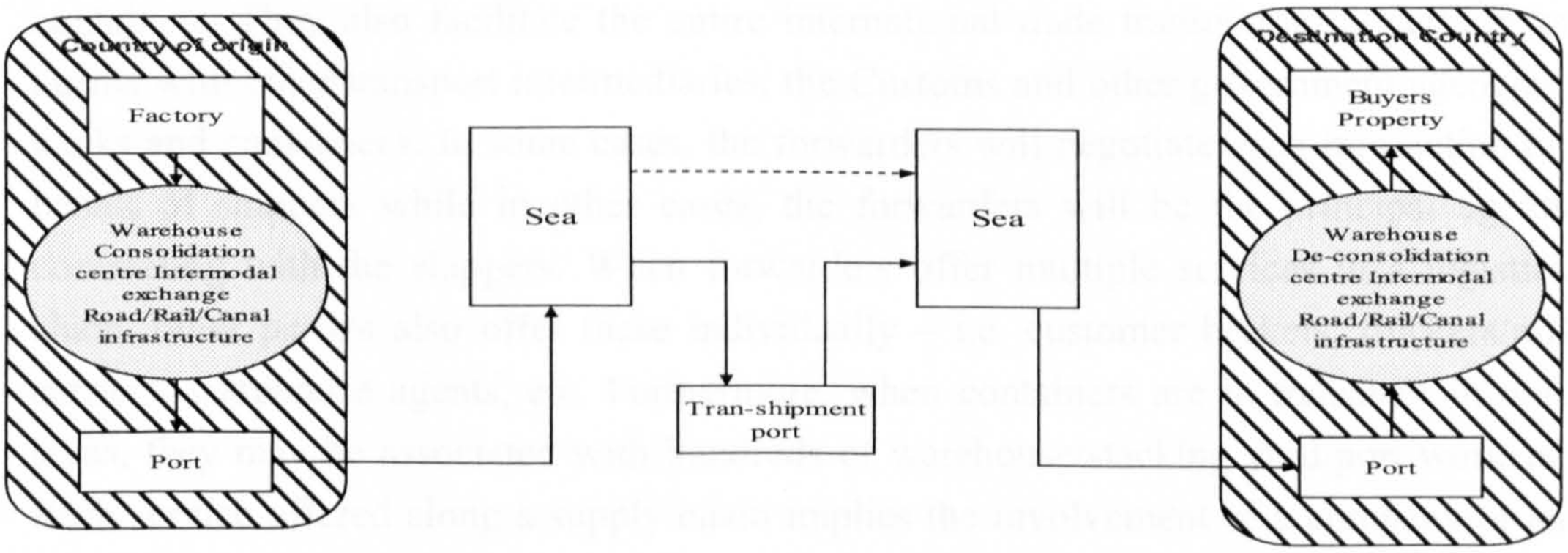
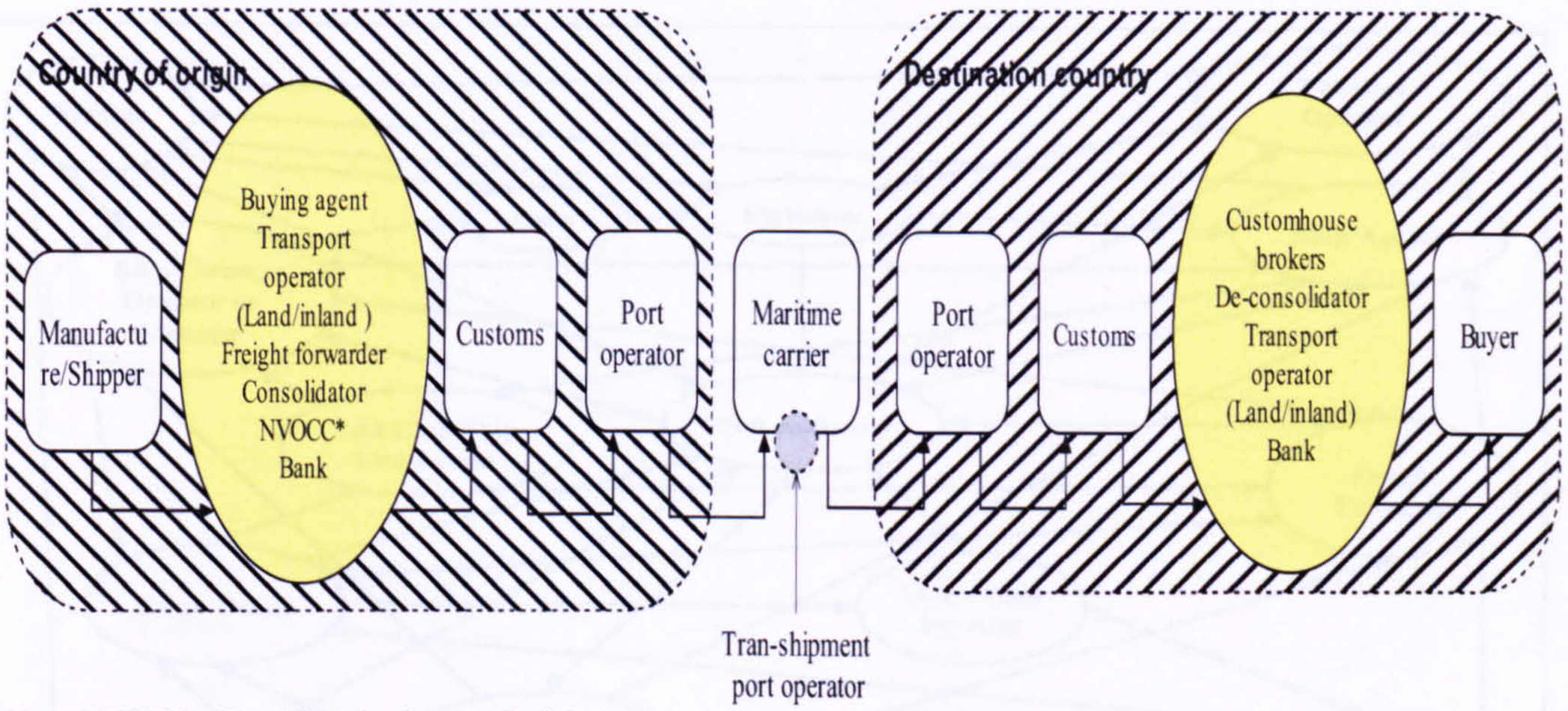


Figure 2.1. The physical flow of a *CSC*

2.2.2 Custody Flow

With the physical container flow, the movements of the custody of containers from person to person, which are presented in Figure 2.2, should be carefully studied. Every



Note: NOVCC (Non-Vessel Operating Common Carrier)

Figure 2.2. The custody flow of a *CSC*

CSC includes dozens of stakeholders who can physically come into contact with containers and their contents or are potentially related with the container trade and transportation. At the beginning of every container journey there is an originating shipper -- most often a manufacturer. There are hundreds of thousands of manufacturers around the world and many of them are active in international trade. These manufacturers may produce high enough volumes that they can ship full container loads (*FCL*) directly. Most, however, produce less than container load (*LCL*) shipments that must be consolidated before being shipped by sea. Buying agents and/or freight forwarders serve as the most common intermediaries between originating shippers and ocean carriers. While many freight forwarders handle *FCL* shipments for their clients, their principal task revolves the assembly and consolidation of *LCL* shipments into full containers. They also facilitate the entire international trade transaction by serving as agents with other transport intermediaries, the Customs and other government agencies, banks and consignees. In some cases, the forwarders will negotiate each transaction on behalf of shippers while in other cases, the forwarders will be the principal agents contracting with the shippers. When forwarders offer multiple services in a logistics chain, other parties also offer these individually – i.e. customer brokers, truckers/rail carriers, warehouse agents, etc. Furthermore, when containers are in transit or in port areas, they may be associated with hundreds of warehouse/stacking yard/port workers. Each service offered along a supply chain implies the involvement of a company or an organization with several to several hundred people, any one of whom may potentially affect the chain's operation or be affected by an accident or by the cost effectiveness of either any proposed new regulatory requirement set by authority departments or a new insurance rule issued by underwriters (OECD, 2003). The principal stakeholders of a *CSC* have been identified and their interrelationships considered as shown in Figure 2.3.

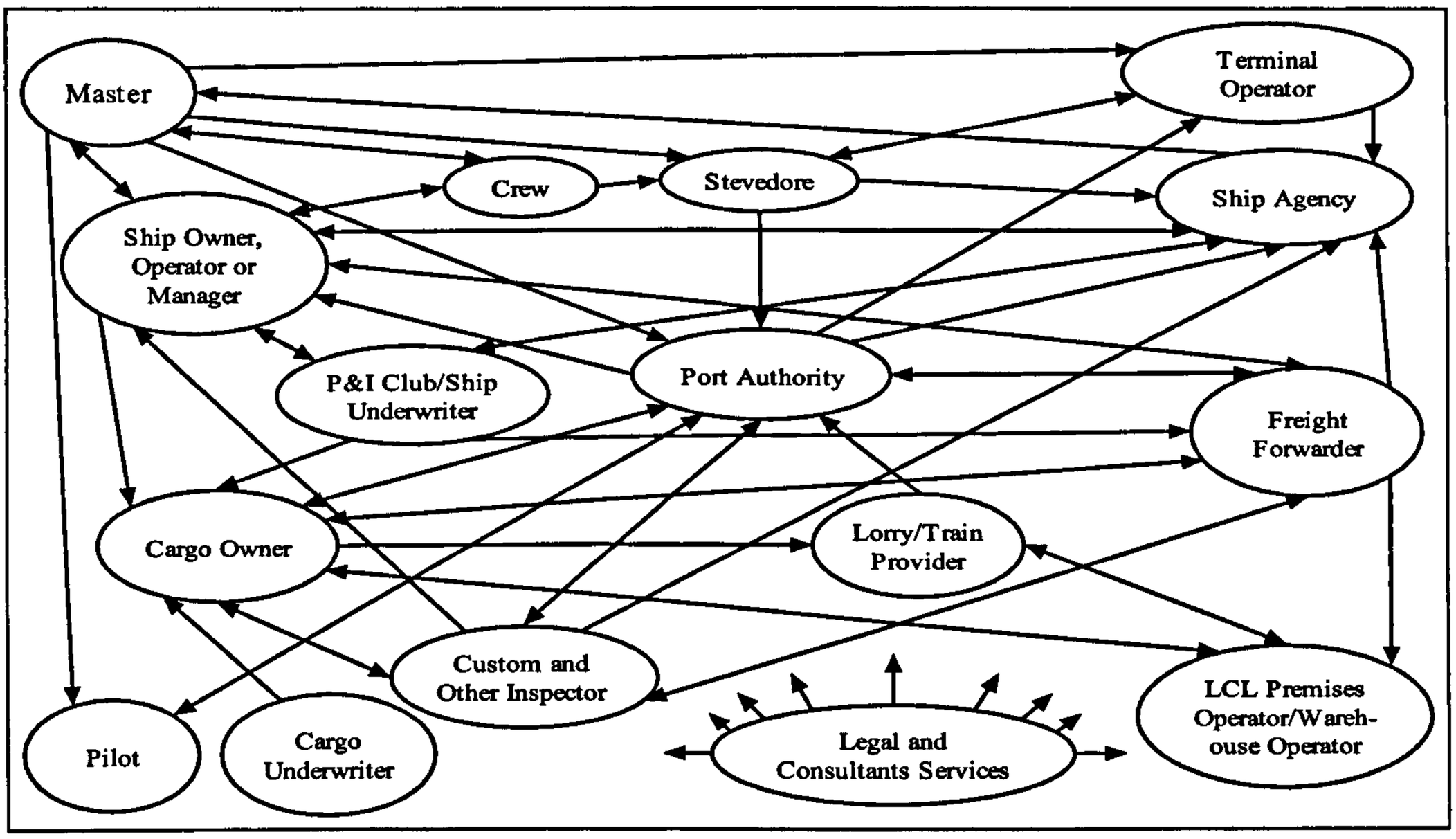


Figure 2.3. Stakeholder influence map

2.2.3 Information Flow

The information transmission is required to comply with the physical cargo flow of a *CSC*, but be ahead of it. When shippers sign contracts with their freight forwarders, the information about cargoes can be transmitted and keyed to forwarders' information management systems with certain editions and amendments. Considering the requirements of shippers and the vessel schedules of shipping lines, the forwarders make bookings for the cargoes and distribute the information to the liner shipping information networks, which are supported by new information technology and can provide help to realise the instantaneous communication and information share between shipping lines, ports, container terminals and stevedores (internal network), even freight forwarders and shippers to a certain degree (external network). After confirming the bookings, the shipping lines pass the information to inland transport companies in order to arrange the collection and delivery of the container cargoes. At the same time, the information flowing in the network will be updated according to the loading and discharging of the cargoes during the lines' voyages. Those later ports of call will receive updates as the information is changed as a result of the operation in the previous ports. When the cargoes finally arrive at their destination ports, the information will be passed to notify parties/consignees by shipping lines' agencies so that they can make full preparation for accepting the cargoes. Simultaneously, it is noteworthy that the information flows may trivially change depending on different operations. Figure 2.4 shows a comparatively popular information flow model.

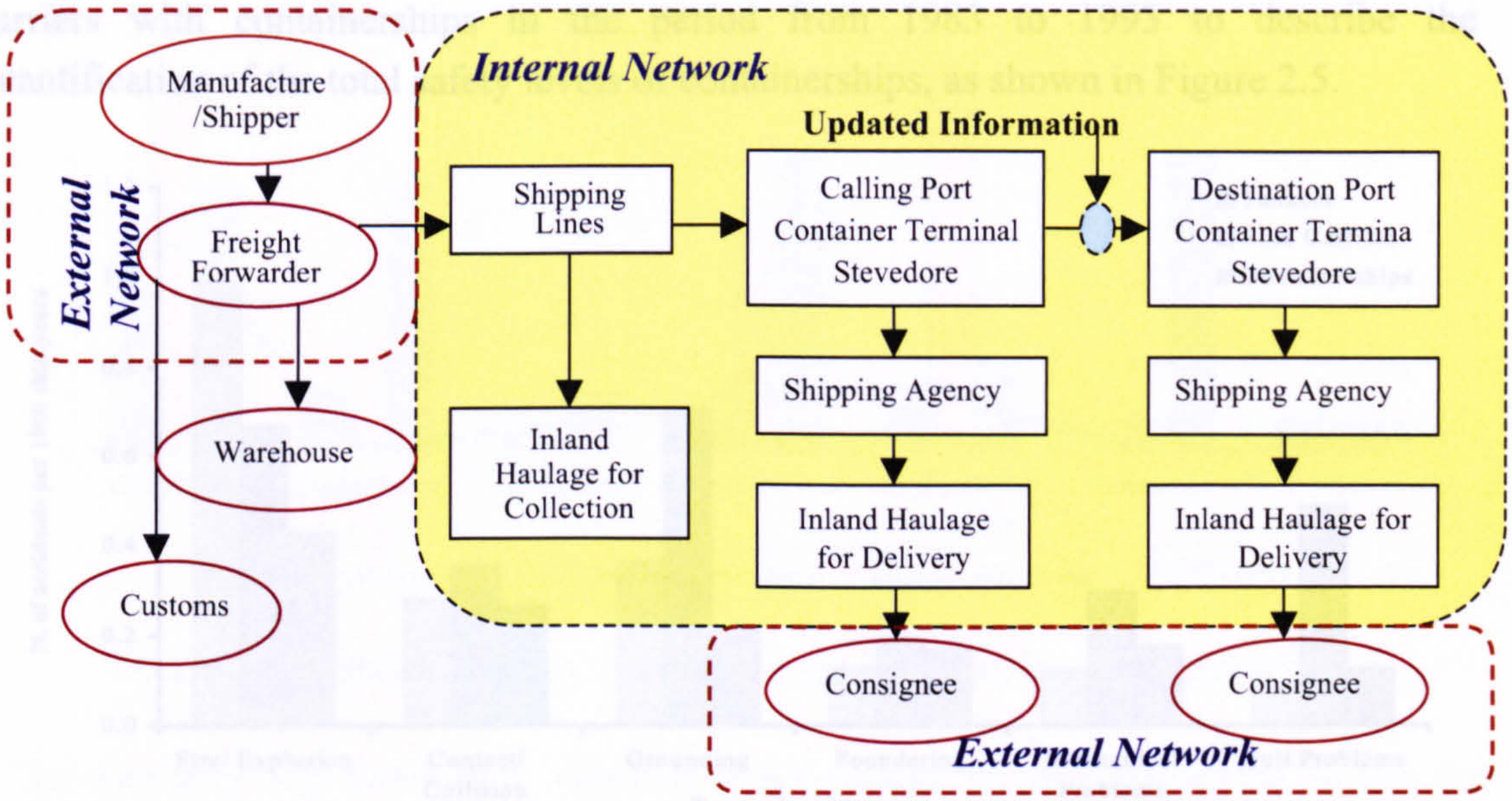


Figure 2.4. The information flow of a *CSC*

2.3. Historical Failure Data of *CSCs*

In order to carry out any kind of safety analysis, either qualitative or quantitative, it is essential to obtain reliable failure data. The amount of data available will determine the choice of risk analysis methods and the relevance and accuracy of data used will increase confidence in risk assessment (Wang and Foinikis, 2001). There are several databases available at international, national and company levels. However, the various data and databases are usually collected and designed on different bases using changing risk criteria according to individual research interest and perspectives. Therefore, the accident statistics for this study may have to be judged by experts when necessary. The following are some typical accident databases associated with *CSCs*:

- Data collection programmes by *IMO* and United Nations (*UN*).
- Data collection programmes by British Department of Transport (*BDT*) and the UK Health & Safety Executive (*HSE*).
- Data collection programmes by Lloyds Register, P&I Clubs and *DNV*.
- Data collection programmes by the Institute of Shipping and Logistics (*ISL*) and many relevant research groups.
- Data collection programmes by international ports (i.e. Shanghai and Liverpool).
- Statistics maintained by private shipping and logistics companies (i.e. COSCO).

The Lloyds Maritime Information Services (*LMIS*) casualty database is a sophisticated one, recognized as one of the most reliable existing databases (Lloyds Register, 1978-2004). The database compares the analysis of accident statistics of tankers and bulk

carriers with containerships in the period from 1983 to 1993 to describe the quantification of the total safety levels of containerships, as shown in Figure 2.5.

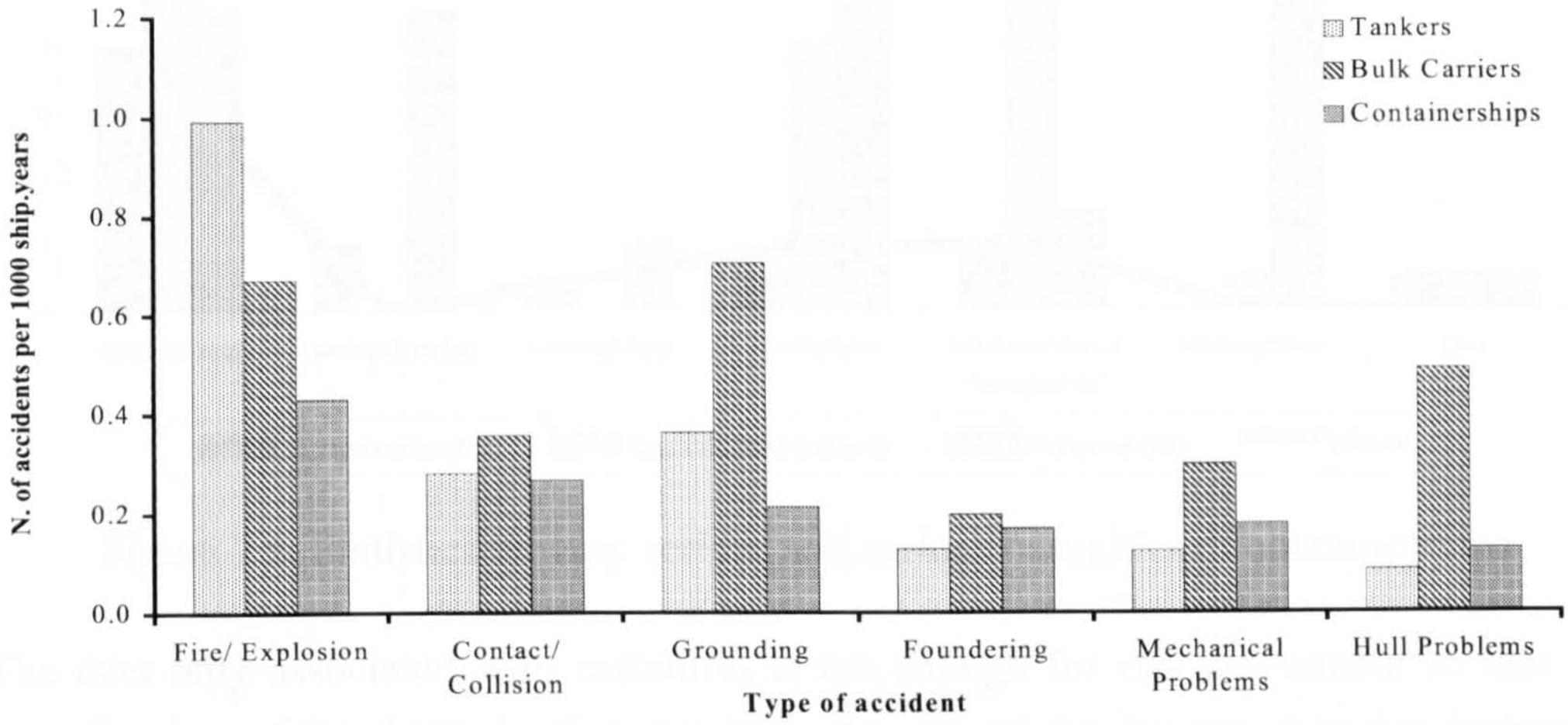


Figure 2.5. Distribution of annual average rate of the initial event by ship types

Although containerships keep good safety records in all international trading cargo ships, their risk problems are still worrisome, especially considering the high value of their cargoes. The Sub-Committee on Flag State Implementation (*FSI*) of *IMO* used the data received from Rescue Co-ordination Centers (*RCCs*) (*FSI* of *IMO*, 1999-2002) to provide the casualty comparison between containership and other ship types in the period of 1998-2000. This is shown in Table 2.1.

Table 2.1. Distribution of casualty statistics by ship types

Year	General cargo	Bulk carrier	Container	Tanker	Passenger	Reefer	Ro/Ro	Others	Total
1998	124	52	16	35	4	6	19	31	287
1999	223	75	20	56	9	10	14	109	516
2000	185	89	22	45	17	16	39	85	498
Total	532	216	58	136	30	32	72	225	1301
Percent	41%	17%	5%	10%	2%	2%	6%	17%	100%

In terms of casualty categories, Figure 2.6 with reference to the statistics obtained from *RCCs* shows six principal risk areas for containerships. It describes these with reference to four parameters, which are defined as very serious casualties, serious casualties, loss of life and total loss of containerships. Observing the figure, one result found is that contact/collision, with 8 very serious and 9 serious casualties is on the top of the list of casualty categories and the three most significant categories resulting in the loss of life are the failure of hull/watertight doors (with 13 lives), contact/collision (with 10 lives) and fire/explosion (with 8 lives).

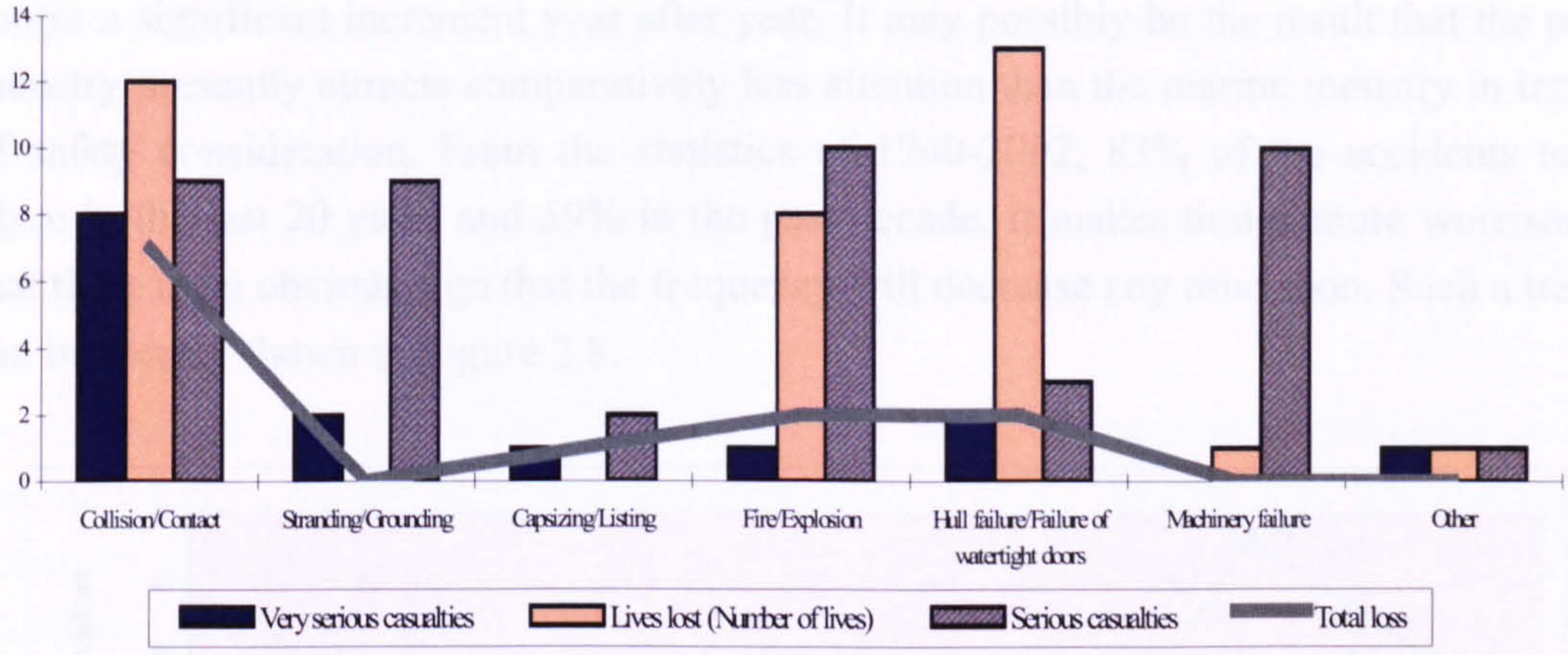


Figure 2.6. Statistics on very serious and serious casualties of containerships

The data only associated with casualties is not enough for risk assessment so that the investigation of incidents is also required. As one of the largest shipping insurance companies, P&I Clubs can be a very useful source of failure data mainly because of the large amount of vessels they represent. Compared with Lloyds Register who tends to look into safety from the viewpoint of compliance with the various sets of rules in force, P&I Clubs tend to deal with the risks from the aspect of financial losses due to lack of safety. Therefore, their database also includes the statistic of all incidents for claims. A research project carried out by the UK P&I Club (1999) shows that for the 10-year period from 1989 to 1999 incidents involving containerships account for up to 7% of the total and these incidents with 273 claims of USD 110 million in total are distributed between the different categories as shown in Figure 2.7 (as far as the number of claims is concerned).

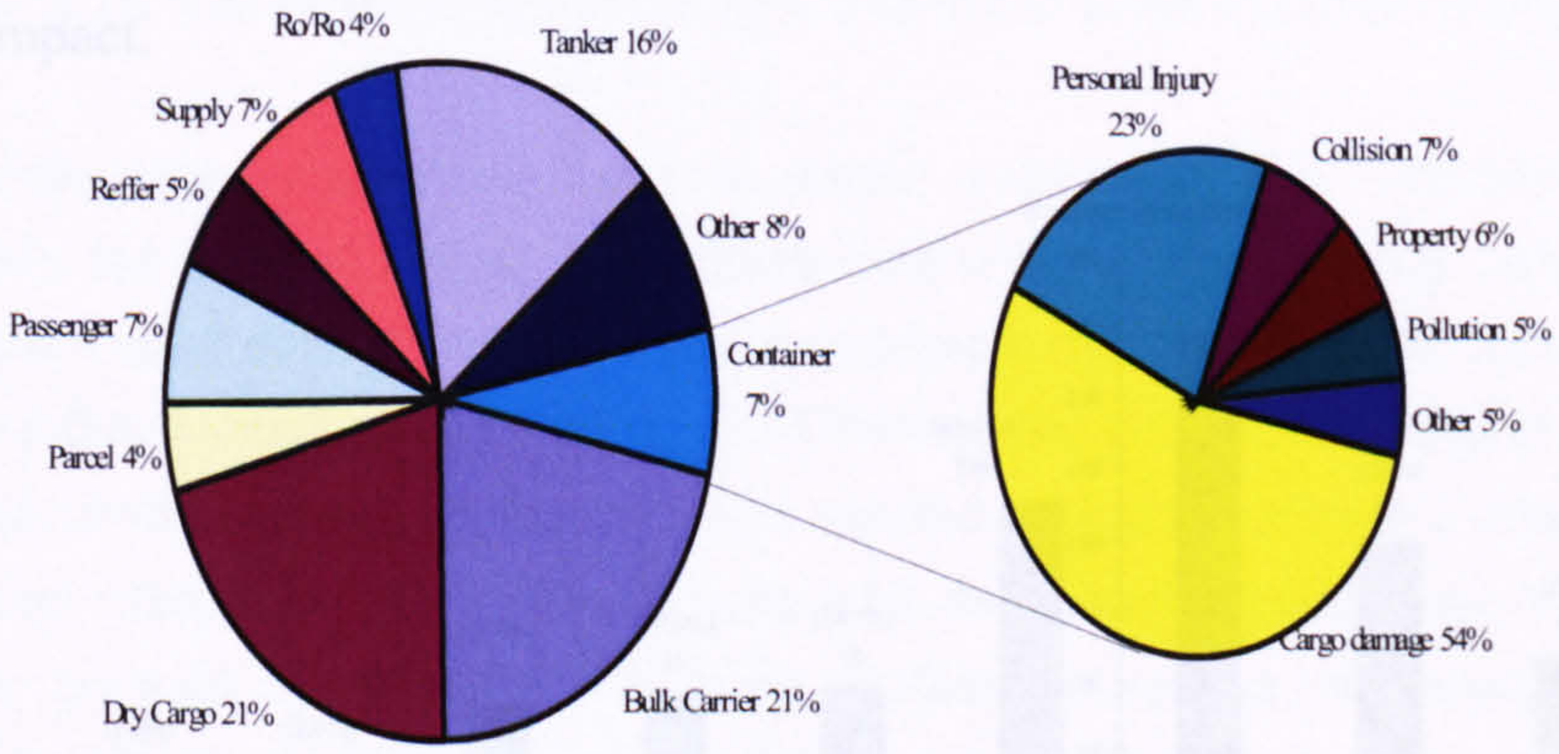


Figure 2.7. Distribution of incidents per ship type and incidents involving containerships

Apart from containership failure statistics, a database from the Major Hazard Incident Data Service (*MHIDS*) (*HSE*, 2003), which is developed and managed by the safety and reliability directorate of the *UK HSE*, has been used to carry out this study and provide port accident data. The database includes accidents occurring in 95 countries. In comparison to the shipping industry, the frequency of accidents in the port industry

shows a significant increment year after year. It may possibly be the result that the port industry presently attracts comparatively less attention than the marine industry in terms of safety consideration. From the statistics of 1940-2002, 83% of the accidents took place in the last 20 years and 59% in the past decade. It makes things more worrisome that there is no obvious sign that the frequency will decrease any time soon. Such a trend can be clearly shown in Figure 2.8.

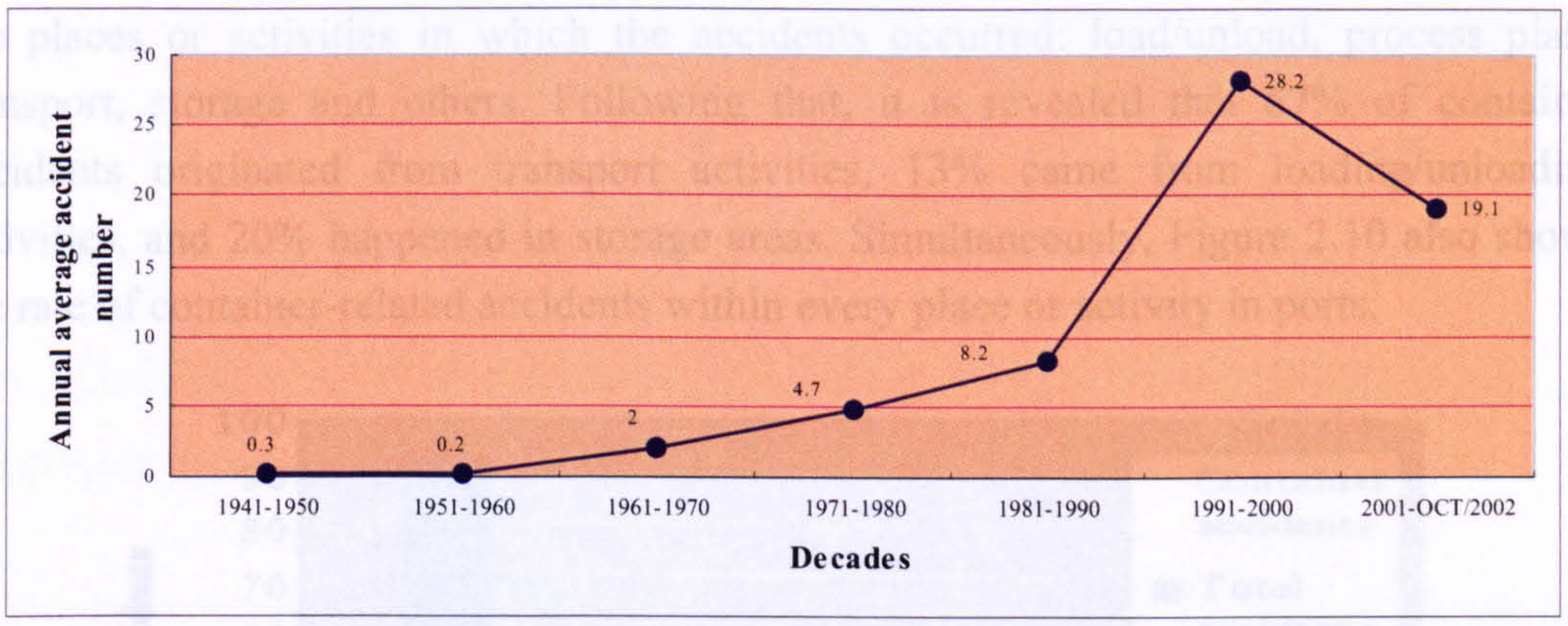


Figure 2.8. Distribution of annual average accident number in ports

As far as the cause categories of port accidents are concerned, they differ from those in the marine categories because most accidents associated with ports only arise from a few general causes. Figure 2.9, which is developed on the basis of the *MHIDS* database, indicates that 94.4% of port accidents were due to four causes: impact, mechanical, external and human. Furthermore, approximately 50% of them were concentrated in the category of impact.

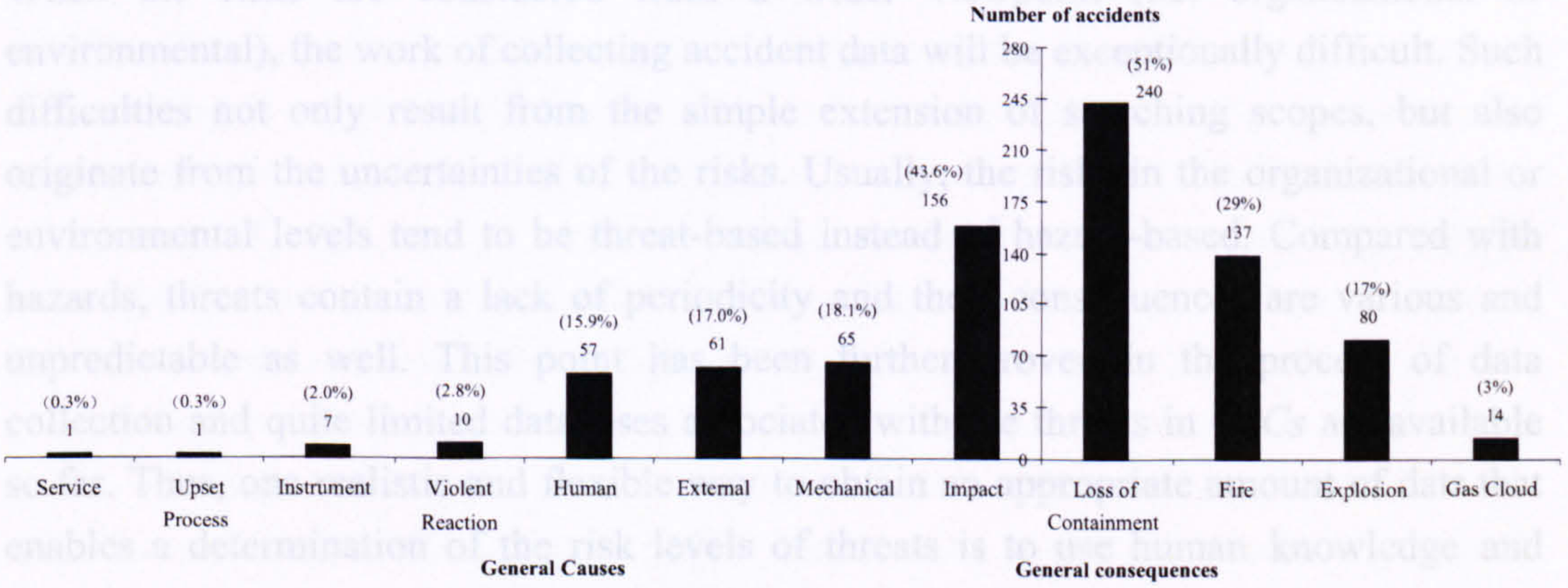


Figure 2.9. The general causes and consequences of port accidents (Darbra and Casal, 2004)

Further analysing the 471 port-related accidents in the *MHIDS*, almost half of them, 234 accidents are related to ocean going vessels in port areas and the remaining 237

accidents are "pure" port accidents. Having researched containership accident and incident statistics above, the emphasis will be focused on the confined container accidents occurring in the scope of those "pure" port accidents. Unlike the good safety record kept by containerships in the marine industry, the accidents related to containers in the port industry account for a high failure rate of 18.6% with 44 accidents in total.

In terms of the origin of accidents, five different categories are considered to designate the places or activities in which the accidents occurred: load/unload, process plant, transport, storage and others. Following that, it is revealed that 67% of container accidents originated from transport activities, 13% came from loading/unloading activities, and 20% happened in storage areas. Simultaneously, Figure 2.10 also shows the rate of container-related accidents within every place or activity in ports.

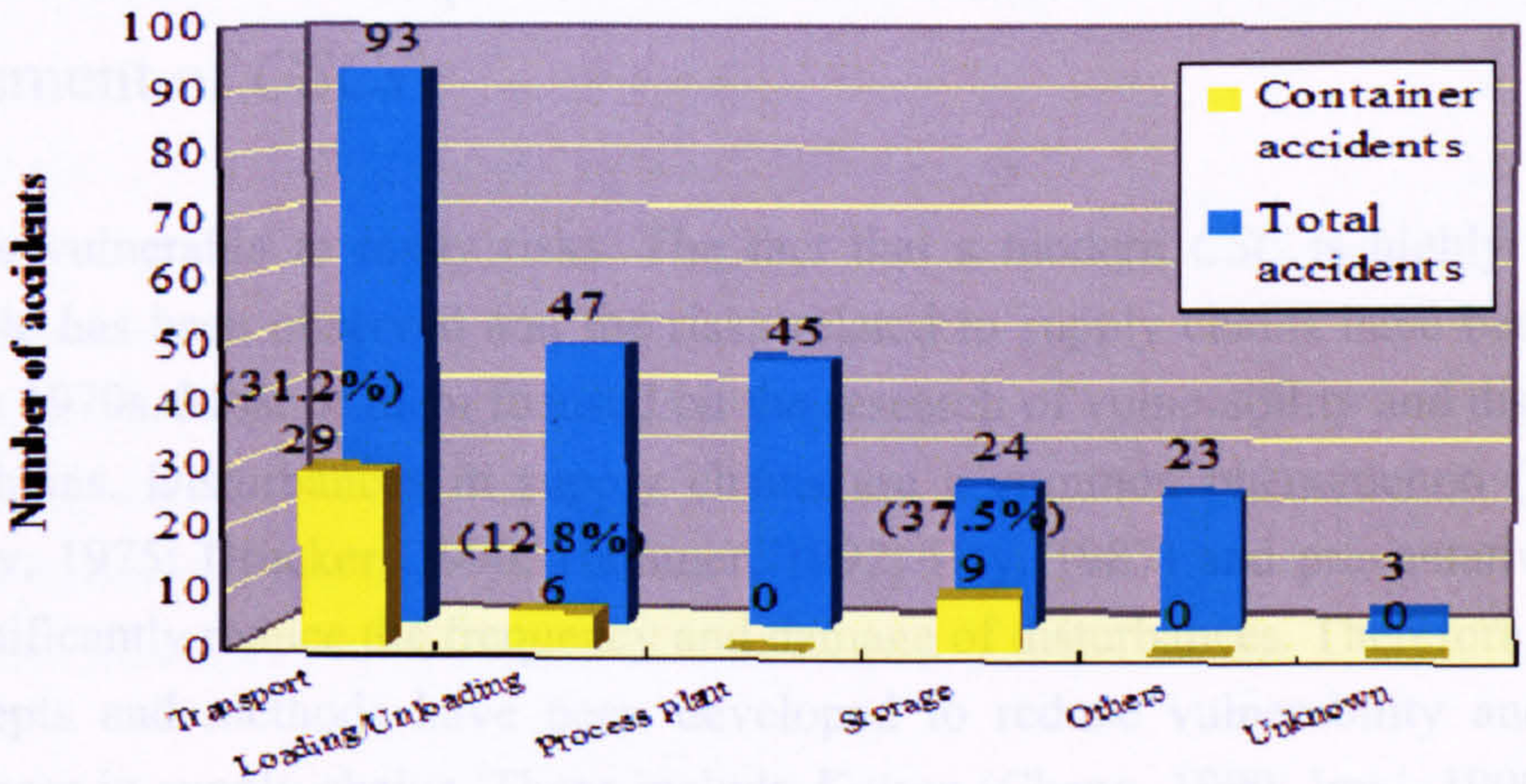


Figure 2.10. Distribution of container accidents in ports in terms of origin

When the risks are considered from a wider viewpoint (i.e. organizational or environmental), the work of collecting accident data will be exceptionally difficult. Such difficulties not only result from the simple extension of searching scopes, but also originate from the uncertainties of the risks. Usually, the risks in the organizational or environmental levels tend to be threat-based instead of hazard-based. Compared with hazards, threats contain a lack of periodicity and their consequences are various and unpredictable as well. This point has been further proven in the process of data collection and quite limited databases associated with the threats in *CSCs* are available so far. Thus, one realistic and flexible way to obtain an appropriate amount of data that enables a determination of the risk levels of threats is to use human knowledge and experience. Consequently, a research project funded by the *BDT* has been conducted by Cranfield University to investigate those risks carried by leaner, faster and more efficient supply chains through a survey of 137 senior supply chain managers (Peck and Jüttner, 2002). One of the findings has revealed that the most widely catered for risks in supply chains are focused on ten scenarios, as shown in Figure 2.11.

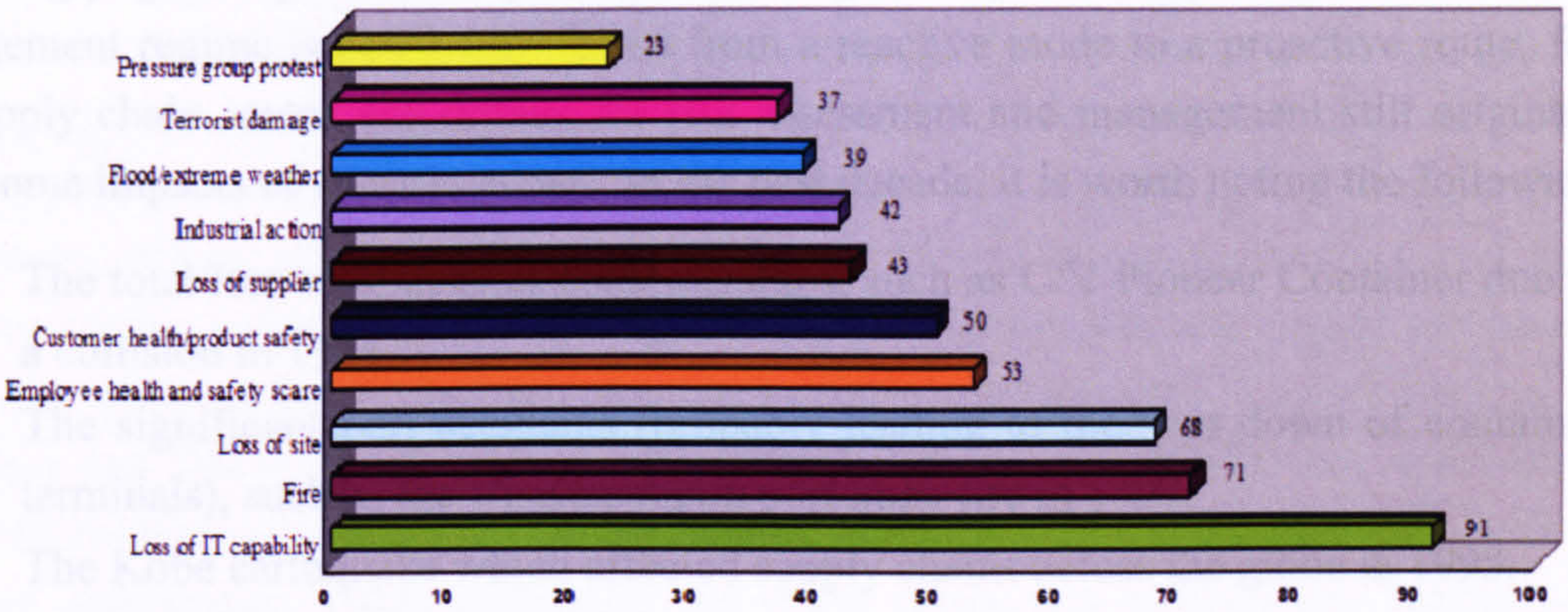


Figure 2.11. The top ten risk scenarios in supply chains

2.4. Historical Developments and Prior Studies Related to Risk Assessment of *CSCs*

CSCs are vulnerable to many risks. The fact that a modern *CSC* is highly risky and vulnerable has been observed and the risks related to supply chains have been studied since the 1970s. Most of them focused on the research of vulnerability and disturbances in the chains. Disturbances in supply chains are a common phenomenon (Bruk and El'Yanov, 1975; Drucker, 1990; Hammer, 1992; Hay, 1987) and preventative actions may significantly reduce the frequency and damage of disturbances. Therefore, a variety of concepts and methods have been developed to reduce vulnerability and prevent disturbances in supply chains. These include *Kaizen* (Cheng, 1990; Imai, 1990), *Jidoka* (Sugimori *et al.*, 1977), *Andon* (Monden, 1994), *the Seven Q:s and the Seven New Q:s* (Ohno, 1988), *Autonomation* (Monden, 1994; Carr, 1992), *Five why* (Ohno, 1988), *Total productive maintenance (TPM)* (Nakajima, 1989), *Single-minute exchange of die (SMED)* (Shingo, 1985) and *5S* (Monden, 1994). Furthermore, much research about the vulnerability in supply chains has been conducted and positioned under the concept of contingency planning (*CP*). Ballou (1987) and Johnson and Wood (1993) identified two sub-groups of *CP*, namely system breakdown and product recall. Principally, vulnerability research belongs to the category of system breakdown. Thus, in order to better review the risk research in supply chains, the studies about *CP*, especially the sub-group of system breakdown studies, are important information resources. Coyle *et al.* (1996) stated that *CP* considers preparing to deal with calamities (i.e. flood) and non-calamitous situations (i.e. strikes) before they occur. Many risk/uncertainty models (Knight, 1921; Ganesan, 1994) and reliability analyses (Sandler, 1963; Frankel, 1988; Evans, 1993) under the umbrella of *CP* are closely related to the vulnerability research in supply chains.

The attention paid to and research conducted on the risk studies of supply chains are

increasingly growing as time goes on. Although today in many industries the risk management regime is being transferred from a reactive mode to a proactive route, for the supply chain sector, the drivers for risk assessment and management still originate from some impacts of specific events. In the past decade, it is worth noting the following:

- The total loss of dozens of containerships, such as C/V Pioneer Container due to a collision in 1994.
- The significant port accidents (probably leading to the shut down of container terminals), such as the Visahapatnam port huge fire in 1997.
- The Kobe earthquake which affected supply chains across the globe in 1995.
- The Asian economic crisis in 1997 affecting world trade and container transport.
- The Toyota fire which forced a component supplier to shut down its production in 1997.
- The Y2K-related IT problems at the end of the 20th century influencing the information flow of *CSCs* (1998-2000).
- The fuel protest of September 2000 across Europe.
- The spread of foot and mouth disease throughout the UK early in 2001.
- The British transportation infrastructure failures.
- The terrorist attacks of 11th September 2001 in USA making more container security issues to be considered.
- The lockout of American West Ports of October 2002.
- The breakout of SARS disease in the world in 2003.

These events have stimulated discussions more than ever on the need to find ways to avoid potential vulnerability and thus improve the reliability of supply chains. People started to adopt more systematic and effective methods to assess and manage their supply chains. A method of quantifying the reliability of supply chains for contingent logistics systems was developed based on *a reliability interference theory* (Thomas, 2002). Some of the strategies for risk management were presented and applied to assess and mitigate the risks in inbound logistics (Siferd and Smeltzer, 1997). Introducing the concept of *Six Sigma* into the context of supply chains, Narahari *et al.* (2000) and Garg *et al.* (2003) developed and applied an innovative approach for designing a *Six Sigma* supply chain network to qualify supply chains in terms of synchronized delivery. After reviewing existing techniques used in decision making for risk analysis, Pai *et al.* (2003) presented a modelling and analysis framework for assessing logistics risks and evaluating safeguards to secure supply chains. Svensson (2000, 2002) generated a framework for managing vulnerability in supply chains and analysing it from firms' inbound and outbound logistics flows. Chapman *et al.* (2002) identified supply chain vulnerability and used an advanced "*3-P*" approach to manage risks in logistics supply chains. Peck and Jüttner (2002) further identified the vulnerability in logistics supply chains and gave its failure modes in detail by a survey to 137 senior supply chain

managers. Wang and Foinikis (2001) used a *FSA methodology* to give an overall analysis of the risks of containerships. Ronza *et al.* (2003) and Darbra and Casal (2004) carried out risk assessment in the subject of ports through a historical analysis of accidents. Responding to increasing terrorism attacks in the globe after 11th September 2001, many efforts were made to enforce the security of international ships and port facilities against terrorism risks. Many authorised regulations, reports, papers and books came out, such as those produced by *IMO* (2002), Organisation for Economic Co-operation and Development (*OECD*, 2003), and Burns *et al.* (2003), etc. Apart from such risk studies, some thoughts from previous scholars were also made to the field of logistics information risks, especially the Y2K crisis and information security in logistics supply chains. Labib (1998) applied a logistics approach to manage the millennium information system problem. Golter and Hawryl (1998) illustrated the serious harmfulness of the Y2K issue to logistics outsourcing in the fifth circle of his study -- "Circle of Risk". The works of De Jager and Bergeon (1997), Keogh (1997), Murray and Murray (1996), Ragland (1996) and Ulrich and Hayes (1997) also addressed the millennium problem. Since logistics have been increasingly dependent on new information technology, information security becomes the key and foundation to guarantee the success of logistics businesses. Hence, the research in this field ranging from information security policies (i.e. the works of Parker, 1998; Perry, 1985; Warman, 1992) to the concrete technical methods of managing information systems (i.e. the works of James, 1996; Siponen and Baskerville, 2001) has been conducted by many scholars, with promising results achieved.

Although the studies about risks or safety have attracted unprecedented attention from academic researchers and the public, the current research has revealed that there are few support tools that provide conceptually analytical or methodological support for risk research in supply chains in general, in *CSCs* in particular like the Probabilistic Risk Assessment (*PRA*) in the unclear area and *FSA* in the marine and shipping field. Simultaneously, the research also found that few previous risk studies for supply chains were conducted from both the engineering and managerial viewpoints. Instead, some of the former works concentrated on the components in the system (i.e. information security studies) and others that focused on risks or vulnerability from a whole logistics managerial perspective, were mostly related to how to practically reduce risks and prevent vulnerability. One major reason resulting in this phenomenon is that *CSCs* are the growing systems made up of many sub-systems and sub-functions each of which has been, and may still be treated as a distinct management operation. For example, previous attempts to address container liner shipping safety in the international framework have focused on the containership itself and, at most, the immediate area surrounding the vessel in container ports/terminals. This focus was an outgrowth of the ship-focused mandate given to the *IMO*.

2.5. Risk Assessment Techniques

Risk assessment has been part of decision analysis since human was able to reason. However, the formalised process of making decisions about risks was formed much later and began with probability theory. Probability theory, the foundation of contemporary risk analysis, was based on the discoveries in the 16th and 17th centuries by notable scholars, such as Girolamo Cardano, Galileo Galilei, Blaise Pascal, Pierre de Fermat, and Chevalier de Me´re´ (Garrick *et al.*, 2004).

Although such pioneers made important contributions on probability and frequency expressions of past events, statistical inference and the concept of the number theory about the same time etc., until the middle of the 18th century, Thomas Bayes with his Bayesian probability theory was first considered as the real father of contemporary risk assessment (Garrick *et al.*, 2004). The greatness of the theory lies on the Bayesian theorem rooted in the fundamental logic that enables the combination of old information with new information for the assignment of probabilities. Such an advantage was made use of in the subjects of early analytical explorations and precursors to the new science of risk assessment, such as gambling strategies, military strategies and determining mortality rates. Typical scholars in the period included Jeffreys, Raiffa and Jaynes.

The widespread, formal application of the *PRA* to critical infrastructure began in earliest in the late 1900s. Some typical safety analysis techniques developed and applied in that period include: the Risk Matrix Method (Halebsky, 1989; Tummala and Leung, 1995), Preliminary Hazard Analysis (*PHA*) (Military Standard, 1969, 1999; Henley and Kumamoto, 1992), What If Analysis (Pillay and Wang, 2003a), HAZard and OPerability (*HAZOP*) Studies (Bendixen *et al.*, 1984), *FTA* (Ang and Tang, 1984), Event Tree Analysis (*ETA*) (Henley and Kumamoto, 1992), Markov Chains (*MCs*), (Norris, 1998), Failure Mode, Effects and Criticality Analysis (*FMECA*) (Andrews and Moss, 2002) and other analysis methods such as Diagraph based Analysis (*DA*) (Kramer and Palowitch, 1987), Decision Table Method (Dixon, 1964) and Limited State Analysis (Bangash, 1983), etc.

According to different application contexts, such traditional safety analysis techniques may expose disadvantages. For example, *FTA* and *ETA* are the most widely used modelling methods for risk analysis. *FTA* and *ETA* are popular because they are easy to use, present the designer with an intuitive high-level abstraction of the systems, and can be efficiently applied to reasoning and inference using techniques such as Binary Decision Diagrams (*BDD*). However, traditional hierarchical fault and event trees themselves are lack of the capability in handling partial dependence between components. *MCs* and their extensions have proven to be versatile tools for modelling complex

dynamic component behaviours (Modarres, 1993). However, *MCs* present two main shortcomings: a) manually generating an *MC* describing the system's behaviour is an error prone task (Boudali and Dugan, 2005); b) *MCs* are faced with the infamous state space explosion problem (De Souza and Pedro, 1992). For this reason, a class of tools such as the Galileo tool (Sullivan *et al.*, 1999) provides a higher-level description of a system model, which is then automatically converted into an *MC* (Boudali and Dugan, 2005). Also, Bouissou and Bon (2003) have extended traditional fault trees by combining them and Markov processes into a new formalism called Boolean logic Driven Markov Processes (*BDMP*). *FMECA* has been a well-accepted safety analysis method. The traditional *FMECA* employs Risk Priority Numbers (*RPNs*), a merit for simplification, to evaluate the risk level of a component or process and achieve a risk ranking. However, it is due to such a "merit" that *FMECA* suffers from several weaknesses. One of the critically debated weaknesses is that equal aggregate *RPN* values, obtained by the simple multiplication of the individual scores of the three safety parameters, possibly generate different risk implications (Gilchrist, 1993; Ben-Daya and Raouf, 1993). The others include the ignorance of the relative importance among the three safety parameters when multiplied. Therefore, the method may in a certain level lose important information and worsen an already critical situation. To reflect the problem, a series of variations of the traditional *FMECA* have been developed, such as the use and incorporation of fuzzy theory and grey theory for *FMECA* discussed by Pillay and Wang (2003b).

With the further development of the probability theory in risk assessment in the 20th century, many had indicated that the applications in the behavior-based or management-based fields (i.e. economic, financial and commercial) were more possibilistic than probabilistic, more experience-based than analytical and more qualitative than quantitative. It has been stated that safety analysis can be generally divided into two broad categories namely quantitative and qualitative analysis (Wang and Ruxton, 1998). Depending on the safety data available to the analysis, either a quantitative or a qualitative safety analysis can be carried out to study risks. In the studies of qualitative (possibilistic) risk analysis, the most popular methods are developed on the basis of the fuzzy logic theory into two main categories, fuzzy arithmetic calculation based or fuzzy knowledge rule based.

Fuzziness is an aspect of vagueness and possibilistic uncertainty, which is indeed different from probabilistic one. Briefly, probability is a measure of the undecidability in the output of clearly defined and randomly occurring events, while fuzzy sets are concerned with the ambiguity inherent in the description of the event itself (Pan and McMichael, 1998). Informally, it can be said that the nature of possibility differs from a numerical variable and its values are not expressed using numbers but words in a natural or artificial language. Therefore, possibility theory, which emerged in the 1970s' (Zadeh,

1965), was developed quickly and became one of the most popular approaches in expert decision systems. Simultaneously, its uniqueness in dealing with vagueness, which differentiates with probability theory, leads to the inevitability of being widely applied in risk assessment. Jenson (2001) stated that except for probability theory, the most prominent approach to reasoning under uncertainty is possibility theory, which in certain contexts is called fuzzy logic*. Fuzzy logic is an extension of classical Boolean logic from crisp sets to fuzzy sets. As a logic for reasoning, there is nothing fuzzy about fuzzy logic. Zadeh conceived the notion of fuzzy logic in 1965, the first new method of dealing with uncertainty since the development of probability (Zadeh, 1965). Since then, fuzzy logic has been a user-friendly profitable tool for analysing and controlling complex engineering systems and industrial processes (Deshpande, 1999) as well as knowledge-based expert decision systems (Bordogna *et al.*, 1997). As a theoretical framework of expert decision making under uncertainty, fuzzy logic has been widely applied in the context of risk assessment (Wang *et al.*, 1995; Sii *et al.*, 2001; Andrews and Moss, 2002; Pillay and Wang, 2003a).

The significance of fuzzy sets is that they facilitate gradual transition between states and consequently possess a natural capability to express and deal with observation and measurement uncertainties (Pillay and Wang, 2003b). Such a capability proves *FST* to be a useful tool in risk analyses as these analyses often require the use of subjective judgement and uncertain data. In principle, *FST* can restore integrity to the risk analyses by allowing uncertainty and not forcing precision where it is not possible. However, the theory can be difficult to apply without using linguistic variables as mediums. Since words in general are less precise than numbers, the concept of a linguistic variable serves the purpose of providing a means of approximate characterisation of phenomena, which are too complex or ill defined to be amenable to description in conventional quantitative terms (Schmucker, 1984). The linguistic variables representing risk parameters are connected with fuzzy membership functions. Due to the advantage of simplicity, straight-line membership functions, especially triangular and trapezoidal membership functions have been commonly used to describe risks in safety assessment (Wang, 1997b). After defining the membership functions of the risk related linguistic variables, the risk parameters can be assessed using subjective judgements. They can be expressed by either a complete linguistic term (a specific pre-defined fuzzy number), multiple linguistic terms with partial confidence or a new independent fuzzy number (i.e. approximately 20 percent). Furthermore, various fuzzy arithmetic calculations (i.e. the combination of Cartesian operation and decomposition operation, α-cuts and interval arithmetic, etc.) or rule-based definitions can be performed to obtain the fuzzy safety

---

* Conceptually, *FST* is much broader than fuzzy logic and contains the latter as one of its branches. Practically, the general tendency today, however, is to use term fuzzy logic in its broad sense, also including *FST* as its foundation.

possibility estimations of the interested risk focuses. Finally, such fuzzy safety possibility estimations can be duffuzified to a crisp value, which can make more sense in risk ranking and *SA*.

In order to avoid the loss of useful information, a sign of attempting to synthesise possibilistic and probabilistic theories emerges as the direction of more scientifically based ways to assess risks. Recently, *BNs*[*] have led to many new applications of uncertainty modelling, in particular to very complex problems where a large of number of variables contribute to overall uncertainty. Such success of applying *BNs* stimulates and inspires researchers' interest of using *BNs* in system risk and reliability studies. Within risk analysis and safety decision management, the research related to *BNs* has been largely dominated in the scope of their practical applications. Faber and his colleagues (Faber *et al.*, 2001) have proposed a formalism that uses *BNs* to assess the risks associated with the decommissioning of offshore facilities. Friis-Hansen (2001) in his PhD thesis has considered a number of problems in the marine industry to which *BNs* can be fruitfully applied. Hudson *et al.* (2001) have used *BNs* to assist military planners in determining the level of risks related to their antiterrorism system networks and King (2001) has presented *BNs* as a solution for operational risk management. Considering them in higher level risk industries, Kardes and Luxhøj (2004) have extended *BNs* to the risk assessment of the aviation industry and Fullwood (2000) has discussed the probabilistic safety assessment in the chemical and nuclear industries using *BNs*. Extending their popularity to medicine and pharmacy, Lovell and his coworkers (Lovell *et al.*, 1997) have constructed a systematic model on the basis of *BNs* to develop risk prediction systems in obstetrics and Barker *et al.* (2002) have discussed how *BNs* can help to deal with risks stepping from clostridium botulinum. Studying from the viewpoint of risk categories, Garrote *et al.* (2003) have applied *BNs* to real-time flood risk estimation and Holicky and Schleich (2000) have estimated risks under fire design situation. Moreover, Marsh and Bearfield (2000) have successfully applied *BNs* to model accident causation in the UK railway industry and He *et al.* (2002) have explored the possibility of using *BNs* to assess credit guarantee risk.

Whilst such studies focus on the practical application of risk-based *BNs*, another emphasis associated with *BNs* in the risk context has mainly been placed on their combination with traditional risk assessment methods to form more powerful analysis tools from the point of theory research. Bobbio *et al.* (2001) have mapped fault trees into *BNs* for improving the effectiveness of risk analysis of dependable systems. Combining *BNs* and Failure Mode and Effects Analysis (*FMEA*), Lee (2001) has conducted a *BN-FMEA* model to provide a basis for improving the safety performance of design and diagnostic modelling of mechatronic systems. The synthesis of Analytic Hierarchy

[*] More details about *BNs* can be found in Section 2.6 and Chapter 7.

Process (*AHP*) and *BNs* was originally introduced to the field of risk assessment through the work by Cagno *et al.* (2000) and Ha and Seong (2004). Furthermore, applying *BNs* into the research of reliability also enables the exploration and development of novel reliability analysis models. Some typical studies in this category include the work by Boudali and Dugan (2005) and Langseth (2002).

A common criticism of the Bayesian approach is that it requires too much information in the form of prior probabilities, and that this information is often difficult or impossible to obtain in risk assessment. In practice, therefore, it is often necessary to rely on subjective probability estimates provided by expert judgements. It has been reported that linguistic expressions of probabilistic uncertainty may be more accurate than numerical values in estimating risk variables (Wang *et al.*, 1995) and that forcing the input of a crisp non-overlapping subjective probability is in many circumstances misleading and likely to lead to instability of the Bayesian system performance (Pan and McMichael, 1998). Consequently, an interesting circle (defined as *FBNs*) connecting *FST* with *BNs* may be formed. The use of fuzzy sets requires the support of *BNs* to deal with interactive dependence between risk variables (randomness of uncertainty) and *BNs* rely on *FST* to cope with haziness of prior subjective probability (fuzziness of uncertainty).

To address this issue, earlier work has indicated that there are many challenges in developing the concepts of fuzzy probability or the models related to *FBNs*. Zadeh (1975; 1984) has first used the term "fuzzy probability" and defined the fuzzy probability of a fuzzy event in terms of its fuzzy cardinality with respect to some universe of discourse. Whilst Zadeh's approach may be useful for data-centred applications, it is somewhat dubious as it seems to rest on the assumption that the set of outcomes consists of a finite number of elements having equal probability (Halliwell, 2003). The work by Jain and Agogino (1990) has arguably been the most influential of publications in unifying the concepts of Bayesian probability and fuzzy possibility. However, it has not possibly given significant contributions to this research because for technical reasons the theory it presents cannot provide a satisfactory model for qualitative probability assessments. The typical studies by Pan and McMichael (1998) and Pan and Liu (2000) have successfully developed a complete formalism for inference involving fuzzy random variables (*RVs*) in fuzzy causal probabilistic networks. Unfortunately, the failure of dealing with the overlapping of the states of fuzzy *RVs* puts them on a conflicting point, where the arguments of the "mutually exclusive" characteristics of the states as the foundation of the Bayesian approach harass the inference formalism. The linguistics probability theory by Halliwell *et al.* (2002) might be the first attempt to use fuzzy numbers as a substitute for real numbers distributed into various states. Although showing much attractiveness such as effective qualitative probability assessments and a reasonable inferring mechanism, such a theory has still

been found to have some theoretical and applicable problems, in which typical ones include the ignorance of the requirement of "completeness" of states and the complexity of computing algorithms. More effective and novel models are required.

2.6. Decision Making Techniques

BNs, fuzzy logic and *MAUT* have proven to be powerful tools for decision making. While *BNs* and fuzzy logic deal with the decisions under uncertainty, *MAUT* focuses on the problems with multiple attributes or criteria. In complex safety critical systems, decisions are usually made on multiple uncertain attributes. Therefore, it is possible to consider the synthesis of *BNs*, fuzzy logic and *MAUT* (or its extension – *Multiple Criteria Decision Making (MCDM)*) together in the forming of a more powerful risk based decision support tool. Although the work by Fenton and Neil (2001) has provided a theoretical foundation for the combination of *BNs* and *MCDM*, it uses subjective point estimation to define attribute states, which may not be well suited to modelling the safety attribute, and thus, cannot be appropriately applied to the risk domain without further research. Actually, the attempt to synthesise these techniques can be better considered as an alternative explanation to simple influence diagrams (*IDs*) including one decision node (Howard and Matheson 1981). In order to make use of the advantages of *BNs*, fuzzy logic and *MCDM* in risk based decisions, the relevant literature needs to be reviewed in the following context.

BNs and Influence Diagrams

A *BN* (also called belief network, or probabilistic network) is a graphical presentation of probability combined with a mathematical inference calculation. It is used to represent dependencies between *RVs*. Each variable represented as a node, is connected by directed links, represented as arrows or arcs, with conditional probability table (*CPT*) values assigned to the variables making up a *BN*. The nodes in a *BN* are called chance nodes. Chance nodes represent uncertain events or variables. They can be a continuous or discrete *RV*, or a set of events. A deterministic node is a special case of chance nodes, which operates deterministically on other nodes. The arrows are the directed links between nodes and this direction represents the conditional dependent relationship of these nodes.

The graphical representation makes *BNs* a flexible tool for constructing the models of causal impact between events, in particular when the causal impact has a random nature. Also, the specification of probabilities is focused on very small parts of the model (a variable and its parents). Having constructed the model, it can be used to compute effects of information as well as interventions from deterministic nodes. When the states of some variables are fixed, the posterior probability distributions for the remaining

variables can be computed. Algorithms based on the Bayes' rule and Chain rule (Jensen, 2001) are developed for probability updating, and they perform very efficiently on a large variety of models. This makes *BNs* well suitable for forecasting and diagnosing.

A *BN* serves as a model for a part of the world and the relations in the model reflect casual impact between events. The reason for building these models is to use them when making decisions. In other words, the probabilities provided by the network are used to support some kind of decision making (Jensen, 2001).

It is often said that "Decision Theory = Probability Theory + Utility Theory" (Murphy, 1998). *BNs* have outlined how joint probability distributions are modelled in a compact way using sparse graphs to reflect conditional independence relationships. Therefore, it is possible to decompose multi-attribute utility functions in a similar way: a node is created to represent the attribute of interest, which has as its parents all the other attributes on which it depends. Furthermore, the utility node(s) will be created to have decision/deterministic and chance node(s) as parents, since the utility depends both on the state of the world and the actions performed by decision makers. The resulting graph is called an *ID*.

An *ID* was originally developed to substitute conventional decision trees in modeling and solving real world symmetric decision problems. Nowadays, it can be considered as a *BN* augmented with decision variables and utility functions and provides a language for dealing with both simple decision problems (only one decision node (action)) and sequential decision problems (more than one decision node and utility node), which are also known as dynamic decision modelling. An *ID* is solved by computing a strategy yielding the highest expected utility. A strategy is a set of functions; to each decision variable, a function, which from the relevant path returns a decision, is specified. The *BN* algorithms for probability updating can be modified to solve *IDs*. The framework of *IDs* (Howard and Matheson, 1981) provides a natural representation for capturing the semantics of decision making with a minimum of clutter and confusion for decision makers (Shachter and Peot, 1992) and offers comparative advantages of easy numerical assessment and effective representation of independencies between variables over trees. These factors contributed to the wide spread use of *IDs* as a tool for representing and analysing complex risk related decision problems in recent years (Willems *et al.*, 2005; Diehl and Haimes, 2004).

Although considered as the extension of *BNs* in the decision making context, an *ID* is still a type of causal model that differs from a *BN*. They indicate different meanings in different studies. For example, Kjærulff and Madsen (2005) concluded that a *BN* is a model for reasoning under uncertainty, whereas an *ID* is a probabilistic network for

reasoning about decision making under uncertainty. From the viewpoint of analysing decision support tools' capability, *BNs* and influence diagrams can be respectively defined as single attribute and multiple attribute decision making (*MADM*) techniques in this study. In order to clarify the difference, the definition of an *ID* is provided as follows (Kjærulff and Madsen, 2005):

An *ID* $N = (X, G, P, U)$ is a four-element collection consisting of a set of random and decision variables X, an acyclic directed graph G, a set of conditional probability distributions P and a set of utility functions U. The acyclic directed graph $G = (V, E)$, contains the nodes V representing *RVs*, decision variables, and utility functions (also known as value or utility nodes) and directed links E including precedence links between decision nodes and information links from change nodes to decision nodes. Each decision variable $D \in X$, includes the decision options or alternatives represented by the states $(d_1, \ldots, d_n)$. The decision options are mutually exclusive and exhaustive. The usefulness of each decision option is measured by the local utility functions associated with D or one of its descendants in G. Each local utility function $u(X_{pa(v)}) \in U$, where *pa* means the parents of v and $v \in V_U$ is a utility node, represents an additive contribution to the total utility function $u(X)$ in N. Thus, the total utility function is the sum of all the utility functions in the *ID*, i.e., $u(X) = \sum P_{v \in V_U} \times u(X_{pa(v)})$. When making decisions, each action will influence the probabilities of the configurations of the network. Consequently, $P_{v \in V_U}$ changes to respond to various decision actions and the total utility values associated with all the actions (called expected utility *EU*) are different. The decision alternative with the highest expected utility is chosen; this is known as the maximum expected utility principle (*MEU*).

Given their general information above, some special structural properties still need to be emphasised in order to better understand the meaning of *IDs* as follows (Jensen, 2001):

- There is a directed path (ordered combination of all precedence links) comprising all decision nodes.
- The utility nodes (V_U) have no children.
- The decision nodes (V_D) and the chance nodes (V_C) have a finite set of mutually exclusive states.
- The utility nodes (V_U) have no states.
- To each decision node (V_D) and the chance node (V_C), there is an attached conditional probability table $P(V|pa(V))$.
- To each utility node (V_U), there is an attached real-value function $u(X_{pa(v)}) \in U$ over $pa(V_U)$.

As one kind of uncertainty treatment techniques, *BNs* have characterised significant

strengths in the risk based decision making, which may be not always shown in the other decision making techniques such as *MAUT* and fuzzy logic. They are shown as follows:

- The graphical nature of *BNs* allows risk variables to be added or removed without significantly affecting the remainder of the networks because modifications to the networks may be isolated.
- The *BNs* have the capability of adjusting risk variables to be risk input or output without redesigning the system. In other words, they can accept risk evidence at any point in the system and likewise, provide output at any point in the system.
- The comparison between Bayesian prior and posterior probabilities with flexibility enables the conduction of the *SA* in *BNs*, which can be used to rank the importance of risk variables.
- The concept of d-separation in *BNs* provides a basis for overall improvement in computation; once conditionally independent due to some blocking nodes, the probability of one node can be evaluated without consideration of the others.
- As one kind of expert system, *BNs* like fuzzy rule based systems, may be developed using expert opinions instead of too much objective data.

However, on the other side, *BNs* have also exposed some weaknesses when applied to a risk domain, as follows:

- The general lack of understanding of probability definitions leads to failing to precisely probabilistically estimate subjective fuzziness, which widely exists in representing risk variables.
- As acyclic graphs, *BNs* require that all arrows in the networks must not form a directed cycle or loop, which constrains the construction of the qualitative structure associated with risk variables to a certain degree.
- Most importantly, *BNs* themselves, having no incorporation with utility theory, cannot deal with multiple risk attribute decision problems.

As the extension of *BNs*, *IDs* succeed in their advantages in dealing with risk based decision problems and simultaneously, equipped with decision nodes and utility functions, they obtain a solution to overcoming the partial disadvantages discussed above. The utility functions allow *IDs* to incorporate the notation of preference, which is necessary to wider risk decisions with multiple attributes. The precedence links attached in the diagrams make it possible to take decisions or perform actions in a sequential order. This point has a significant sense in engineering risk control areas, where an interruptive action will normally not be performed until its antecedents fail to work. However, similar to the other disadvantages of *BNs* described above, the chance and utility nodes in *IDs* are incompatible with fuzziness. Furthermore, the *MEU* principle requiring linear additive functions may also hinder the application of the diagrams in risk based *MADM*.

Fuzzy Logic and ER

Fuzzy logic is a superset of conventional Boolean logic with extensions to account for imprecise information. Fuzzy logic permits vague information, knowledge and concepts to be used in an exact mathematical manner. Linguistic variables such as "definite", "likely", "average", "unlikely" and "impossible" are necessary media used to describe continuous and overlapping states. This enables qualitative and imprecise reasoning statements to be incorporated with fuzzy algorithms or fuzzy rule bases producing simpler, more intuitive and better-behaved models. Fuzzy logic is based on the principle that every crisp value belongs to all relevant fuzzy sets to various extents, called the degrees of membership.

Pure fuzzy logic has extremely limited applications (the only popularised application is the Sony Palmtop) and the main use of fuzzy logic is as an underlying logic system for fuzzy expert decision making systems (Pai, *et al.*, 2003). Roubens (1996) described a typical fuzzy decision making problem as follows. Consider j ($j \in C$) as one of given criteria C upon which the alternatives A are evaluated. A fuzzy objective may be characterised on this criterion by a fuzzy set $\mu_j(x)$, $x \in X_j$, where X_j represents the evaluation scale on the dimension j. The next step is to associate an evaluation with each alternative i ($i \in A$) on dimension j. Ill-known or ill-defined evaluations can be represented by a possibilistic distribution $\beta_{ij}(x)$, which represents the fuzzy consequence of alternative i for criterion j. Based on fuzzy knowledge bases, such possibilistic distributions on various criteria can be unified and transferred to one common space $P_{ij}(x)$, the preferences of decision makers. Sonmez (2002) indicated that the preferences of decision makers are very often represented by a "Preference structure", which can be displayed according to different guidelines such as graph, numerical or functional representations. In nature, it is a problem of the exploitation of preference models. After the preference structure analysis, Herrara and Verdegay (1997) suggested that another (the last) main problem using a fuzzy decision making tool is associated with the aggregation of preferences, which can be given more detailed discussion in the following context related to an *ER* approach.

Fuzzy logic has been successfully applied for a wide range of single and *MCDM* problems. Yager (1981) proposed a fuzzy logic based methodology for qualitative multicriteria decisions. Shipley *et al.* (2001) described a multiple criteria linguistic decision model to satisfy goals for successful product/service introduction. A fuzzy logic based methodology for qualitative multicriteria decisions in facilities planning has been proposed by Kapoor and Tak (2003). Singh and Tiong (2000) described a multiple criteria linguistic decision model using *FST* to evaluate the capability of a contractor to deliver projects as the owner's requirements. Chen (2001) used a new multiple criteria decision-making method to solve the distribution center location selection problem

under fuzzy environment. Fuzzy discrete *MCDM* algorithms for optimising the cost of steel structures have been developed and studied by Sarma and Adeli (2000). Khouja and Booth (1995) applied a fuzzy cluster analysis to choose industrial robots. Wang and Lin (2003) produced a fuzzy logic approach for configuration item selection in software development based on multiple qualitative criteria. A multicriteria port competitiveness evaluation problem was solved by Huang *et al.*, (2003) using a fuzzy multicriteria grade classification approach. Liang (1999) combined the idea of the Technique for Order Preference by Similarity to an Ideal Solution (*TOPSIS*) with *FST* to propose a novel fuzzy *MCDM* based on the concepts of ideal and anti-ideal points.

The theory of evidence was first generated by Dempster (1967) and further developed by Shafer (1976). As such, the theory is often referred to as Dempster-Shafer theory of evidence or *D-S* theory. The *D-S* theory was originally used for information aggregation in expert systems as an approximate reasoning tool (Buchanan and Shortliffe, 1984; Lopez de Mantaras, 1990) and then used in decision making under uncertainty and risk in contrast to Bayes decision theory (Yager, 1992; 1995). *ER* is developed on the basis of the *D-S* theory. The use of *ER* as a decision making tool has been widely reported in the literature. Some typical studies making useful contributions towards the use of *ER* for representing and managing uncertainty in decision analysis include the works produced by Yen (1990), De Korvin and Shipley (1993), Xu (1997), Denoeux (1999), Murphy (2000) and Vourous (2000). Through the studies, it is concluded that when using *ER* to design a decision making model, the following items are noteworthy (De Korvin and Shipley, 1993):

- To simplify complex systems.
- To incorporate subjective factors in a systematic way.
- To combine evidence from independent sources of information.
- To account for the uncertainty inherent in complex decision making processes.

An important achievement of applying *ER* to decision analysis is to incorporate it into traditional *MCDM* methods, which has been claimed by Beynon *et al.* (2000). *MCDM* problems with both qualitative and quantitative attributes are sometimes called hybrid *MCDM* problems (Sonmez, 2002). When faced with a hybrid *MCDM* problem, the first thing to tackle is how to measure the qualitative criteria (Yang and Sen, 1994). An *ER* based decision making approach for *MCDM* problems with both qualitative and quantitative criteria under uncertainty was developed in the early 1990's (Yang and Singh, 1994; Yang and Sen, 1994). The major contribution of the approach lies in that it uses a distributed evaluation framework to overcome the inability of the *D-S* theory when conflicting evidence exists in *MCDM* problems. In the framework, assessments provided in terms of degrees of belief at lower level criteria are aggregated through their weightings. The kernel of such an approach is an *ER* algorithm, which was generated by

Yang and Singh, (1994), later updated by Yang and Sen (1994) and further modified by Yang (2001). The approach is continuously regenerated and the newest algorithm can be found and fully explained in Yang and Xu (2002). The phrase "*ER* approach" throughout this thesis refers to the algorithm. Several applications of this approach can be addressed in the literature (Wang *et al.*, 1995, 1996; Yang and Sen, 1996, 1997; Graham *et al.*, 2000; Yang, 2001; Sii *et al.*, 2002; Yang *et al.*, 2004). Consequently, the process of applying the *ER* approach to *MCDM* can be concluded and briefly described as follows (Sonmez, 2002):

- Display a decision problem in a hierarchical structure.
- Assign weights to each criterion and also to their sub-criteria.
- Choose a method for assessing a criterion weight quantitatively or qualitatively.
- Evaluate each alternative based on the lowest level criteria in the hierarchical structure.
- Transform assessments between a main criterion and its associated sub-criteria if they are assessed using different methods (i.e. qualitative and quantitative).
- Generate an overall distributed assessment for each alternative at the top level and quantify it if necessary so as to determine an average value for the alternative.
- Rank alternative and choose the one with the highest average value.

The *ER* approach developed particularly for *MCDM* problems with both qualitative and quantitative criteria under uncertainty utilises individuals' knowledge, expertise and experience in the forms of belief functions. The major advantages of *ER* are:

- To handle incomplete, uncertain and vague as well as complete and precise data.
- To provide its users with a greater flexibility by allowing them to express their judgements both subjectively and quantitatively.
- To accommodate or represent the uncertainty and risk that is inherent in decision analysis.
- As a hierarchical evaluation process, to offer a rational and reproducible methodology to aggregate the data assessed.
- To easily obtain the assessment output using mature computing software, *IDS*.

MAUT and TOPSIS

MAUT is an application tool for estimating the utilities of multiple objectives, which are under study by decision makers. In other words, decisions on different problems or situations are taken after the careful analysis of the utilities that are given a set of well-defined objectives. *MAUT* shares the same philosophy as *AHP*. It is a decision making tool, which assists in the solution of problems where a plethora of factors are involved and their assessment is essential to the final outcome. Edwards (1954, 1961), Fishburn (1968), Feridman and Savage (1952) and Keeney and Raiffa (1976) have been among

the first to develop this methodology. According to Edwards and Newman (1982), a seven-step *MAUT* framework can be represented as follows:

- Identify objectives and functions.
- Identify stakeholders.
- Identify attributes and construct value trees.
- Assess relative importance of attributes.
- Ascertain location measures.
- Aggregate weights and utilities.
- Perform *SA*.

MAUT has been used in a serial of cases and in a variety of contexts depending on the scientific fields in which it has been applied. In the business field the research of Zhang *et al.* (2003) studying the applicability of utility and decision theory at a managerial level is presented. At a strategic level, the studies of Min (1994) and Talluri and Narasimhan (2003) on supplier selection and Platts *et al.*, (2002) on making against buying decisions are found in the literature. In the risk sector, the studies include the one of Khan *et al.* (2004) on the risk-based inspection and maintenance of oil and gas installation and operations, the work by Wang *et al.* (1996) dealing with subjective safety and cost assessment and the research of Linares (2002) using *MCDM* and risk analysis for power system planning, etc. A number of studies have also taken place in the fields of energy (von Winterfeldt, 1982), fishery (McDaniels, 1995), and hazardous materials (Erkut and Verter, 1998), etc.

Compared to other decision analysis tools, *MAUT* has its own superiority or robustness, which can be defined as the ability to analyse and formulate problems with imprecision. This robustness appears in three key areas: problem formulation, preferences and probabilities,

- Problem formulation is associated with the set of available alternatives, which are not fixed but can be extended (Korhonen, *et al.*, 1986).
- Preference can be expressed in an imprecise and intransitive way, which gives the scope for more in depth analysis of the plausible scenarios under study (Fishburn, 1991).
- Probabilities provide decision makers with the ability to conduct robust analysis and facilitate the creation of a set of alternatives which will determine the future course of actions depending on the assumptions made and prevailing conditions at the time the actions need to be taken (Keeney and Raiffa, 1993).

Three critical assumptions related to *MCDM* have been studied and described to be associated with well defined, certain and independent relevant attributes. When *MCDM* is applied to solve a realistic risk based decision problem, such assumptions have

possibly been confirmed not to be true. Consequently, they are considered as the limitations that must be improved. More details about them are discussed to represent how significantly *BNs* and fuzzy logic can function in terms of the effectiveness of improving the limitations.

In most realistic risk decision problems, the attributes interested/chosen are not necessarily well defined in sense of *MCDM*. There are two kinds of such attributes: one can be called "synthetic", which can normally be decomposed into lower level attributes that are assumed to be well defined (Roberts, 1979) and the other can be defined as "fuzzy", which is caused from the lack of objective real numbers/values to support its meaning (quantitative description). For example, for the "synthetic" attributes, in the *FMECA* method, safety can be decomposed into occurrence likelihood, consequence and the probability of consequence. Using the *SERENE* approach (*SERENE*, 1999), such decompositions can be part of a class of *BNs*. It is noteworthy that the decomposition alone is not sufficient to define the higher level attributes (Fenton and Neil, 2001) because there may be many ways to define the safety in *FMECA* as a combined measure of the lower level attributes such as *PRN* methods and *ER* approaches (Li and Liao, 2004). In other words, the *BN* technique is a key here. On the other hand, the "fuzzy" attributes can be defined using linguistic variables (qualitative description) based on the fuzzy logic theory. When utility values/functions are considered, the linguistic variables can be expressed by fuzzy numbers. For instance, one of the lower level attributes of safety, occurrence likelihood can be defined using "highly likely", "likely", "average", "unlikely" and "highly unlikely", if it has no objective information support in the form of "occurrence frequencies/time". In such a process, one must not confuse the definition of fuzzy numbers of the linguistic variables with the requirement of mutually exclusive states in *BNs*. If the attribute occurrence likelihood becomes the node of a *BN* with the five states expressed by the linguistic variables above, then such five states can still keep a mutually exclusive relationship although they will be endowed with overlapped fuzzy numbers when the corresponding utilities are needed. This point can be further demonstrated using a real-world example. The variable, a person's height is considered as a node in a *BN* with five mutually exclusive states, "180-175", "174-170", "169-165", "164-160" and "159-155"(cm). Now, although a special decision making scenario may require assigning the utility value "1" to the states with the height no less than 165cm and "0" to the others, three inclusive (completely overlapped) "1" and two "0" do not influence the mutually exclusive relationship of the five states.

It is true that most risk attributes/criteria are uncertain so that risk research is usually closely connected with probability theory. For example, given an event "fire", the consequence of the fire is highly possibly stochastic rather than deterministic. Such uncertainty is called randomness and the definition of the *RVs* in *BNs* can well model the

randomness using prior probability distributions to various states. The assumption that the risk attributes/criteria are independent of each other is not valid in many risk based decision analyses. For example, a classical *MCDM* problem may be to assess the navigation safety of ships based on the attributes: ship structure, ship speed, ship manipulability and location. Such attributes may be both well defined and certain, however they are not independent; ship speed will depend on ship structure and its location (i.e. possibly related to traffic intensity) and affect ship manipulability. *BNs* precisely provide the necessity for dealing with the dependency between risk attributes when their qualitative graph structures and quantitative conditional probability distributions are concerned.

Hwang and Yoon (1981) developed the *TOPSIS* method based on the intuitive principle that the chosen alternative should have the shortest distance from the positive-ideal solution and the longest distance from the negative-ideal solution. *TOPSIS* is quite effective in identifying the best alternative quickly. The underlying logic premise of the *TOPSIS* method is that an alternative that is more like an ideal alternative (the best that could be imagined) and more unlike a negative-deal alternative (the worst that could be imagined) should be preferred. In the *TOPSIS* method, the ideal alternative is constructed out of exclusively the best attribute values attainable and therefore it is usually an invented alternative. The negative-ideal alternative is also usually an invented alternative that is constructed out of exclusively the worst attribute values attainable. The relative closeness (similarity) of each alternative to the ideal alternative is rated on the basis of its distances from both the positive-ideal and the negative-ideal alternatives simultaneously. Finally, the preference order of the alternatives is obtained by their rank on a descending order of those ratings. The computational procedure of the *TOPSIS* method is straightforward and its framework can be described as follows (Ölcer and Majumder, 2006):

- Calculate normalised ratings.
- Calculate weighted normalised ratings.
- Identify positive-ideal and negative-ideal solutions.
- Calculate separation measures.
- Calculate similarities to the positive-ideal and negative solutions.
- Rank preference order.

The *TOPSIS* method as a modified form of *MCDM* methodology does not require attribute sets to be independent as the *ER* approach does. It can also be easily incorporated with the fuzzy logic theory to combine fuzzy and crisp attribute values (Chen and Huang, 1992) and with the entropy theory (Zeleny, 1976) to deal with context dependency (i.e. the influence of constraints to risk attributes) (Rillet and Park, 2001).

2.7. Conclusion

The operational process of *CSC* systems including physical cargo flow, information flow and custody flow has been reviewed, followed by a careful analysis of some typical historical failure data in the process. In order to ensure the origination of the study, this chapter has also given a comprehensive literature review associated with the risk assessment of *CSCs*. It emphasizes the explanation of applying uncertainty treatment methods and techniques to risk assessment and decision making in previous studies.

Chapter 3 – Formal Safety Assessment of Container Supply Chains

SUMMARY

This chapter develops a conceptual safety assessment methodology for CSCs based on a modified FSA framework that takes risks from vulnerability rather than hazards into account. Five interlocking steps are described to construct a safety model including novel risk analysis and decision-making approaches. The advantages of the vulnerability-based risk analysis approach over the hazard-based one are clarified and the aggregation of engineering-based and managerial risk analysis is also discussed. An anti-terrorism case study is finally carried out to test the feasibility of the proposed methodology.

3.1. Introduction

CSCs have made significant contributions in facilitating the world prosperity and economic development experienced over the past twenty years. However, based on a near-frictionless international transport belief, the chains have exposed themselves uniquely vulnerable to various risks. Some special events such as the 9/11 terrorists attacks and the lock-out of American West Ports have gradually shown that *a)* the safety and reliability in the chains are facing an unprecedented challenge and *b)* traditional engineering-based risk assessment methods and safety protective measures are inadequate to deal with the threats from variational environments, especially in the era of terrorism rampancy. Born in the 90s of the 20^{th} century, Safety Case and *FSA* approaches attempted to develop a broad regime to cope with marine related risks against international shipping and offshore safety. However, with the outgrowth of the ship-focused mandate given from the *IMO*, such frameworks can only be competent to the containership itself and, at most, the immediate area surrounding the vessel in container ports/terminals. Thus, there is a need to develop a framework to address the safety requirements of *CSCs* as a whole appropriately.

Evolving from the multi-purpose general-cargo liner, modern *CSCs* have more and more vulnerability by many diversiform risks. These risks not only range from the possibility of physical breaches in the integrity of shipments and the interruption of information communication, but also come from the vulnerability in wider levels that may be personnel, managerial or environmental. Obviously, it will be very difficult for the classical approaches aiming at hazard-based risks to deal with the wider vulnerability-based risks in *CSC* systems. Thus, a subjective risk analysis approach combining *FST* and the *ER* approach is generated to deal with the highly uncertain situations resulting from threat-based risks. A techno-economic modelling technique is applied to construct

a novel multi-attribute decision-making model to cope with the evaluation of benefits of *RCOs* under uncertainty.

The current study aims at examining the application of a modified *FSA* framework to a *CSC* system from both engineering-based and managerial viewpoints. In order to achieve this aim, the chapter discusses *CSC* vulnerability; demonstrates the proposed methodology by unifying the traditional *FSA* framework and the special safety requirements and economic consideration of the chains; generates an unique subjective risk analysis approach for managing vulnerability in the chains; develops a novel decision-making technique for selecting the most effective *RCOs* in terms of safety and cost; and validates their feasibility by a case study related to a terrorism threat.

3.2. Major Problems in the Application of *FSA* to *CSCs*

The proposed *FSA* methodology consists of the solutions of three major problems, which outline the necessary steps required for risk and economic analysis using fuzzy set and *ER* methods.

3.2.1 Complex CSCs

The generic model of a *CSC* has been enlightened by the *IMO FSA* Guidelines and developed by following the processes of *CSC* operations. It as far as possible describes the functions, features, characteristics and attributes, which are common to all *CSCs*. The generic model is therefore not a 'typical' container transport chain considered in isolation but the hub of a chain of systems -- with a physical cargo flow system at the centre, following an information flow system at the beginning and deciding a custody flow system at the end (see Figure 3.1). Each of these systems interacts dynamically with the others at and across all levels to constitute a comprehensive picture of the *CSC* operation process. Therefore, the generic model has been developed by considering the systems and characteristics required to transport containers in supply chains. The functions and systems of *CSCs* are broken down to appropriate levels and the interactions of functions and systems are investigated as well.

3.2.2 Definition of Vulnerability

Although the vulnerability concept has been in use for more than twenty years since Timmerman's conceptualisation (Timmerman, 1981), presently, there is still no common definition of vulnerability, and the meanings of vulnerability are still ambiguous and fuzzy (Weichselgartner, 2001). Many of the discrepancies in the meanings of vulnerability arise from different epistemological orientations and subsequent

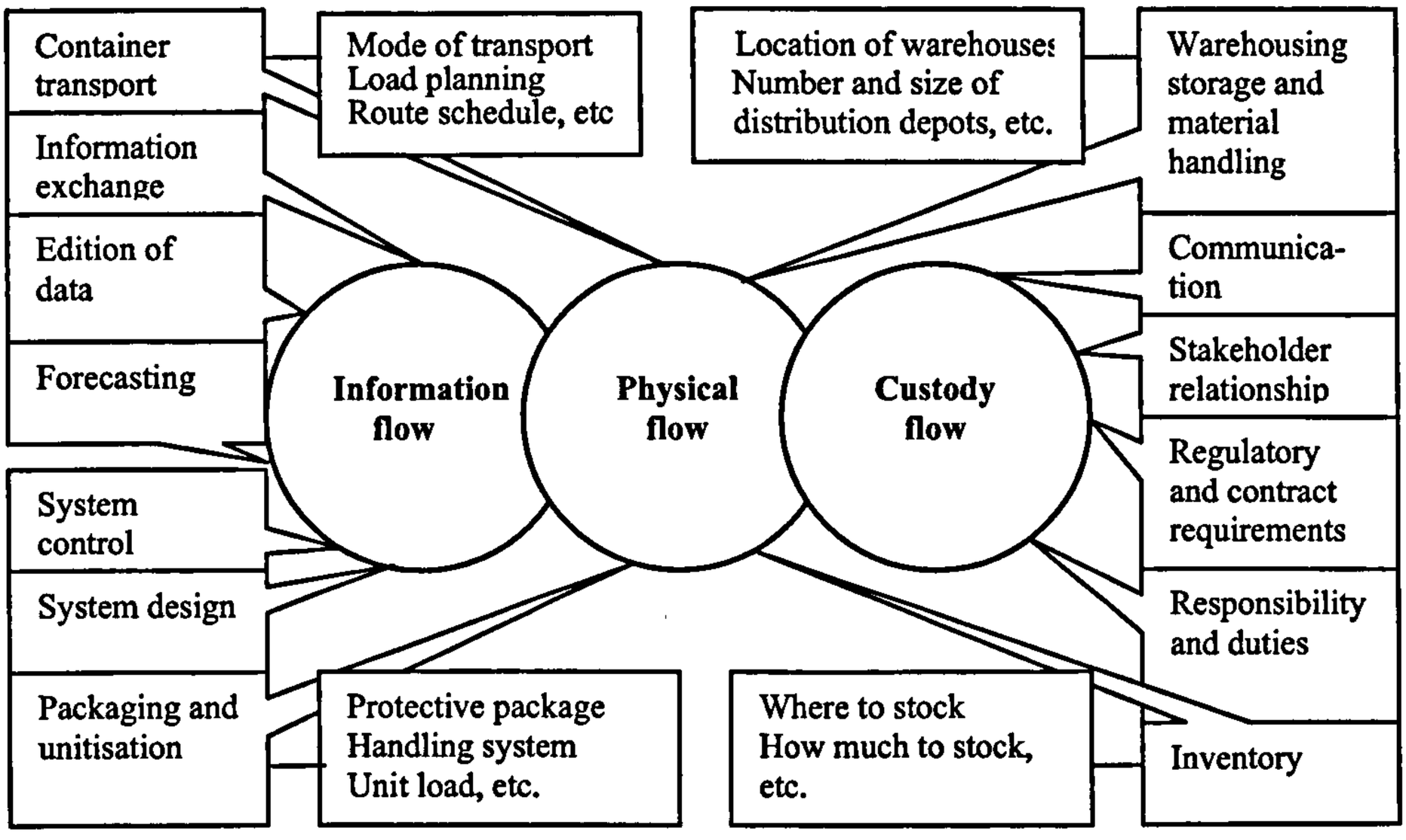


Figure 3.1. The generic model of *CSCs*

methodological practices. Nevertheless, one can find three distinct themes in vulnerability studies: vulnerability as risk exposures, vulnerability as social responses, and vulnerability as places (Cutter, 1996; Weichselgartner, 2001). The third one, vulnerability as places, combines elements of the former two and is conceived as both a biophysical risk and a social response within a specific area (Weichselgartner, 2001). In a supply chain context, logistics internal risks and external risks together endangered the continuity and reliability of the supply chain operation. Thus, the supply chain vulnerability can be defined as 'an exposure to serious disturbances, arising from risks within the supply chain as well as risks external to the supply chain (Chapman *et al.*, 2002). However, the current research has indicated that either internal or external risks would originate from a hazard or threat. Thus, the vulnerability will be considered from another viewpoint -- its nature and consequently is defined as 'an exposure to serious disturbances, arising from a hazard or threat'. Compared with Chapman *et al.*'s concept, the analysis from vulnerability nature will more redound to risk analysis. After all, the first step to achieve any effective risk analysis is to better understand the true nature of those risks.

Further studying the definition of the vulnerability of the chains, one will appreciate the distinction between hazards and threats. Differing from the definition of a hazard, a threat can be defined as an action or a potential action rather than a physical situation likely to cause damage, harm or loss (Burns *et al.*, 2003). It means that the hazard-based vulnerability is more likely to perform mechanistic probability distributions, while the threat-based vulnerability is closely connected to behavioural probability distributions. Thus, the understanding of the hazard-based vulnerability may come from objective historical accident statistics as well as subjective judgements if necessary, while threat-based vulnerability may better be described and presented using expert judgements based

on human knowledge and experience. Additionally, it is noteworthy that the threat-based risks are potentially greater than hazard-based risks because they are often not within the focal companies' direct control. Furthermore, they may be expressed in vague or qualitative terms, but it is inherently difficult to quantify them.

3.2.3 Application of FTA

FTA is a diagrammatic method used to evaluate the probability of an accident resulting from sequences and combinations of faults and failure events (Pillay and Wang, 2003a). Because of its many advantages, especially in combining qualitative and quantitative analysis to provide decision makers with an objective means of measuring the risk levels of a targeting system, *FTA* has been widely applied to the risk analysis of various industries, including logistics chains. The application of *FTA* to the current study, however, is worth noting the following:

i) *The qualitative FTA diagram is considered as a hierarchical structure to apply the ER approach.*

   The hierarchical structure should be a qualitative *FTA* diagram, which means that the fault tree has been reduced to a logically equivalent form (minimal cut sets) by using the Boolean algebra in terms of the specific combination of basic events sufficient for the undesired top event to occur (Henley and Kumamoto, 1992).

ii) *The weights of all events are distributed according to a specifically defined rule.*

   The weights of all events in applying the *ER* approach are determined considering that the fault tree, which can be considered as a hierarchical diagram, consists of many '*OR*' and '*AND*' gates. Therefore, a specific rule is required to assign the weights on a rational basis and defined as "all input events of an '*OR*' gate are given the same weight equal to that of the output event of the gate, and the weights of all input events of an '*AND*' gate are assigned through dividing the weight of the output event of the gate by the number of the input events".

3.3. The Proposed *FSA* Methodology

FSA, as a rational and systematic methodology for assessing risks and evaluating the costs and benefits of different options for the reduction of those risks, has been successfully applied to various types of ships and some marine related areas. Trial applications include bulk carriers (IACS, 2001), passenger vessels (*IMO*, 1997; *IMO*, 1998a; Lois *et al.*, 2004), high-speed catamaran ferries (Vivalda, 2000), and fishing vessels (Loughran *et al.*, 2001; Pillay *et al.*, 2003). In addition, other developments in specific *FSA* projects include those in ballast water management (*DNV*, 2000), helicopter landing areas on passenger vessels (Spouge, 1998; *IMO*, 1998b), and life saving appliances for bulk carriers (*IMO*, 2001; Skjong and Wentworth, 2000).

According to the benefits of adopting *FSA* for a marine related system described by the UK Maritime and Coastguard Agency (previously known as Maritime Safety Agency) (*MSA* 1993), together with the outcomes of prior *FSA* related studies, the application of a modified *FSA* framework for *CSCs* will *a)* effectively address all aspects of safety in an integrated way under the condition of cost effectiveness; *b)* present a proactive approach to consider the vulnerability that is full of the whole system operational processes that have not led to the rise of accidents; and *c)* provide a rational basis for recognising new risks posed by ever changing technology.

Judging from its development process, *FSA* originated from the marine industry and was also applied to marine and marine related areas. Although *CSCs* operate mainly based on maritime liner shipping services, they are constitutionally different according to the previous discussion. Therefore, in the context of *CSCs*, the *FSA* methodology will be modified to consider more elements like threats for the feasibility and reliability of its application. The methodology for the current study can be formulated to include the following five steps:

1. Identification of vulnerability.
2. Quantified assessment of the risks arising from the vulnerability identified in Step 1.
3. Development of safety options for controlling the high level risks estimated in Step 2.
4. Economic analysis associated with the *RCO*s identified in Step 3.
5. Recommendation for decision making, based upon the information derived in the preceding steps.

Established techniques are employed at each step of the *FSA* process. These include, for example, brainstorming, risk matrix, analysis of historical accident data, *FTA* and *ETA*, net present value calculations of costs and benefits, techno-economic modelling and *MADM*, etc. Simultaneously, some new techniques like subjective risk analysis and fuzzy cost and benefit analysis (*FCBA*) are also developed in this chapter. The modified *FSA* methodology designed for *CSCs* is described in detail in the following discussion.

3.3.1 Identification of Vulnerability

The first step in achieving any effective risk assessment or management is the better understanding of the true nature of those risks. The vulnerability in the chains comes from many guises and operates at several different levels. They are inextricably linked, but for clarification purposes are described here within four interlocking levels of analysis:

- Level 1 – Process (assets, infrastructures and supporting facilities)
- Level 2 – People
- Level 3 – Organisation and management
- Level 4 – Environment

At level 1, the *CSC* vulnerability is examined from a prevailing engineering-based process perspective, seeing the chains as a linear pipeline flowing through and between assets, infrastructures and supporting facilities. The emphasis is firmly on the efficient and continuously operating facilities and assets, which can be connected with the "links and nodes" of *CSCs*. The links are trucks, trains, containerships, information transmission facilities (e.g. computers) and also their infrastructures - roads, rail, inland waterways, liner shipping lanes and cables/satellites. The nodes are warehouses, *LCL* premises, rail termini/stations and ports. From a purely process-based viewpoint, *CSC* risks are principally the damage or loss of the links, nodes and other essential operating facilities and assets. The popular analogy of a supply chain as a seamless pipeline is a useful metaphor. However the realistic *CSCs* are rarely fixed, discrete, self-propelling or self-protecting. Therefore, except for the damage or loss of links or nodes, the combination points of them - transhipments from link to node or from node to link - are also the main points of vulnerability existing in the chains and need to be given more attention in risk assessment. Basically, the vulnerability in Level 1 belongs to a hazard-based scope considering the fact that the vulnerability resulting from any element discussed in this level can only be associated with a situation rather than one kind of behaviour.

Level 2 represents the vulnerability in *CSCs* in terms of people dependencies. No links or nodes will function without the people who understand how to run and maintain them. Therefore, any deviating activity coming from such persons may lead to a severe disruption in the chains. The vulnerability related to working employees mainly originates from a) human errors, which include wrong doing and negligence; b) deliberate risk-taking, such as putting late arriving containers on a vessel that is ready to sail under the insistence of shippers; c) employee health and safety scare, which have been considered as the fourth most important scenario covered by Formal Business Continuity Planning (*FBCP*) (Peck and Jüttner, 2002) d) deliberate destroying, which can be evidenced by many cases of careless loading/unloading of stevedores. The fatal vulnerability of the chains in this level may also be driven by the baleful attacks of external people, such as terrorist attacks and hacker activities, which are beyond the chains' direct control. Naturally, this category is in the field of threat-based vulnerability.

At level 3, the *CSC* is reviewed as an inter-organisational network and the assessment of the chain's vulnerability is moved up to the level of business strategy and microeconomics. The principles of an integrated *CSC* aspire to seamless flows of information and materials, facilitated by all supply chain partners thinking and acting as one. To achieve this objective, close cooperative partnering relationships need to be established and monitored. However, it is resource-intensive and thus, the organisations in the chains begin to reduce the number of their direct suppliers so as to adopt a single sourcing for keeping the lowest cost to develop and manage their supply chain relationships (*CLSCM*, 2003). One of the most widely considered vulnerability factors

of supply chains can be identified as the disruptions caused by the failure of a single (or a few) source supplier(s) from the organisational point of view. For example, the loss of a single discharging port leads to the total failure of all *CSCs* in the destination country. Obviously, this kind of vulnerability results directly from the organisational activities and thus it is dealt with as a kind of threat-based vulnerability.

The vulnerability of *CSCs* is explained at level 4 with respect to the macroeconomic and natural environment within which organizations do business, people operate physical and information flows, and facilities and assets are positioned. Factors for consideration are the political, economic, social and technological elements of the operating environment, as well as natural phenomenon -- geological, meteorological and pathological (*CLSCM*, 2003). Therefore, major and familiar environmental vulnerability steps from *a)* socio-political reasons, such as wars, regulatory changes and protests; *b)* geo-political reasons, such as the consolidation or disorganisation of countries union; *c*) economic reasons, such as economic crisis, currency fluctuation and other cyclical downturns; *d)* technological reasons, such as new technique flaws and new substitute transport modes; e) natural reasons, such as earthquake, flood and diseases. The nature of environmental vulnerability may be arguable, mainly because it includes not only operating environmental vulnerability that is obviously threat-based but also natural phenomena that many people consider as situations rather than actions. In this study, the natural disasters can be considered as "Act of God" and be categorised into the threat-based vulnerability. Actually, it can be more clearly seen from the ensuing analyses that it is difficult to define the frequency and consequence of the natural vulnerability in many situations so that the application of subjective assessment may be preferred.

The vulnerability in a *CSC* results from two distinctive resources (hazards and threats) and four levels (process, people, organization and environment). Vulnerability identification can be based on historical accident data, expert judgments and some typically established identification techniques. Historical failure statistics are associated with many available databases analyzed in Section 2.3. Expert judgments are provided by multiple experts based on their knowledge and experience in order to compensate the absence of objective statistical data and deal with uncertainty caused by incompleteness. The techniques used include brainstorming, *HAZOP* study and *FMEA*, etc.

To review all the vulnerability existing in the chains, by setting professional and disciplinary boundaries in both time and space, is usually difficult. Therefore, only the descriptions of the potential hazards identified with regard to the containerships and ports and some typical threats in the chains are given in the following:

Containerships:

- Contact and/or collision

Threats:

- Human errors

- Explosion and fire (including flame and heat)
- Flooding
- Grounding and/or stranding
- Loss of hull integrity
- Machinery failure
- Cargo damage
- Hazards related to hazardous cargoes

Ports:

- Impact (including collision and contact)
- Machinery failure
- Loss of containment/release
- Fire and explosion (including gas cloud)
- Deliberate risk-taking
- Employee health and safety scare
- Pressure group protest/strikes
- Terrorist damage
- Loss of suppliers
- Wars/society turbulence
- Economic crisis and currency fluctuation
- Bad weather
- Diseases

Once the vulnerability is identified with respect to each of the compartments in the chains, it is essential to carry out the screening of the risks associated with the vulnerability in order to rank their importance and exclude the trivial ones from further investigation. The screening is only a preliminary estimation and thus the parameters of evaluating the risks, both hazard-based and threat-based, can be defined as failure frequency "*F*" and consequence severity "*S*". Using the "Risk Matrix" approach (Wang, *et al.*, 1999), the rankings of occurrence probability and consequence are combined to obtain the "Risk Ranking Number" (*RRN*), which can categorise the risks according to their importance.

3.3.2 Risk Estimation

Following the application of the "Risk Matrix" approach, those important risks are forwarded for further analysis while trivial ones can be disregarded. The objective of the second step is to evaluate the factors contributing to the important risks on a prioritized list. Following the study of the escalation of the initiating events to accidents and their final outcomes, it is necessary to construct a risk contribution tree. Generally speaking, a hazard-based contribution tree is the combination of a fault tree, which looks at the circumstances and failures leading to an accident event, and an event tree that investigates all possible outcomes from the accident while a threat-based contribution tree is constructed by a single qualitative fault tree diagram, which is considered as a hierarchical structure to apply the *ER* approach.

For the hazard-based risk assessment, *F-N* curves and *PLL* are calculated by following the hazard contribution tree. Each *F-N* curve determines the *PLL* for a particular sub-category so that the final *PLL* for the whole accident category can be estimated. Simultaneously, those basic events and sub-categories can also be ranked with reference to their frequency values.

However, in the realistic life of *CSCs*, it is not easy to produce the *F-N* curves and *PLL* for those threat-based risks. Differing from the hazard-based risks, the threat-based ones are more ruleless and unpredictable in terms of failure likelihood and the severity of consequences so that it may be difficult to define them precisely in numerical terms. One realistic way to cope with imprecision is to use linguistic assessments. However, such linguistic descriptions define risk assessment parameters to a discrete extent so that they can at times be inadequate. *FST* is well suited to modelling subjective linguistic variables and dealing with discrete problems (Wang *et al.*, 1996). In the theory, linguistic variables can be characterised by their membership functions to a set of categories, which describe the degrees of the linguistic variables. From the viewpoint of risk analysis, a *CSC* can be regarded as a complex engineering system, which is constructed by some subsystems (i.e. ports and containerships) with the support of many components (i.e. cranes and engines). In such a hierarchical structure, it is usually the case that safety analysis at a higher level makes use of the information produced at lower levels. It is therefore extraordinarily important to synthesise the risk evaluations of the components in a rational way in order to obtain the risk estimations of the subsystems and the whole system. Actually, the importance of such a synthesis means is further enforced by the requirements of combining all judgements of multiple experts on either one component or the whole system.

Unlike the risk estimation in *QRA*, which is precisely expressed by some numerical values (e.g. *PLL*), the risk analysis results using fuzzy sets are impossibly synthesized using normal mathematical logical operations. The *ER* approach is well suited to modelling subjective credibility induced by partial evidence. The kernel of this approach is an *ER* algorithm developed on the basis of the *D-S* theory, which requires modelling the narrowing of the hypothesis set with the accumulation of evidence (Yang and Xu, 2002). Consequently, a subjective safety modelling tool using the combination of the *FST* and the *ER* approach is proposed to deal with threats and to provide a basis for assigning priorities for corrective actions.

After the study of traditional quantitative safety methods like *FMECA*, it can be seen that there are three basic parameters -- failure likelihood, consequence severity and failure consequence probability (i.e. the probability that possible consequences happen, given the occurrence of the failure), which are used in assessing the safety associated with each failure mode of a component and in determining safety level through "Safety scores" (Wang *et al.*, 1996). Given that the consequence severity of a threat is determined by its own damage capability and external recall ability, four new parameters are proposed to carry out threat-based risk estimation. They are "*Will (Intention)*", "*Damage capability*", "*Recall(Recovery) difficulty*" and "*Damage probability*". "*Will*" decides the failure likelihood of a threat-based risk. The combination of "*Damage capability*" and "*Recall difficulty*" responds to the

consequence severity of the threat-based risk. "*Damage probability*" represents the failure consequence probability of the risk.

In *FST*, linguistic variables that are used to describe the probability of the four parameters can be characterised by their fuzzy set membership functions to a set of categories which describe the degrees of "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*" and which are usually graduated from low to high. The typical linguistic variables and their membership functions for the four parameters of a threat may be defined and characterised as shown in Tables 3.1-3.4. It is obviously possible to have some flexibility in the definition of membership functions to suit different situations.

Table 3.1. The linguistic variables and their membership functions of *Will*

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Extremely strong	0	0	0	0	0	0.75	1
Strong	0	0	0	0	0.75	1	0.25
Moderately strong	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately weak	0	0.25	1	0.75	0	0	0
Weak	0.25	1	0.75	0	0	0	0
Extremely weak	1	0.75	0	0	0	0	0

Table 3.2. The linguistic variables and their membership functions of *Damage capability*

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Extremely big	0	0	0	0	0	0.75	1
Big	0	0	0	0	0.75	1	0.25
Moderately big	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately small	0	0.25	1	0.75	0	0	0
Small	0.25	1	0.75	0	0	0	0
Extremely small	1	0.75	0	0	0	0	0

Table 3.3. The linguistic variables and their membership functions of *Recall difficulty*

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Very difficult	0	0	0	0	0	0.75	1
Difficult	0	0	0	0	0.75	1	0.25
Moderately difficult	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately easy	0	0.25	1	0.75	0	0	0
Easy	0.25	1	0.75	0	0	0	0
Very easy	1	0.75	0	0	0	0	0

Table 3.4. The linguistic variables and their membership functions of *Damage probability*

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Definite	0	0	0	0	0	0.75	1
Highly likely	0	0	0	0	0.75	1	0.25
Reasonably likely	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Reasonably unlikely	0	0.25	1	0.75	0	0	0
Unlikely	0.25	1	0.75	0	0	0	0
Absolutely unlikely	1	0.75	0	0	0	0	0

Once *W, D, R* and *P* represent respectively "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*", the fuzzy safety score *S* can be defined using the following fuzzy set manipulation, which is developed on the basis of Karowski and Mital's formula (Karowski and Mital, 1986 and Wang *et al.*, 1996):

$$S = (R \times D) \circ (P \times W) \tag{3.1}$$

where the symbol "°" represents the composition operation and "×" the Cartesian product operation in *FST*. The membership value of *S* is thus described by:

$$\mu_S = \mu_{(R \times D) \circ (P \times W)} \tag{3.2}$$

Judging from the above formula, the membership function of *S* is denoted by the membership values of four parameters (*R, D, P* and *W*) respectively. Suppose the membership values for the elements in *S, R, D, P* and *W* can be expressed as follows:

$$\begin{aligned} \mu_S &= (\mu^1{}_S, \mu^2{}_S, \ldots, \mu^7{}_S) \\ \mu_R &= (\mu^1{}_R, \mu^2{}_R, \ldots, \mu^7{}_R) \\ \mu_D &= (\mu^1{}_D, \mu^2{}_D, \ldots, \mu^7{}_D) \\ \mu_P &= (\mu^1{}_P, \mu^2{}_P, \ldots, \mu^7{}_P) \\ \mu_W &= (\mu^1{}_W, \mu^2{}_W, \ldots, \mu^7{}_W) \end{aligned} \tag{3.3}$$

Then, those fuzzy operations in Equation (3.2) can be analysed and described as follows:

i). Cartesian product. Two Cartesian product operations can be separately defined by:

$$\begin{aligned} \mu_{R \times D} &= (\mu^{ij}{}_{R \times D})_{7 \times 7} \\ \mu_{P \times W} &= (\mu^{ij}{}_{P \times W})_{7 \times 7} \end{aligned} \tag{3.4}$$

where $\mu^{ij}{}_{R \times D} = \min(\mu^i{}_R, \mu^j{}_D)$, $\mu^{ij}{}_{P \times W} = \min(\mu^i{}_P, \mu^j{}_W)$, both i and $j = 1, 2, \ldots, 7$.

ii). Composition. The composition operation can be defined by:

$$\mu_S = \mu_{(R \times D) \circ (P \times W)} = (\mu^j{}_S)_{1 \times 7} \tag{3.5}$$

where $\mu^j{}_S = \max(\max_{1 \le i \le 7} (\min(\mu^{1i}{}_{R \times D}, \mu^{ij}{}_{P \times W})), \max_{1 \le i \le 7} (\min(\mu^{2i}{}_{R \times D}, \mu^{ij}{}_{P \times W})), \ldots,$

$\max_{1 \le i \le 7} (\min (\mu^{7i}{}_{R \times D}, \mu^{ij}{}_{P \times W})))$, for $j = 1, 2, \ldots, 7$.

However, the μ_S obtained only presents a relative safety level. A safety value can be measured in terms of the defined fuzzy safety expressions (i.e. "*Poor*", "*Fair*", "*Average*" and "*Good*"). In other words, the risk of a threat requires to be expressed by degrees to which it belongs to the safety expressions. The safety expressions defined on the basis of Tables 3.1-3.4 can be shown in Table 3.5 through satisfying the following conditions:

- *The expressions are exclusive for each category by normalizing the membership values of the variables.*
- $S_{Poor} = (R_{Very\ difficult} \times D_{Extremely\ big}) \circ (P_{Definite} \times W_{Extremely\ strong})$.
- $S_{Fair} = (R_{Moderately\ difficult} \times D_{Moderately\ big}) \circ (P_{Reasonably\ likely} \times W_{Moderately\ strong})$.
- $S_{Average} = (R_{Moderately\ easy} \times D_{Moderately\ small}) \circ (P_{Reasonably\ unlikely} \times W_{Moderately\ weak})$.
- $S_{Good} = (R_{Very\ easy} \times D_{Extremely\ small}) \circ (P_{Absolutely\ unlikely} \times W_{Extremely\ weak})$.

Table 3.5. The linguistic variables and their membership functions of *Safety Expressions*

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Poor	0	0	0	0	0	0.75	1
Fair	0	0	0	0. 5	1	0.25	0
Average	0	0.25	1	0. 5	0	0	0
Good	1	0.75	0	0	0	0	0

Using the Best-Fit method (Wang *et al.*, 1996), the obtained fuzzy safety score description S_i of a threat judged by assessor i can be mapped onto one (or all) of the defined safety expressions. The method uses the distance between S_i and each of the safety expressions to represent the degree to which S_i is confirmed to each of them. For example, the distance between S_i and the safety expression "*Poor*" can be shown as follows:

$$d_{i1}(S_i, Poor) = \left[\sum_{k=1}^{7}(\mu_{S_i}^k - \mu_{Poor}^k)^2\right]^{1/2} \tag{3.6}$$

The analyses for other distances between S_i and other safety expressions can be conducted in a similar way. The smaller the distance, the closer S_i is to the corresponding safety expressions. When the distance d_{ij} (j=1, 2, 3 or 4) is equal to zero, S_i is just the same as the *jth* safety expression in terms of membership functions. Because each d_{ij} is an unscaled distance, in order to more clearly express the safety level of S_i, the reciprocals of the relative distances between S_i and each safety expression d_{ij} are normalised into a new index α_{ij}, (j=1, 2, 3, 4). If d_{ij}= 0, it follows that α_{ij} is equal to 1 and the others are equal to 0. The α_{ij} can be defined as follows in other situations:

$$\alpha_{ij} = \frac{1/d_{ij}}{\sum_{j=1}^{4} 1/d_{ij}} \quad j = 1, 2, 3, 4 \tag{3.7}$$

Each α_{ij} (j = 1, 2, 3, 4) represents the extent to which S_i belongs to the *jth* defined safety expression. Thus, the safety levels of the threat-based risks determined using a fuzzy set can be expressed as follows:

$$S(S_i) = \{(\alpha_{i1}, \text{“}Poor\text{”}), (\alpha_{i2}, \text{“}Fair\text{”}), (\alpha_{i3}, \text{“}Average\text{”}), (\alpha_{i4}, \text{“}Good\text{”})\}$$

To produce the risk degree of a threat for ranking purposes, it is necessary to describe the four safety expressions using numerical values. The numerical values associated with the defined safety expressions can be calculated by studying the categories and membership values in Table 3.5. Suppose W'_p, W'_f, W'_a and W'_g represent the unscaled numerical values associated with *“Poor”*, *“Fair”*, *“Average”* and *“Good”*, respectively. W'_s, W'_m, W'_p and W'_g can be calculated as follows:

$$W'_p = [0.75/(0.75 + 1)] \times 5/6 + [1/(0.75 + 1)] \times 1 = 0.927$$
$$W'_f = [0.5/(0.75 + 1 + 0.25)] \times 1/2 + [1/ (0.75 + 1+ 0.25)] \times 2/3 + [0.25/(0.75 + 1 + 0.25)] \times 5/6 = 0.644$$
$$W'_a = [0.25/(0.25 +1 + 0.5)] \times 1/6 + [1/(0.25 + 1 + 0.5)] \times 1/3 + [0.5/(0.25 + 1 + 0.5)] \times 1/2 = 0.356$$
$$W'_g = [1/(1+0.75)] \times 0 + [0.75/(1 + 0.75)] \times 1/6 = 0.073 \qquad (3.8)$$

The above values give numerical relations between the safety expressions. The reciprocally normalized vector [w_p, w_f, w_a, w_g] is then obtained as follows, where *“Good”* takes the largest value of 1 (i.e. $w_g = 1$):

$$[w_p, w_f, w_a, w_g] = [0.079, 0.384, 0.695, 1]$$

Naturally, a numerical risk degree of the threat can be obtained by the following calculation:

$$P_{S(Si)} = \alpha_{i1} \times 0.079 + \alpha_{i2} \times 0.384 + \alpha_{i3} \times 0.695 + \alpha_{i4} \times 1 \qquad (3.9)$$

The $S(S_i)$ obtained represents the piece of estimation from one assessor. When more pieces of estimation from different assessors emerge, they can be effectively synthesized using the *ER* approach. The approach has been widely applied to risk and safety assessment (Wang *et al.*, 1996; Sii *et al.*, 2001). In continuously researching and practicing processes, the *ER* algorithm has been developed, improved and modified towards a more rational way (Yang and Xu, 2002). The algorithm can be analysed and explained in this study as follows.

Let A represent the set of the four safety expressions, which has been synthesized by two subsets A_1 and A_2 from two different assessors. Then, A, A_1 and A_2 can separately be expressed by:

$$A = \{\alpha^1 \text{“}Poor\text{”}, \alpha^2 \text{“}Fair\text{”}, \alpha^3 \text{“}Average\text{”}, \alpha^4 \text{“}Good\text{”}\}$$

$$A_1 = \{\alpha^1_1 \text{“}Poor\text{”}, \alpha^2_1 \text{“}Fair\text{”}, \alpha^3_1 \text{“}Average\text{”}, \alpha^4_1 \text{“}Good\text{”}\}$$
$$A_2 = \{\alpha^1_2 \text{“}Poor\text{”}, \alpha^2_2 \text{“}Fair\text{”}, \alpha^3_2 \text{“}Average\text{”}, \alpha^4_2 \text{“}Good\text{”}\}$$

Suppose the normalized relative weights of two safety assessors in the safety evaluation process are given as ω_1 and ω_2 ($\omega_1 + \omega_2 = 1$) and ω_1 and ω_2 can be estimated by using established methods such as simple rating methods or more elaborate methods based on pair-wise comparisons (Yang *et al.*, 2001).

Suppose M^m_1 and M^m_2 ($m = 1, 2, 3$ *or* 4) are individual degrees to which the subsets A_1 and A_2 support the hypothesis that the safety evaluation is confirmed to the four safety expressions. Then, M^n_1 and M^n_2 can be obtained as follows:

$$M^n_1 = \omega_1 \alpha^m_1$$
$$M^n_2 = \omega_2 \alpha^m_2 \qquad (3.10)$$

where $m = 1, 2, 3, 4$. Therefore,

$$M^1_1 = \omega_1 \alpha^1_1 \qquad M^1_2 = \omega_2 \alpha^1_2$$
$$M^2_1 = \omega_1 \alpha^2_1 \qquad M^2_2 = \omega_2 \alpha^2_2$$
$$M^3_1 = \omega_1 \alpha^3_1 \qquad M^3_2 = \omega_2 \alpha^3_2$$
$$M^4_1 = \omega_1 \alpha^4_1 \qquad M^4_2 = \omega_2 \alpha^4_2 \qquad (3.11)$$

Suppose H_1 and H_2 are the individual remaining belief values unassigned for M^m_1 and M^m_2 ($m = 1, 2, 3, 4$). Then, H_1 and H_2 can be expressed as follows (Yang and Xu, 2002):

$$H_1 = \overline{H}_1 + \tilde{H}_1$$
$$H_2 = \overline{H}_2 + \tilde{H}_2 \qquad (3.12)$$

where $\overline{H}_n$ ($n = 1$ *or* 2), which represents the degree to which the other assessor can play a role in the assessment, and $\tilde{H}_n$ ($n = 1$ *or* 2), which is caused by the possible incompleteness in the subsets A_1 and A_2, can be described as follows respectively:

$$\overline{H}_1 = 1 - \omega_1 = \omega_2$$
$$\overline{H}_2 = 1 - \omega_2 = \omega_1$$
$$\tilde{H}_1 = \omega_1 (1 - \sum_{m=1}^{4} a_1^m) = \omega_1 [1 - (\alpha^1_1 + \alpha^2_1 + \alpha^3_1 + \alpha^4_1)]$$
$$\tilde{H}_2 = \omega_2 (1 - \sum_{m=1}^{4} a_2^m) = \omega_2 [1 - (\alpha^1_2 + \alpha^2_2 + \alpha^3_2 + \alpha^4_2)] \qquad (3.13)$$

Suppose $\alpha^{m'}$ ($m = 1, 2, 3$ *or* 4) represents the non-normalized degree to which the safety evaluation is confirmed to the four safety expressions as a result of the synthesis of the

judgments produced by assessors 1 and 2. Suppose H_U' represents the non-normalized remaining belief unassigned after the commitment of belief to the four safety expressions as a result of the synthesis of the judgments produced by assessors 1 and 2. The *ER* algorithm can be stated as follows (Yang and Xu, 2002):

$$a^m' = K\ (M^n_1 M^n_2 + M^n_1 H_2 + H_1 M^n_2)$$
$$\overline{H}_U' = K\ (\overline{H}_1 \overline{H}_2)$$
$$\tilde{H}_U' = K\ (\tilde{H}_1 \tilde{H}_2 + \tilde{H}_1 H_2 + H_1 \tilde{H}_2)$$

$$K = [1 - \sum_{T=1}^{4} \sum_{\substack{R=1 \\ R \neq T}}^{4} M_1^T M_2^R]^{-1} \tag{3.14}$$

After the above aggregation, the combined degrees of belief are generated by assigning $\overline{H}_U'$ back to the four safety expressions using the following normalization process:

$$a^m = a^m'/1 - \overline{H}_U' \ (m = 1, 2, 3, 4)$$
$$H_U = \tilde{H}_U'/1 - \overline{H}_U' \tag{3.15}$$

where H_U is the unassigned degree of belief representing the extent of incompleteness in the overall assessment.

The above gives the process of combining two fuzzy sets. If three fuzzy sets are required to be combined, the result obtained from the combination of any two sets can be further synthesized with the third one using the above algorithm. In a similar way, multiple fuzzy sets from the judgements of multiple assessors or the safety evaluations of lower level risks in the chain systems (i.e. components or subsystems) can also be combined. The two different and noteworthy points are that the relative weights of every assessor will be normalized first; and the relative weights of the lower level risks should satisfy the requirements of the specific rule in Section 3.2.3.

3.3.3 RCOs/Risk Control Measures (RCMs)

RCOs/RCMs are selected to manage the high-risk areas identified in the previous step. At this stage the implementation costs and potential benefits of *RCMs* are not of concern and attention is only focused on how to avoid or lessen the impact of the potential risks. In general, three main characteristics according to which *RCMs* are evaluated can be summarised as follows (MSA, 1993):

- Those relating to the fundamental type of risk reduction like the preventative and mitigating measures.
- Those relating to the type of action required (i.e. engineering or procedural).

- Those relating to the confidence that can be placed in the measure (active or passive, redundant or auditable).

In order to achieve risk reduction, a list of countermeasures based on human, procedure or equipment solutions can be applied to reduce either the likelihood of occurrence or the severity of the consequences of hazards or control the four parameters of threat-based risks. Human managerial solutions aim at dealing with more effective organisational management and fewer emergences of human errors in operations. The best way to achieve this is to develop a safety culture, in which the key factors for their success are effective human communication and training. Operational procedure solutions mean the introduction and development of appropriate procedures for carrying out risk-critical tasks and thus, include safety procedures, safe working practices, *CPs* and safety exercises. Engineering equipment solutions involve the design and/or construction of containerships, ports, inland transport tools & infrastructures and corresponding supporting facilities (i.e. continuously updated X-ray scanners for checking containers). Equipment solutions have inherent advantages that can be clearly identifiable and relatively easily address vulnerability at the starting point of a *CSC* cycle. Nevertheless, large-scale engineering solutions suffer from lack of historical data on design aspects, inability of full-scale experimentation and difficulty of modification or replacement once in operation (Wang and Ruxton, 1998).

In order to accurately and effectively take *RCMs*, one way is to create a "Causal Chain" (Passenger Vessel Association (*PVA*), 1997; Lois *et al.*, 2004) through which a hazard/threat or an initiating event can be controlled not to be developed into final accidents or serious disasters. The philosophy of this method is to display the causal development of an accident from its initial stage to final serious consequences and then use various intervention or barriers to as early as possibly block the development.

3.3.4 Economic Analysis

The aim of this step is to identify those cost-effective *RCMs* and ensure that the benefit gained will be greater than the cost incurred as a result of the adoption (Kuo, 1998; Wang *et al.*, 1999; *MSA*, 1993). The economic analysis in the risk assessment of *CSCs* is not straightforward, mainly because of the following reasons:

i). The estimation of the benefits obtained for the reduction of some threat-based risks (i.e. terrorism attacks) is usually difficult. The calculation of such benefits will be influenced by not only direct and indirect factors but also some additional impacts, which may not be associated with the original task of *RCMs* at all. Hence, it will be more feasible and reasonable that the economic analysis for the *RCMs* of some threat-based risks focuses on single cost analysis.

ii). The choice of a common unit of measurement is required. In order to give the conclusion of taking one *RCM* or not, a common measure unit must be expressed as a bottom line. The most convenient common unit is money. This means that all benefits and costs of an *RCM* for *CSCs* should be measured in terms of their equivalent monetary values.

iii). The relationship between those situations with and without *RCMs* is often complex. Judging the effectiveness of one *RCM* to a *CSC* system, its influence can be defined by considering the difference between the situations with and without this *RCM.* Therefore, a base is required to incorporate the comparisons and normally the situation without the *RCM* is chosen as such a base.

iv). The *CBA* in *FSA* is an imprecise science in nature due to many unclear benefits and costs, such as the cost of time and the value of human life. One limitation for using *CBA* in *FSA* is how to measure the valuation of life and time, in other words, how to change their valuation into the common unit of measure – monetary value. This limitation will undoubtedly lead to the emergence of imperfect data and uncertainty. Thus, it must be pointed out that *CBA*, as suggested for use in *FSA* is not a precise science, but only a way of evaluation. It cannot be used mechanistically, but only as a consulting instrument in making decisions (Wang and Foinikis, 2001).

The evaluation of costs and benefits can be carried out by subjective methods. One subjective *CBA* technique used in the case of the North Ferry Company (*PVA*, 1997) offers a useful tool for the development of a generic *CBA* framework. The theory of this technique is to compare the benefit and cost estimates of countermeasures and choose the countermeasure with the biggest gap between the benefit and cost estimates as the best *RCM.* However, there is a limitation in this technique, which can be identified as the discrete scales of estimates of benefits and costs. The situation where realistic cost or benefit evaluations belong to certain values between two discretely defined neighbouring values may greatly discount the accuracy of such a technique. Although the use of *CBA* in *FSA* surely does not require precise estimations and calculation, this method will still not be competent under certain situations. For example, the emergence of thousands of *RCMs* for a very complex system may lead to that many *RCMs* have the same gaps between the benefits and costs estimated. More precise estimations are required.

A new technique for the use of *CBA* in the *CSC* risk assessment framework is produced, namely *FCBA*. The development of this technique is based on the aforesaid *FST*, which is well suited for handling discrete estimates of costs and benefits, and the *ER* approach, which is capable of conducting the incomplete assessment of uncertainty so as to synthesise the fuzzy estimates of costs and benefits together. Having introduced them in Section 3.3.2, a generic *FCBA* framework can be generated in a similar manner as follows:

i). Separately defining cost expressions and benefit expressions using FST.

The costs and benefits incurred for one *RCM* can be described using linguistic variables such as "*Very low*", "*Low*", "*Moderately low*", "*Average*", "*Moderately high*", "*High*" and "*Very high*", which are referred to as cost and benefit expressions. Such linguistic variables can also be described using fuzzy set membership functions to a set of categories, which describe the degrees of the cost and benefit expressions.

ii). Separately describing the RCM's costs and benefits in fuzzy sets.

In such a procedure, the membership values describing the costs and benefits incurred for the *RCM* may be given by assessors with reference to the defined fuzzy set membership functions. Of course, each assessor has some flexibility in the formulation of membership values to reflect his own option.

iii). Mapping the estimates of costs and benefits onto utility expressions.

It can be noted that the costs and benefits of an *RCM* are described separately in terms of the cost and benefit expressions. It is necessary to define a utility space to evaluate the *RCM*'s benefits and costs on the same scale. Like the common unit of measure - money existing in *CBA*, utility expressions are required in *FCBA* to define the utility space. Seven utility expressions – "*Extremely subsidiary*", "*Subsidiary*", "*Moderately Subsidiary*", "*Average*", "*Moderately preferred*", "*Preferred*" and "*Extremely preferred*", which can be considered to be matched with the cost and benefit expressions simultaneously, are defined using fuzzy set membership functions. Given the membership values of the fuzzy cost and benefit sets of an *RCM*, the Best-Fit method described in Section 3.2 can be used to map the fuzzy cost and benefit sets onto the defined utility expressions.

iv). Using the ER algorithm to synthesize the estimates of costs and benefits expressed by the utility expressions and obtain the synthesized preference estimate of an RCM.

Assessors can regard the utility estimates of an *RCM* as a hypothesis and consider the estimates of costs and benefits as two pieces of evidence. Given that the fuzzy estimates of costs and benefits in *FCBA* are considered to be equally important, they can be synthesised using the *ER* approach to obtain a preference estimate in terms of the utility expressions.

v). Production of the preference degree of an RCM.

To produce the preference degree of an *RCM* for ranking purposes, it is necessary to describe the four utility expressions using numerical values. The numerical values associated with the defined utility expressions can be calculated in a similar way to that used to obtain the preferred numerical values of the safety expressions in Section 3.3.2.

However, the described *FCBA* method is not a panacea. Having analysed the difficulties faced in the economic analysis, it can be clearly noted that even the fuzzy benefit estimation of some threat-based *RCMs* may be very difficult. Under such a situation, only the cost analysis of the *RCMs*, either precise or fuzzy, can be considered to be the single reference for adopting the *RCMs* from an economic perspective. Actually, such a

consideration may be especially meaningful since the cost analysis can still function as a supporting parameter on making decisions. The specific operations will be described in Section 3.3.5. Additionally, the economic analysis of *CSCs* needs to be paid particular attention to their operational procedure, where the evaluation of costs and benefits should be carried out for both the overall situation and each particular accident category and should be fair enough for every stakeholder.

3.3.5 Decision Making

Following the economic analysis of all *RCMs*, decisions should be made in the final step of the risk assessment framework. Decision making aims at giving recommendations and making decisions to improve the safety of the whole operational processes of *CSCs*. Thus all pieces of information generated in the previous steps are collected and used in selecting the *RCOs* which best balance the reduction of risks with cost effectiveness for the whole situation as well as the particular stakeholders.

The task of picking up the *RCOs* for those hazard-based or threat-based risks, in which *CBA* or *FCBA* can be carried out, seems to be relatively straightforward. Under this situation, the benefits (including the risk reduction) and costs can be effectively evaluated and expressed by a common unit. This demonstrates that the two decision making parameters (the reduction of risks and the corresponding economic considerations) have been ably integrated into one attribute, through which risk ranking can be conducted and the best *RCO* can be selected.

However, it is usually not easy to efficiently estimate the benefits of *RCMs* for some threat-based risks, which means that the two decision parameters -- the reduction of risks and its economic factors cannot be united into one with confidence. Therefore, here a techno-economic model is formulated to simultaneously consider the two parameters (Yang *et al.*, 2005a). It includes safety and economic models. The safety model can be constructed as follows:

Max: the reduction of risks
subject to: risks > negligible risks

where the risks may be denoted by the "*Will*", "*Damage capability*", "*Recall difficulty*" and "*Damage probability*" from a threat. The value of the reduction of risks can be calculated by the fuzzy safety evaluation, which can be obtained by using the *FST* and *ER* approach described previously. In terms of the economic model, the costs of the *RCO* consist of the first time investment costs (C_i) and the operational costs (C_o) normally. Thus the economic model can be constructed as follows:

Min: Costs $= C_i + C_o$
subject to: risks > negligible risks

Once the techno-economic model is constructed, all *RCMs/RCOs* can be effectively expressed in two attributes, through which decisions can be made. Generally speaking, safety is closely related to cost, which means high cost should achieve a big reduction of risks. Therefore, assessors will ignore those *RCOs*, by which high cost only limitedly plays the level of risks down, and fully concentrate on the others, from which the decision makers can select appropriate ones with respect to particular requirements on safety and costs. An ideal *RCO*, which can be represented by the maximized safety and minimized cost simultaneously is not feasible. Therefore, only a compromise one can be obtained. If the safety and cost objectives are of equal importance, the best compromise option can be obtained using a minmax approach. When the requirements of safety and costs change, some neighbouring *RCOs* of the best compromise one defined above can be appropriately considered.

The results produced from the techno-economic model can be used to assist decision makers in understanding the interaction between safety and economic considerations and consequently, balance and best utilize resources in the risk assessment process. However, the techno-economic decision-making method is firmly based on the precise calculation of costs. Although the costs of *RCOs*, not like the benefits, in most cases, can be estimated, the decision makers may not know or possibly calculate the accurate costs of *RCOs* due to their complexity under some particular situations. Alternatively, fuzzy sets can be used to estimate costs incurred in the reduction of risks using linguistic variables. Once the costs occurred for the *RCOs* are defined using fuzzy sets, there are two methods to synthesise them and the reduction of risks for making decisions. One is to defuzzify the fuzzy cost estimation, obtain the different quantitative cost expressions for various *RCOs* and then use the techno-economic method above. The other is to fuzzify the reduction of risks based onto a utility space of cost and safety, transfer the cost fuzzy estimation on the utility space and then use the *ER* approach. The philosophy and methodology of the method is similar to the *FCBA* approach. The difference lies in the fuzzy benefit estimates that are substituted by the fuzzy estimates of risk reduction.

3.4. Case Study

Immediately after the devastating terrorism attacks on the World Trade Centre on the 11th September 2001, people recognised that the risk of mega-terrorism extremely possibly and suddenly became very real. Governments, organisations and companies around the globe scrambled to assess their vulnerability to highly organised terrorist groups willing to sacrifice thousands of lives or billions of dollars to achieve their aims. *CSC* systems have loomed large in the eyes of security agencies worldwide as a prime target and/or vehicle for future attacks.

The world has thankfully not experienced a major terrorist attack on the chains using containers or their supporting infrastructures. This status may be easily changed, however, in one horrible day like 11th September of 2001. Many accidents from the other relevant areas have driven the chains to enforce their safety consciousness. In October 2002, a single attack happened on a tanker - *Limberg*. Despite Al'Qaeda's claim of responsibility for the attack, the accident generated relatively little disruption of global oil trade. This may be due to a perception that the risk to tankers is extremely localized and therefore easily mitigated (OECD, 2003). If the terrorist attacks were combined with shipping containers, their consequences would be extremely serious and not limited in the local region any more. The American west coast port 11-day lockout in October 2002 provided an ideal supposition platform, on which one can judge how serious the impacts of a major sophisticated attack related to container ports can be. The losses resulting from the 11-day lockout were approximately USD 19.4 billion, which would increase exponentially as time went on (Patrick, 2002). This estimate did not cover costs borne by non-American ports and manufacturers faced with container backlogs and increased warehousing costs. This figure would be dramatically increased given the loss of lives and property damage costs imposed by a shutdown of the same ports from terrorist attacks. The marriage of inland transport to container chains enables terrorism attacks associated with container shipping emerging in any corner of the world. A more recent terrorist attack occurring in the Madrid train station in March 2004 further offered people a bigger image of how likely and serious an attack can happen using the inland transport links of the container chains. Furthermore, because of the uncertainty of container cargo, *CSCs* surely easily offer many opportunities for terrorists -- just as they currently do for drug, stowaways and contraband smugglers.

One fortunate thing is that people have focused their minds on finding ways to avoid potential vulnerability of a terrorist attack in the chains. Today, the US government reports that it inspects roughly 5.5-6% of all inbound containers (roughly 550,000 containers/year), using either X-ray or gamma ray technology (or both) or by physical devanning of the container (Christopher, 2005). Customs and Border Protection (*CBP*) of America has deployed radiation scanning equipment at all major American container ports with the objective of being able to check every container entering the U.S. for radiation by the end of 2005 (Christopher, 2005). *Cargo Security International* reported that more than a fifth of containers through the Port of Fremantle, Australia can be checked by the fourth generation of X-ray container scanners. People have also recognized that the effectiveness of *CSCs* must be balanced with tightened security measures that address the chains' vulnerability and weaknesses. The newly developed measures related to *CSCs* have mainly emerged from two sources. One came from the International Ship and Port Facility Security (*ISPS*) code, which was produced by the *IMO* in December 2002 and incorporated into the Convention on the Safety of Life at

Sea (*SOLAS*). The other originated from the USA and EU security measures, which include the United States Maritime Transport Security Act of 2002, 96-hour advance notification of arrival and 24-hour advance manifest rules, *CSI* (Container Security Initiative) and *C-TPAT* (Customs-Trade Partnership Against Terrorism), etc. These regulations are largely supplementary to the *ISPS* and have been developed in response to the more and wider vulnerability in *CSCs*.

However, all anti-terrorism measures are cost-based but not all of them are mandatory. The adoption of such measures for the entities related to *CSCs* should be diverse enough. The selection of the most effective *RCOs* will be carried out with the full consideration of both safety and cost factors. Therefore, the case study will provide its two core contributions – a test of the feasibility of the generated *FSA* methodology and a guideline for the anti-terrorism operations in *CSCs*, through addressing the following specific questions:

- Which sectors in *CSCs* are vulnerable facing a terrorism attack?
- What are those major factors that lead to the emergence of such vulnerability?
- What kinds of measures can be effectively adopted to prevent the vulnerability?
- Are these measures cost-effective?
- How these measures are ranked with reference to the different requirements of safety and cost?

3.4.1 The Vulnerable Sectors of CSCs Facing A Terrorist Attack

The sectors in *CSCs* where a terrorism attack possibly occurs can be identified as follows:

- Containerships
- Ports
- Trains
- Trucks
- Employees
- Cargoes
- Warehouses/intermediate premises
- Information control centers
- Shipping lanes
- Railways
- Roads
- Cables/satellites

In these sectors, tens of thousands of vulnerabilities exist. Some major ones can be described to demonstrate their wide distribution scopes and expressional modes. Containerships may transit through various routes and make multiple stops at diverse ports posing different levels of security risks. Port/terminal operators may not adequately screen their employees for criminal backgrounds. Some containers may be at significant risk given that they will stay in ports for a period before loading onto a containership. Between the ports and containerships, containers experience loading and discharging processes, which may be vulnerable because the containers are not carefully and routinely inspected. On the other end of the chain, warehouses may have weak

controls and very dangerous personnel practices. For example, the access to container storage is not secure and no countermeasures for checking employee and visitor backgrounds are taken. Furthermore, the trucking connections between warehouses and ports may be invisible in transit activities and the locations of trucks and containers may be not known and tracked.

Despite these facts, it is noteworthy that *a)* not all of such sectors will become vulnerable facing a terrorism threat; and *b)* not all components in the vulnerable sectors contribute to their vulnerability. For example, a terrorism attack influences a containership's survivability through only two key ways: attacking the engine room or hitting a bulkhead between two compartments, both of which require design knowledge and the ability to get onboard the vessel (Noble, 2004). Therefore, in order to understand the vulnerability of *CSCs* in a terrorism attack, it will be essential to investigate the major reasons/factors (including those vulnerable components) resulting in the emergence of the vulnerability and to carefully analyse risk contributing factors using the *FTA* technique. The screening technique based on the "Risk Matrix" approach is used to obtain the important risks in such five sectors as ports, containerships, employees, trains and trucks.

3.4.2 Risk Factors and Estimations

CSCs, by their nature as complex and international open distribution networks, pose a great challenge from a security standpoint. Such a challenge can be evidenced by the multiplicity of risk factors associated with a terrorist attack. Facing a terror threat, the chains can be the vectors for, or targets of attacks, as well as a vehicle to other attacks organised by terrorists. The principal risk factors related to the chain in a terrorist attack stem from cargoes, containerships, ports, trucks, trains and people. Simultaneously, these risk factors should be considered in an integrated way so that governments, organisations and companies can address the threat with broad-based security policy responses, since simply responding to risk factors in isolation to one another will be both ineffective and costly.

Cargo: Most of the world's non-bulk cargo travels in marine shipping containers. These standardized boxes have revolutionized the transport of goods by sea since their first appearance in 1956 (Chadwin *et al.*, 1999) and have given rise to a multitude of specialized road and rail carriers, a fleet of 2,905 modular container vessels (*ISL*, 2003) and the emergence of a global network of over 430 highly automated port handling facilities (Fairplay, 2004). In 2002, the Bureau International des Containers estimated that approximately 15 million containers were in circulation (*OECD*, 2003). Data from *ISL* indicates that 250 million containers were moved through container ports in 2002 (*ISL*, 2003).

In considering a terrorist attack using containers, it is very easy to imagine that a sealed container fully equipped with global positioning satellite-enabled bombs can remotely detonated when arriving at the heart of a major population center. The likelihood of success of such an operation would increase, considering the fact that only a small number of containers can be physically examined in practice in order to maintain the container flow speed. Containers also pose a threat when they carry legitimate cargo that can be used by terrorists for nefarious purposes. Many containers or tank-containers are used to ship hazardous cargoes. It may be safe to keep separately some hazardous cargoes in normal situations. However, a huge explosion may occur, if they access each other. This phenomenon has been evidenced by thousand of accidents. The serious consequences resulting from the accidents have no doubt urged terrorists to recognize that it is feasible of adopting hazardous cargoes to carry out a terror attack. The fact that some unscrupulous shippers and careless carriers sometimes mask the true identity of hazardous cargoes emphasises the ease with which terrorists could do the same for more sinister purposes.

Vessel: The above discusses the dangers posed by cargoes. These dangers highlight the potential for an entire vessel to be used as a weapon in a terrorist strike just as jet aircraft were used in the 2001 World Trade Center attacks. In such cases, containerships can be used against a population center adjacent to port facilities or shipping channels, to damage port or bridge facilities or to sink themselves and block the access to a port facility. While the potential damage from such an attack is great, previous terrorist incidents involving ships have tended to target vessels rather than use them. The terrorism attacks against the cruise vessel Achille Lauro, the USS Cole and the oil tanker Limberg, and the discovery of an Al'Qaeda linked plot to attack vessels passing through the straits of Gibraltar, all point to the risks of attacks faced by vessels (*OECD*, 2003). If this tendency is extended to containerships, an engine room and a bulkhead between two compartments are considered as the most vulnerable components in an attack.

The consideration of bulk carriers as a risk factor for *CSCs* is because it is possible that one bulk vessel fully loaded with highly dangerous cargoes could be used in a "suicide" operation aimed at targeting a container port facility or containership so as to break the chains. Unlike container shipping, bulk shipping has generally received less attention from security authorities. This sector is divided into bulk liquid carriers (their cargoes ranging from crude oil, distilled oil derivatives, LPG and LNG to molasses and vegetable oils) and bulk solid carriers (i.e. fertilizer carriers). By the explosive nature of these bulk cargoes, the carriers and their cargoes can be deemed as legally mobile and natural bombs in some situations. The configuration of international ports further contributes to making these shipments a prime terrorist vehicle. For example, in 1997, over 400,000 tonnes of ammonium nitrate (one kind of explosive fertilizer) were

shipped along the winding 235-mile-long lower Mississippi waterway, the world's largest bulk commodity port area (*OECD*, 2003).

The risks to shipping from terrorist attacks are highlighted by the persistent problem of modern day piracy. Recently, some scholars (Ong, 2002; Raymond, 2005) pointed out that it would be a bigger challenge for maritime security to consider the emergence of the cooperation between the terrorism groups and traditional pirates. Given the relative difficulty in triggering a major explosion through an attack on a vessel, it is more likely that terrorists attack a containership principally by piracy, through which they would hijack its cargoes, hold its crew as hostages for ransom or political purposes, sink the vessel and cause as much loss of life as possible, or cripple trade by threatening to close down access to ports and/or valuable trade routes.

Port: The World Trade Center attacks revealed that one of the terrorism groups' principal motivations was to inflict massive economic losses on their targeting countries, such as the United States and its allies. Given the facts that *a)* most of the world's trade travels by sea, *b)* most seaborne trade (by value) travels in containers, and *c)* most containers are operated through relatively few international transfer terminals due to the concentration of liner shipping and ports, one can easily see the potential for major economic disruption following a terrorist attack on ports, which undoubtedly attracts terrorists to select them as an ideal vehicle to achieve their aims. The attacks on major international transfer ports such as Hong Kong, Singapore, Long Beach/Los Angeles, Rotterdam or Antwerp could have devastating impacts on both the regional and global economy. Such a horrible disaster would be highly likely to happen through two ways: to attack the channel/waterway or bomb the quayside infrastructures/facilities (i.e. cranes) of the terminals. The waterway/channel design structures and their arrangements are the most important risk factors contributing to the vulnerability of ports. The narrow access channel of Rotterdam port is a typical representative with the vulnerable feature. The quayside infrastructures/facilities (i.e. cranes) of the terminals are also vulnerable components in ports. Approximate construction costs for a modern 16 hectares container terminal are $32 million, which has not included land acquisition costs and container handling equipment including several cranes at $4.7 million per piece (*OECD*, 2003).

Train and trunk: The container-carrying trains and trucks in *CSCs*, unlike the containerships or ports, are not capital-intensive or people-intensive sectors. If the aim of a terrorism attack is to maximize the damage of the property or the losses of lives, either the trains or trunks are obviously not an ideal choice as the target of attacks. However, given their abilities to easily access a business or population center, especially the flexibility of the trucks in the chains, they will be greatly preferred by terrorists as vehicles of attacks. The fear that terrorists could exploit the container-carrying trains or trucks as a mobile bomb into a business or population center can be highlighted by the

accidents of Madrid train station bomb attacks and uncountable Middle East or Iraq terrorism attacks using car bombs. Additionally, the experience absorbed from those accidents shows that the damage capability of train/truck-related attacks is closely associated with the explosive ability of container cargo carried by trains/trucks rather than themselves. This also proves the above point that the risk factors should be treated in an integrated way and not considered in isolation.

People: There are approximately 1,227,000 officers manning the merchant fleet (*OECD*, 2003). Not all of these seafarers operate on international liner containerships but a significant portion does. The terrorism-related risks involving this vast labour force are two-fold. As seen in the previous section, seafarers are often directly targeted (in many cases of piracy) and/or indirectly suffer from terrorist attacks targeting vessels (as in the case of the Limberg). The second risk factor is that some seafarers may actually be accomplices of members of the terrorist groups. The latter is especially worrisome given that seafarers have traditionally been granted relatively liberal travel rights by governments through non-immigrant crew list visas, or simply upon presentation of their seafarer identity documents (*OECD*, 2003). Furthermore, such seafarer identity documents are relatively easily forged and falsified and can be bought on black markets, which has been evidenced by several recent high-profile cases involving major registries and seafarer-supplying nations.

Compared to the crew on the sea, staff working on the shore sectors in the chains face relatively less personal risks. The terrorism-based risks related to the shore working staff are mainly focused on the fact that some of them have a terrorism background or cooperate/work with terrorism groups. This point can be emphasised by the fact that the losses of container cargo in the main Western European ports are a result of the cooperation between internal staff and external thieves. If unscrupulous persons are already aware of these facts and are already operating in the chains, it is not unreasonable to assume that terrorist groups have also recognised these possibilities and are planning to exploit them.

Having analysed the risk factors in *CSCs* with their causes and results, a fault tree can be constructed to further assess the potential risk factors in Figure 3.2.

Following the fault tree, the basic events can be synthesised using the fuzzy set and *ER* approaches and the risk level of the top event can be calculated. However, it is noteworthy that the weights of all basic events in applying the *ER* method are different because the contribution tree, which can be considered as a hierarchical diagram, consists of many '*OR*' and '*AND*' gates. The estimation and calculation of the risk levels can be conducted as follows.

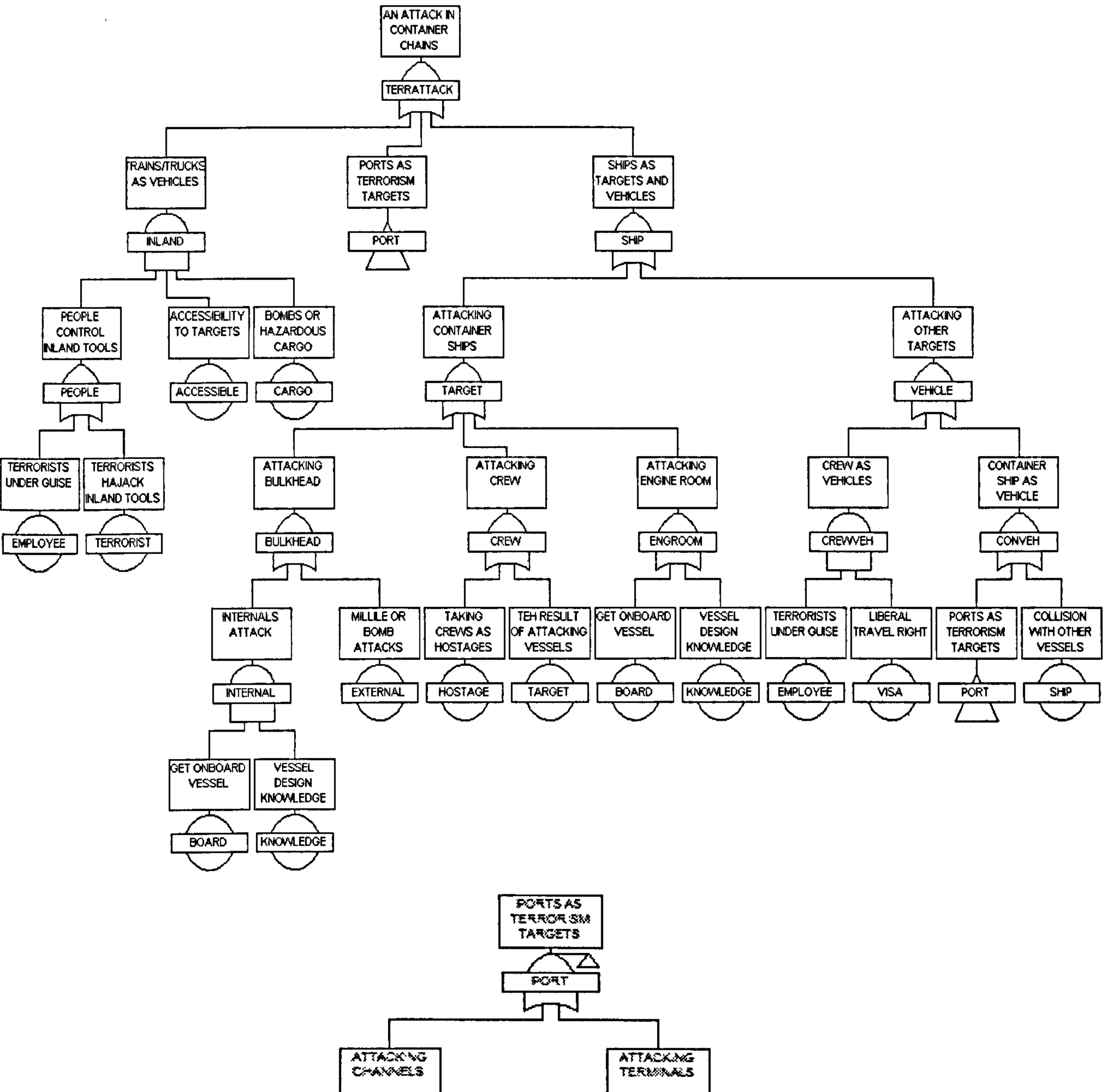


Figure 3.2. A terrorism attack contribution tree

Step 1 assigns the weights of basic events by the rule introduced in Section 3.2.3. The weight assignments of the events in Figure 3.2 can be obtained in Table 3.6.

Table 3.6. The weight assignments of all events

Gates	Weights	Basic events	Weights
TERRATTACK	1	VESSEL	1
PORT	1	EXTERNAL	1
SHIP	1	CARGO (under 'CONTAINER' gate)	0.5
INLAND	1	EMPLOYEE (under 'CONTAINER' gate)	0.5
PEOPLE	0.3333	HOSTAGE	1
CHANNEL	1	TARGET	1
TERMINAL	1	BOARD	0.5
TARGET	1	KNOWLEDGE	0.5
VEHICLE	1	VISA	0.5
CONTAINER	1	SHIP	1
BULKHEAD	1	CARGO (under 'INLAND' gate)	0.3333
CREW	1	ACCESSIBLE	0.3333
ENGROOM	1	TERRORIST	0.3333
INTERNAL	1	EMPLOYEE (under 'PEOPLE' gate)	0.3333
CREWVEH	1		
CONVEH	1		

Step 2 calculates the risk scores of the basic events on the basis of the fuzzy estimations of the four parameters from Tables 3.1 – 3.4. The risk scores are calculated by using the fuzzy operations of the formula '$\mu_S = \mu_{(R \times D) \circ (P \times W)}$' and the Best-Fit method in Section 3.3.2. The ranking of the basic events can be clearly obtained using the method of studying the fuzzy membership values and categories, and shown in Table 3.7.

Table 3.7 The risk estimations of all basic events

Basic events	Parameters				Risk scores	Risk rank
	Will (W)	Damage capability (D)	Recall difficulty (R)	Damage probability (P)		
VESSEL	W = {0, 0, 0, 0, 0.75, 1, 0.25} D = {0, 0, 0, 0, 0, 0.75, 1} R = {0, 0, 0, 0, 0,75, 1, 0.25} (P) = {0, 0, 0, 0.75, 1, 0.25, 0}				***S*** = {0.021, *"Poor"*, 0.934, *"Fair"*, 0.027, *"Average"*, 0.018, *"Good"*}	0.31 **2**
EXTERNAL	W = {0, 0.25, 1, 0.75, 0, 0, 0} D = {0, 0, 0.5, 1, 0.5, 0, 0} R = {0, 0, 0.5, 1, 0.5, 0, 0} (P) = {0, 0, 0, 0.75, 1, 0.25, 0}				***S*** = {0.1, *"Poor"*, 0.128, *"Fair"*, 0.664, *"Average"*, 0.108, *"Good"*}	0.613 **11**
CARGO	W = {0, 0, 0, 0, 0, 0.75, 1} D = {0, 0, 0, 0, 0.75, 1, 0.25} R = {0, 0, 0.5, 1, 0.5, 0, 0} (P) = {0, 0, 0.5, 1, 0.5, 0, 0}				***S*** = {0.444, *"Poor"*, 0.199, *"Fair"*, 0.184, *"Average"*, 0.173, *"Good"*}	0.412 **5**
EMPLOYEE	W = {0, 0, 0.5, 1, 0.5, 0, 0} D = {0, 0.25, 1, 0.75, 0, 0, 0} R = {0, 0.25, 1, 0.75, 0, 0, 0} (P) = {0, 0, 0, 0.75, 1, 0.25}				***S*** = {0.139, *"Poor"*, 0.361, *"Fair"*, 0.361, *"Average"*, 0.139, *"Good"*}	0.44 **8**
HOSTAGE	W = {0, 0, 0, 0.75, 1, 0.25, 0} D = {0, 0, 0, 0.75, 1, 0.25, 0} R = {0, 0, 0, 0, 0,75, 1, 0.25} (P) = {0, 0, 0, 0, 0, 0.75, 1}				***S*** = {0.102, *"Poor"*, 0.686, *"Fair"*, 0.116, *"Average"*, 0.096, *"Good"*}	0.373 **4**
TARGET	W = {0.25, 1, 0.75, 0, 0, 0, 0} D = {0.25, 1, 0.75, 0, 0, 0, 0} R = {0, 0, 0, 0, 0,75, 1, 0.25} (P) = {0, 0, 0, 0.75, 1, 0.25}				***S*** = {0.183, *"Poor"*, 0.195, *"Fair"*, 0.337, *"Average"*, 0.285, *"Good"*}	0.536 **12**
BOARD	W = {0, 0, 0, 0, 0, 0.75, 1} D = {0, 0, 0, 0, 0.75, 1, 0.25} R = {0, 0, 0.5, 1, 0.5, 0, 0} (P) = {0, 0, 0.5, 1, 0.5, 0, 0}				***S*** = {0.444, *"Poor"*, 0.199, *"Fair"*, 0.184, *"Average"*, 0.173, *"Good"*}	0.412 **5**
VISA	W = {0, 0, 0, 0, 0, 0.75, 1} D = {0, 0, 0, 0.75, 1, 0.25, 0} R = {0, 0, 0, 0.75, 1, 0.25, 0} (P) = {0, 0, 0, 0, 0, 0.75, 1}				***S*** = {0.274, *"Poor"*, 0.367, *"Fair"*, 0.184, *"Average"*, 0.175, *"Good"*}	0.426 **7**
KNOWLEDGE	W = {0, 0, 0.5, 1, 0.5, 0, 0} D = {0, 0, 0, 0, 0.75, 1, 0.25} R = {0, 0, 0.5, 1, 0.5, 0, 0} (P) = {0, 0, 0, 0, 0.75, 1, 0.25}				***S*** = {0.165, *"Poor"*, 0.335, *"Fair"*, 0.335, *"Average"*, 0.165, *"Good"*}	0.452 **9**
SHIP	W = {0, 0, 0.5, 1, 0.5, 0, 0} D= {0, 0, 0.5, 1, 0.5, 0, 0} R = {0, 0, 0, 0, 0,75, 1, 0.25} (P) = {0, 0, 0, 0, 0, 0.75, 1}				***S*** = {0.165, *"Poor"*, 0.335, *"Fair"*, 0.335, *"Average"*, 0.165, *"Good"*}	0.452 **9**
ACCESSIBLE	W = {0, 0, 0, 0, 0.75, 1, 0.25} D= {0, 0, 0, 0, 0.75, 1, 0.25} R = {0, 0, 0.5, 1, 0.5, 0, 0} (P) = {0, 0, 0, 0, 0.75, 1, 0.25}				***S*** = {0.686, *"Poor"*, 0.119, *"Fair"*, 0.101, *"Average"*, 0.094, *"Good"*}	0.324 **3**
TERRORIST	W = {0, 0, 0, 0.75, 1, 0.25, 0} D= {0, 0, 0, 0.75, 1, 0.25, 0} R = {0, 0, 0, 0.75, 1, 0.25, 0} (P) = {0, 0, 0, 0.75, 1, 0.25, 0}				***S*** = {0, *"Poor"*, 1, *"Fair"*, 0, *"Average"*, 0, *"Good"*}	0.249 **1**

Step 3 applies the *ER* approach and its attached software *IDS* to calculate risk scores of the 16 Gates in Figure 3.2 and finally the safety level of the top event can be expressed by its risk score shown as follows:

$$S_{top\ event} = \{0.2086, \textit{"Poor"}, 0.5266, \textit{"Fair"}, 0.1756, \textit{"Average"}, 0.0892, \textit{"Good"}\}$$

The above gives an overall picture of the safety estimate of this top event*. The risk score representing the safety level of the top event can be seen as a reference for considering the effectiveness of the *RCOs* discussed later and compared with other hazardous events for making decisions if necessary.

3.4.3 The Adoption of RCMs and Development of RCOs

Soon after the World Trade Centre attacks, attention shifted from aviation to maritime security, especially to *CSC* security as it becomes evident that the vulnerabilities detailed earlier could potentially and positively be targeted by organised terrorist groups. Following the unprecedented maritime security measures generated by *IMO*, it is necessary to develop a strategy to reduce the danger from terrorism attacks on *CSCs*. Four principal elements require consideration: the need to ensure the integrity of containerized cargo, the need to address the security of containerships and ports, the need to track containerships and trains and to restrict the access areas and time of trucks, and the need to verify and authenticate the identity of working staff. In order to develop the strategy, a review has been given to analyse some major anti-terrorism *RCMs* associated with *CSCs*. They include (See Appendix 2 for their security functions):

1) Automatic identification systems (*AIS*) 2) Ship identification number
3) Ship security alert system 4) Security officer
5) Security assessment and plan 6) Security training and drills
7) Security equipment and security guards 8) Record-keeping
9) *IMO ISPS* code voluntary measures 10) Advance notification of arrival of vessel
11) Advance manifest rule of container cargo 12) *CSI*
13) *C-TPAT*

Using the casual chain method, the security measures related to *CSCs* can be adopted as shown in Table 3.8.

Facing different degrees of terror threats, an assessor or a safety designer can select appropriate *RCOs* by adopting different *RCMs*. When the threat of terrorist attacks becomes higher, more and more strict and effective measures require application. Some relatively loose safety measures are considered as the response to the low level threats. Another point needed to be mentioned is that the *RCOs* should be considered to have a

---

* More detailed analysis of the application of the subjective risk analysis method to a case study is described in Section 4.4.1.

Table 3.8. The adoption of *RCMs* against a terrorism attack

	Causes	Incidents	Accidents	Consequences
	1. The failure of container cargo checking. 2. The failure of controlling container access. 3. The failure of the identities of working staff (i.e. seafarers and workers in ports). 4. The cooperation between terrorists and pirates. 5. The failure of surveillance and alarm systems. 6. The hole of security networks.	1. Bombs and hazardous cargoes (controlled by terrorists) packed into a container. 2. Terrorists with the knowledge of vessel design getting on board. 3. Terrorists accessing the vessels or ports under cover of employees' identities. 4. Terrorists accessing a population or business centre in a targeting country under cover of crew' identities. 5. Terrorists hijacking vessels or trains. 6. The deviation from sea routes or access to the ports of vessels controlled by terrorists. 7. The misdirection or access to the stations of trains controlled by terrorists.	1. Using bombs or hazardous cargoes to attack crew, vessels and port facilities. 2. Using the cover of seafarers or staff identities to organise terrorism operations. 3. Using vessels as weapons to attack ports or other ships (i.e. passenger ships). 4. Using vessels to launch an attack. 5. Sinking vessels to disrupt infrastructure. 6. Using the cover of crew identities to operate terrorist attacks in targeting countries. 7. Using trains as weapons to attack train stations or other passenger trains. 8. Using trucks with bombs or hazardous materials sealed in a container to attack a business or population centre.	1. Explosion. 2. Damage of property. 3. Loss of life. 4. Break of chains. 5. Disruption of trade. 6. Impact of economy.
Human managerial solutions	1. A designated person who will pay more attention to the selection of staff, including the consideration of the background of employees or the reputation of the labour agencies. 2. Periodic background checks of the staff. 3. Security awareness education. 4. Security training and drills.	1. The positive identification of all employees, visitors and vendors. 2. Periodic background checks of the staff. 3. Security awareness education. 4. Security training and drills. 5. Designating specific security officers.	1. More effort in searching appropriate staff. 2. The positive identification of all employees, visitors and vendors. 3. Periodic background checks of the staff. 4. Security awareness education. 5. Security training and drills. 6. Designating specific security officers.	1. Security and rescue training and drills.
Engineering equipment solutions	1. Adequate perimeter fencing, lighting and locking, defending and cargo scanning devices. 2. Increased cargo scanning facilities. 3. Emergency substitutes of monitoring devices.	1. Adequate security equipment. 2. *AIS*. 3. Automatic monitoring systems for trains. 4. Ship identification number. 5. Developing and using IT-enable and secure containers.	1. Developing and using IT-enable and secure containers. 2. Increasing the frequency of waterside boat patrols. 3. Security alert systems on ships and trains. 4. *AIS*. 5. Automatic monitoring systems for trains. 6. Ship identification number.	1. Lifesaving and fire extinguishing equipment.
Operational procedure solutions	1. Supervising the transfer of container cargo. 2. Properly marking, weighting, counting, and documenting products. 3. Verifying seals on containers. 4. Detecting and reporting shortages and overages. 5. Proper storage of containers to prevent unauthorized access. 6. Limiting the number of access points to containers. 7. Challenging all unauthorized/unidentified persons. 8. Enforcing the cooperation between those intelligent networks from different countries. 9. Establishing security criteria to identify high-risk containers.	1. Increasing the frequency of physical checks or the use of scanning/detection equipment, mechanical devices. 2. Pre-screening the containers from loading ports. 3. Verifying the inventory of dangerous goods and hazardous substances carried on board, and confirming the hazardous cargoes being properly manifested and stowed. 4. Formulating a special hazardous cargo office in a company for the responsibility of the transportation of hazardous cargoes. 5. Restricting access to some key areas on board. 6. Performing a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines. 7. Carrying out ship and port security assessment. 8. Developing ship and port security plans. 9. 96-hour advance notification of arrival of vessels. 10. Crew visa requirements. 11. 24-hour advance manifest rule of container cargo.	1. Intensified checks of cargoes and seals. 2. Suspension of the loading or unloading of cargoes. 3. Regular checks of key areas. 4. Control of the high risk ships. 5. Regular inspection of surveillance equipment. 6. Restricting the access time and points of container-carrying trucks to a population or business area. 7. Using technological means to track the high-risk containers in the whole flow process. 8. Regular security patrols.	1. Formulating an emergency response authority department and arranging a special emergency telephone number. 2. Fully or partly closing related 'nodes' or 'links' to avoid further terrorist attacks. 3. Evacuating persons. 4. Redesigning the supply chain to keep it productive as soon as possible. 5. Adopting measures to increase managers' confidence of resuming operations

capability to deal with the risk factors in an overall rather than individual perspective. Three *RCOs* are developed according to the requirements of different safety levels and countermeasures as shown in Table 3.9.

Table 3.9. The development of *RCOs* against a terrorism attack

RCOs / *RCMs*	Option 1	Option 2	Option 3
Human managerial measures	1. A designated person in a human resource department who will pay more attention on the selection of staff, including the consideration of the background of employees or the reputation of the labour agencies. 2. Security awareness education. 3. Rescue training and drills.	1. The identification of all employees, visitors and vendors. 2. Security training and drills. 3. Designating specific security officers. 4. Employment periodic background checks.	1. More frequent and detailed checks of people and personnel effects.
Engineering equipment measures	1. Adequate perimeter fencing, lighting and locking, defending and cargo scanning devices. 2. Emergency substitutes of monitoring devices. 3. AIS. 4. Automatic monitoring systems for trains. 5. Ship identification number. 6. Security alert systems on ships and trains. 7. Lifesaving and fire extinguishing equipment.	1. Adequate security equipment. 2. More cargo scanning facilities.	1. Developing and using IT-enable and secure containers 2. Increasing the frequency of waterside boat patrols
Operational procedure measures	1. Supervising the transfer of container cargo. 2. Properly marked, weighed, counted, and documented products 3. Verifying seals on containers. 4. Detecting and reporting shortages and overages. 5. Proper storage of containers to prevent unauthorized access. 6. Verifying the inventory of dangerous goods and hazardous substances carried on board, and properly manifesting and stowing the hazardous cargoes. 7. Cooperation between those intelligent networks from different countries. 8. Formulating a special hazardous cargo office in a company for the responsibility of the transportation of hazardous cargoes. 9. Restricting access to some key areas on board. 10. Carrying out ship and port security assessment. 11. Developing ship and port security plan. 12. Restricting the access time and points of container-carrying trucks to a population or business area. 13. Constructing an emergency response authority department and arranging a special emergency telephone number. 14. Evacuation.	1. Challenging all unauthorized/ unidentified persons. 2. Intensified checks of cargoes and seals. 3. Limiting the number of access points to containers. 4. Establishing security criteria to identify high-risk containers. 5. Pre-screening the containers from loading ports. 6. 96-hour advance notification of arrival of vessels. 7. Crew visa requirements. 8. Regular inspection of key areas. 9. Regular inspection of surveillance equipment. 10. Redesigning the supply chain to keep it productive as soon as possible. 11. Using technological means to track the high-risk containers in the whole flow process. 12. Regular security patrols.	1. Fully or partly closing related 'nodes' or 'links' to avoid further terrorism attacks. 2.24-hour advance manifest rule. 3. Adopting measures to increase managers' confidence of resuming operation. 4. Performing a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines 5. Suspension of the loading or unloading of cargoes 6. Control of the high risk ships

3.4.4 The Cost Analysis of The RCOs Designed

The benefit analysis of a terrorism attack threat is difficult and thus, the economic analysis of the three *RCOs* can concentrate on their cost analysis. The costs incurred for the reduction of the terrorist attacking risk associated with the three above design options are usually affected by many factors. Classical ones include the investment and maintenance costs of the options. Considering dozens of various measures included in each option and the limited experience with so many measures, it may be very difficult, if not impossible, to give precise assessment and calculation of the relative costs. Therefore, as described in the generated framework, the fuzzy set and *ER* approach may be appropriately applied to the cost analysis.

Although fuzzy cost assessment requires less detailed data to a certain degree, compared to precise *CBA*, a certain amount of relative data as references is still necessary to determine the cost levels. Thus, appropriate measures need to be carefully analysed to define the references for the cost levels of the *RCOs*/*RCMs*. Some typical cost analyses of the *RCMs* related to *CSC* security are provided in Appendix 2.

Using the cost analyses of the corresponding *RCMs* and the *ER* approach, the costs of the three *RCOs* can be estimated and calculated as follows:

C_{O1} = {0.2513, *"Very high"*, 0.0902, *"High"*, 0.2640, *"Moderately high"*, 0.1072, *"Average"*, 0.1471, *"Moderately low"*, 0.0329, *"Low"*, 0.1073, *"Very Low"*}
C_{O2} = {0.2843, *"Very high"*, 0.1125, *"High"*, 0.3292, *"Moderately high"*, 0.0842, *"Average"*, 0.0853, *"Moderately low"*, 0.0203, *"Low"*, 0.0842, *"Very Low"*}
C_{O3} = {0.3227, *"Very high"*, 0.1717, *"High"*, 0.2717, *"Moderately high"*, 0.0709, *"Average"*, 0.0746, *"Moderately low"*, 0.0176, *"Low"*, 0.0708, *"Very Low"*}

3.4.5 Ranking the RCOs

In Section 3.3, four different decision making approaches have been introduced and shown their individual advantages and disadvantages. The *CBA* method is straightforward and easily operational, but it simultaneously requires that the costs and benefits of one *RCO* can be precisely estimated. Although the *FCBA* method may not require the precise estimations of costs and benefits, its operation is more complex. The precondition to apply both *CBA* and *FCBA* methods is that the benefits of the corresponding *RCOs* can be effectively estimated, either precisely or subjectively. The techno-economic modelling approach can cope with the limitation of estimating the benefits and help decision makers to select appreciated *RCOs* through considering their costs and the reduction of risks. One shortcoming of this approach, however, is lack of the flexibility to consider the adoption of different *RCOs* when the importance ratio of their costs and reduction of risks changes. The marriage of fuzzy set and *ER* methods can effectively deal with such a problem and therefore, it is desirable to apply it in this case study, where the benefits of the *ROCs* for a terrorism attack are difficult to measure, and the importance ratios of security levels and their corresponding costs are changeable under different situations.

Using the fuzzy sets and *ER* method, the decision making process can be detailed into the following steps:

1) Obtaining the fuzzy safety level (S_{before}) of a *CSC* under a terrorism attack before taking any measure, as demonstrated in Section 3.4.2.

   S_{before} = {0.2086, *"Poor"*, 0.5266, *"Fair"*, 0.1756, *"Average"*, 0.0892, *"Good"*}

2) Redefining the four risk parameters of 12 basic events and calculating their risk scores after adopting each of the three *RCOs* in a similar way to obtaining the ones in Table 3.7.
3) Using the *ER* method to obtain three new safety levels (S_{RCO1}, S_{RCO2}, S_{RCO3}) corresponding to the three *RCOs* as follows:

S_{RCO1} = {0.1073, *"Poor"*, 0.2082, *"Fair"*, 0.2379, *"Average"*, 0. 4576, *"Good"*}
S_{RCO2} = {0.0998, *"Poor"*, 0.1032, *"Fair"*, 0.2684, *"Average"*, 0.5286, *"Good"*}
S_{RCO3} = {0.0628, *"Poor"*, 0.0847, *"Fair"*, 0.3154, *"Average"*, 0.5371, *"Good"*}

4) Calculating the reduction of the risk. The numerical values of the safety expressions are described as [w_p, w_a, w_g, w_e], = [0.079, 0384, 0.695, 1] in Section 3.3.2. The reduction of the risks can be obtained as follows:

$$S_{RCO1} - S_{before} = (0.1073 \times 0.079 + 0.2028 \times 0.384 + 0.2379 \times 0.695 + 0.4576 \times 1) - (0.2086 \times 0.217 + 0.5266 \times 0.294 + 0.1756 \times 0.455 + 0.0892 \times 1) = 0.3401$$

$$S_{RCO2} - S_{before} = (0.0998 \times 0.079 + 0.1032 \times 0.384 + 0.2684 \times 0.695 + 0.5286 \times 1) - (0.2086 \times 0.217 + 0.5266 \times 0.294 + 0.1756 \times 0.455 + 0.0892 \times 1) = 0.3935$$

$$S_{RCO3} - S_{before} = (0.0628 \times 0.079 + 0.0847 \times 0.384 + 0.3154 \times 0.695 + 0.5371 \times 1) - (0.2086 \times 0.217 + 0.5266 \times 0.294 + 0.1756 \times 0.455 + 0.0892 \times 1) = 0.4246$$

Obviously, the minimum crisp risk reduction value can be equal to 0, which means that the corresponding *RCO* cannot improve the safety level of the top event. The maximum crisp risk reduction value can be equal to 0.6308 (0.6308= (0 × 0.079 + 0 × 0.384 + 0 × 0.695 + 1 × 1) - (0.2086 × 0.079 + 0.5266 × 0.384 + 0.1756 × 0.695 + 0.0892 × 1)). This indicates that the corresponding *RCO* improves the safety level of the top event to "Good" with a 100 percent degree. Based on such an interval [0, 0.631], the three crisp values can be reassessed and expressed by risk reduction related linguistic variables.

5) Developing the fuzzy membership functions of the risk reduction expressions in Table 3.10 and fuzzifying the three crisp risk reduction results in Step 4 as follows:

The fuzzy set of the risk reduction of *RCO1* is {0, 0.25, 1, 0.5, 0, 0, 0}
The fuzzy set of the risk reduction of *RCO2* is {0.1, 0.5, 0.75, 0.25, 0, 0, 0}
The fuzzy set of the risk reduction of *RCO3* is {0.15, 0.7, 0.9, 0.3, 0, 0, 0}

Table 3.10. The expressions of risk reduction

Linguistic variables	Categories						
	0	1/6	1/3	1/2	2/3	5/6	1
Very unsatisfied	0	0	0	0	0	0.75	1
Unsatisfied	0	0	0	0	0.75	1	0.25
Moderately unsatisfied	0	0	0	0.75	1	0.25	0
Average	0	0	0.5	1	0.5	0	0
Moderately satisfied	0	0.25	1	0.75	0	0	0
Satisfied	0.25	1	0.75	0	0	0	0
Extremely satisfied	1	0.75	0	0	0	0	0

The risk reduction from *RCO1*, *RCO2* and *RCO3* can be individually mapped onto the risk reduction expressions by using the Best-Fit method:

R_{O1} = {0, *"Very unsatisfied"*, 0, *"Unsatisfied"*, 0, *"Moderately unsatisfied"*, 0, *"Average"*, 1, *"Moderately satisfied"*, 0, *"Satisfied"*, 0, *"Very satisfied"*}
R_{O2} = {0.0828, *"Very unsatisfied"*, 0.0818, *"Unsatisfied"*, 0.0928, *"Moderately unsatisfied"*, 0.1216, *"Average"*, 0.2914, *"Moderately satisfied"*, 0.2238, *"Satisfied"*, 0.1058, *"Very satisfied"*}
R_{O3} = {0.0773, *"Very unsatisfied"*, 0.0765, *"Unsatisfied"*, 0.0857, *"Moderately unsatisfied"*, 0.1122, *"Average"*, 0.2543, *"Moderately satisfied"*, 0.2894, *"Satisfied"*, 0.1046, *"Very satisfied"*}

6) Mapping the risk reduction estimates and the corresponding cost estimates onto a utility space, which is generated in Table 3.11. This is shown as follows:

Table 3.11. The matches between the expressions

Utility expressions	**Risk reduction expressions**	**Cost expressions**
Extremely subsidiary	Very unsatisfied	Very high
Subsidiary	Unsatisfied	High
Moderately subsidiary	Moderately unsatisfied	Moderately high
Average	Average	Average
Moderately preferred	Moderately satisfied	Moderately low
Preferred	Satisfied	Low
Extremely preferred	Extremely satisfied	Very Low

U_{R1} = {0, *"Extremely subsidiary"*, 0, *"Subsidiary"*, 0, *"Moderately subsidiary"*, 0, *"Average"*, 1, *"Moderately preferred"*, 0, *"Preferred"*, 0, *"Extremely preferred"*}
U_{R2} = {0.0828, *"Extremely subsidiary"*, 0.0818, *"Subsidiary"*, 0.0928, *"Moderately subsidiary"*, 0.1216, *"Average"*, 0.2914, *"Moderately preferred"*, 0.2238, *"Preferred"*, 0.1058, *"Extremely preferred"*}
U_{R3} = {0.0773, *"Extremely subsidiary"*, 0.0765, *"Subsidiary"*, 0.0857, *"Moderately subsidiary"*, 0.1122, *"Average"*, 0.2543, *"Moderately preferred"*, 0.2894, *"Preferred"*, 0.1046, *"Extremely preferred"*}
U_{C1} = {0.2513, *"Extremely subsidiary"*, 0.0902, *"Subsidiary"*, 0.2640, *"Moderately subsidiary"*, 0.1072, *"Average"*, 0.1471, *"Moderately preferred"*, 0.0329, *"Preferred"*, 0.1073, *"Extremely preferred"*}
U_{C2} = {0.2843, *"Extremely subsidiary"*, 0.1125, *"Subsidiary"*, 0.3292, *"Moderately subsidiary"*, 0.0842, *"Average"*, 0.0853, *"Moderately preferred"*, 0.0203, *"Preferred"*, 0.0842, *"Extremely preferred"*}
U_{C3} = {0.3227, *"Extremely subsidiary"*, 0.1717, *"Subsidiary"*, 0.2717, *"Moderately subsidiary"*, 0.0709, *"Average"*, 0.0746, *"Moderately preferred"*, 0.0176, *"Preferred"*, 0.0708, *"Extremely preferred"*}

7) Assigning an importance ratio between risk reduction and cost estimations.

8) Synthesising the risk reduction and cost with different importance ratios. For example, when the important ratio between the risk reduction and cost is 2:1, the synthesis U^1_{U1} of the risk reduction estimation U_{R1} and cost estimation U_{C1} of RCO1 is obtained as follows:

U^1_{U1} = {0.0475, *"Extremely subsidiary"*, 0.017, *"Subsidiary"*, 0.0499, *"Moderately subsidiary"*, 0.0202, *"Average"*, 0.8389, *"Moderately preferred"*, 0.0062, *"Preferred"*, 0.0203, *"Extremely preferred"*}

9) Using the categories and memberships values to calculate the numerical utility value of each U^j_{Ui}, where *i* indicates the categories of different importance ratios and *j* (=1, 2, 3) means the categories of the three *RCOs*. The numerical values of the seven utility expressions can be obtained using the method of calculating the numerical values of the four safety expressions and shown as follows:

[0.217, 0.248, 0.294, 0.357, 0.455, 0.635, 1]

For example, the preference degree related to U^1_{U1} can be obtained as follows:

$U^1_{U1} = 0.0475 \times 0.217 + 0.017 \times 0.248 + 0.0499 \times 0.294 + 0.0202 \times 0.357 + 0.8389 \times 0.455 + 0.0062 \times 0.635 + 0.0203 \times 1 = 0.4442$

In a similar way, the numerical utility values of the *RCOs* with different importance ratios can be obtained and shown in Table 3.12.

Table 3.12. The ranking of *RCOs*

Situations / Options	Situation 1 (S1) (Safety: Cost=2:1)	Situation 2 (S2) (Safety: Cost=1:1)	Situation 3 (S3) (Safety: Cost=1:2)
RCO#1	0.4442	0.4238	0.4044
RCO#2	0.4607	0.4190	0.3799
RCO#3	0.4671	0.4166	0.3682
Ranking *RCOs*	*RCO*#3>*RCO*#2>*RCO*#1	*RCO*#1>*RCO*#2>*RCO*#3	*RCO*#1>*RCO*#2>*RCO*#3

10) Producing the ranking of *RCOs*. The result in Table 3.12 shows that when the risk reduction is twice as important as the cost, the strictest option (*RCO*#3) is the best choice; when the importance of risk reduction is reduced (which means that the level of the realistic threat may be decreased), the relatively loose option (*RCO*#1) becomes more preferred. Simultaneously, such a result is also in harmony with the realistic situation in terms of dealing with security problems (i.e. the three security level requirements in the *ISPS* code).

3.5. Conclusion

The safety consciousness in the supply chain industry has been significantly growing over the last several years and becomes one of the most important criteria for supply

chain management decisions. This chapter generated a conceptual risk assessment framework for improving the safety performance of *CSCs* enabling the possibility of assessing the vulnerability of the chains and supporting the safety planning for both mitigating and continuity actions. Such a methodology is designed and generated on the basis of the concept of *FSA* in the shipping industry, but extends the *FSA* framework from a shipping domain to a wider supply chain area closely related to container shipping. To address the special safety requirements and economic considerations, the new framework employs many well established techniques (i.e. *FTA* & *ETA*) in the traditional *FSA* methodology and also develops some novel risk and economic analysis methods as well as decision-making approaches (i.e. subjective safety model and *FCBA*).

In the process of attempting to obtain the reliability of the chains, the conceptual methodology also provides new insights that should be of particular interest to academics and practitioners. Firstly, it is desirable to identify the vulnerability in the chains from two different views of threats and hazards. Traditional single hazard analysis may not be suitable for dealing with complex *CSCs*. Also, those threat-based risks widely exist and attract more attention from the managers of the chains because they are usually beyond the chains' direct management and control. Next, the marriage of fuzzy sets and *ER* to deal with uncertainty resulting from threats can facilitate risk assessment and be tailored to be applied to more management-related industries, where risks usually arise from threats rather than hazards. Furthermore, use of the framework enables the assessment of the risks from both the engineering-based and managerial viewpoints. It can thus be seen as a flexible unifying tool, which makes it possible to benefit maximally from the strengths of the individual risk assessment and safety management.

Although the methodology does provide a comprehensive view of safety assessment for *CSCs*, it by no means is meant to be perfect. One significant characteristic of the chains is a close collaboration between the entities involved. While such a close cooperation (interactive relationship) ensures effective cargo and information flows, it can also redound to risk free flows. It may be difficult to use traditional risk analysis methods with a hierarchical structure such as *FTA* to deal with the risks with an interactive nature. Therefore, new models need to be constructed.

Chapter 4 – An Advanced Fuzzy Based Risk Assessment Technique

SUMMARY

After the 9/11 terrorism attack, the lock-out of the American West Ports in 2002 and the breakout of SARS disease in 2003 have further focused the minds of both the public and industrialists to take effective and timely measures to assess and control the risks related to CSCs. Achieving such a functionality requires enabling the possibility of combining the objective and subjective risk estimations in view of the challenges and uncertainties posed by the unavailability and incompleteness of historical failure data. However, due to the complexity of the risks in the chains, either conventional QRA methods or the subjective safety assessment method introduced in Chapter 3 may not be capable of providing sufficient safety management information. This chapter, as the extension of Chapter 3, combines the FST and the ER approach and presents an advanced continuous fuzzy set method to deal with the risk assessment based on both objective failure data and subjective expert judgements, which are more functional in the safety management of the chains.

4.1. Introduction

An important consideration of the effectiveness of the subjective risk analysis approach discussed previously is related to its capability of combining objective hazard-based safety evaluations. The risk assessment of *CSC* systems is possibly highly dependent on both hazard-based and threat-based risk implications simultaneously in a particular situation. Thus, it will be desirable that the subjective approach can be used to carry out a unification of the two different risk implications in order to avoid loss of useful information. However, as the hazard-based risks may be described using objective precise quantities and the threat-based risks may be described using subjective fuzzy sets, it is not convenient to directly implement such a synthesis using either a normal mathematical logical operation or the *ER* approach. It is therefore necessary to define a utility space to evaluate objective and subjective safety expressions on the same scale. This chapter uses the concept of continuous fuzzy sets to fuzzify the numerical hazard-based risk attributes, transfer the risk estimations into a form, which can be mapped onto the four safety expressions defined in Chapter 3 and then realise the synthesis of the hazard-based and threat-based risks.

4.2 The Review of The Discrete Risk Analysis Approach

A subjective safety modelling method is proposed in Chapter 3 to deal with threats and

to provide a basis for assigning priorities for corrective actions. For the purpose of comparison and combination, the framework of this method is reviewed and expressed using the six interlocking steps in the following context:

Step 1. Identify the risk parameters for measuring threat-based risks as "*Will (W)*", "*Damage capability (D)*", "*Recall difficulty (R)*" and "*Damage probability (P)*".
Step 2. Define discrete fuzzy set membership functions for the risk parameters identified in Step 1.
Step 3. Calculate fuzzy risk scores using the fuzzy sets of the four safety parameters defined in Step 2.
Step 4. Transform the risk scores obtained in Step 3 to the defined fuzzy safety expressions *(i.e. "Poor", "Fair", "Average" and "Good")* to obtain safety estimations.
Step 5. Synthesise the safety estimations in Step 4 from different assessors or components using hierarchical *ER*.
Step 6. Rank the synthesised safety evaluations obtained in Step 5.

4.3. Combination of the Hazard-Based and Threat-Based Risk Estimations

In comparison to the difficulty of precisely defuzzifying a fuzzy set to a crisp number, it is reasonably easy to fuzzify a numerical objective hazard-based risk parameter to appropriate linguistic terms described by fuzzy membership sets using some pre-defined categories. Taking into account this fact, the utility scale in this study is selected as the four fuzzy safety expressions in Table 3.5. Note that the categories in Tables 4.1 and 4.2 provide engineers with measures with which a linguistic variable can be modelled. A linguistic variable may be modelled in terms of membership values with respect to more than one probability related category. For example, in Table 4.1, "Extremely Remote" is modelled by membership values 0.5 and 1 with respect to the two categories, which are respectively related to $1/6$ and 0.

Risk is traditionally characterised by the occurrence of accidental events and their undesired effects. In traditional engineering risk assessment approaches, risk is often described in terms of the frequency of consequences, such that

$$Risk = Failure\ frequency \times Consequence\ severity$$

However, different from the quantitative numerical means in *QRA* by which the frequency and severity are determined, here they are expressed using fuzzy membership sets and calculated using fuzzy algorithms.

Table 4.1. An example of fuzzy frequency index of containership accidents

Frequency	Definition	Per ship - year
Extremely Frequent	**-Likely to occur once per year for a containership**	**0.1< F**
Frequent	**-Likely to occur once in the lifetime of a containership**	**0.01< $F \leq$ 0.1**
Likely	**-Likely to occur 10 times per year for all cellular containerships**	**0.001< $F \leq$ 0.01**
Occasional	**-Likely to occur once per year for all cellular containerships**	**0.0001< $F \leq$ 0.001**
Remote	**-Likely to occur once times in 10 years for all cellular containerships**	**0.00001< $F \leq$ 0.0001**
Extremely remote	**-Likely to occur once in the lifetime of all cellular containerships**	**$F \leq$ 0.00001**

Membership sets							
				Category			
Extremely Frequent	0	1/6	1/3	1/2	2/3	5/6	1
Frequent	**0**	**0**	**0**	**0**	**0**	**0**	**1**
Likely	**0**	**0**	**0**	**0**	**0.5**	**1**	**0**
Occasional	**0**	**0**	**0**	**0.5**	**1**	**0**	**0**
Remote	**0**	**0**	**1**	**0.5**	**0**	**0**	**0**
Extremely remote	**0**	**1**	**0.5**	**0**	**0**	**0**	**0**
Extremely Frequent	**1**	**0.5**	**0**	**0**	**0**	**0**	**0**

Table 4.2. An example of fuzzy severity index of containership accidents

Severity	Definition	Number of fatalities
Catastrophic	**-The total loss of a containership -Many fatalities or the severe pollution to the environment**	**1< S**
Critical	**-Major casualties including the severe damage to the containership -Severe injuries or the significant pollution to the environment**	**0.1< $S \leq$ 1**
Severe	**-Failure that requires professional repair -Injuries requiring first aid or the pollution to the environment in a small scope**	**0.01< $S \leq$ 0.1**
Trivial	**-Minor failure that can be easily repaired -Injuries not requiring first aid or the slight pollution to the environment**	**0.001< $S \leq$ 0.01**
Marginal	**-Failure that can be readily compensated by the crew of the containership -Injuries not requiring first aid or the slight pollution to the environment**	**0.0001< $S \leq$ 0.001**
Negligible	**-The cosmetic damage to the containership -No significant harm to people, property or the environment**	**$S \leq$ 0.0001**

Membership sets							
				Category			
Catastrophic	0	1/6	1/3	1/2	2/3	5/6	1
Critical	**0**	**0**	**0**	**0**	**0**	**0**	**1**
Severe	**0**	**0**	**0**	**0**	**0.5**	**1**	**0**
Trivial	**0**	**0**	**0**	**0.5**	**1**	**0**	**0**
Marginal	**0**	**0**	**1**	**0.5**	**0**	**0**	**0**
Negligible	**0**	**1**	**0.5**	**0**	**0**	**0**	**0**
Catastrophic	**1**	**0.5**	**0**	**0**	**0**	**0**	**0**

In the fuzzy theory, given any set, it is possible to perform a similar fuzzification. The Extension Principle (*EP*) in the theory identifies a natural way to extend maps on classical sets to maps on their fuzzy extensions. It can be described in the following:

EP: Given a map, $f(x_1, x_2, ..., x_n) = y$, then, the natural fuzzy extension, $\tilde{f}$, is given by:

$$u_{\tilde{f}(a_1,a_2,...,a_n)}(y) = \sup_{f(x_1,x_2,...,x_n)=y} \min[u_{a_1}(x_1), u_{a_2}(x_2), ..., u_{a_n}(x_n)] \quad (4.1)$$

which means that the degree of y being a fuzzy set under an extended function, $\tilde{f}(a_1, a_2, ..., a_n)$, is the maximum of the minimum of the membership values, $u_{a_i}(x_i)$, $i = (1,2,...n)$, of elements, x_i, $i = (1,2,...n)$, mapped to the original fuzzy set functions, a_i, $i = (1,2,...n)$, by ordering all elements, x_i, $i = (1,2,...n)$ to follow the function, $f(x_1, x_2, ..., x_n) = y$.

In the context of fuzzy risk assessment, the *EP* may be used to define fuzzy counterparts of standard arithmetic operations. If the standard arithmetic operators are considered as maps from $F \times S \to R$, then the straightforward application of the principle yields,

$$u_{a \otimes b}(R) = \sup_{F \times S = R} \min(u_a(F), u_b(S)) \quad (4.2)$$

where a and b separately represent the fuzzy functions of two risk parameters, frequency and severity; F and S individually mean the categorised probabilities of the two risk parameters in membership sets; and R indicates the categorised probabilities of risk itself in the sets.

Consequently, the risks can be easily expressed using a fuzzy set. For example, if one particular kind of hazard related to containerships occurs 0.01 times per ship – year and it will lead to the loss of 1 life, the risk is then calculated as follows:

Risk = "*Likely*" × "*Critical*"

$$R = F \times S =$$

$$\left[\left(0, \tfrac{1}{6}, \tfrac{1}{3}, \tfrac{1}{2}, \tfrac{2}{3}, \tfrac{5}{6}, 1\right) \times \left(0, \tfrac{1}{6}, \tfrac{1}{3}, \tfrac{1}{2}, \tfrac{2}{3}, \tfrac{5}{6}, 1\right)\right]$$

=

$$u_{Likely\ Critical}(R) = \sup_{F \times S = R} \min[u_{Likelly}(F), u_{Critical}(S)]$$

$$= \sup \min[(0,0,0,0.5,1,0,0), (0,0,0,0,0.5,1,0)]$$

$$= \begin{bmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1/36 & 1/18 & 1/12 & 1/9 & 5/36 & 1/6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1/18 & 1/9 & 1/6 & 2/9 & 5/18 & 1/3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1/12 & 1/6 & 1/4 & 1/3 & 5/12 & 1/2 \\ 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1/9 & 2/9 & 1/3 & 4/9 & 5/9 & 2/3 \\ 0 & 0 & 0 & 0 & 0.5 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 5/36 & 5/18 & 5/12 & 5/9 & 25/36 & 5/6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1/6 & 1/3 & 1/2 & 2/3 & 5/6 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1/36 & 1/18 & 1/12 & 1/9 & 5/36 & 1/6 & 2/9 & 1/4 & 5/18 & 1/3 & 5/12 & 4/9 & 1/2 & 5/9 & 2/3 & 25/36 & 5/6 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0.5 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

In the first matrix above, the elements of the odd rows represent "R", which can be calculated using "$F \times S$" (for example, the fifth element '$1/3$' of the seventh row is obtained using the fourth element '$1/2$' in F to multiply the fifth one '$2/3$' in S). The elements of the even rows indicate the membership values of "R", $\min[u_{Likelly}(F), u_{Critical}(S)]$ (for example, the fifth element '0.5' of the eighth row is obtained by comparing the fourth element '0.5' in $u_{Likelly}(F)$ and the fifth one '0.5' in $u_{Critical}(S)$). In the second matrix, the first row shows all possible values of "R" obtained from the odd rows in the first matrix and the second row gives their corresponding membership values, $u_{Likely \otimes Critical}(R)$, which can be computed using $\sup_{F \times S = R} \min[u_{Likelly}(F), u_{Critical}(S)]$. For example,

$$u_{Likely \otimes Critical}(1/3) = \sup_{F \times S = R} \{\min[u_{Likelly}(1/3), u_{Critical}(1)],$$

$$\min[u_{Likelly}(1/2), u_{Critical}(2/3)], \min[u_{Likelly}(2/3), u_{Critical}(1/2)],$$

$$\min[u_{Likelly}(1), u_{Critical}(1/3)]\} = \sup_{F \times S = R} [\min(0,0), \min(0.5,0.5), \min(1,0),$$

$$\min(0,0)] = \sup_{F \times S = R} (0, 0.5, 0, 0) = 0.5.$$

Like μ_S obtained from Equation (3.5), $u_{a\otimes b}(R)$ acquired only represents a relative safety level and requires to be mapped onto the four linguistic safety expressions in Table 3.5. Due to the different probability categories between the fuzzy sets representing $u_{Likely\otimes Critical}(R)$ and the safety expressions, the Best-fit method may not be directly applied to deal with the mapping problem. Therefore, a transferring tool for extending the probability categories of the fuzzy sets of the safety expressions is needed. Because the belief degrees to the safety expressions have a characteristic of classical linear distribution, the extension is straightforward. For example, the fuzzy set of one of the safety expressions, "*Poor*" from Table 3.5 can be extended as,

$$\begin{bmatrix} 0 & 1/36 & 1/18 & 1/12 & 1/9 & 5/36 & 1/6 & 2/9 & 1/4 & 5/18 & 1/3 & 5/12 & 4/9 & 1/2 & 5/9 & 2/3 & 25/36 & 5/6 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.75 & 1 \end{bmatrix}$$

Furthermore, the objective numerical risks can be expressed by the subjective safety expressions using Equations (3.6) and (3.7). Using the *ER* approach, the combination of objective hazard-based and subjective threat-based safety evaluations can be implemented. It is noteworthy that the set represented by the letter "*k*" in Equation (3.6) should be equal to [1, 2, …, 19] rather than [1, 2, …, 7] here.

Despite functioning on the synthesis, such an approach still reveals certain application problems. The principal limitations include that the complex fuzzy arithmetic operations are not friendly enough to mathematically unsophisticated users; that the accuracy of extending the fuzzy sets of the four safety expressions may be arguable and that the non-linear membership value distribution of the fuzzy risk sets acquired (i.e. the zero membership value corresponding to the risk probability category denoted by '$1/2$' in the second matrix on Page 85) is difficult to explain and justify. A novel combining tool is thus generated using continuous fuzzy sets. Note that the term "continuous" can be graphically explained. Considering the fact that triangular and trapezoidal membership functions have been commonly used to describe risks in safety assessment (Wang, 1997b), the membership functions represented by the discrete membership sets in Tables 4.1 and 4.2 can be approximately graphically described using continuous fuzzy sets in Figure 4.1. In a similar way, the membership functions represented by the discrete membership sets in Table 3.5 can also be approximately described as $\tilde{S}a_i$ ($i = 1, 2, 3,$ or 4) in Figure 4.2. Consequently, the tool can be presented as follows:

Let $\tilde{F}_i$ ($i = 1, 2, \ldots$ or 6) represent the continuous fuzzy sets of the frequency linguistics terms and $\tilde{S}_j$ ($j = 1, 2, \ldots$ or 6) be the continuous fuzzy sets of the severity linguistics terms. Given the characteristics of their triangular membership functions, $\tilde{F}_i$ and $\tilde{S}_j$ can be assigned triangular fuzzy numbers, $\overline{F}_i$ and $\overline{S}_j$.

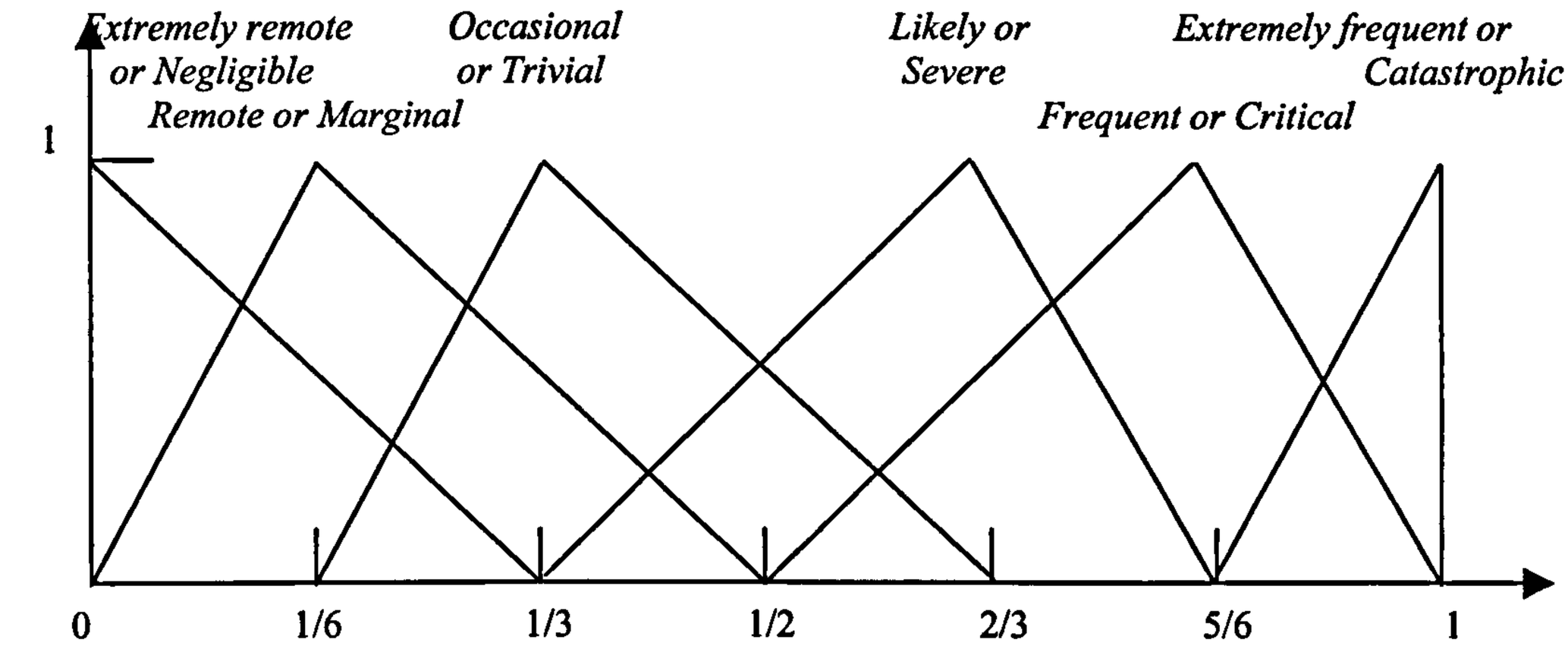


Figure 4.1. Graphical explanations of the fuzzy frequency and severity linguistics terms

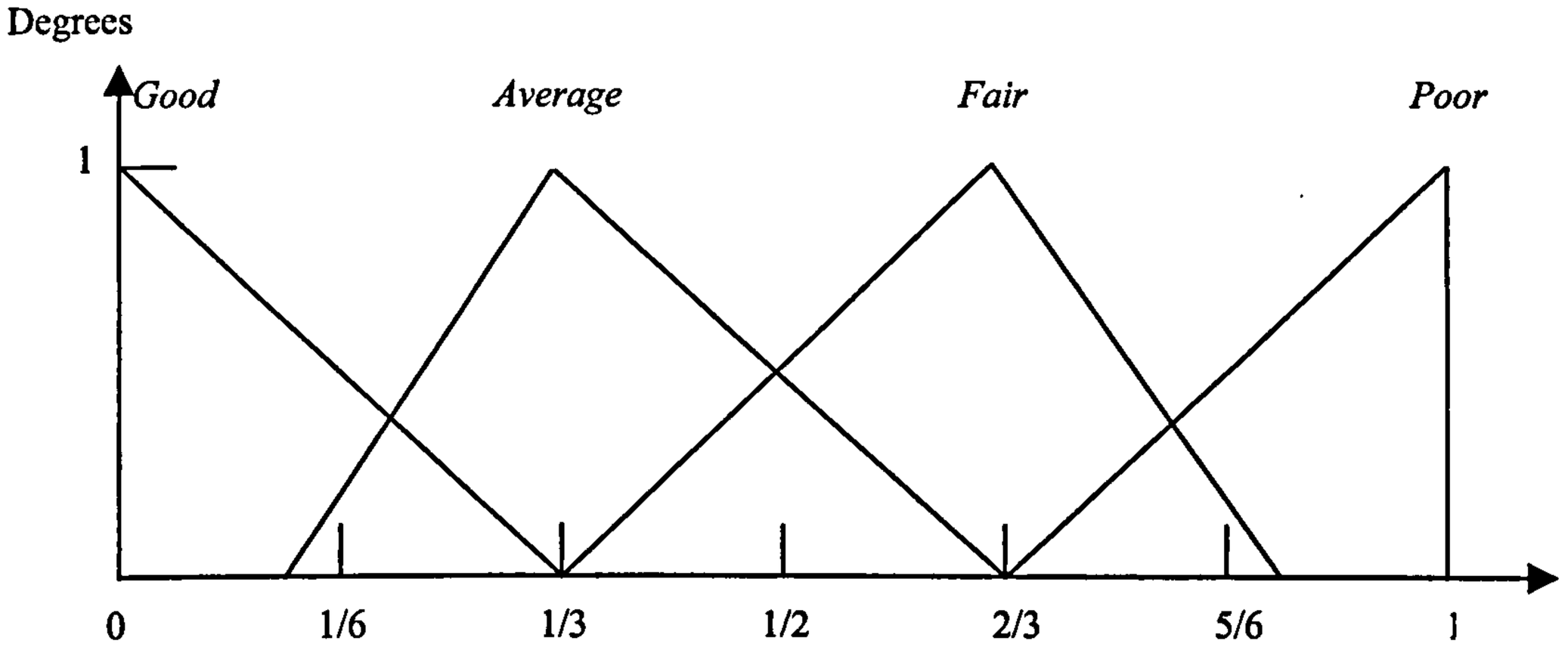


Figure 4.2. Graphical explanations of the safety expressions

Let $\overline{F}_i = (f_{i1} / f_{i2} / f_{i3})$ and $\overline{S}_j = (s_{j1} / s_{j2} / s_{j3})$, then,

$$\overline{F}_i[0] = [f_{i1}, f_{i3}],\ \overline{F}_i[1] = [f_{i2}]$$
$$\overline{S}_j[0] = [s_{j1}, s_{j3}],\ \overline{S}_j[1] = [s_{j2}] \qquad (4.3)$$

Following the solution of fuzzy *EP* equation in Equation (4.2), the product of $\overline{F}_i$ and $\overline{S}_j$, $\overline{R}_{ij}$, representing the triangular fuzzy risk numbers can be obtained as follows:

$$\overline{R}_{ij} \cong [(f_{i1} \times s_{j1}) / (f_{i2} \times s_{j2}) / (f_{i3} \times s_{j3})] \qquad (4.4)$$

where i and $j = (1, 2, \ldots \text{ or } 6)$.

Obviously, the Best-fit method may not effectively map continuous fuzzy sets onto the four safety expressions and thus, a new approach is employed. It is related to the

distance measurement between continuous fuzzy sets (a fuzzy Best-fit method). The distance measurement between two continuous fuzzy sets is developed on the basis of the Best-fit method and thus they have many common characteristics. However, the major difference exists and lies on the distances obtained using two distinctive methods. The distances obtained using Equation (3.6) depend on the degrees (real numbers) distributed to the discrete probability categories, while the new fuzzy Best-fit method aims at investigating the distance between two continuous fuzzy sets (fuzzy numbers).

Given $\tilde{R}$ and $\tilde{S}a_i$ sets with their α-cut representations, $\tilde{R}[\alpha]=[R_1(\alpha),R_2(\alpha)]$ and $\tilde{S}a_i[\alpha]=[Sa_{i1}(\alpha),Sa_{i2}(\alpha)]$, $0 \le \alpha \le 1$. Define $K(\alpha)=\left|R_1(\alpha)-Sa_{i1}(\alpha)\right|$ and $L(\alpha)=\left|R_2(\alpha)-Sa_{i2}(\alpha)\right|$. Then (Buckley and Eslami, 2002),

$$d(\tilde{R},\tilde{S}a_i)=\max\{\max[K(\alpha),L(\alpha)]\,|\,0 \leqslant \alpha \leqslant 1\} \tag{4.5}$$

Since $K(\alpha)$ and $L(\alpha)$ are continuous, the term "max" instead of "*sup*" is used.

Having analysed the Best-fit method, the other steps of the new approach can be carried out in a similar way (i.e. after $d(\tilde{R},\tilde{S}a_i)$ is calculated, Equation (3.7) can be used to calculate α_{ij}). However, it is particularly noteworthy that the four safety expressions obtained and used in linguistically expressing relative safety scores of threat-based risks may not be well suited to the hazard-based risks without appropriately defining specific situations of the distance between two fuzzy sets. For example, from a realistic viewpoint, if the frequency of a hazard is "*Extremely Remote*", represented by $\overline{F}_{ExtremelyRemote}=(0/0/\frac{1}{3})$, and its consequence is "*Negligible*", expressed by $\overline{S}_{Negligible}=(0/0/\frac{1}{3})$, then the risk ought to be "*Good*" with one hundred percent certainty, symbolised by $\overline{R}_{Good}=(0/0/\frac{1}{3})$. However, using the fuzzy *EP* method the risk with the fuzzy membership function can be calculated as $\overline{R}=\overline{F}_{ExtremelyRemote}\otimes\overline{S}_{Negligible}=(0/0/\frac{1}{9})$, which means the risk acquired has a better safety level than the one expressed by "*Good*" in terms of fuzzy safety numbers. Under this circumstance, still using the fuzzy Best-fit method will easily lead to conflict in calculation (i.e. the risk expressed by $\overline{R}=\overline{F}_{ExtremelyRemote}\otimes\overline{S}_{Severe}=(0,0,\frac{5}{18})$ will have a higher degree to the "*Good*" linguistic safety term than that represented by $\overline{R}=\overline{F}_{ExtremelyRemote}\otimes\overline{S}_{Negligible}=(0/0/\frac{1}{9})$, although it is not a realistic case). Therefore, the definition of fuzzy orderings is introduced to avoid such conflict and justify the use of the four safety expressions as the common space of combining hazard-based and threat-based risks.

Definition: *Fuzzy orderings*

On real numbers, $a \preccurlyeq b$ if and only if $a = \min(a,b)$. Following this observation, the *EP* in Equation (4.1) may be used to induce a natural partial order, $\subseteq$, on the fuzzy numbers as follows (Halliwell and Shen, 2002):

$$\begin{aligned} a \subseteq b &\Leftrightarrow a \doteq \tilde{\min}(a,b) \\ &\Leftrightarrow u_a(z) = \sup_{\min(x,y)=z} \min(u_a(x), u_b(y)) \end{aligned} \tag{4.6}$$

Another partial order on the fuzzy sets can be generated by the fuzzy subset relation, i.e.

$$a \subseteq b \Leftrightarrow u_a(x) \preccurlyeq u_b(x) \tag{4.7}$$

Applying such a definition to the context of mapping the hazard-based safety score to the four pre-defined safety expressions, $\tilde{S}a_i$, the following can be reasonably given:

- If and only if $\tilde{R} \subseteq \tilde{S}a_i$ (i =1, 2, 3 or 4), then $d(\tilde{R}, \tilde{S}a_i) = 0$, which means the safety score represented by $\tilde{R}$ belongs to the safety expression expressed by $\tilde{S}a_i$ with one hundred percent degree and belongs to the others with zero degrees.
- If, $\tilde{R} \not\subset \tilde{S}a_i$ (i =1, 2, 3 or 4), then four $d(\tilde{R}, \tilde{S}a_i)$ require to be calculated and the degrees to which the risk belongs to the four safety expressions can be obtained using the previous discussion.

Using such a method, the objective hazard-based risks can be successfully mapped onto the four safety expressions and further synthesised with the subjective threat-based risks with the assistance of the *ER* approach.

4.4. Case Study

4.4.1 A Risk Analysis of Terrorists Attacking Ports

The American West Coast Ports 11-day lockout in October 2002 has caused a growing concern on how serious the impacts of a major sophisticated attack related to container ports can be. Such a concern has further been highlighted by progressive terrorism groups' activities. Therefore, in this section, risk analysis is carried out to assess the safety level of ports in *CSCs* and identify the major factors causing the risk on a prioritised list.

As described previously, terrorists attacking ports would most likely occur through two ways: to attack the channel/waterway or bomb the quayside infrastructures/facilities of the terminals. Using the *FTA* method, a fault tree related to a terrorism threat in ports can be constructed in Figure 4.3.

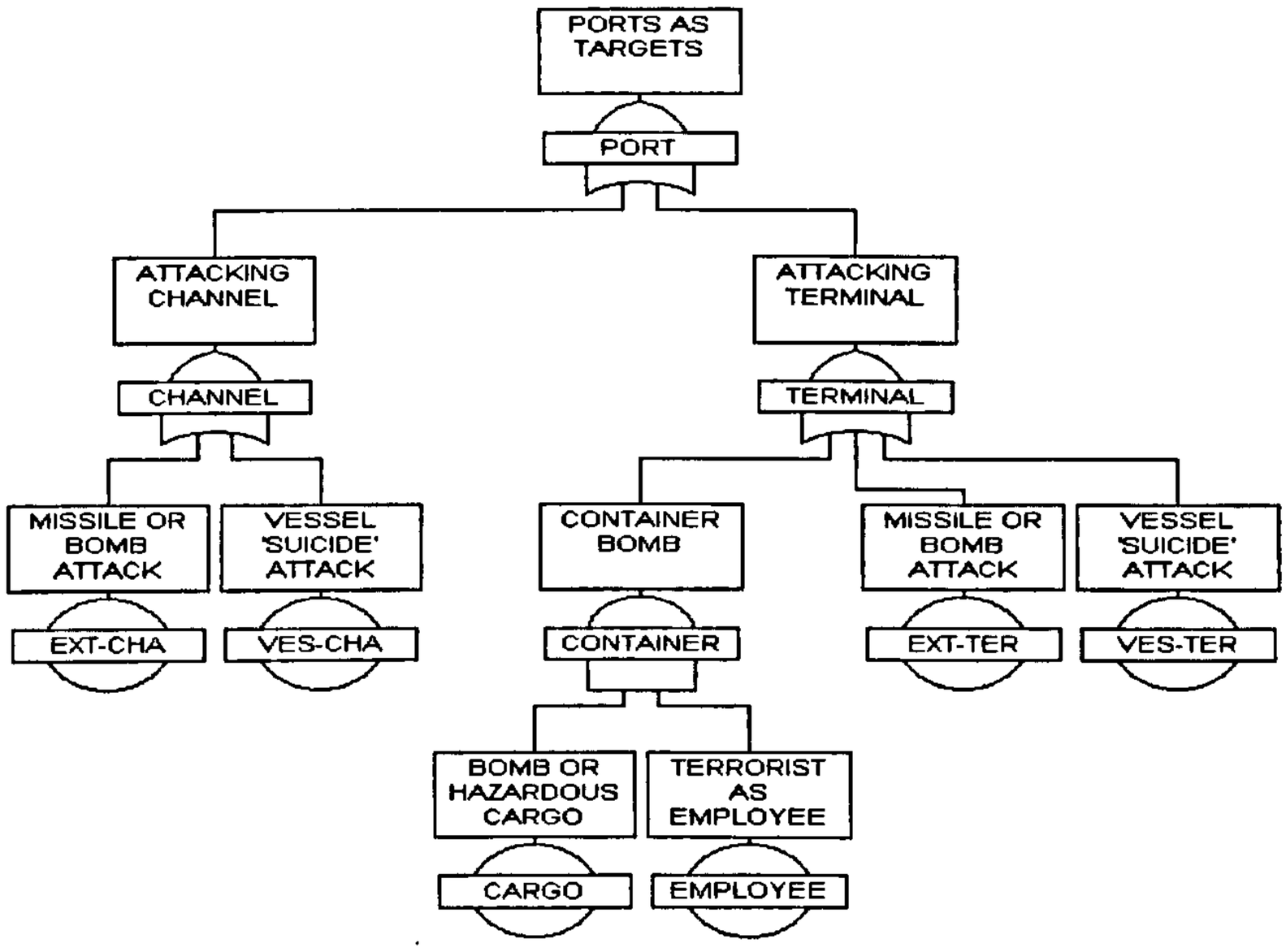


Figure 4.3. A fault tree of terrorists attacking ports

Following the fault tree, the basic events can be ranked in terms of their risk levels using the fuzzy set approach described. The risk level of the top event can be calculated using the *ER* approach. The estimation and calculation of the risk levels can be conducted as follows:

Step 1 assigns the relative weights of the events in Figure 4.3 using the rule in Section 3.2.3, where the top event is assigned value 1 as its weight. The results of the assignments are shown in Table 4.3.

Table 4.3. The weight assignments of all events

Events	Weights	Events	Weights
PORT	1	CONTAINER	1
CHANNEL	1	EXT-TER	1
TERMINAL	1	VES-TER	1
EXT-CHA	1	CARGO	0.5
VES-CHA	1	EMPLOYEE	0.5

Step 2 calculates the safety scores of the basic events on the basis of the fuzzy estimations of the four parameters from Tables 3.1-3.4. The safety scores are calculated by using the fuzzy operations of the formula '$\mu_S = \mu_{(R \times D) \bullet (P \times W)}$' and the Best-Fit method in Section 3.3.2. The ranking of the basic events can then be obtained using the method of studying the fuzzy membership values and categories. For example, the subjective risk parameters of the basic event "EXT-CHA" are initially assessed as moderate weak "*Will*", average "*Damage capability*", average "Recall difficulty" and reasonably likely "Damage probability", respectively. Consequently, the fuzzy estimations of the four parameters can be obtained as using Equation (3.3):

$\mu_W = (0, 0.25, 1, 0.75, 0, 0, 0)$

$\mu_D = (0, 0, 0.5, 1, 0.5, 0, 0)$

$\mu_R = (0, 0, 0.5, 1, 0.5, 0, 0)$

$\mu_P = (0, 0, 0, 0.75, 1, 0.25, 0)$

Using Equations (3.2) – (3.5), μ_S can be calculated as follows:

$$\mu_{R \times D} = (\mu^{ij}{}_{R \times D})_{7 \times 7}$$

$$= (0, 0, 0.5, 1, 0.5, 0, 0) \times (0, 0, 0.5, 1, 0.5, 0, 0)$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 1 & 0.5 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0.5 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mu_{P \times W} = (\mu^{ij}{}_{P \times W})_{7 \times 7}$$

$$= (0, 0, 0, 0.75, 1, 0.25, 0) \times (0, 0.25, 1, 0.75, 0, 0, 0)$$

$$= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.25 & 0.75 & 0.75 & 0 & 0 & 0 \\ 0 & 0.25 & 1 & 0.75 & 0 & 0 & 0 \\ 0 & 0.25 & 0.25 & 0.25 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\mu_S = \mu_{(R \times D)} \circ (P \times W) = (\mu^j{}_S)_{1 \times 7}$$

$$= (0, 0.25, 0.75, 0.75, 0, 0, 0)$$

Using Equations (3.6) and (3.7), the safety score of the basic event "EXT-CHA" can be obtained as follows:

$$d_1(S, Poor) = \left[\sum_{k=1}^{7} (\mu_S^k - \mu_{Poor}^k)^2\right]^{1/2} = 1.658$$

$$d_2(S, Fair) = \left[\sum_{k=1}^{7} (\mu_S^k - \mu_{Fair}^k)^2\right]^{1/2} = 1.299$$

$$d_3(S, Average) = \left[\sum_{k=1}^{7} (\mu_S^k - \mu_{Average}^k)^2\right]^{1/2} = 0.25$$

$$d_4(S, Good) = \left[\sum_{k=1}^{7} (\mu_S^k - \mu_{Good}^k)^2\right]^{1/2} = 1.541$$

$$S_{EXT\text{-}CHA} = \{0.1, \textit{“Poor”}, 0.128, \textit{“Fair”}, 0.664, \textit{“Average”}, 0.108, \textit{“Good”}\}$$

Using Equation (3.9), a numerical risk degree based on the safety score can be calculated as:

$$P_{S_{EXT-CHA}} = 0.1 \times 0.079 + 0.128 \times 0.384 + 0.644 \times 0.695 + 0.108 \times 1 = 0.613$$

The results of the calculations associated with other basic events are shown in Table 4.4.

Table 4.4. The risk estimations of all basic events

Basic events	Parameters				Safety scores	Risk rank
	Will (W)	Damage capability (D)	Recall difficulty (R)	Damage probability (P)		
EXT-CHA	W = {0, 0.25, 1, 0.75, 0, 0, 0} R = {0, 0, 0.5, 1, 0.5, 0, 0}		D = {0, 0, 0.5, 1, 0.5, 0, 0} P = {0, 0, 0, 0.75, 1, 0.25, 0}		***S*** = {0.1, *“Poor”*, 0.128, *“Fair”*, 0.664, *“Average”*, 0.108, *“Good”*}	0.613 **6**
VES-CHA	W = {0, 0, 0, 0, 0.75, 1, 0.25} R = {0, 0, 0, 0, 0,75, 1, 0.25}		D = {0, 0, 0, 0, 0, 0.75, 1} P = {0, 0, 0, 0.75, 1, 0.25, 0}		***S*** = {0.021, *“Poor”*, 0.934, *“Fair”*, 0.027, *“Average”*, 0.018, *“Good”*}	0.31 **1**
CARGO	W = {0, 0, 0, 0, 0, 0.75, 1} R = {0, 0, 0.5, 1, 0.5, 0, 0}		D = {0, 0, 0.5, 1, 0.5, 0, 0} } P = {0, 0, 0.5, 1, 0.5, 0, 0}		***S*** = {0.444, *“Poor”*, 0.199, *“Fair”*, 0.184, *“Average”*, 0.173, *“Good”*}	0.4115 **3**
EMPLOYEE	W = {0, 0, 0.5, 1, 0.5, 0, 0} R = {0, 0.25, 1, 0.75, 0, 0, 0}		D = {0, 0.25, 1, 0.75, 0, 0, 0} P = {0, 0, 0, 0.75, 1, 0.25}		***S*** = {0.139, *“Poor”*, 0.361, *“Fair”*, 0.361, *“Average”*, 0.139, *“Good”*}	0.44 **4**
EXT-TER	W = {0, 0, 0, 0.75, 1, 0.25, 0} R = {0, 0, 0.5, 1, 0.5, 0, 0}		D = {0.25, 1, 0.75, 0, 0, 0, 0} P = {0, 0, 0, 0.75, 1, 0.25, 0}		***S*** = {0.139, *“Poor”*, 0.361, *“Fair”*, 0.361, *“Average”*, 0.139, *“Good”*}	0.44 **4**
VES-TER	W = {0, 0, 0, 0., 0.75, 1, 0.25} R = {0, 0, 0.5, 1, 05, 0, 0}		D = {0, 0, 0, 0, 0.75, 1, 0.25} P = {0, 0, 0, 0, 0.75, 1, 0.25}		***S*** = {0.686, *“Poor”*, 0.119, *“Fair”*, 0.101, *“Average”*, 0.094, *“Good”*}	0.324 **2**

Step 3 applies the *ER* approach and its attached software *IDS* (Yang and Xu, 2000) to calculate the safety level of the top event which can be expressed by its safety score shown in Figure 4.4:

$$S_{Terrorism} = \{0.276, \textit{“Poor”}, 0.461, \textit{“Fair”}, 0.17, \textit{“Average”}, 0.093, \textit{“Good”}\}$$

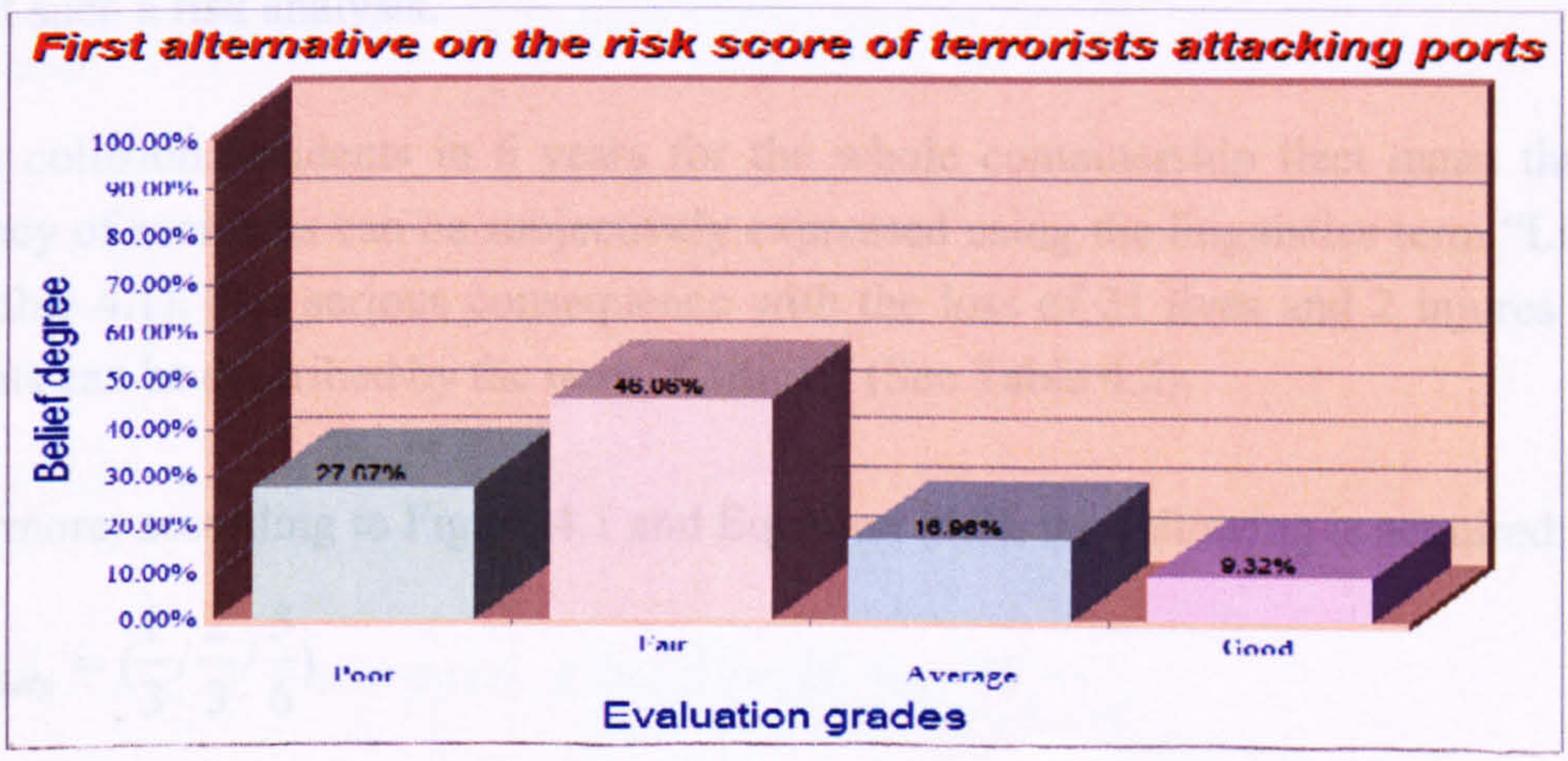


Figure 4.4. The safety level expressed by safety scores

From the above results, it is obvious that the six basic events (i.e. EXT-CHA and VES-CHA) have been assessed as '*Good*' to a quite small extent. For example, the event EXT-CHA has been assessed as '*Good*' with a belief of 10.8 percent; the event VES-CHA has been evaluated to a significantly smaller extent as '*Good*' with 1.8 percent. Since the safety of the top event is determined by the safety of each basic event, the top event safety should be evaluated as '*Good*' to a small extent. This is in harmony with the results obtained above as the safety of the top event has been assessed as '*Good*' to the extent of 9.3 percent.

The above gives an overall picture of the safety estimate of this top event. The safety score representing the safety level of the top event can be seen as a reference for considering the effectiveness of *RCOs* and the comparison with the other hazard-based risk analysis in Section 4.4.2.

4.4.2 A Risk Analysis of Serious Container Ship Collision

The risk related to ship collision has been actively investigated for a long time. However, with the extension of world merchant fleets, the associated hazards still need to be carefully investigated to improve human safety, shipping economy and ocean environment. The problem is particularly prominent in the context of containerships considering their significant contributions to the international trade. A research project carried out by the UK P&I Club (1999) shows that for the 10-year period from 1989 to 1999 incidents involving containership collision accounted for up to 7% of the total containership incidents. The situation is more awful and worrisome given the statistics provided by the *IMO* (1999-2005) that in the period of 1998-2003, 24 serious containership collision accidents with the loss of 21 lives accounted for 25.3% of the total serious containership accidents. Given this fact and considering the possibility of comparing or combining with other threat-based risk evaluations, it is meaningful to conduct such a risk analysis.

The 24 collision accidents in 6 years for the whole containership fleet mean that the frequency of accidents can be subjectively expressed using the linguistics term "Likely" (See Table 4.1). The serious consequence with the loss of 21 lives and 2 injures in 24 accidents can be described by the term "Critical" (See Table 4.2).

Furthermore, according to Figure 4.1 and Equation (4.3), the following is acquired:

$$\overline{F}_{Likely} = (\frac{1}{3}/\frac{2}{3}/\frac{5}{6})$$

$$\overline{S}_{Critical} = (\frac{1}{2}/\frac{5}{6}/1)$$

Using Equation (4.4), the risk evaluation, $\overline{R}$, expressed using fuzzy numbers can be calculated as:

$$\overline{R} = \overline{F}_{Likely} \otimes \overline{S}_{Critical}$$
$$\cong (\frac{1}{6}/\frac{5}{9}/\frac{5}{6})$$

Mapping $\overline{R}$ back to Figure 4.2 (See Figure 4.5), the un-scaled similarity degrees between the fuzzy risk evaluation and the four safety expressions can be calculated using the fuzzy Best-fit method and its corresponding Equation (4.5):

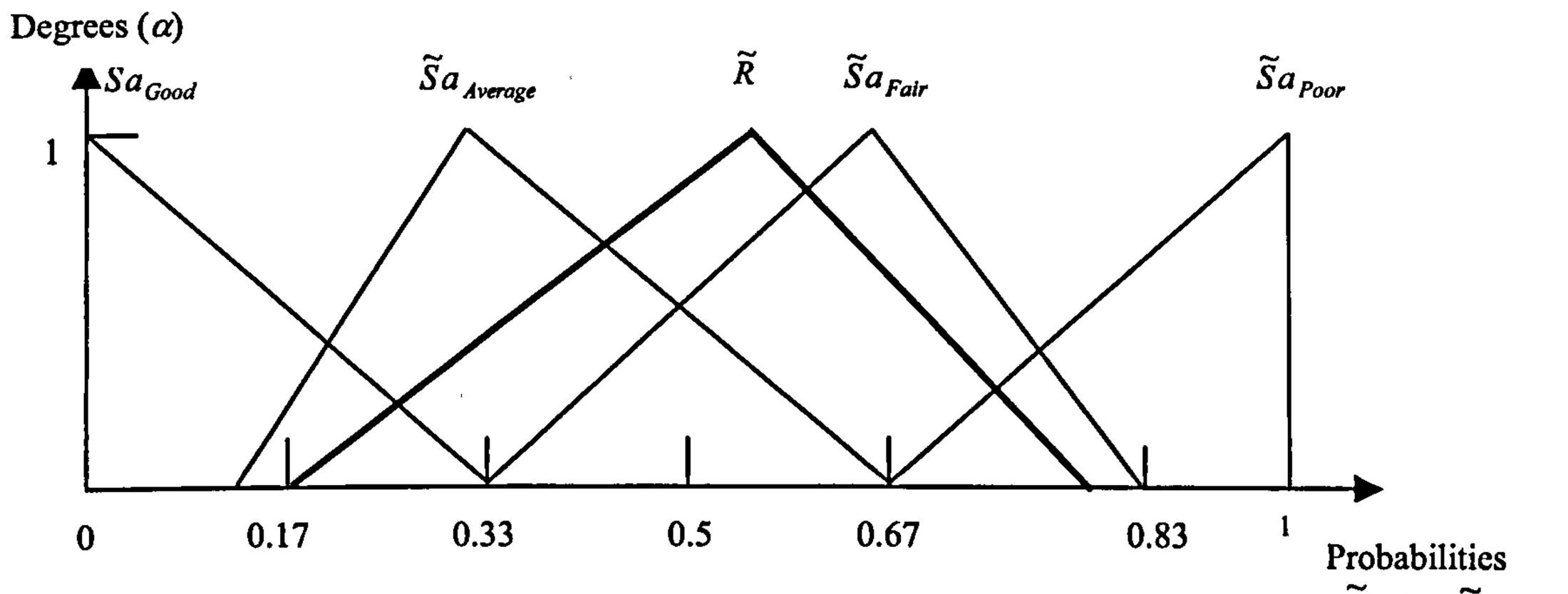


Figure 4.5. Mapping the risk evaluation onto the safety expressions

The fuzzy Best-fit method is then employed to map the fuzzy risk evaluation onto the four safety expressions. Observing Figure 4.5, the following is obtained,

$$\tilde{R}[\alpha] = [(\frac{7}{18}\alpha + \frac{1}{6}), (-\frac{5}{18}\alpha + \frac{5}{6})]$$

$$\tilde{S}a_{Good}[\alpha] = [(0), (-\frac{1}{3}\alpha + \frac{1}{3})] \qquad 0 \le \alpha \le 1$$

Then,

$$K(\alpha) = \left|\frac{7}{18}\alpha + \frac{1}{6}\right|$$

$$L(\alpha) = \left|\frac{1}{18}\alpha + \frac{1}{2}\right| \qquad 0 \le \alpha \le 1$$

$$d(\tilde{R}, \tilde{S}a_{Good}) = \max\{\max[K(\alpha), L(\alpha)] \mid 0 \leqslant \alpha \leqslant 1\} = \frac{5}{9}$$

where $\max[K(\alpha), L(\alpha)]\ (0 \le \alpha \le 1) = (\frac{1}{18}\alpha + \frac{1}{2})$, and $\max(\frac{1}{18}\alpha + \frac{1}{2}) = \frac{5}{9}$.

In a similar way, one can easily acquire the following:

$$d(\widetilde{R},\widetilde{S}a_{Average})=\frac{2}{9}$$

$$d(\widetilde{R},\widetilde{S}a_{Fair})=\frac{1}{9}$$

$$d(\widetilde{R},\widetilde{S}a_{Poor})=\frac{1}{2}$$

Normalising $d(\widetilde{R},\widetilde{S}a_{Poor})$, $d(\widetilde{R},\widetilde{S}a_{Fair})$, $d(\widetilde{R},\widetilde{S}a_{Average})$ and $d(\widetilde{R},\widetilde{S}a_{Good})$ enables the risk evaluation to map the safety expression as follows:

$S_{Collision}$ = {0.116, *"Poor"*, 0.52, *"Fair"*, 0.26, *"Average"*, 0.104, *"Good"*}

4.4.3 Synthesis of the Risk Analyses with Different Natures

The two case studies above individually contribute two different risk analyses of both hazard-based and threat-based risks using the subjective risk assessment method. Validating the feasibility of the subjective risk assessment method, they enable the rank of the risks on a prioritised list and combining them with a distinctive nature as shown in the following.

Using Equation (3.9), the numerical values of $S_{Terrorism}$ and $S_{Collision}$ can be obtained for ranking purposes as follows:

$$S_{Terrorism} = 0.276 \times 0.079 + 0.461 \times 0.384 + 0.17 \times 0.694 + 0.093 \times 1 = 0.41$$

$$S_{Collision} = 0.116 \times 0.079 + 0.52 \times 0.384 + 0.26 \times 0.694 + 0.104 \times 1 = 0.494$$

Therefore, from the viewpoint of risk assessment, the risk related to terrorists attacking ports is categorised to a relatively lower safety level compared to the risk associated with containership collision and may require more attention. For a whole supply chain risk analysis, risk evaluations at a higher level may need to be carried out, where containerships and ports may only be considered as subsystems. It is noted that the risks terrorist attacks and containership collisions are often connected with their higher level event using a OR gate in a hierarchy. Therefore, according to the weight distribution rule in Section 3.2.3, the combination of $S_{Terrorism}$ and $S_{Collision}$ can be expressed using the *ER* approach as:

$S_{Terrorism+Collision}$ = {0.182, *"Poor"*, 0.525, *"Fair"*, 0.204, *"Average"*, 0.089, *"Good"*}

The result of such a combination can effectively respond to the safety levels of its individuals (i.e. $S_{Terrorism}$ and $S_{Collision}$). To test the safety evaluation associated with terrorists attacking ports, the subjective safety assessments of the two subsystems have been observed to a large extent as '*Fair*' and to a small belief degree as '*Good*' respectively. For example, the risk associated with terrorists attacking ports has been assessed as '*Fair*' with a belief of 46.1 percent and as 'Good' with 9.3 percent; the risk associated with containership collisions has a larger extent (52 percent) evaluated as '*Fair*'. Such distribution trends of subjective safety beliefs are well reflected in the combination result ('*Fair*' with 52.5 percent belief degrees and '*Good*' with 8.9 percent).

4.5. Conclusion

This chapter provides a subjective risk assessment method for the organisations involved in *CSCs*. It enables the assessment of the vulnerability based risks of the chains and to support the safety planning for both mitigating and continuity actions. The marriage of fuzzy sets and *ER* to deal with uncertainty can also facilitate risk assessment and be tailored and applied to more management-related industries, where risks usually arise from both threats and hazards. However, the simplification of the complex fuzzy operations and the permission of more risk parameters involved require to be considered in order to facilitate the application of the fuzzy set theory in risk assessment.

Chapter 5 – A Risk-Based Decision Making Framework Using Fuzzy Evidential Reasoning Approaches with Belief Structure

SUMMARY

The chapter illustrates a subjective risk-based decision making framework using the combination of two fuzzy ER approaches. The framework includes three interactive parts. The first one is for risk estimation and synthesis including fuzzy rule-based risk estimation using a fuzzy rule-based ER (FRB-ER) approach, as well as the risk synthesis using the ER approach. Considering the other decision attributes such as the cost and time associated with the risk reduction in RCOs, the second part focuses on synthesising the risk and other decision attributes using a fuzzy link-based ER (FLB-ER) approach to obtain the overall evaluation of a whole CSC system for each RCO. The third part is to apply the overall evaluation for the best RCO selection. The major contributions of the study are to simplify the complex fuzzy calculations and extend the capability of accommodating more risk parameters.

5.1. Introduction

Developing a highly capable risk-based decision support tool in the context of *CSCs* depends on the techniques, which enable the accurate assessment of risk priority and effectively address potential decision attributes, particularly in the absence of precise *CBA*. The previous studies have been generated to deal with the threat-based risk estimation with unavailable or incomplete historical data, the combination of the threat-based and hazard-based risk estimations and safety-cost based decision making. However, the studies may often expose some disadvantages in practical applications and fall short in their ability to permit the simplification of complex fuzzy operations, incorporation of more risk parameters and synthesis of various decision attributes with different amounts of linguistic variables, when a wider analysis is required. This chapter, therefore, establishes a general framework with novel risk and decision methods to provide a basis and tool for risk analysis and synthesis with multiple decision attributes in complex *CSC* systems.

One realistic way to replace the complex fuzzy operations in the discrete and continuous fuzzy set risk assessment methods and deal with the inference between fuzzy risk input and output is to employ fuzzy *IF-THEN* rules in fuzzy logic theory. The approach based on the fuzzy rules, where conditional parts and/or conclusions contain linguistic variables (Zimmermann, 1991) can model the qualitative aspects of human knowledge and reasoning process without employing precise quantitative analysis. It does not

require an expert to provide a precise point at which a risk factor exists. This actually provides a tool for working directly with the linguistic information, which is commonly used in representing risk factors and carrying out safety assessment (Karwowski and Mital, 1986; Keller *et al.*, 1989; Duckstein, 1994; Bell and Badiru, 1996; Bowles and Petaez, 1995; An *et al.*, 2000; Wang *et al.*, 1995 and 1996; Wang, 1997a; Sii *et al.*, 2001; Liu *et al.* 2004). In this context, a risk analysis model using a fuzzy rule-based inference system can be appropriately used to conduct the threat-based and hazard-based risk assessment and synthesis in *CSC* systems.

The purpose of analysing risks is to estimate those high-level ones in a prioritised list so as to ensure the correct decisions to be made and appropriate *RCO(s)* to be selected. However, realising such an objective requires other factors or constraints from economical, technical and environmental considerations to be satisfied. The factors can be defined as multiple decision attributes in analysing a complex decision making problem and normally investigated by the rules of a knowledge base in a hierarchical structure, in which the sub-criteria of the attributes can be further developed. In general, a bottom-up approach can be used to solve such a problem. Pieces of evidence from the lowest level criteria are aggregated as evidence for the second lowest-level criteria/ attributes, which is in turn aggregated to produce evidence for higher-level attributes. The *ER* approach has presented the superiority in dealing with the synthesis of various pieces of evidence obtained/evaluated based on the same universe. The *FRB-ER* inference mechanism is able to transform the different linguistic variables associated with the lower-level criteria/attributes to the unified linguistic expressions at higher-level ones. However, the complex processes of both constructing fuzzy rule bases and conducting inference reasoning are not desirable in multi-level hierarchical decision analysis. Necessary simplification is required to facilitate the development of the method.

A fuzzy link-based method, which is based on a linked belief structure between the linguistic variables expressing the attributes at different levels, can unify all hierarchical fuzzy rule bases and transform the fuzzy input associated with the lowest level attributes to the corresponding fuzzy output on the highest level attributes without employing multiple *FRBs*. Next, the *ER* approach can be used to synthesise all output on the common space and obtain the overall scores of decision options.

In the following, Section 5.2 outlines the risk analysis and synthesis framework using a *FRB-ER* approach. The framework of synthesising risk estimation and other multiple decision attributes is provided in Section 5.3, where the synthesis result can be used to produce the preference estimates associated with *RCOs* for ranking purposes. An illustrative example is used to demonstrate the application of the proposed framework in Section 5.4. Section 5.5 concludes this chapter.

5.2. Fuzzy Rule-based Risk Analysis Framework

The proposed framework for modelling *CSC* system risks consists of six major components, which outline all the necessary steps required for risk estimation at the bottom level of a hierarchical system (i.e. the basic events in a *FTA*) and synthesis from the bottom level to the top level using the *ER* approach proposed in Chapter 3.

5.2.1 Identify Risk Causes/Factors

In this component, all anticipated causes/factors to failure of a *CSC* system are identified. This can be done by a panel of experts during a brainstorming session using a *FTA* technique. The identification of the factors and the construction of the hierarchical structure will follow the rules established in Section 3.2.3.

5.2.2 Identify and Define Fuzzy Input and Output Variables

The threat-based risk parameters used to define the subjective risk estimates include those at both the senior and junior levels. The senior parameter is "***Safety estimate (SE)***", the single fuzzy output variable, which can be defuzzified to prioritise the risks. The variable is described linguistically and is determined by some junior parameters. In risk assessment, it is common to express a safety level by degrees to which it belongs to such linguistic variables as "Poor", "Fair", "Average" and "Good" that are referred to as safety expressions (Wang *et al.*, 1995 and 1996; Yang *et al.*, 2004).

In Section 3.3.2, the four junior/fundamental risk parameters used to subjectively assess the safety level of a *CSC* system have been identified and defined as "*Will*" ***(W)***, "*Damage capability*" ***(D)***, "*Recall difficulty*" ***(R)*** and "*Damage probability*" ***(P)***. ***W*** decides the failure likelihood of a threat-based risk, which directly represents the degrees that one tries to take a certain action. To estimate ***W***, one may choose to use such linguistic terms as "Very weak", "Weak", "Average", "Strong" and "Very strong". The combination of ***D*** and ***R*** responds to the consequence severity of the threat-based risk. Specifically speaking, ***D*** indicates the destructive force/execution of a certain action and ***R*** hints the resilience of the system after a failure or disaster. The following linguistic terms can be considered as a reference to be used in subjectively describing the two sister parameters: "Negligible", "Moderate", "Critical" and "Catastrophic" for ***D*** and "Easy", "Average", "Difficult" and "Extremely Difficult" for ***R***. ***P*** means failure consequence probability and can be defined as the probability that damage consequences happen given the occurrence of the event. One may choose to use such linguistic terms as "Unlikely", "Average", "Likely" and "Definite" to describe it.

Fuzzy logic, based on *FST*, accommodates such linguistic terms through the concept of partial membership. In *FST*, everything is a matter of degree. Therefore, any existing element or situation in risk assessment could be analysed and assigned a value (a degree) indicating how much it belongs to a member of the five sets of the risk parameters. Furthermore, five sets of membership functions can be defined as five curves to describe how each point in the input and output spaces is mapped to a membership value (or degree of membership) between 0 and 1. Due to the advantage of simplicity, straight-line membership functions, especially triangular and trapezoidal membership functions have been commonly used to describe risks in safety assessment (Wang, 1997b). Consequently, the fuzzy membership functions in the risk analysis of *CSCs*, consisting of five sets of overlapping triangular or trapezoidal curves, are generated using the linguistic categories identified in knowledge acquisition and the fuzzy Delphi method (Bojadziev and Bojadziev, 1995), which are described in the following context. They are shown in Figures 5.1 – 5.5. Although it is possible to have some flexibility in the definition of the five membership functions to suit different situations in various supply chains, the reasonable changes are required by the support of multiple experts, who should be appropriately chosen so as to ensure realistic and non-biased membership functions (Kuusela *et. al.*, 1998).

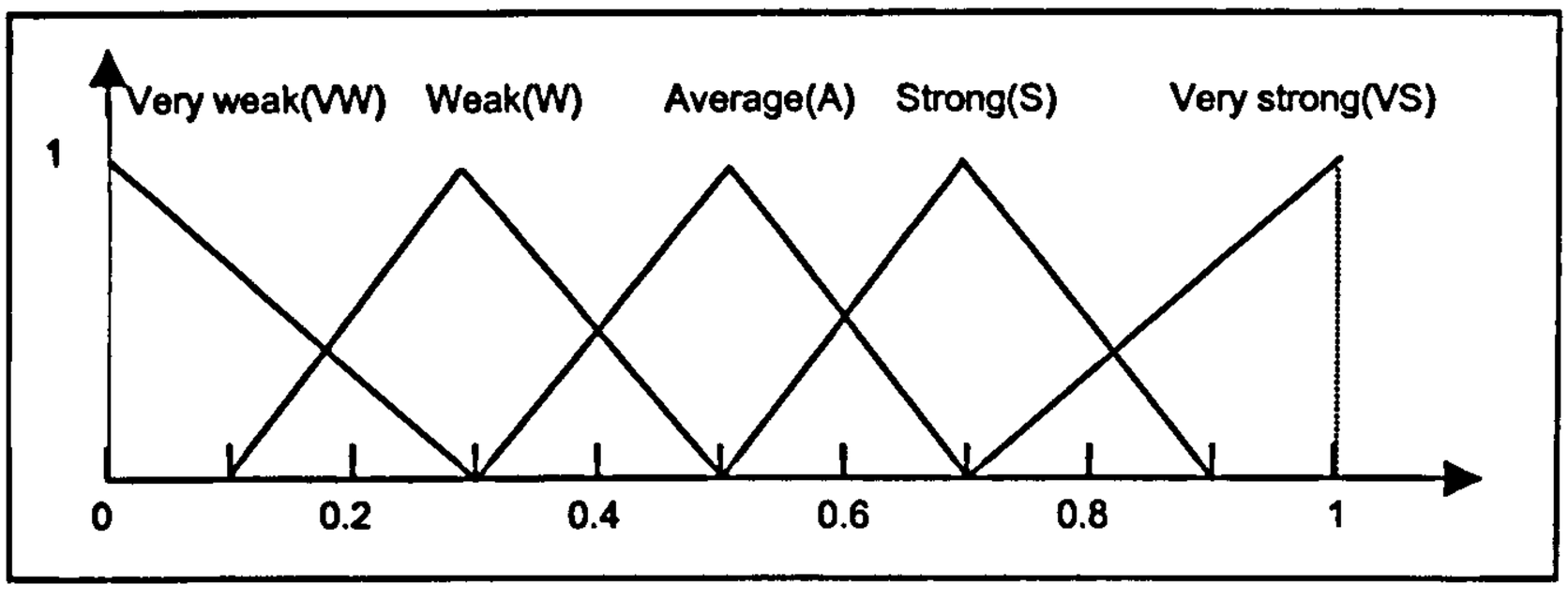


Figure 5.1. Membership function for *Will*

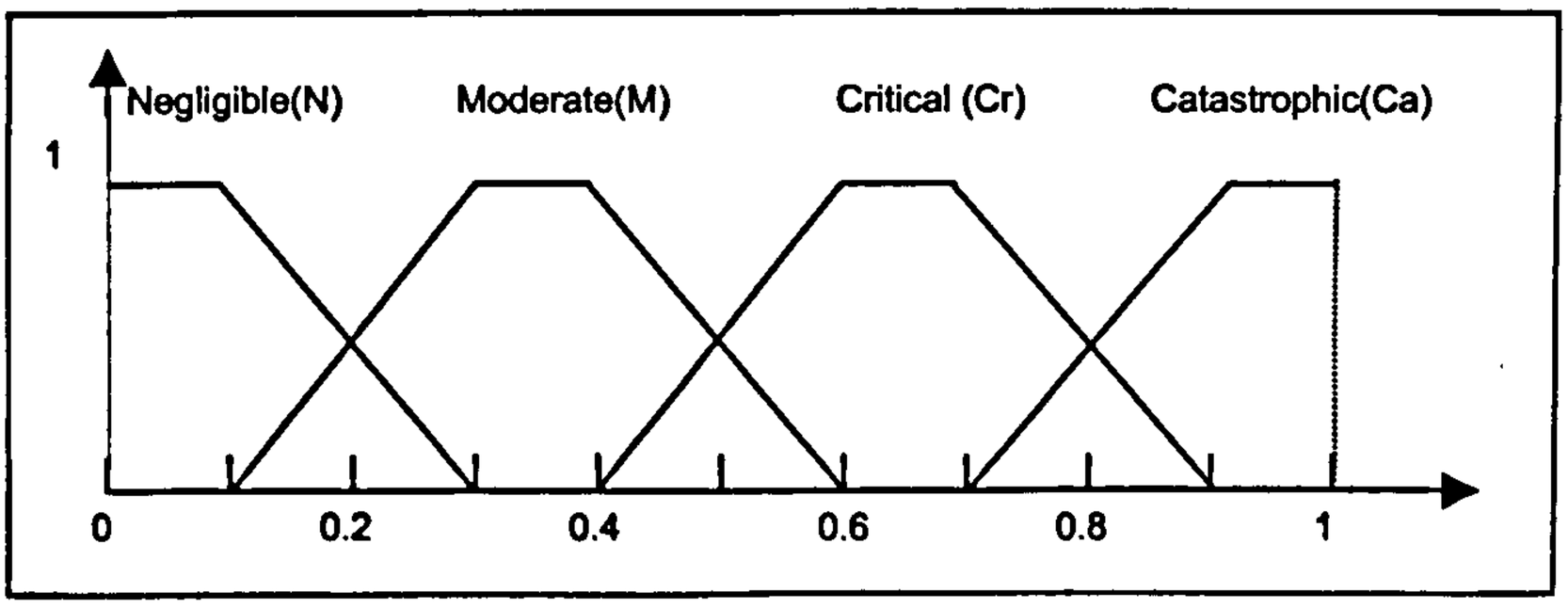


Figure 5.2. Membership function for *Damage capability*

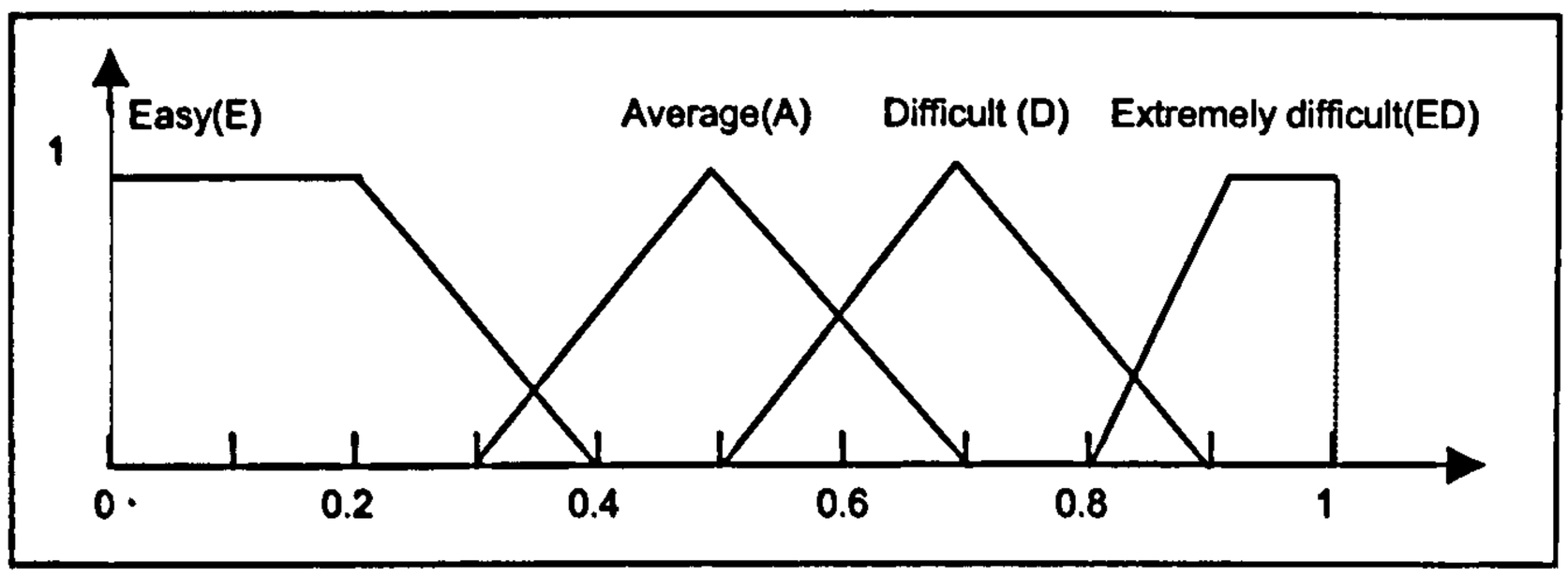


Figure 5.3. Membership function for *Recall difficulty*

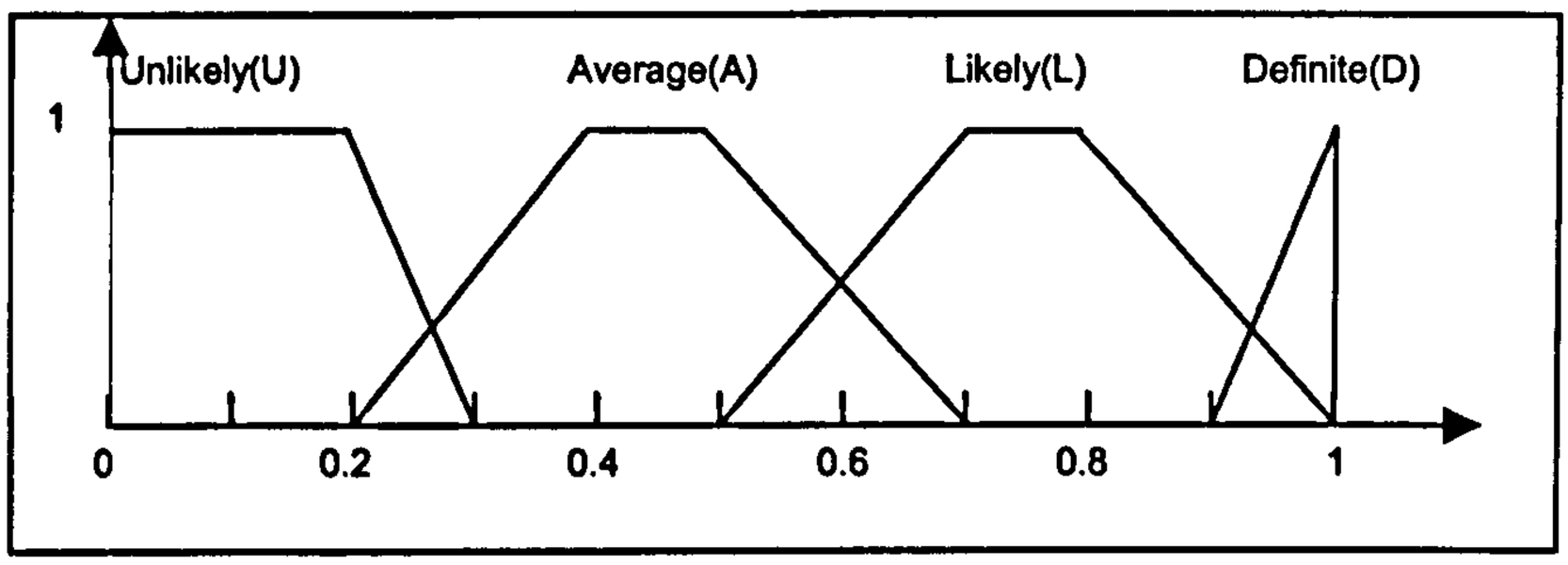


Figure 5.4. Membership function for *Damage probability*

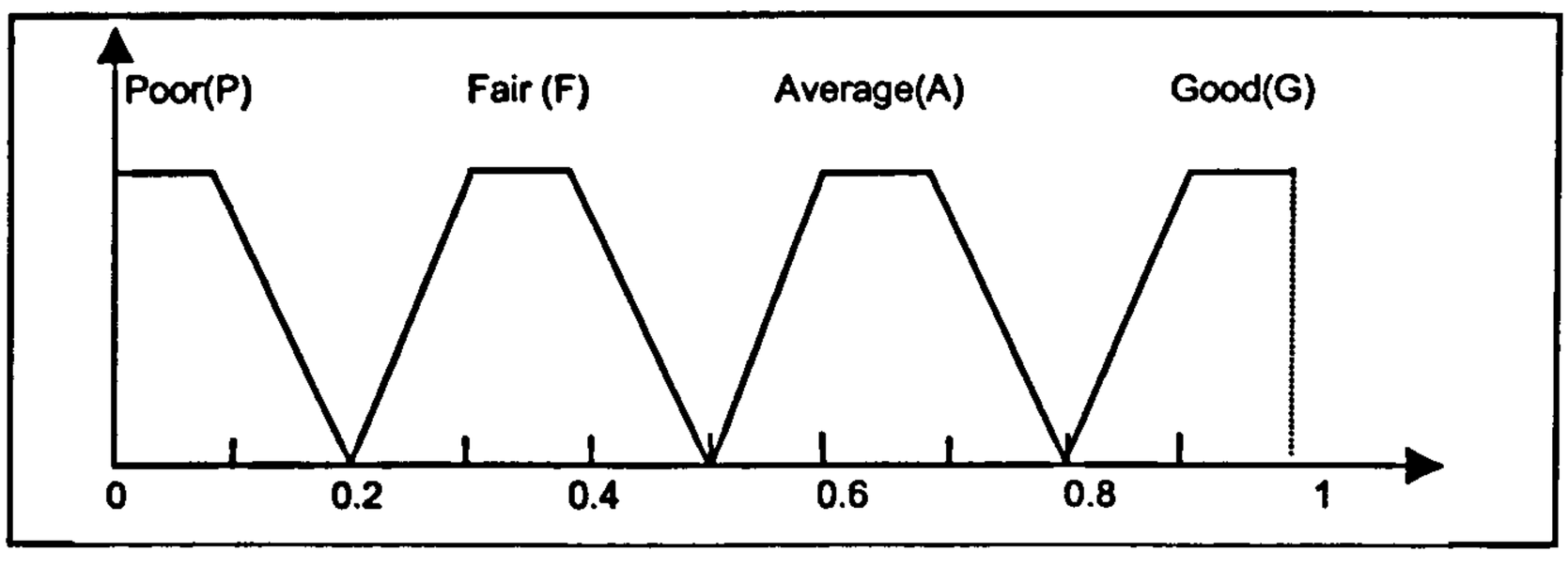


Figure 5.5. Membership function for *Safety Estimation*

The membership degrees (or the fuzzy membership functions) of the risk parameters can be assigned (subjectively decided) by multiple experts. The fuzzy Delphi method (Bojadziev and Bojadziev, 1995) can be employed in this process of achieving the consensus condition. The process of determining membership function μ_i is described as follows (Cheng and Lin, 2002; Li and Liao, 2005):

1) Suppose each expert E_l, l=1, 2, …, n, provides the membership function μ_i^l with their knowledge in various fields, which can be presented in the form of a trapezoidal/triangular fuzzy number $\mu_i^l = (a_{i1}^l, a_{i2}^l, a_{i3}^l, a_{i4}^l)$, l=1, 2, …, n.
2) The mean μ_i^m of all membership functions μ_i^1, μ_i^2, …, μ_i^n is calculated as follows:

$$\mu_i^m = (a_{i1}^m, a_{i2}^m, a_{i3}^m, a_{i4}^m)$$

$$= \left(\frac{1}{n}\sum_{l=1}^{n} a_{i1}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i2}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i3}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i4}^{l} \right) \tag{5.1}$$

Then for each expert E_l, l=1, 2, …, n, the differences (σ_i^l) between μ_i^l and μ_i^m

$$\sigma_i^l = (a_{i1}^m - a_{i1}^l, a_{i2}^m - a_{i2}^l, a_{i3}^m - a_{i3}^l, a_{i4}^m - a_{i4}^l)$$

$$= \left(\frac{1}{n}\sum_{l=1}^{n} a_{i1}^{l} - a_{i1}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i2}^{l} - a_{i2}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i3}^{l} - a_{i3}^{l}, \frac{1}{n}\sum_{l=1}^{n} a_{i4}^{l} - a_{i4}^{l} \right) \tag{5.2}$$

are computed and sent back to the experts E_l for reassessment.

3) Each expert E_l, l=1, 2, …, n, presents a revised trapezoidal/triangular fuzzy number, which goes to Equations (5.1) and (5.2). The process is repeated until successive means become reasonably close to individual estimations made by the experts. Note that the term "reasonably" can be made precisely by selecting a threshold θ and requiring that any element of σ_i^l, $\left| \frac{1}{n}\sum_{l=1}^{n} a_{i,j}^{l} - a_{i,j}^{l} \right| < \theta$ (j=1, 2, 3, 4). (5.3)

5.2.3 Construct a Fuzzy Rule-Base with the Belief Structure

Fuzzy logic systems are knowledge-based or rule-based ones constructed from human knowledge in the form of fuzzy *IF-THEN* rules (Wang, 1997b). An important contribution of the fuzzy system theory is that it provides a systematic procedure for transforming a knowledge base into a non-linear mapping (Sii and Wang, 2002). A fuzzy *IF-THEN* rule is 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 W* of a threat is "Very strong" AND *D* is "Catastrophic" AND *R* is "Extremely difficult" AND *P* is "Definite", *THEN SE* is "Poor". The descriptions of *W*, *D*, *R*, *P* and *SE* are characterised by membership functions. A fuzzy system is constructed from a collection of fuzzy *IF-THEN* rules from human experts or based on the domain knowledge and is then completed by combining these rules into a single system.

Obviously, the *IF-THEN* rules in this study can have two parts: an antecedent that responds to the fuzzy input and a consequence, which is the result/fuzzy output. In classical fuzzy rule-based systems, such input and output are usually expressed by single linguistic variables with 100% certainty and the rules constructed are also always considered as single output cases. However, when observing realistic supply chain situations, the knowledge representation power of the fuzzy rule systems will be severely limited if only single linguistic variables are used to represent uncertain knowledge. Four fuzzy input parameters include 17 (=5+4+4+4) linguistic variables, which can be assembled to produce 320 (=5×4×4×4) antecedents. Given a combination of input variables, *SE* may belong to more than one safety expression with appropriate

belief degrees. For example, a fuzzy rule with certain degrees of belief can be described as: *IF W* of a threat is "Very strong" AND ***D*** is "Catastrophic" AND ***R*** is "Extremely difficult" AND ***P*** is "Likely", *THEN SE* is "Poor" **with a belief degree of 0.9**, "Fair" **with a belief degree of 0.1**, "Average" **with a belief degree of 0** and "Good" **with a belief degree of 0.**

In order to model general and complex uncertain problems in safety analysis of *CSCs*, the classical fuzzy rule-based systems are extended to assign each consequent variable a degree of belief. Assume that the four antecedent parameters, U_1=***W***, U_2=***D***, U_3=***R*** and U_4=***P*** can be described by linguistic variable A_{iJ_i}, where i=1, 2, 3, or 4 respectively and J_1 = 1, …, or 5, J_2, J_3 and J_4 = 1, …, or 4. One consequent variable ***SE*** can be described by 4 linguistic terms, D_1, D_2, D_3 and D_4. Let $A_{iJ_i}^k$ be a linguistic term corresponding to the i^{th} parameter in the k^{th} rule, with i=1, 2, 3 and 4. Thus, the generic k^{th} rule in the rule base can be defined as follows:

R_k: IF W is $A_{1J_1}^k$ AND D is $A_{2J_2}^k$ AND R is $A_{3J_3}^k$ AND P is $A_{4J_4}^k$, THEN SE is D_1 with a belief degree of β_{1k}, D_2 with a belief degree of β_{2k}, D_3 with a belief degree of β_{3k} and D_4 with a belief degree of β_{4k}.

where $\sum_{i=1}^{4}\beta_{ik} = 1, k \in \{1, \ldots, 320\}$.

It is noted that all the parameters and the belief degrees of the rules are usually assigned at the knowledge acquisition phrase by multiple experts on the basis of subjective judgements. A rule base including 320 rules with a belief degree structure is listed in Appendix 3 (of course, such belief degrees listed can be reassigned with some flexibility to consider different applications in various supply chains).

5.2.4 Application of A FRB-ER Approach

Once a rule based system is established, it can be used to perform inference for given fuzzy or incomplete observations to obtain the corresponding fuzzy output, which can be used to assess the safety of *CSCs*. The inference procedure is basically composed of four steps, summarized in the following sub-sections.

5.2.4.1 Observation Transformation

Before starting the inference process, observations available should be analysed to determine their relationship with each junior risk parameter in the antecedents. Four kinds of possible observations may be represented using membership functions to suit

conditions under this study. They are either a single deterministic value with 100% certainty, a closed interval, a triangular distribution or a trapezoidal distribution (Sii and Wang, 2002). Having defined the four junior risk parameters in Figures 5.1, 5.2, 5.3 and 5.4, a matching function method (Liu *et al.*, 2004) can be employed to perform the observation transformation and determine the belief degrees to which actual observations, which have been numerically described, match to each linguistic variable in the antecedent.

The matching function method chooses the *Max-Min* operation to show the similarity between the real input fuzzy set A^r and the corresponding fuzzy linguistic variables A_{iJ_i}, because it is a classical tool to set the matching degree between fuzzy sets (Zimmermann, 1991). Therefore, the similarity degree between A^r and A_{iJ_i} can be defined as follows:

$$a_{iJ_i} = M(A^r, A_{iJ_i}) = \max[\min(\mu_{A^r}(x), \mu_{A_{iJ_i}}(x))] \tag{5.4}$$

where x covers the domain of the input A^r. Each a_{iJ_i} represents the extent to which A^r belongs to the defined linguistic variables in the i^{th} risk parameter in the antecedents. The observation transformation to the risk parameters with the similarity degrees using a matching function method can be expressed as follows:

$T(A^r_{1J_1})$ = {(α_{11}, "*Very strong*"), (α_{12}, "*Strong*"), (α_{13}, "*Average*"), (α_{14}, "*Weak*"), (α_{15}, "*Very weak*")}

$T(A^r_{2J_2})$ = {(α_{21}, "*Catastrophic*"), (α_{22}, "*Critical*"), (α_{23}, "*Moderate*"), (α_{24}, "*Negligible*")}

$T(A^r_{3J_3})$ = {(α_{31}, "*Extremely Difficult*") (α_{32}, "*Difficult*"), (α_{33}, "*Average*"), (α_{34}, "*Easy*")}

$T(A^r_{4J_4})$ = {(α_{41}, "*Definite*"), (α_{42}, "*Likely*"), (α_{43}, "*Average*"), (α_{44}, "*Unlikely*")}

It is noteworthy that the fuzzy input may directly be judged and expressed by experts using linguistic variables without the requirements of observation transformation.

5.2.4.2 Activation of Rule Weights

The aim of the observation transformation to the risk parameters is to obtain the corresponding safety levels for further evaluating the priority of risks. Thus, the introduction of the risk parameters with some similarity degrees transformed from the realistic observations into the rule-based inference system constructed in Section 5.2.3 is necessary. An activating rule weight method is used to implement such an introduction. In other words, the distributions of different weights to all rules can be used to describe the relationship between the risk input transformed from observations and the rules in

the system. In order to obtain an appropriate weight for the k^{th} rule, the similarity degrees related to the k^{th} rule are required to be synthesised in a logic way that can reflect the *AND* connective between their representing safety parameters. Liu *et al.* (2004) recommended using the *Product* operator as the logical tool to synthesise the degrees and deal with the dependencies of the antecedent parameters in a belief rule base. Consequently, since the four junior risk parameters have the same importance, the weight of the k^{th} rule can be calculated as follows:

$$\theta_k = \frac{\prod_{i=1}^{4} \alpha_{iJ_i}^{k}}{\sum_{m=1}^{320} (\prod_{i=1}^{4} \alpha_{iJ_i}^{m})} (i = 1, 2, 3 \text{ or } 4; J_1 = 1, \ldots, \text{or } 5; J_2, J_3, J_4 = 1, \ldots, \text{or } 4) \qquad (5.5)$$

Note that the situations where some of $\alpha_{iJ_i}^{m}$ are equal to zero will geminately simplify the calculation through the ignorance of the rules including those linguistic variables with a zero similarity degree.

5.2.4.3 Rule Inference for the Calculation of Safety Levels Using the ER Approach

Use of the rule weight method can successfully distribute different weights to all related rules to connect the fuzzy input with one part of the whole rule base and thus, enable the establishment of a new rule-based system, which can be summarized using the following rule expression matrix shown in Table 5.1.

Table 5.1. A new rule expression matrix for the introduction of observations

Antecedent / Belief / Consequence					Poor	Fair	Average	Good
$A^{1}_{1J_1}$	$A^{1}_{2J_2}$	$A^{1}_{3J_3}$	$A^{1}_{4J_4}$	θ_1	β_{11}	β_{21}	β_{31}	β_{41}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$A^{k}_{1J_1}$	$A^{k}_{2J_2}$	$A^{k}_{3J_3}$	$A^{k}_{4J_4}$	θ_k	β_{1k}	β_{2k}	β_{3k}	β_{4k}
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
$A^{n}_{1J_1}$	$A^{n}_{2J_2}$	$A^{n}_{3J_3}$	$A^{n}_{4J_4}$	θ_n	β_{1n}	β_{2n}	β_{3n}	β_{4n}

In the matrix, n represents the number of all rules whose weights are not zero.

Having represented each rule using the rule expression matrix, the *ER* approach (Yang *et al.*, 2001; Yang and Xu, 2002) can be used to combine the rules and generate a final conclusion, which is a belief distribution on the safety expressions and will also give a panoramic view about the safety level for a given observation. The kernel of this approach, an *ER* algorithm has been analysed in Section 3.3.2. Therefore, in this chapter, if B represents the combined final output set consisting of the four safety expressions

with belief degrees, which is the synthesis of B_1 and B_2 in a rule expression matrix, then B, B_1 and B_2 can separately be expressed by:

B = {β^1 "Poor", β^2 "Fair", β^3 "Average", β^4 "Good"}
B_1 = {$\beta^1{}_1$ "Poor", $\beta^2{}_1$ "Fair", $\beta^3{}_1$ "Average", $\beta^4{}_1$ "Good"}
B_2 = {$\beta^1{}_2$ "Poor", $\beta^2{}_2$ "Fair", $\beta^3{}_2$ "Average", $\beta^4{}_2$ "Good"}

where β is a belief degree measuring the subjective uncertainty that "***SE*** belongs to each linguistic variable" and β^i (i = 1, ..., 4) can be calculated using a group of equations similar to Equations (3.10) – (3.15), in which α is replaced by β.

5.2.5 Safety Synthesis in a Hierarchy

The discussion above focuses on the risk estimation of basic events at the bottom level of a hierarchical fault tree done by an expert. The safety of a *CSC* system is often determined by all the associated failure events of their individual components, which make up the structure. Therefore, it is necessary to conduct:

- The synthesis of risk estimates of a specific failure event for a component done by a panel of experts.
- The synthesis of safety estimates of various failure events for each component, for each sub-system and finally for the system being investigated.

Consequently, the multi-expert, multi-attribute and multi-level safety synthesis can be carried out to obtain the safety estimate of the system using the *ER* approach introduced previously.

Simultaneously, it is noteworthy that the above inference process can be slightly changed to adapt the hazard-based risk analysis and synthesis. The change is mainly associated with the identification of fuzzy input, which is defined as "*Likelihood*" (***L***) and "*Consequence*" (***C***) in the context of the hazard-based risks (it is also possible to identify other parameters like "Probability of consequence"). The following linguistic terms can be considered as a reference to be used in subjectively describing the two parameters: "Extremely frequent", "Frequent", "Likely", "Average", "Occasional", "Remote", and "Extremely remote" for ***L*** and "Catastrophic", "Critical", "Severe", "Trivial", "Marginal" and "Negligible" for ***C***. The associated inference process can be very similar to the one described above.

5.2.6 Ranking Safety Estimates

In order to rank the safety estimates expressed by fuzzy sets, the fuzzy linguistic variables require to be defuzzified by giving each of them an "appropriate" utility value

(U_v). There are many defuzzification methods available. However, every method has its pitfalls in some aspects, such as inconsistency with human intuition, indiscrimination and difficulty of interpretation, implying the non-existence of a unique or best defuzzification method (Zhang *et al.*, 2004). Therefore, some previous studies (Bortolan and Degani, 1985; Chen and Hwang, 1992) have suggested the evaluation criteria of defining the term "appropriate", including complexity, robustness, flexibility, transitivity, and ease of interpretation.

The defuzzification operation is not easy. Many defuzzification algorithms have been developed, of which the weighted mean of maximums (*WMoM*) (Andrews and Moss, 2002) is probably the simplest. The *WMoM* method gives a best-estimate of the average, weighted by the truth degree at which the membership functions reach their maximum values. However, based on the above criteria such a simplified transformation from fuzzy numbers to crisp numbers may lose much fuzzy information and lead to serious deviation, especially when many trapezoidal membership functions exist. When fuzzy numbers transformation requires more accuracy, not only D_m (Dm_1 and Dm_2) but also D_1 and D_2 in Figure 5.6 must be considered. Chen and Klien (1997) proposed an easy defuzzification method for reasonably obtaining the crisp number of a fuzzy set and this method is shown as follows:

$$U_v = \frac{D_1 + D_{m1}}{(D_1 + D_{m1}) + [(1 - D_{m2}) + (1 - D_2)]} \tag{5.6}$$

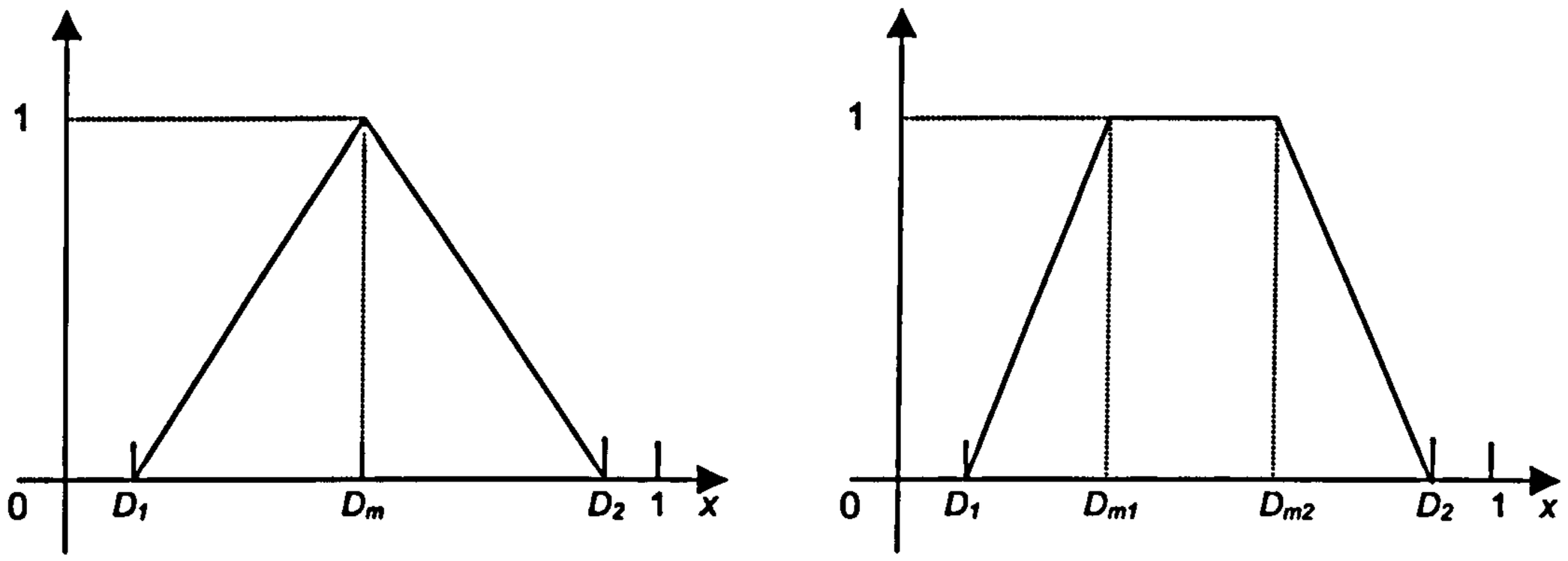


Figure 5.6. The deviation of the *WMOM* method

Consequently, the four safety linguistic expressions of the senior risk parameter can be defuzziffied as the set of [0, 0.3125, 0.5926, 1]. The index value (N_v) for ranking the safety estimates can be calculated as follows:

$$N_v = \beta^1 \times 0 + \beta^2 \times 0.3125 + \beta^3 \times 0.5926 + \beta^4 \times 1 \tag{5.7}$$

5.3. Fuzzy Link-Based *MADM* Framework

The study of this section is to synthesise the safety estimates acquired above with other associated decision attributes (i.e. cost and time) and obtain the overall performance scores for each *RCO*. The steps used in the framework are outlined in the following context.

The analysis of a complex risk-based decision making problem can be carried out using a hierarchical structure, where the top decision making issue is often determined by multiple attributes. Each attribute usually has several parameters and the parameters may be further decomposed into more detailed sub-parameters. Such a top-down hierarchy can be kept under analysis until the lowest level factors can be effectively assessed by domain experts using their subjective knowledge possibly based on objective information. The generic model of the hierarchy is shown in Figure 5.7.

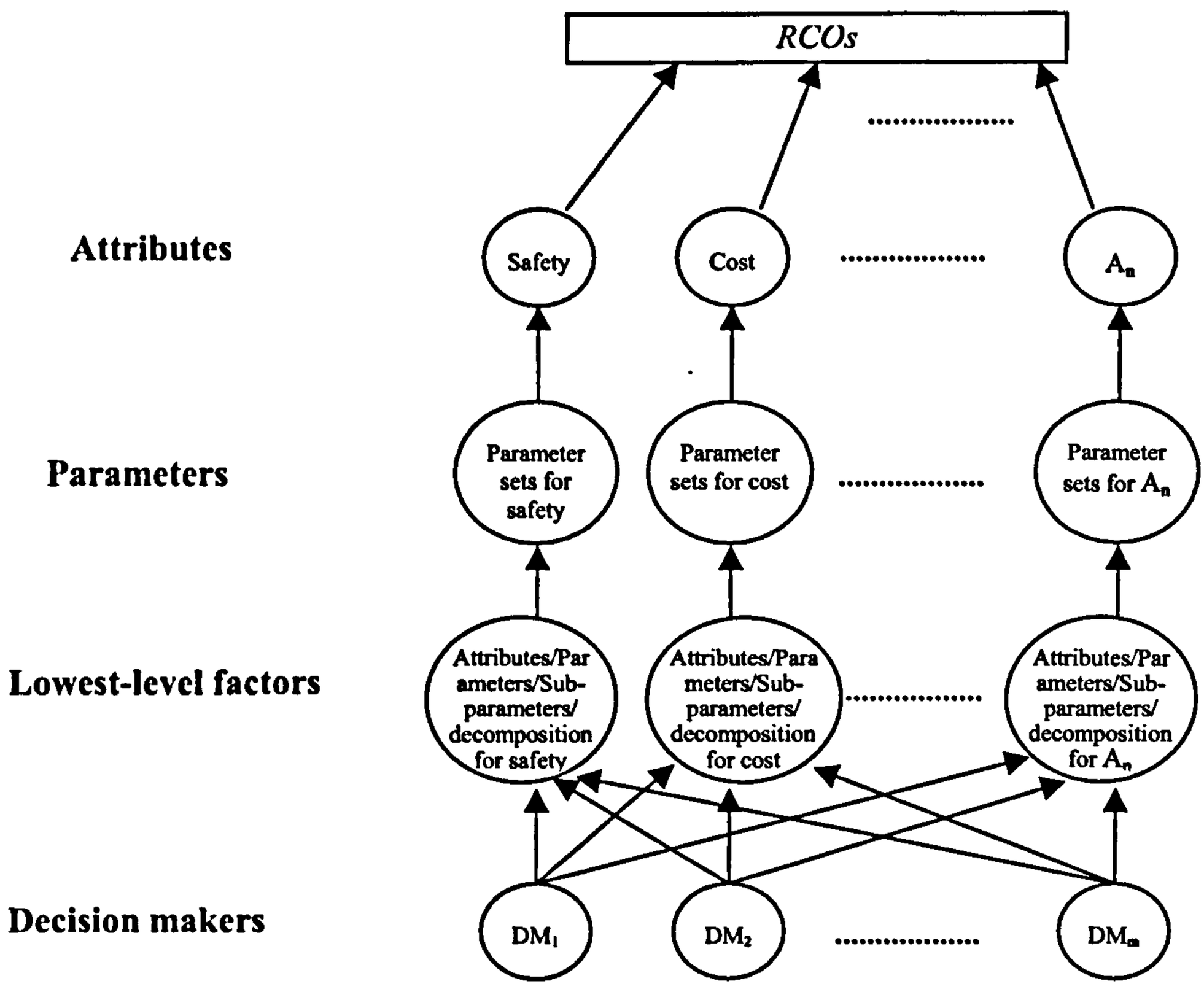


Figure 5.7. A generic model of risk-based decision making hierarchy

Once the hierarchy is constructed, the next step is to synthesise all evaluations from the experts to obtain the overall performance score of the top level event based on a bottom-up analysis. Let the estimation of the lowest-level factors based on all expert judgements be the inference input with fuzzy expressions (i.e. linguistic variables) and the overall performance scores be the output expressed by linguistic variables with belief degrees.

Then, the calculation of the input is straightforward and can be obtained by combining the expert judgements using the *ER* approach. Here, the *ER* approach rather than the fuzzy Delphi method introduced above is used to appropriately incorporate and present the different weights of various decision makers. The transformation from the input to output is usually complex and requires careful analysis of appropriate synthesising approaches.

A traditional safety-cost based decision making method has been developed using the *ER* approach to provide a possible basis for the synthesis (Wang *et al.*, 1996). However the applications of such a conventional method requires many assumptions such as the same amount of decision attribute linguistic variables and the unilateral-order relationship between the linguistic variables. For example, it will be very difficult to incorporate a new bilateral-order decision attribute "time" expressed by five linguistic variables, "Too long", "Long", "Appropriate", "Short" and "Too short" into the safety-cost decision making model.

Having given the risk analysis framework in Section 5.2, the *FRB-ER* method can be repeatedly used for the transformation from fuzzy input to fuzzy output when more decision making related attributes (i.e. cost and time) are required. It requires establishing multiple fuzzy rule bases by following the top-down hierarchy, which can be produced by investigating individual family branches including a parent variable and its attached children. In the fuzzy rule bases, the linguistic variables used to express children constitute the antecedent part and the ones used to describe parent make up the consequence. This method can function very well on dealing with risk based *MADM* problems, although the construction and calculation associated with multiple fuzzy rule bases may sometimes be time consuming.

A fuzzy link-based method is developed for risk-based multiple attribute decision-making analysis in *CSC* systems based on the work by Sonmez (2002). The *ER* approach has proven to be an effective tool to deal with multidisciplinary information and data. However, the application of the approach requires the assumption that all information and data is assessed or obtained on the basis of the same universe (one common utility space), which is often not the case in *MADM*. Therefore, the information and data needs to be transformed before being aggregated using either the rules based on fuzzy logic theory (which is related to the *FRB-ER* method) or the belief distributions based on the utility theory (which is associated with the *FLB-ER*) by decision makers. By taking the attribute "cost" in one *MADM* analysis as an example, the *FLB-ER* approach can be introduced in the following context.

Assume the attribute "Cost" has its parent event "*RCO*" and children parameters "Investment" and "Maintenance" in a decision-making hierarchy. The top level event "*RCO*" can be expressed using such linguistic variables as "Slightly preferred",

"Moderately preferred", "Average", "Preferred" and "Greatly preferred". The attribute "Cost" is described linguistically as "Very High", "High", "Average", "Low" and "Very Low". The linguistic variables used to assess the parameters "Investment" and "Maintenance" are individually the sets of ("Substantive", "Large", "Moderate", "Little") and ("Excessive", "Reasonable", "Marginal", "Negligible"). Then, a belief structure link between the linguistic variables expressing different three-level attributes can be generated for the transformation from fuzzy input to output and shown in Figure 5.8.

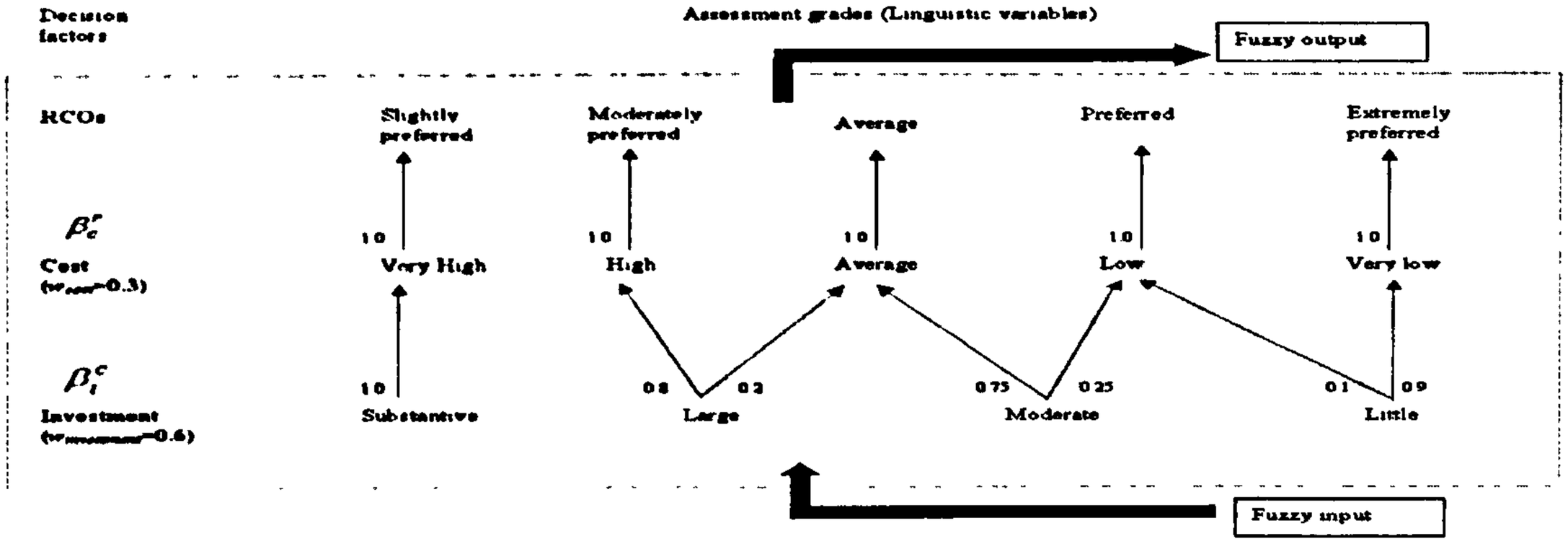


Figure 5.8. An example of transforming fuzzy input to output

In Figure 5.8, *w* represents the relative (normalised) weights of each attribute/parameter (same-level factors) under the same parent. The values attached to the arrows are the belief degrees β distributed by experts for indicating the relationships between linguistic variables of different-level decision factors. Note that the sum of the belief values from one linguistic variable is equal to one. For example, the parameter "Investment" with "Large" expression indicates that the level of the attribute "Cost" can be believed as 80% ($\beta_{i=2}^{c=2}$) "High" and 20% ($\beta_{i=2}^{c=3}$) "Average" without the presence of other evidence. As far as selecting the best "*RCO*" is concerned, the "High" cost evaluation can support "*RCO*" to 100% ($\beta_{c=2}^{r=2}$) "Moderately preferred" and the "Average" cost evaluation can be transformed into 100% ($\beta_{c=3}^{r=3}$) "Average" on the universe expressing "*RCO*". Such a linked belief structure can be used as a channel to transform the fuzzy input to fuzzy output by aggregating all values of fuzzy input, factor weights and belief degrees. The transform process and aggregating calculations can be described as follows.

Suppose I^i (i = 1, 2, 3, 4) represents the fuzzy input (subjective assessment) associated with the parameter "Investment", which can be obtained using a similar philosophy to the *Max-Min* operation in Equation (5.4), if directly assigning a belief function is impossible; I^c (c = 1, 2, ..., 5) stands for the corresponding fuzzy input of the attribute "Cost" transformed from the "Investment" related fuzzy input I^i; and O^r (r = 1, 2, ..., 5) indicates the fuzzy output transformed from I^c. Then,

$$O^r = \sum_{c=1}^{5} I^c \beta_c^r = \sum_{c=1}^{5} (\sum_{i=1}^{4} I^i \beta_i^c) \beta_c^r \quad (r = 1, 2, ..., 5) \tag{5.8}$$

where $\sum_{r=1}^{5} O^r = 1$.

Assume that w^r indicates the relative weight associated with the fuzzy output transformed by the fuzzy input associated with the parameter "Investment". Then,

$$w^r = w_{investement} \bullet w_{cost} \tag{5.9}$$

Note that the sum of the relative weights of the fuzzy output transformed by the input associated with all the lowest level factors is equal to one.

Suppose there are p *RCOs*, which are studied using s lowest-level factors and assessed by q experts. For the j^{th} *RCO* ($j = 1, 2, ..., p$), the fuzzy input of the i^{th} factor ($i = 1, 2, ..., s$) can be obtained by combining its t assessments from all experts on the basis of the *ER* approach. In a similar way, the weight w_i of the i^{th} factor can also be calculated. Furthermore, using the fuzzy link-based approach, all fuzzy input estimations can be transformed into their corresponding fuzzy output O_i^r with the individual weights w_i^r based on the same space, the utility expressions of *RCOs*. Then, all O_i^r can be further synthesised using the *ER* approach to obtain a preference estimate associated with the j^{th} *RCO* in terms of the utility expressions. The synthesised preference estimate U_j for the j^{th} *RCO* can be expressed as follows:

$U_j = \{u_j^1$, *"Slightly preferred"*, u_j^2, *"Moderately preferred"*, u_j^3, *"Average"*, u_j^4, *"Preferred"*, u_j^5, *"Greatly preferred"*$\}$

where u_j^r (r = 1, 2, ..., 5) is a belief degree used to measure the degree to which the j^{th} *RCO* belongs to the five linguistic variables. Preference degree P_j associated with the j^{th} *RCO* can be obtained by:

$$P_j = \sum_{t=1}^{5} u_j^t K_t \tag{5.10}$$

where the numerical values of K_t ($t = 1, 2, ..., 5$) are assigned to describe the five utility expressions. To calculate the values, the membership functions of the preference estimate require to be decided by experts using many techniques such as the fuzzy Delphi method [•]. Then the defuzzification method associated with Equation (5.6) is used to obtain the numerical values expressing the parameter preference as follows:

$$K_1 = 0, K_2 = 0.3, K_3 = 0.5, K_4 = 0.7, K_5 = 1$$

RCO selection can therefore be carried out on the basis of the preference degrees associated with the s *RCOs* with regard to the particular considerations of safety and

[•] More details will be displayed in Figure 9.2.

other decision attributes. It is obvious that a larger P_j means that the j^{th} *RCO* is more desirable. The best *RCO* with the largest preference degree may be selected on the magnitudes of P_j.

5.4. An Illustrative Example

The case introduced in Section 4.4.1 is extended to illustrate the applicability of the proposed framework in *RCO* selection and the inference reliability of the fuzzy rule-based approach in risk assessment by comparing it with the result obtained in Section 4.4.1.

It has been described that a port is highly likely to be attacked by attacking the channel/waterway or bombing the quayside infrastructures/facilities of the terminals. Either of them can be associated with several attacking modes (See the analysis related to Figure 4.3 and Table 4.3). Suppose there are four safety analysts. There are four *RCOs*, which are described as follows:

RCO#1: Using *AIS* to monitor the movement of ships.
RCO#2: Security awareness education as well as security and rescue training and drills.
RCO#3: Adequate perimeter fencing, lighting and locking, defending and cargo scanning devices and security equipments as well as supervision of transferring container cargo.
RCO#4: A security officer designated in the selection of staff (including the consideration of the background of employees or the reputation of the labour agency) as well as the positive identification of all visitors and vendors.

5.4.1 Ranking Basic Safety Events and Calculating Prior Safety Estimate of Top Events

Suppose four safety analysts make the judgements on each attacking mode for the calculation of the prior safety level of a target port. The judgements are assessed on the basis of the four defined junior safety parameters. For example, the mode of "using a missile or bomb to attack the channel" (*EXT-CHA*) can be analysed in Table 5.2.

Table. 5.2. An example of the subjective assessment of the junior safety parameters

Expert	*Will*	*Damage capability*	*Recall difficulty*	*Damage Probability*
E # 1	1, "Weak(W)"	0.5, "Moderate(M)", 0.5, "Critical(Cr)"	1, "Average(A)"	1, "Likely(L)"
E # 2	(0.2, 0.3, 0.4)	(0.3, 0.5, 0.7)	(0.3, 0.5, 0.7)	(0.7, .08, 0.9)
E # 3	[0.2, 0.4]	[0.4, 0.6]	[0.4, 0.6]	[0.6, 0.8]
E # 4	0.3	{0.3, 0.4, 0.6, 0.7}	{0.3, 0.4, 0.6, 0.7}	{0.5, 0.6, 0.8, 0.9}

Using Equation (5.4), the input (observations) in Table 5.2 can be transformed and the judgements can be uniquely expressed by linguistic variables in Table 5.3. Then the fuzzy input based on all expert judgements can be obtained using the *ER* approach.

Table. 5.3. The unique linguistic variable expressions of the junior safety parameters

Expert	*Will*	*Damage capability*	*Recall difficulty*	*Damage Probability*
E # 1	1, "W"	0.5, "M", 0.5, "Cr"	0.06, "E", 0.82 "A", 0.12, "D"	1, "L"
E # 2	0.21, "VW", 0.53, "W", 0.26, "A"	0.5, "M", 0.5, "Cr"	0.14, "E", 0.57 "A", 0.29, "D"	0.07, "A", 0.93, "L"
E # 3	1, "W"	0.5, "M", 0.5, "Cr"	1, "A"	1, "L"
E # 4	1, "W"	0.5, "M", 0.5, "Cr"	1, "A"	1, "L"
Fuzzy input	0.04, "VW", 0.92, "W", 0.04, "A"	0.5, "M", 0.5, "Cr"	0.17, "E", 0.5 "A", 0.33, "D"	0.43, "A", 0.57, "L"

Having known the fuzzy input, the evaluation of the senior risk parameter, *SE* can be performed using the proposed *FRB-ER* method. In the rule base, 320 rules have been established, of which only 36 rules are fired in this particular case, i.e. Rules #18, #19, #22, #23, #26, #27, #34, #35, #38, #39, #42, #43, #82, #83, #86, #87, #90, #91, #98, #99, #102, #103, #106, #107, #146, #147, #150, #43, #82, #83, #86, #87, #90, #91, #98, #99, #102, #103, #106, #107, #146, #147, #150, #151, #154, #155, #162, #163, #166, #167, #170 and #171. These rules are all listed in the complete rule base given in Appendix 3. Based on the individual matching belief degrees, the activation weight θ_k ($k = 1, \ldots, 36$) of each rule in the fired sub-rule base is calculated using Equation (5.5). The fuzzy rule expression matrix for the sub-rule base with the employed 36 rules is shown in Table 5.4.

Table 5.4. The fuzzy rule expression matrix of the *EXT-CHA* risk analysis

Rule No	Antecedent attribute (input)					Safety estimate (output)			
	W	D	R	D	θ	Poor	Fair	Average	Good
18	Very weak	Moderate	Easy	Average	0.000084			0.5	0.5
19	Very weak	Moderate	Easy	Likely	0.001116			0.55	0.45
22	Very weak	Moderate	Average	Average	0.001148			0.7	0.3
23	Very weak	Moderate	Average	Likely	0.015252			0.75	0.25
26	Very weak	Moderate	Difficult	Average	0.000168			0.75	0.25
27	Very weak	Moderate	Difficult	Likely	0.002232			0.8	0.2
34	Very weak	Critical	Easy	Average	0.000084		0.2	0.7	0.1
35	Very weak	Critical	Easy	Likely	0.001116		0.35	0.65	
38	Very weak	Critical	Average	Average	0.001148		0.3	0.7	
39	Very weak	Critical	Average	Likely	0.015252		0.5	0.5	
42	Very weak	Critical	Difficult	Average	0.000168		0.5	0.5	
43	Very weak	Critical	Difficult	Likely	0.002232		0.6	0.4	
82	Weak	Moderate	Easy	Average	0.002016			0.6	0.4
83	Weak	Moderate	Easy	Likely	0.026784			0.75	0.25
86	Weak	Moderate	Average	Average	0.027552			0.8	0.2
87	Weak	Moderate	Average	Likely	0.366048			0.9	0.1
90	Weak	Moderate	Difficult	Average	0.004032			0.9	0.1
91	Weak	Moderate	Difficult	Likely	0.053568			1	
98	Weak	Critical	Easy	Average	0.002016		0.2	0.8	
99	Weak	Critical	Easy	Likely	0.026784		0.4	0.6	
102	Weak	Critical	Average	Average	0.027552		0.25	0.75	
103	Weak	Critical	Average	Likely	0.366048		0.45	0.55	
106	Weak	Critical	Difficult	Average	0.004032		0.5	0.5	
107	Weak	Critical	Difficult	Likely	0.053568		0.6	0.4	
146	Average	Moderate	Easy	Average	0.000084			0.9	0.1
147	Average	Moderate	Easy	Likely	0.001116		0.05	0.95	
150	Average	Moderate	Average	Average	0.001148			1	
151	Average	Moderate	Average	Likely	0.015252		0.1	0.9	
154	Average	Moderate	Difficult	Average	0.000168		0.1	0.9	
155	Average	Moderate	Difficult	Likely	0.002232		0.25	0.75	
162	Average	Critical	Easy	Average	0.000084		0.35	0.55	0.1
163	Average	Critical	Easy	Likely	0.001116		0.55	0.35	0.1
166	Average	Critical	Average	Average	0.001148		0.3	0.7	
167	Average	Critical	Average	Likely	0.015252		0.5	0.5	
170	Average	Critical	Difficult	Average	0.000168		0.5	0.5	
171	Average	Critical	Difficult	Likely	0.002232		0.7	0.3	

In Table 5.4, the *ER* approach is used to implement the combination of the 36 rules and generate the safety estimate of the EXT-CHA threat. The final assessment result can be computed as follows and is shown in Figure 5.9.

The prior SE of the EXT-CHA threat: {0, "Poor", 0.1884, "Fair", 0.7706, "Average", 0.0410, "Good"}

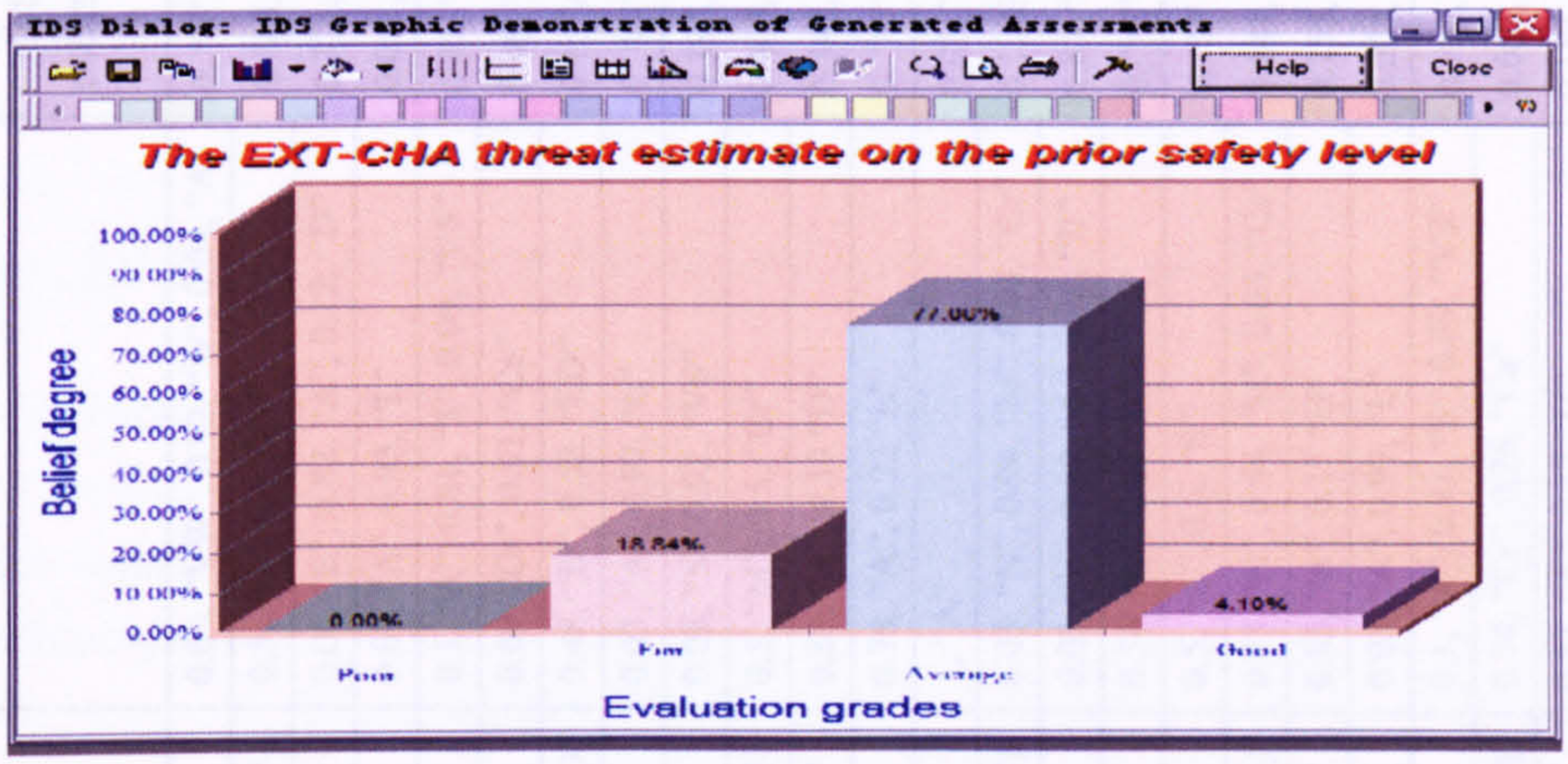


Figure 5.9. The safety estimate of the *EXT-CHA* threat

This result can be interpreted in such a way that the safety estimate of the EXT-CHA threat is "Poor" with a belief degree of 0, "Fair" with a belief degree of 0.188, "Average" with a belief degree of 0.771, and "Good" with a belief degree of 0.041.

Next, Equation (5.7) can be used to calculate the index value of the safety estimate obtained for a ranking purpose as follows:

$$N_v = 0 \times 0 + 0.1884 \times 0.3125 + 0.7706 \times 0.5926 + 0.0410 \times 1 = 0.5566$$

Similar computations are performed for the other five basic events in Figure 4.4. The safety estimates generated for the VES-CHA, CARGO, EMPLOYEE, EXT-TER and VES-TER threats are summarised in Table 5.5. Since the *FRB-ER* and discrete fuzzy set approaches have the same fuzzy input (subjective judgements), the fuzzy output should be kept in harmony to a significant extent in order to validate the reliability of the two different inference engines. The results have shown that the six basic events have been assessed with defuzzified values and ranked in a quite similar order compared to the results obtained in Section 4.4.1. The slight output difference in terms of defuzzified values and ranking order is partly because of the applications of different defuzzification methods and partly due to the accuracy of entirely subjective belief degree distributions in the rule bases*.

* More details about belief assignment will be addressed in Chapter 6.

Table 5.5. Risk analysis and ranking of the basic events

Events	Junior safety para-meters	E # 1	E # 2	E # 3	E # 4	Synthesised fuzzy input	Senior safety estimates	Ranking (defuzz-ified values)
EXT-CHA	***W***	1, "W"	(0.1, 0.3, 0.5)	[0.2, 0.4]	0.3	0.04, "VW", 0.92, "W", 0.04, "A"	0, "P", 0.188, "F", 0.771, "A", 0.041, "G"	0.557 **6**
	D	(0.3, 0.5, 0.7)	0.5, "M", 0.5, "Cr"	[0.4, 0.6]	{0.3, 0.4, 0.6, 0.7}	0.5, "M", 0.5, "Cr"		
	R	{0.3, 0.4, 0.6, 0.7}	(0.3, 0.5, 0.7)	[0.4, 0.6]	1, "A"	0.06, "E", 0.82, "A", 0.12, "D"		
	P	1, "L"	{0.5, 0.6, 0.8, 0.9}	[0.6, 0.8]	(0.7, 0.8, 0.9)	0.07, "A", 0.93, "L"		
VES-CHA	***W***	1, "S"	(0.5, 0.7, 0.9)	{0.5, 0.7, 0.8, 0.9}	0.7	0.1, "A", 0.81, "S", 0.09, "VS"	0.42, "P", 0.48, "F", 0.1, "A", 0, "G"	0.21 **1**
	D	(0.7, 0.9, 1)	1, "Ca"	[0.8, 1]	{0.8, 0.9, 1, 1}	0.09, "Cr", 0.91, "Ca"		
	R	{0.7. 0.8, 0.9, 1}	(0.7, 0.8, 1)	[0.7, 0.9]	0.5,"D",0.5, "ED"	0.48, "D", 0.52, "ED"		
	P	1, "L"	{0.6, 0.7, 0.8, 0.9}	[0.75, 0.85]	(0.7, 0.8, 0.9)	0.03, "A", 0.97, "L"		
CAR GO	***W***	1, "VS"	(0.8, 1, 1)	{0.8, 0.9, 1, 1}	1	0.08, "S", 0.92, "VS"	0.195, "P", 0.463, "F", 0.342, "A", 0, "G"	0.347 **3**
	D	(0.3, 0.5, 0.7)	0.5, "M", 0.5, "Cr"	[0.4, 0.6]	{0.3, 0.4, 0.6, 0.7}	0.5, "M", 0.5, "Cr"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	0.7, "A", 0.3 "L"	{0.3, 0.4, 0.5, 0.6}	0.55	(0.4, 0.5, 0.6)	0.78, "A", 0.22 "L"		
EMPL OYEE	***W***	1, "A"	[0.45, 0.55]	0.5	1, "A"	1, "A"	0.03, "P", 0.1, "F", 0.87, "A", 0, "G"	0.492 **4**
	D	(0.3, 0.35, 0.4)	1, "M"	[0.3, 0.4]	{0.2, 0.3, 0.4, 0.5}	0.03, "N", 0.94, "M", 0.03, "Cr"		
	R	{0.3, 0.4, 0.5, 0.6}	(0.4, 0.5, 0.6)	[0.4, 0.6]	1, "A"	0.03, "E", 0.89, "A", 0.08, "D"		
	P	0.5, "L", 0.5 "D"	{0.7, 0.8, 0.9, 1}	[0.8, 1]	(0.8, 0.9, 1)	0.56, "L", 0.44 "D"		
EXT-TER	***W***	0.5, "A", 0.5, "S"	(0.5, 0.6, 0.7)	[0.5, 0.7]	0.6	0.5, "A", 0.5, "S"	0, "P" 0.241, "F", 0.755, "A", 0.004, "G",	0.527 **5**
	D	(0.3, 0.35, 0.4)	1, "M"	[0.3, 0.4]	{0.2, 0.3, 0.4, 0.5}	0.03, "N", 0.94, "M", 0.03, "Cr"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	1, "L"	{0.6, 0.7, 0.8, 0.9}	[0.75, 0.85]	(0.7, 0.8, 0.9)	0.03, "A", 0.97, "L"		
VES-TER	***W***	1, "S"	(0.5, 0.7, 0.9)	{0.5, 0.7, 0.8, 0.9}	0.7	0.1, "A", 0.81, "S", 0.09, "VS"	0.151, "P", 0.665, "F", 0.184, "A", 0, "G"	0.317 **2**
	D	(0.6, 0.7, 0.8)	0.7, "Cr", 0.3 "Ca"	0.75	{0.6, 0.7, 0.8, 0.9}	0.74, "Cr", 0.26, "Ca"		
	R	{0.4, 0.5, 0.6, 0.7}	(0.4, 0.5, 0.6)	[0.4, 0.6]	0.8, "A", 0.2 "D"	0.83, "A", 0.17 "D"		
	P	0.5, "L", 0.5 "D"	{0.7, 0.8, 0.9, 1}	[0.8, 1]	(0.8, 0.9, 1)	0.56, "L", 0.44 "D"		

The *ER* approach can be used not only to aggregate fuzzy rules for the safety estimation of the basic events in the *FRB-ER* framework but also to assess the safety of the whole system (top level event) as well. According to the rule introduced in Section 3.2.3 and Table 4.8, the weights of the basic events can be appropriately distributed and obtained. Consequently the prior safety estimate of the top level event can be calculated by synthesising all fuzzy input of the basic events in Table 5.5 with their individual weights as follows:

The prior SE of the threat of terrorist attacking the port: {0.12, "Poor", 0.371, "Fair", 0.501, "Average", 0.008, "Good"}

5.4.2 Making Safety-Based Decision Making and Selecting the Best RCO

The *FRB-ER* approach contributes itself to the subjective safety assessment and also exposes its weaknesses such as the complexity of inference. When more elements require to be considered in a wider context such as the safety-based *MADM*, the *FLB-ER* approach proposed in Section 5.3 can be used.

In this example, suppose there are four criteria chosen to decide the preference of the four *RCOs*. They are separately Safety Change (SC), Cost (C), Technique Requirement (TR) and Implement Time (IT). Some criteria have their sub-criteria. For example, the prior and posterior safety estimations are developed as the two sub-criteria of SC, to demonstrate the safety level changes after the implement of the *RCOs* (i.e. the prior safety estimation with a high level "Good" indicates that SC will have a large extent evaluated as "Small" and furthermore, *RCOs* will be assessed as "Slightly Preferred" with a high belief degree). Such a hierarchy can be constructed in Figure 5.10.

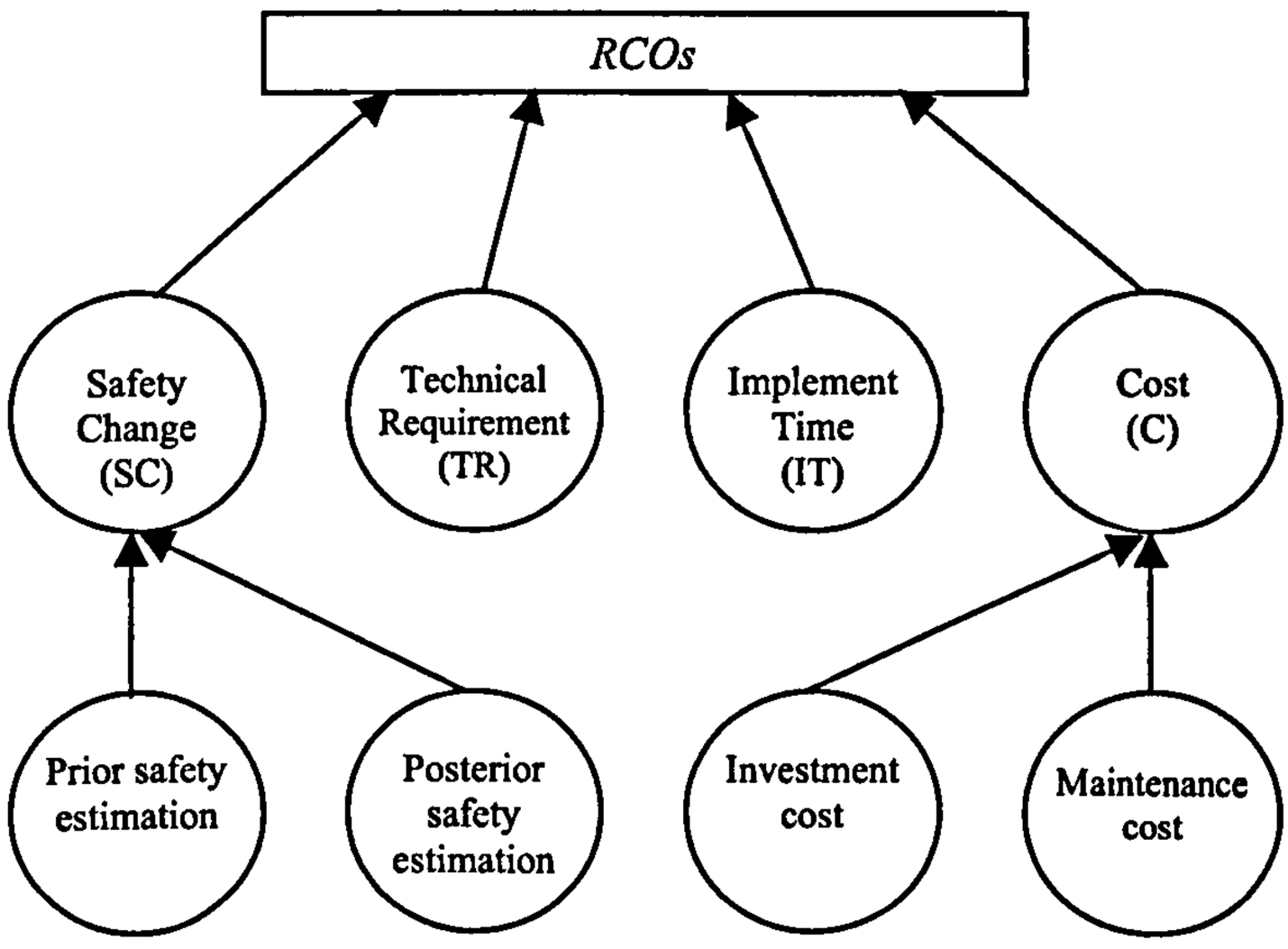


Figure 5.10. The hierarchy of safety based decision making

Suppose the four safety analysts make their judgments on the lowest level criteria, which have been synthesised using the *ER* approach and shown in Table 5.6. Note that the judgements associated with the posterior safety estimates are obtained using the *FRB-ER* approach in a similar way in which the prior safety estimates are calculated. The linguistic terms used to express TR and IT are separately the sets of ("Very high(VH)", "High(H)", "Average(A)", "Low(L)", "Very low(VL)") and ("Very long(VL)", "Long(L)", "Average(A)", "Short(S)").

Table 5.6. The decision making attribute assessments

Lowest level criteria	*RCO*#1	*RCO*#2	*RCO*#3	*RCO*#4
Prior safety estimate	0.008, "G", 0.501, "A", 0.371, "F", 0.12, "P"	0.008, "G", 0.501, "A", 0.371, "F", 0.12, "P"	0.008, "G", 0.501, "A", 0.371, "F", 0.12, "P"	0.008, "G", 0.501, "A", 0.371, "F", 0.12, "P"
Posterior safety estimate	0, "P", 0.221, "F", 0.236, "A", 0.543, "G"	0, "P", 0.033, "F", 0.247, "A", 0.72, "G"	0.04, "P", 0.288, "F", 0.433, "A", 0.239, "G"	0.012, "P", 0.35, "F", 0.534, "A", 0.104, "G"
Technical requirement	0, "VH", 02, "H", 0.5, "A", 0.3, "L", 0, "VL"	0, "VH", 0.7, "H", 0.3, "A", 0, "L", 0, "VL"	0, "VH", 0, "H", 0, "A", 0, "L", 1, "VL"	0, "VH", 0, "H", 0, "A", 0.2, "L", 0.8, "VL"
Implement time	0.9 "VL", 0.1, "L", 0, "A", 0, "S"	0, "VL", 0.4, "L", 0.6, "A", 0, "S"	0, "VL", 0, "L", 0.2, "A", 0.8, "S"	0, "VL", 0, "L", 0, "A", 1, "S"
Investment cost	0, "S", 0.75, "La", 0.25, "M", 0, "Li"	0.4, "S", 0.6, "La", 0, "M", 0, "Li"	0, "S", 0.2, "La", 0.7, "M", 0.1, "Li"	0, "S", 0, "La", 0, "M", 1, "Li"
Maintenance cost	0, "E", 0, "R", 0.9, "M", 0.1, "N"	0.2, "E", 0.8, "R", 0, "M", 0, "N"	0, "E", 0.45, "R", 0.55, "M", 0, "N"	0, "E", 0, "R", 0.25, "M", 0.75, "N"

In order to obtain the best *RCO*, the judgements and estimates associated with each *RCO* require to be considered, combined and then defuzzified. However, as the fuzzy sets used to describe the judgements are defined on the basis of different universes, it may not be convenient to directly implement such a synthesis using the *ER* approach. It will be desirable that the *FLB-ER* approach can be used to carry out a unification of the different decision making attribute estimates in order to avoid loss of useful information. Next, using the transforming graphic technique introduced in Figure 5.8 and Equation (5.8), the judgements listed in Table 5.6 can be transformed and expressed on a unified space, the preference of decision makers, as shown in Table 5.7.

Suppose the weights of decision making attributes and sub-criteria have been distributed in Table 5.8 by the four experts using the *AHP* method and Equation (5.9). Although the attributes SC, TR, IT and C have been given the same weights here, it can be noted that different weights can be judged and assigned according to various decision making requirements in practice. Then, the judgements produced in Table 5.7 can be synthesised to obtain the utility description on the each *RCO* using the *IDS* software, which can be further defuzzified as a crisp value for ranking the *RCOs* using Equation (5.10) as follows:

The preference assessment of the *RCO*#1: P_1 = {0.21, "SP", 0.222, "MP", 0.273, "A", 0.194, "P", 0.101, "GP"} = 0.44

The preference assessment of the *RCO*#2: P_2 = {0.076, "SP", 0.373, "MP", 0.313, "A", 0.119, "P", 0.119, "GP"} = 0.471

The preference assessment of the *RCO*#3: P_3 = {0.009, "SP", 0.081, "MP", 0.265, "A", 0.131, "P", 0.514, "GP"} = 0.836

The preference assessment of the *RCO*#4: P_4 = {0.002, "SP", 0.058, "MP", 0.113, "A", 0.106, "P", 0.721, "GP"} = 0.969

Table 5.7. The unified decision making attribute assessments

Lowest level criteria	*RCO*#1	*RCO*#2	*RCO*#3	*RCO*#4
Prior safety estimate	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"	0.008, "SP", 0.375, "MP", 0.311, "A", 0.21, "P", 0.096, "GP"
Posterior safety estimate	0, "SP", 0.177, "MP", 0.257, "A", 0.159, "P", 0.407,"GP"	0, "SP", 0.026, "MP", 0.229, "A", 0.205, "P", 0.54,"GP"	0.04, "SP", 0.23, "MP", 0.447, "A", 0.103, "P", 0.18, "GP"	0.012, "SP", 0.28, "MP", 0.551, "A", 0.079, "P", 0.078, "GP"
Technical requirement	0, "SP", 02, "MP", 0.5, "A", 0.3, "P", 0, "GP"	0, "SP", 0.7, "MP", 0.3, "A", 0, "P", 0, "GP"	0, "SP", 0, "MP", 0, "A", 0, "P", 1, "GP"	0, "SP", 0, "MP", 0, "A", 0.2, "P", 0.8, "GP"
Implement time	0.9, "SP", 0.08, "MP", 0.02, "A", 0, "P", 0, "GP"	0, "SP", 0.32, "MP", 0.38, "A", 0.3, "P", 0, "GP"	0, "SP", 0, "MP", 0.1, "A", 0.18, "P", 0.72, "GP"	0, "SP", 0, "MP", 0, "A", 0.1, "P", 0.9, "GP"
Investment cost	0, "SP", 0.6, "MP", 0.338, "A", 0.062, "P", 0, "GP"	0.4, "SP", 0.48, "MP", 0.12, "A", 0, "P", 0, "GP"	0, "SP", 0.16, "MP", 0.565, "A", 0.185, "P", 0.09, "GP"	0, "SP", 0, "MP", 0, "A", 0.1, "P", 0.9, "GP"
Maintenance cost	0, "SP", 0, "MP", 0.09, "A", 0.81, "P", 0.1, "GP"	0.2, "SP", 0.16, "MP", 0.64, "A", 0, "P", 0, "GP"	0, "SP", 0.09, "MP", 0.415, "A", 0.495, "P", 0, "GP"	0, "SP", 0, "MP", 0.025, "A", 0.225, "P", 0.75, "GP"

Table 5.8. The weights of decision making attributes

	Prior safety estimate	Posterior safety estimate	Technical requirement	Implement time	Investment cost	Maintenance cost
Weight ratio	0.1	0.9	1	1	0.6	0.4
Normalised weights	0.025	0.225	0.25	0.25	0.15	0.1

It can be noted that in this case, *RCO*#4 is ranked first, *RCO*#3 second, *RCO*#2 third and *RCO*#1 last. This implies that safety and other decision making attributes are considered equally important while carrying out the risk control evaluation, the best selection is *RCO*#4. When the relative importance of safety against other attributes changes, there may be different ranking orders of the *RCOs*. Figure 5.11 shows the preference degrees associated with the four *RCOs* at different values of relative importance of safety and the other attributes (TR, IT, C). For example, when the relative importance of safety against the other attributes increases by 400%, the ranking of the four *RCOs* is SCO#2>SCO#4> SCO#3>SCO#1.

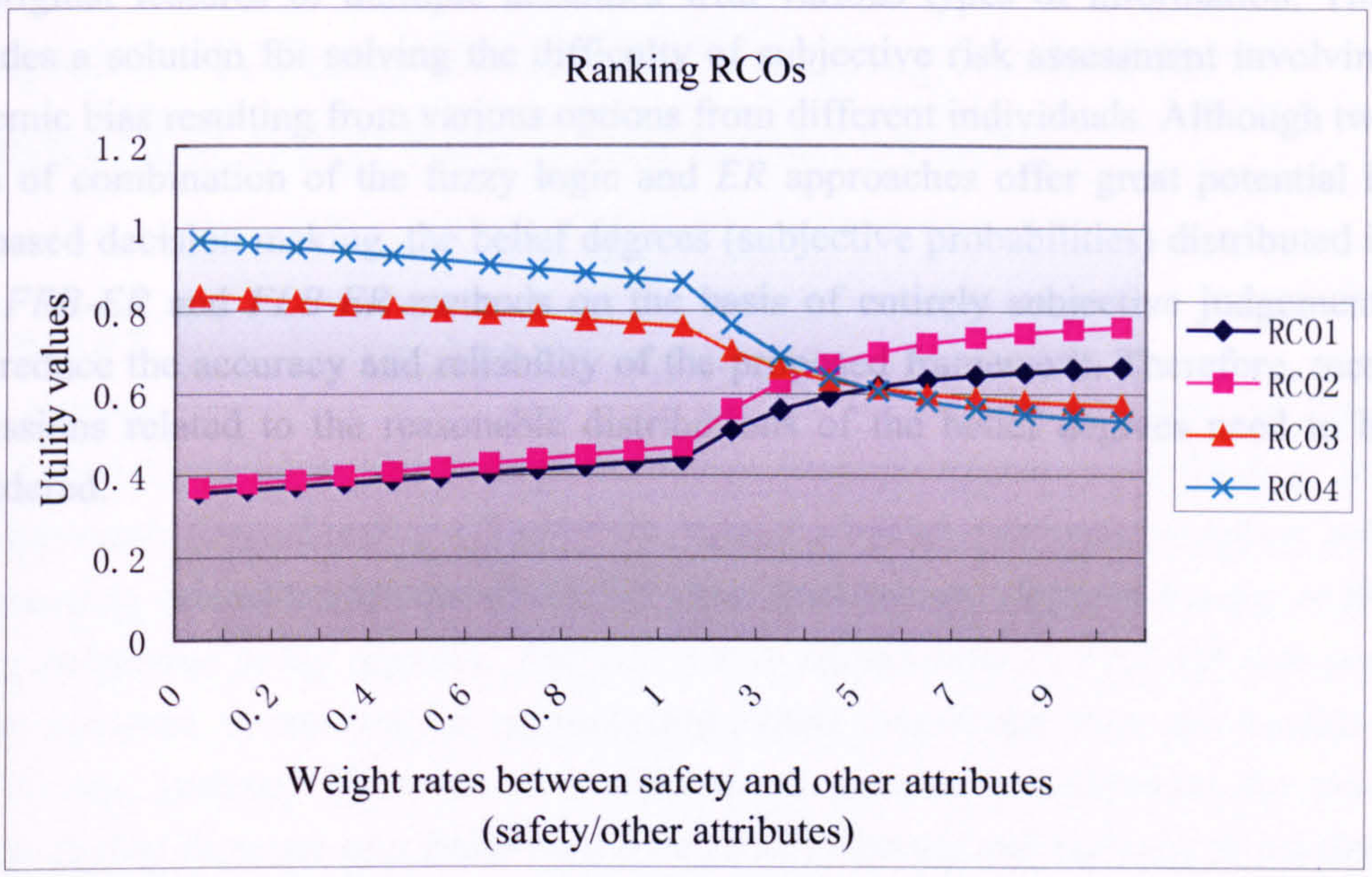


Figure 5.11. Ranking of the *RCOs*

5.5. Conclusion

This chapter outlines and explains a philosophy of subjective risk based decision making modelling for *CSC* risk control and management using fuzzy logic and *ER* approaches. For each *RCO*, the prior and posterior safety estimates of each basic event are first carried out using the risk analysis model based on the application of the *FRB-ER* approach. Then the *ER* approach is used to synthesise the prior/posterior safety estimates to obtain the safety estimates of the top level event as the safety attributes of the *RCOs*. Finally, the synthesis of safety and other decision making attributes are performed using *MADM* modelling based on a *FLB-ER* approach and mapped onto a common utility space before proceeding to the preference estimation and ranking of *RCOs*.

Different from most conventional risk based decision making methodologies, the framework introduced is characterised with a unique feature associated with unification of input and output data. In risk modelling, each input can be represented as a probability distribution on linguistic values for the antecedent using a belief structure. The main advantage of doing so is that precise data, random numbers and subjective judgements with uncertainty can be consistently modelled under a unified form. In decision making modelling, the input data transformed by the linked belief structures can be unified and take into account subjective experts judgements with uncertainties having both probabilistic and possibilistic nature. Moreover, the *ER* approach provides a novel procedure for aggregating calculation, which can preserve

the original features of multiple attributes with various types of information. This provides a solution for solving the difficulty of subjective risk assessment involving academic bias resulting from various options from different individuals. Although two kinds of combination of the fuzzy logic and *ER* approaches offer great potential in risk based decision making, the belief degrees (subjective probabilities) distributed in both *FRB-ER* and *FLB-ER* methods on the basis of entirely subjective judgements may reduce the accuracy and reliability of the proposed framework. Therefore, more discussions related to the reasonable distributions of the belief degrees need to be considered.

Chapter 6 – A Fuzzy Evidential Reasoning Method for Constructing Belief Rule Based Expert Systems

SUMMARY

This chapter presents a novel and generic FER method for constructing belief rule based expert systems in risk assessment. It has been developed on the basis of the FRB-ER approach (introduced in Chapter 5), where a belief rule representation scheme is proposed to extend traditional IF-THEN rules and express the conclusions in the rules using subjective belief degrees. The belief rule expressions in FRB-ER can provide a better compact framework for representing expert knowledge than the traditional IF-THEN rule systems. However, it is difficult to accurately determine the parameter values (belief degrees) of a belief rule base (BRB) entirely subjectively, in particular for a large scale BRB with hundreds of rules. Furthermore, it is highly possible for many realistic risk based BRB systems to have different antecedent attribute weights and a change in an attribute weight may lead to significant changes in the performance of the BRB systems. As such, the new method is proposed for effectively dealing with the difference among the antecedent attribute weights and rationally producing and judging the belief degrees related to the conclusion parameters.

6.1 Introduction

The process of making cost-effective, timely and acceptable decisions associated with increasingly complex and large *CSC* systems has been the subject of considerable debate in recent years. It is due to the fact that modelling and analysing complex risk based decision problems increasingly needs to acquire the historical failure data/ information as sufficient and precise as possible and to train the decision makers' performance as skilful and knowledgeable as possible. However, in realistic *CSCs*, the risk based decision making is often associated with uncertainty. Little numerical data of any statistical significance may be available to support traditional "objective" decision analysis. For example, to analyse system safety in the design and operation of large *CSC* systems with a high level of innovation, it is highly possible that there is a lack of historical failure data. On the other hand, analytical techniques and scientific procedures that standardize a human being's performance should always be employed to support effective, consistent and informative decision making and avoid making costly inappropriate decisions.

In recognition of the need to handle the hybrid of both uncertain/incomplete input and effective decision analysis techniques, a novel rule based method designed on the basis of a belief structure, called *BRB*, has been researched previously. A *BRB* functions on

the solutions of the non-linear causal relationships as well as incompleteness and vagueness associated with risk parameters/decision attributes. It can be represented as a belief rule expression matrix, which forms a basis in the inference mechanism of *FRB-ER* and provides a framework for representing expert knowledge in a compact format (Yang *et al.*, 2006). The feature of the *BRBs* (the difference from the original *IF-THEN* rule bases) lies in the fact that the rules include various belief degrees (subjective probabilities) distributed into the multiple linguistic variables of the conclusion parameters. However, it is difficult to accurately determine such probabilities in a *BRB* entirely subjectively, in particular for a large scale scheme with hundreds of rules. The main reason is related to the confused situations resulting from the term of "subjective probabilities" (one should be very careful when such a term is used in a fuzzy expert system). It is almost impossible for different decision makers to provide exactly the same belief degrees when faced with one same antecedent input (with many various attributes) out of hundreds of rules. The result using a *BRB* (based on subjective probabilities) in a complex system may easily conflict with the principle* of using the fuzzy logic theory in rule based expert systems. Furthermore, a change in an attribute weight may lead to significant changes in the performance of the *BRB* systems. Thus, the relative importance among the antecedent attributes in the process of developing a rule representation should be appropriately considered.

In order to ensure appropriate and rational distributions of the subjective belief degrees, a generic *FER* method is proposed for logically constructing risk based *BRB* expert systems in this chapter. The new method is generated on the basis of the combination of several different theories and techniques, such as the fuzzy logic theory (Zadeh, 1965), an *AHP* (Saaty, 1980) technique and the *ER* approach (Yang and Singh, 1994; Yang and Xu, 2002), etc. The main feature of the new method is to consider the conditional belief degree distributions of the conclusion parameters given the individual antecedent attribute in a *BRB* as the conditions and then synthesise all conditional belief degree distributions using the *ER* approach. In this process, all antecedent attribute weights can be obtained using an *AHP* technique. Also, using a transforming function based on the fuzzy logic theory, input information (antecedent attributes) in a belief rule representation can be skilfully mapped onto the output (conclusion parameters). The method makes the process of judging subjective belief degrees more objective and moves the subjective judgements to the earliest stage of inference. The method can be therefore used to train a *BRB* whose internal structure is decided by experts' knowledge in a meaningful and consistent way, thereby facilitating the construction of *BRB* systems. Contributions drawn from such a generic method are examined by a numerical study associated with risk estimation.

---

* The nature of the principle is to avoid using point estimations in dealing with imprecision.

The remaining part of this chapter is organised as follows. In the subsequent section, a generic *BRB* representation scheme is reviewed and introduced. The methodology for developing the *FER* method and distributing subjective belief degrees is presented in Section 6.3. Section 6.4 presents a risk related numerical case study to illustrate the methodology. The chapter is concluded in Section 6.5.

6.2. *BRB* Expert System Structure and Representation

The generic structure and representation of *BRBs* are summarized in this section. More details have been introduced in Chapter 5 (which however only focuses on the application of *BRB* in the *CSC* risk assessment) and the work by Liu *et al.* (2005) from a general decision making viewpoint. The starting point for constructing a rule based system is to collect fuzzy *IF-THEN* rules from human experts. A knowledge base and an inference engine are then designed to infer useful conclusions from rules and observation facts provided by decision makers. This section concentrates mostly on the collection of the *IF-THEN* rules and the generation of the knowledge base, in part because they are the relatively unsatisfactorily developed in the literature.

A *FRB* model can be established to deal with imprecision using linguistic assessments instead of numerical values. Fuzzy logic approaches (Zadeh, 1965) employing fuzzy *IF-THEN* rules where the antecedent and conclusion parts contain linguistic variables (Zimmerman, 1991), can model the qualitative aspects of human knowledge and reasoning process without employing precise quantitative analysis. The model can be formally represented as follows:

$$R = \langle X, A, D, F, w \rangle$$

where $X=\{X_i,\ i=1,\ ...,\ M\}$ is the set of antecedent attributes, with each of them taking values from an array of fuzzy sets $A=\{A_1, A_2, ..., A_M\}$. A_i represents a set of fuzzy values (linguistic variables) used to describe the attribute X_i ($i=1, ..., M$). The array $\{X_1, X_2, ..., X_M\}$ defines a list of finite conditions, representing the elementary states of a decision problem domain, which may usually be linked by the "*AND*" connective. $D=\{D_j,\ j=1, ..., N\}$ is the set of all consequences, which can be conclusions or actions, representing a utility decision space. F is a logical function, representing the relationship between conditions and their associated conclusions. $w=\{w_i,\ i=1, ..., M\}$ is the set of antecedent attribute weights, which has actually been subjectively incorporated into F in the process of developing a classical fuzzy *IF-THEN* rule base. More specifically, the k^{th} rule in a conventional *IF-THEN* rule base can be written as:

$$R_k\text{: IF } A_1^k \text{ and } A_2^k \text{ and } \ldots \text{ and } A_M^k, \text{ THEN } D_k \qquad (6.1)$$

where A_i^k ($\in A_i,\ i=1,...M$) is the fuzzy value of i^{th} antecedent attribute X_i used in the k^{th}

rule and D_k ($\in D$) is the consequence in the k^{th} rule expressed by one single linguistic variable.

A basic rule base is composed of a collection of such simple *IF-THEN* rules. To take into account a belief degree (β) distribution in a conclusion, attribute weights (ω_i) and a rule weight (θ), a simple *IF-THEN* rule is extended to a belief rule with all possible consequences associated with belief degrees. A collection of belief rules consists of a *BRB* defined as follows (Yang, *et al.*, 2006):

$$R_k\text{: IF } A_1^k \text{ and } A_2^k \text{ and } \ldots \text{ and } A_M^k, \text{ THEN } \{(\beta_1^k, D_1), (\beta_2^k, D_2), \ldots, (\beta_N^k, D_N)\}$$

$$(\sum_{i=1}^{N} \beta_i^k \le 1), \text{ with a rule weight } \theta_k \text{ and attribute weights } w_1^k, \ldots, w_M^k, k \in \{1, \ldots, L\} \tag{6.2}$$

where β_j^k ($j \in \{1, \ldots, N\}$) is the belief degree to which D_j is believed to be the consequence if in the k^{th} rule the input satisfies the antecedent fuzzy value vector $A^k=\{A_1^k, A_2^k, \ldots, A_M^k\}$. It is also the main research target of this chapter. θ_k is the relative weight of the k^{th} rule and w_i^k ($i=1, \ldots, M$) are the relative weights of the antecedent attributes used in the k^{th} rule. L is the number of all belief rules used in the rule base. If ($\sum_{i=1}^{N} \beta_i^k = 1$), the k^{th} belief rule is said to be complete; otherwise, it is incomplete.

Suppose all L rules are independent of each other, which means that the antecedent fuzzy value vectors $A^1, A^2, \ldots, A^L$ are independent of each other. A *BRB* given by Equation (6.2) can then be extended using a belief rule expression matrix as shown in Table 6.1.

Table 6.1. Belief rule expression matrix for a *BRB*

Rule \ Belief degree / Consequence	Antecedent					D_1	...	D_j	...	D_N
1	A_1^1	A_2^1	...	A_M^1	θ_1	β_1^1	...	β_j^1	...	B_N^1
⋮	⋮	⋮	⋮	⋮	⋮					
K	A_1^k	A_2^k	...	A_M^k	θ_k	β_1^K	...	β_j^K	...	B_N^k
⋮	⋮	⋮	⋮	⋮	⋮					
L	A_1^L	A^L_2	...	A^L_M	θ_M	β_1^L	...	β_j^L	...	B_N^L

A *BRB* given in Equation (6.2) represents functional mappings between antecedents and conclusions possibly with uncertainty. It provides a more informative and realistic

scheme than a simple *IF-THEN* rule base for uncertain knowledge representation. However, it is noteworthy that *a)* the degree of belief (β) and the attribute weights (w) could be assigned initially by experts and *b)* the attribute weights (w) and the rule weight (θ) are only considered and activated when *BRB* systems are used to conduct inference and reasoning, and thus, have not been quantitatively and rationally incorporated into the assignment of belief degrees in the process of the generation of the knowledgeable *BRB*. Consequently, the *BRB* with the subjective belief degree distributions may easily be arguable and a new update and development towards more objective inference is desirable.

6.3. Using a *FER* Method to Develop A *BRB* Expert System

The proposed *FER* method consists of four major steps, which outline the necessary steps required for developing a risk based *BRB* expert system. Prior to the presentation of the *FER* methodology and how it actually assists in this process, it is worth making clear that *a)* the aim of the method is to construct a new risk based *BRB* rather than using a developed *BRB* expert system to conduct inference and reasoning, which has been well studied in Chapter 5, the work by Liu, *et al.* (2005) and Yang *et al.* (2006); and *b)* the focus is to make the process of distributing subjective belief degrees more objective. Having said that, the new risk based *BRB* expert system will be related to all the parameters described in Section 6.2 except θ, which is obviously used and activated in the inference process of using *BRB* expert systems. Consequently, the new risk based *BRB* model established on the basis of the *FER* method can be represented as follows:

$$R = \langle X, A, D, F, w, \beta \rangle$$

where all the symbols have the same meaning as indicated in Section 6.2. The methodology is therefore developed in the process of analysing such six parameters.

6.3.1 Define X and D and Assign w Using an AHP Technique

In making complex risk based decisions, a hierarchical structure is usually given to break down a decision problem into its elementary states. These elementary states may play different roles in making appropriate decisions and thus, require some quantified criteria to measure. The term "weights" is usually used to represent their relative importance. *AHP* can be used to obtain the relative weight of each attribute based on a pair-wise comparison matrix. It is a powerful and flexible decision making process to help set priorities and make the best decision when both qualitative and quantitative aspects of a decision need to be considered (Pillay and Wang, 2003a). By reducing complex decisions to a series of one-to-one comparisons then synthesising the results, *AHP* not only helps decision makers arrive at the best decision but also provides a clear

rational pathway that demonstrates the relationship between a problem domain and its elementary attributes. This is useful in describing the clusters (or levels of a decision analysis hierarchy) for effectively defining X and D in constructing *BRBs*. Considering that the size of the developed *BRB* expert systems will exponentially increase with the number of X, the definitions of X and D are strictly limited in the scope of two neighbouring levels (a defined branch (see Figure 6.1)) in a hierarchy. For example, taking the hierarchical structure presented in Figure 6.1 as an example, if X is defined as all attributes in Cluster 3 and D is defined as the attributes in Cluster 1, then the number of the rules in a *BRB* could arrive at 2^9 (even if every attribute has only two fuzzy numbers). However, if the X and D are defined in four individual branches in Figure 6.1 and *BRBs* are constructed on the basis of them, then the number of the rules included in the *BRBs* will be reduced from 2^9 to 2^5 ($2^3+2^3+2^3+2^3$). This requirement (the definition of X and D) shares the same philosophy as the divorcing method used to construct *BNs* (Jensen, 2001).

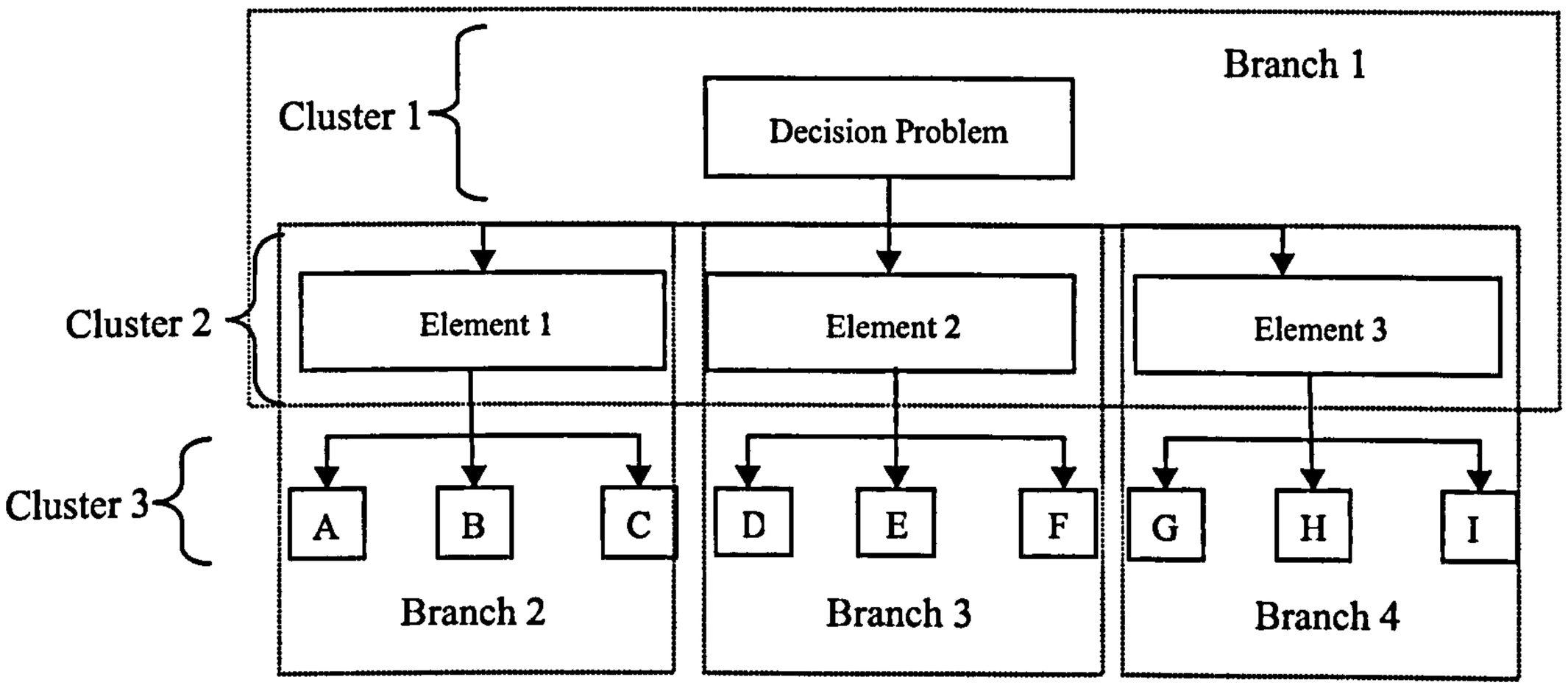


Figure 6.1. An example to illustrate the definition of X and D

Using an *AHP* technique to calculate the relative importance (w) of each attribute (X) requires a careful review of its principles and background (Saaty, 1987). When considering a group of attributes for evaluation, the main objectives of the technique are to provide judgements on the relative importance of these attributes and also to ensure that the judgements are quantified to an extent, which permits a quantitative interpretation of the judgement among these attributes (Pillay and Wang, 2003a).

The quantified judgements on pairs of attributes A_i and A_j are represented by an n-by-n matrix.

$$M = (a_{ij}), \text{ where } i, j = 1, 2, \ldots, n. \tag{6.3}$$

The entries a_{ij} are defined by the following entry rules:

Rule 1. If $a_{ij} = \alpha$, then $a_{ji} = 1/\alpha$, $\alpha \neq 0$.

Rule 2. If A_i is judged to be of equal relative importance as A_j, then $a_{ij} = a_{ji} = 1$.

Obviously $a_{ii} = 1$ for all i. Thus the matrix M has the following form:

$$M = \begin{bmatrix} 1 & a_{12} & ..... & a_{1n} \\ 1/a_{12} & 1 & ..... & a_{2n} \\ . & . & ..... & . \\ 1/a_{1n} & 1/a_{2n} & ..... & 1 \end{bmatrix} \tag{6.4}$$

where each a_{ij} is the relative importance of attribute A_i to attribute A_j. Having recorded the quantified judgements of comparisons on pair (A_i, A_j) as numerical entry a_{ij} in the matrix M, what is left is to assign to the n contingencies $A_1, A_2, A_3, ..., A_n$ a set of numerical weights $w_1, w_2, w_3, ..., w_n$ that should reflect the recorded judgements. One of the approximation calculation algorithms to get the weight of each factor in the pair-wise comparison process is mathematically described as follows (Pillay and Wang, 2003a):

$$w_1 = \frac{1}{n}\left[\left(\frac{a_{11}}{\sum_{i=1}^{n} a_{i1}}\right) + \left(\frac{a_{12}}{\sum_{i=1}^{n} a_{i2}}\right) + ...\left(\frac{a_{1n}}{\sum_{i=1}^{n} a_{in}}\right)\right] \tag{6.5}$$

In general, weights $w_1, w_2, w_3, ..., w_n$ can be calculated using the following equation:

$$w_k = \frac{1}{n}\sum_{j=1}^{n}\left(\frac{a_{kj}}{\sum_{i=1}^{n} a_{ij}}\right) (k = 1, ... n) \tag{6.6}$$

where a_{ij} is the entry of row i and column j in a comparison matrix of order n.

The weight vector of the comparison matrix provides the priority ordering. However, it cannot ensure the consistency of the pair-wise judgements. Thus, *AHP* provides a measure of the consistency for the pair-wise comparisons by computing a consistency ratio*. This ratio is designed in such a way that a value greater than 0.10 indicates an inconsistency in the pair-wise judgements and the decision maker should review the pair-wise judgements before proceeding. Thus, if the consistency ratio is 0.10 or less, the consistency of the pair-wise comparisons is considered reasonable, and the *AHP* can continue with the computations of the weight vectors, (Andersen *et al.*, 2003).

6.3.2 Determine the Fuzzy Membership Functions of A and D Using the Fuzzy Delphi Method

After the hierarchical structures of decision problems are created, the next task is to

* An approximate approach of computing the ratio has been provided by Andersen *et al.* (2003).

measure the value of each elementary attribute. Due to the highly subjective nature and lack of information, it is usually difficult to measure these attributes precisely. A feasible and convenient way to describe the attributes is to use verbal expressions (i.e., linguistic variables). These linguistic variables can be further defined in terms of fuzzy membership functions. A fuzzy membership function is a curve that defines how each point in the input space is mapped onto a membership value between 0 and 1. An example is given to represent the membership function of a supposed elementary attribute with seven linguistic variables, as shown in Figure 6.2. Observing Figure 6.2, it can be obtained that *a)* a trapezoidal fuzzy number can be represented in the form of $\mu_i = (a_{i1}, a_{i2}, a_{i3}, a_{i4})$ $i = 1,3,5,7$, where a_{i1} denotes the lower bound, (a_{i2}, a_{i3}) denotes the most plausible rating and a_{i4} denotes the upper bound; *b)* a triangular fuzzy number is the special case of a corresponding trapezoidal fuzzy number, which can be explained in symbol as, $\mu_i = (a_{i1}, a_{i2}, a_{i3}, a_{i4})$, $a_{i2} = a_{i3}$, $i = 2,4,6$.

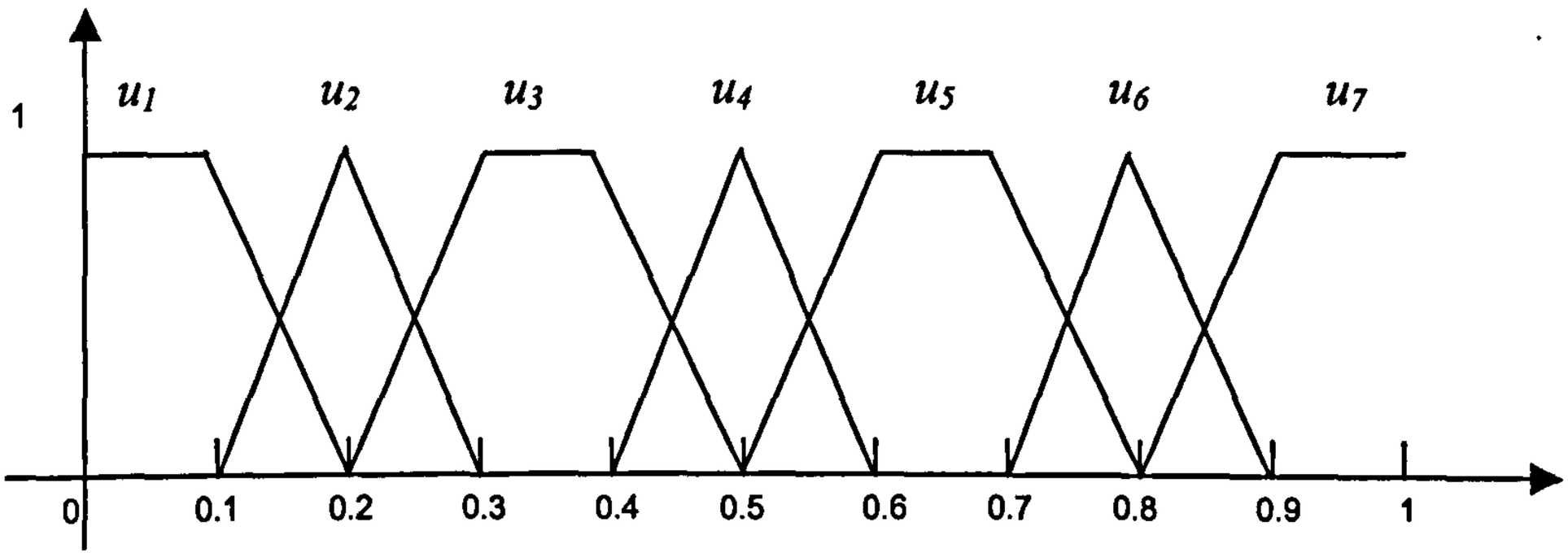


Figure 6.2. The membership functions of linguistic variables

Membership degrees (or fuzzy membership functions) of the elementary attributes of a decision problem can be assigned (subjectively decided) by multiple experts. The fuzzy Delphi method (Bojadziev and Bojadziev, 1995) can be employed in this process of achieving the consensus condition. Generally, the conclusion of a belief rule D may be described by linguistics variables and thus can also be defined in terms of trapezoidal/triangular fuzzy numbers using the same process.

6.3.3 Break Down F into F_i^* and Calculate the Conditional Subjective Belief Degrees β_i Given Individual Attribute A_i

After the fuzzy membership functions associated with all antecedent attributes A and decision conclusion D are obtained, the subjective belief degrees distributed on the

* F_i represents the logical relationship between the individual antecedent attribute and conclusion of a belief rule without knowing more information (other attributes).

conclusion can be theoretically assessed/calculated using the information of these attributes and a logical function F connecting the attributes and conclusion. However, in dealing with realistic decision problems, if too many antecedent attributes are considered as conditions, the corresponding subjective belief degree distributions on the conclusion may be too specific for any expert. Consequently, the assumptions, which reduce the amount of distributions to specify, are required to investigate. One effective simplifying assumption to deal with this situation is *a)* to break down F into F_i and calculate the conditional subjective belief degrees β_i given individual attribute A_i; and *b)* to consider each conditional subjective belief degree distribution as one piece of evidence to support decision conclusions and synthesise them using the *ER* approach. This section focuses on Step *a* and discusses how to transform the fuzzy membership functions into belief structures with the same set of fuzzy membership functions of a utility decision conclusion space. The next section will be associated with Step *b* and cope with the synthesis of the results obtained in Step *a*.

In order to evaluate β_i in terms of the linguistic variables presented in a conclusion, it is necessary to develop an effective method to infer F_i. From a generic viewpoint, F_i may be judged by experts using a rule base or utility base. For example, in the work by Wang *et al.* (1996), the fuzzy variables related to the attribute "safety" can well be mapped to a utility decision space, where each fuzzy variable can have its counterpart in the decision space based on an easily observed transforming function, such as "good" to "highly preferred" and "poor" to "slightly preferred", etc. However, in some specific cases (i.e. different amounts of linguistic variables involved), a new fuzzy mapping approach is proposed to complete this transformation and make the expert judgements more accurate. This mirrors the normalisation process in traditional *MADM* methods to transform attributes to the same space to facilitate trade-off analysis among attributes.

Suppose the trapezoidal fuzzy numbers of D_j, ($j=1, \ldots, N$) are $u_{D1}, u_{D2}, \ldots, u_{DN}$, respectively. The similarity degrees between u_i and u_{Dj} can be calculated as follows (Li and Liao, 2005):

$$S(u_i,u_{Dj}) = \frac{\int_{-\infty}^{+\infty}\left(\min\{u_i(x),u_{Dj}(x)\}\right)\mathrm{dx}}{\int_{-\infty}^{\infty}u_i(x)\mathrm{dx}} \tag{6.7}$$

If two membership functions are the same, that is $u_i = u_{Dj}$, $S(u_i,u_{Dj}) = 1$. If two membership functions do not have any overlap, the similarity degree is zero. For other situations, the higher the percentage of the overlap, the higher the similarity degree.

After all the similarity degrees between u_i and u_{Dj} are computed, a similarity vector $F_i^{'}$ can be constructed as follows:

$$F_i^{'} = (S(u_i, u_{D1}), S(u_i, u_{D2}), ..., S(u_i, u_{DN})) \tag{6.8}$$

Furthermore, $S(u_i, u_{Dj})$ can be normalised by:

$$\beta_{ij} = \frac{S(u_i, u_{Dj})}{\sum_{j=1}^{N} S(u_i, u_{Dj})} \quad j = 1,2,...N \tag{6.9}$$

From Equations (6.7) – (6.9), it can be noted that the more similar u_i is to u_{Dj}, the closer A_i is to D_j and the bigger β_{ij} is and that the sum of β_{ij}, $j = 1,2,...N$ is equal to 1. Thus, β_{ij} may be viewed as a degree of confidence that A_i belongs to D_j. In this way, most fuzzy membership functions of the antecedent attributes can be transformed into the belief structures with the same fuzzy set of a utility decision conclusion space, which is expressed in the following form:

$$F_i = \{(\beta_{i1}, D_1), (\beta_{i2}, D_2), ..., (\beta_{iN}, D_N)\} \tag{6.10}$$

6.3.4 Synthesise the Conditional Subjective Belief Degrees to Form F and Obtain β

Having obtained all F_i, the next task is to calculate F and obtain β. Before that, decision makers may need to clearly know that any F_i represents multiple conditional belief rule expressions, because A_i used to describe one of elementary states X_i is represented using multiple linguistic terms with their fuzzy membership functions. When A_i is given a fixed fuzzy value, one corresponding belief rule expression is formed. Thus, it can be noted that the total number of F_i is decided by the number of the linguistic variables associated with A rather than the number of A. Furthermore, observing Equation (6.2) and Table (6.1), the principle of constructing a *BRB* is to require the comprehensive combination of the fuzzy values of different antecedent attributes. Consequently, to develop a *BRB* with logical β distributions is transferred to the problem of how to reasonably combine all F_i. The *ER* approach introduced in Chapter 3 can be effectively used to deal with such a combination. Using such an approach, together with the weights of all related attributes obtained from Section 6.3.1, the conclusion part (β) of each rule in the expression matrix can be easily obtained and the relationship between input and output (F) can be logically confirmed.

6.4. A Risk Based Numerical Case Study

The risk assessment of a *CSC* system is a typical multi-attribute decision making problem. In such an assessment process, there are multiple risk factors involved and the measures of some factors may possibly be vague due to the highly subjective nature and lack of past experience. Hence, it is difficult to use traditional *MADM* approaches to deal with such problems with uncertainty. In this respect, the combination of the *FRB* and *ER* approaches shows significant potential. Such a combination method has been widely used in the safety research associated with the marine and offshore industries (Sii and Wang, 2002; Pillay and Wang, 2003b; Liu *et al.*, 2005). However, in all related studies, the belief degrees of the output of the rules, either full or partial, are assigned on the basis of entirely subjective expert judgements. This may introduce bias to the studies and easily result in academic arguments. In this section, a decision support framework based on the *FER* method developed above is used for constructing a risk based *BRB* system and capturing non-linear relationships between risk parameters used to measure risk levels.

6.4.1 Identify Risk Parameters Affecting Risk Levels, Construct their Hierarchical Structure and Calculate their Relative Weights

The first step is to define all kinds of risk parameters that are used in developing a risk based *BRB*. There are many parameters that may affect risk levels, such as risk occurrence likelihood and consequence severity. Risk occurrence likelihood (L) describes the frequency of risk occurrence in the life span of a targeting *CSC* system. Consequence severity (C) represents the magnitude of possible loss when risk happens. After the study of traditional quantitative safety methods like *FMECA*, it can be seen that there is the third basic parameter -- failure consequence probability used in assessing risk levels. Failure consequence probability (E) refers to the probability that possible consequences happen given the occurrence of a failure event*. Since the risk levels are decided by three basic risk parameters simultaneously, their hierarchical structure can be simply considered as a single branch, which includes two clusters, a top parameter and three paralleling basic parameters. Consequently, the *AHP* method (Equations 6.4 - 6.6) can be used to calculate their relative weights (in an order of ω_L, ω_C, ω_E) as follows:

---

* Here, the purpose of using three new risk parameters (L, C, E) instead of the classical two (F, S) or four parameters (W, D, P, R) introduced previously to define the safety estimation of *CSC* systems is to compare the result obtained using the proposed framework in this chapter with those in the prior studies in a convenient and feasible manner.

$$M = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 1.98 \\ 0.5 & 0.505 & 1 \end{bmatrix}$$

$[\omega_L, \omega_C, \omega_E] = [0.4, 0.399, 0.201]$

6.4.2 Use the Fuzzy Delphi Method to Determine the Fuzzy Numbers of All Linguistic Terms Associated with Each Risk Parameter

After the hierarchical structure of risk parameters is created, the next task is to appropriately describe such parameters in order to measure their risk levels. Objective failure data has been widely used to describe these parameters in some traditional *QRA* approaches. However, such historical data is not always available, and its collection is time-consuming and expensive as well as depending on many uncertainties. Consequently, they may not be well suited to dealing with the situations of having a high level of uncertainty. One realistic way to cope with imprecision is to use linguistic assessments (Wang *et al.*, 1995 and 1996). In risk assessment, four to seven linguistic variables can be used to describe risk parameters. To estimate the risk occurrence likelihood, for example, one may often use such variables as "very low", "low", "reasonably low", "average", "reasonably frequent", "frequent" and "highly frequent"; to estimate the consequence severity, one may choose to use such linguistic terms as "negligible", "marginal", "moderate", "critical" and "catastrophic"; To estimate the failure consequence probability, one may use such variables as "highly unlikely", "unlikely", "reasonably unlikely", "likely", "reasonably likely", "highly likely" and "definite". An example of the definitions of the linguistic variables is given as a reference in Tables 6.2 – 6.4.

Table 6.2. Risk occurrence likelihood (Sii and Wang, 2002)

Rank	**Risk occurrence likelihood**	Meaning (generic marine system interpretation)
1,2,3	Very low	Failure is unlikely but possible during lifetime
4	Low	Likely to happen once during lifetime
5	Reasonably low	Between low and average
6	Average	Occasional failure
7	Reasonably frequent	Likely to occur from time to time
8,9	Frequent	Repeated failure
9,10	Highly frequent	Failure is almost inevitable or likely to exist repeatedly

Table 6.3. Consequence severity (Sii and Wang, 2002)

Rank	**Consequence severity**	Meaning (generic marine system interpretation)
1	Negligible	At most a single minor injury or unscheduled maintenance required (service and operations can continue)
2,3	Marginal	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	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 a period of no more than 4 hours.
7,8	Critical	Possible single death, probable multiple severe injuries or major system damage. Operations stopped.
9,10	Catastrophic	Possible multiple deaths, probable single death or total system loss. Very high severity ranking when a potential failure mode.

Table 6.4. Failure consequence probability (Sii and Wang, 2002)

Rank	**Failure consequence probability**	Meaning (generic marine system interpretation)
1	Highly unlikely	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	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	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	It is likely that consequences happen given that the failure events occur (a programme is not likely to detect a potential design or operation's procedural weakness).
6,7	Reasonably likely	It is reasonably likely that consequences occur given the occurrence of the failure events (i.e. exist from time to time on the system or during operations, possibly caused by a potential design or operation's procedural weakness).
8	Highly likely	It is highly likely that consequences occur given the occurrence of the failure events (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	Definitely	Possible consequences happen given the occurrence of a failure event (i.e. likely to exist repeatedly during operations due to an anticipated potential design and operation's procedural drawback).

These subjective linguistic variables can be further defined in terms of their fuzzy membership functions. Membership degrees of the three risk parameters can be assigned by experts using the fuzzy Delphi method (Equations (5.1) – (5.3)), with reference to Figures 6.3 – 6.5. The result is described in Table 6.5.

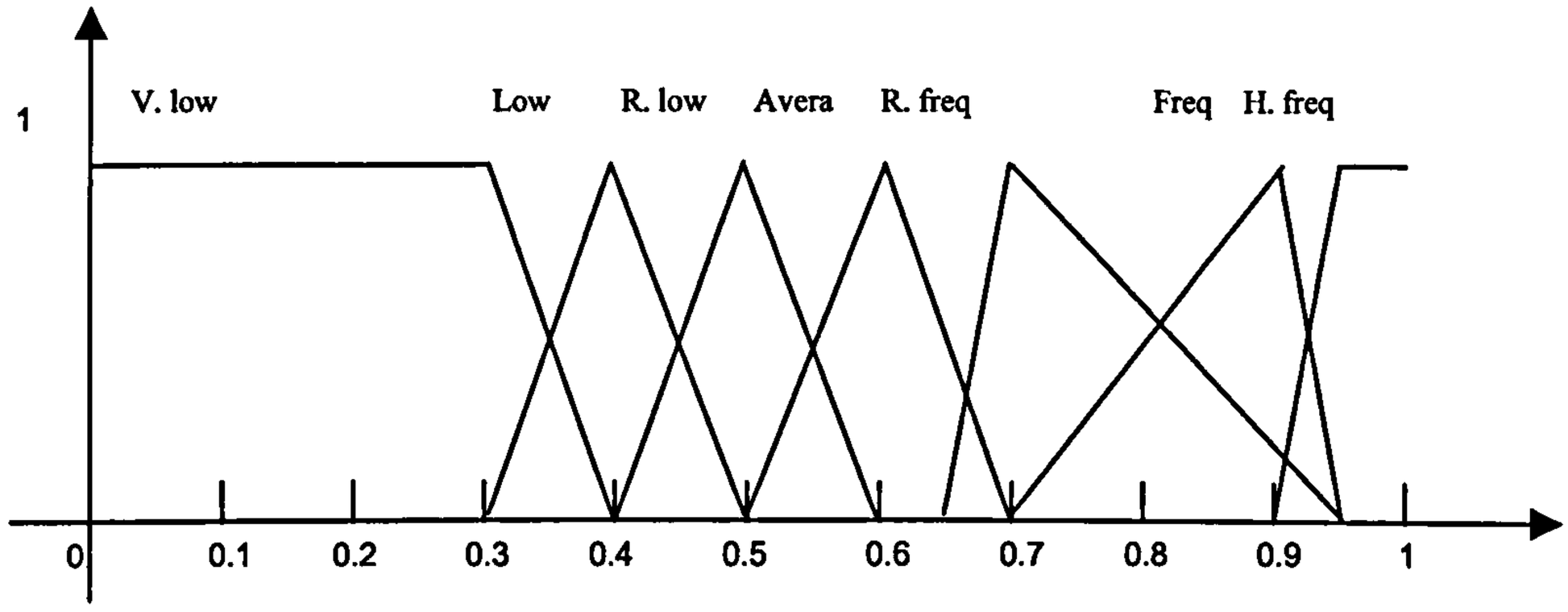


Figure 6.3. Fuzzy risk occurrence likelihood set definition (Sii and Wang, 2002)

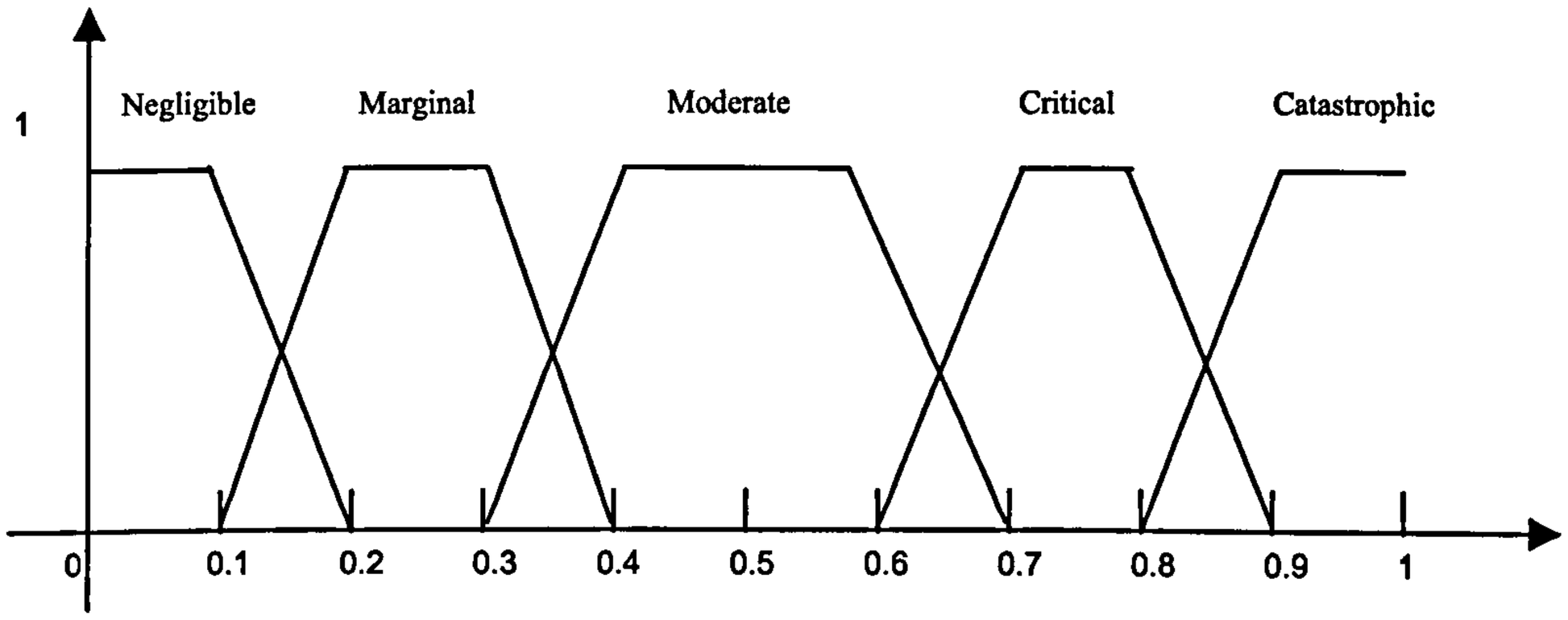


Figure 6.4. Fuzzy consequence severity set definition (Sii and Wang, 2002)

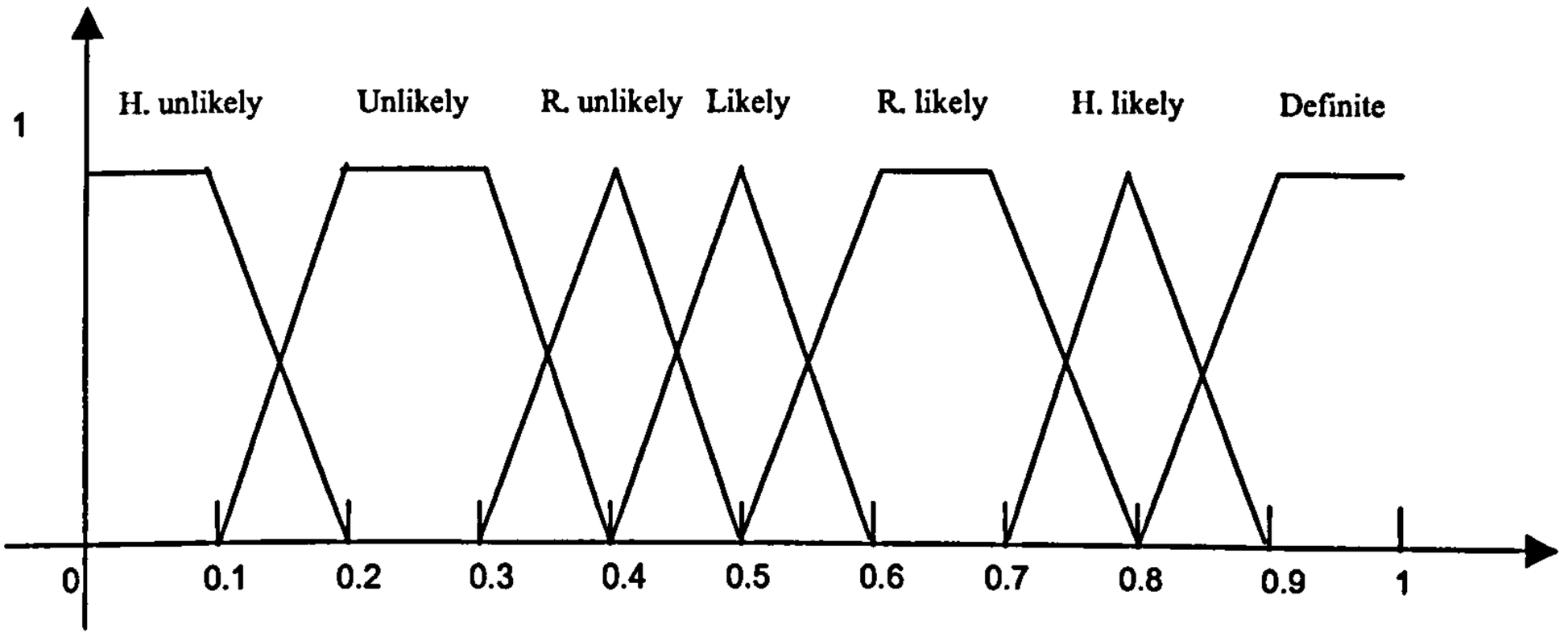


Figure 6.5. Fuzzy failure consequence probability set definition (Sii and Wang, 2002)

Table 6.5. Risk linguistic variables and their fuzzy membership functions

Risk occurrence likelihood	Membership function	**Consequence severity**	Membership function	**Failure consequence probability**	Membership function
Very low	L_1(0,0,0.1,0.2)	Negligible	C_1(0,0,0.1,0.2)	Highly unlikely	E_1(0,0,0.1,0.2)
Low	L_2(0.1,0.2,0.3,0.4)	Marginal	C_2(0.1,0.2,0.3,0.4)	Unlikely	E_2(0.1,0.2,0.3,0.4)
Reasonably low	L_3(0.3,0.4,0.4,0.5)	Moderate	C_3(0.3,0.4,0.6,0.7)	Reasonably unlikely	E_3(0.3,0.4,0.4,0.5)
Average	L_4(0.4,0.5,0.5,0.6)	Critical	C_4(0.6,0.7,0.8,0.9)	Likely	E_4(0.4,0.5,0.5,0.6)
Reasonably frequent	L_5(0.5,0.6,0.6,0.8)	Catastrophic	C_5(0.8,0.9,1,1)	Reasonably likely	E_5(0.5,0.6,0.7,0.8)
Frequent	L_6(0.6,0.8,0.8,0.9)			Highly likely	E_6(0.7,0.8,0.8,0.9)
Highly frequent	L_7(0.8,0.9,1,1)			Definitely	E_7(0.8,0.9,1,1)

In a similar way, the linguistic variables (D_j, j = 1, 2, 3, 4), "Good", "Average", "Fair" and "Poor", presenting risk levels and their fuzzy membership functions (μ_{Dj}, j = 1, 2, 3, 4) can be obtained and described in Figure 6.6, with reference to the work by Li and Liao (2005).

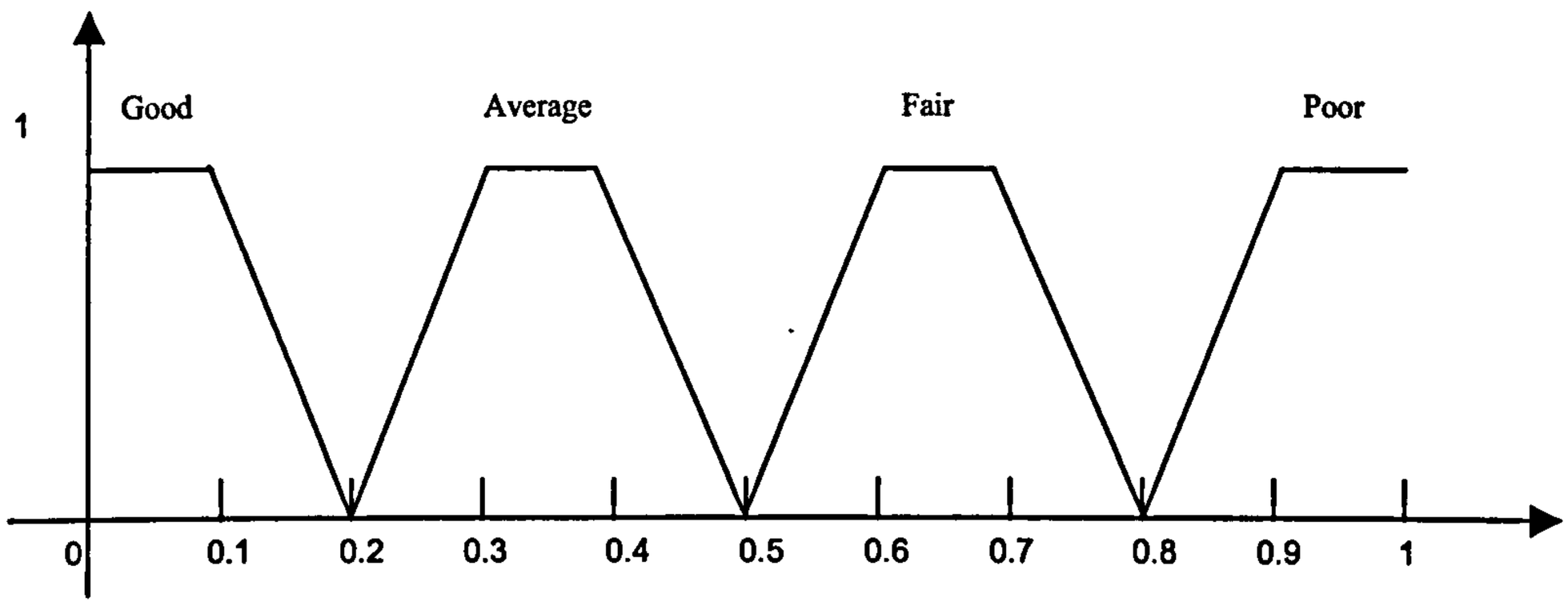


Figure 6.6. The membership functions of linguistic variables for risk levels

6.4.3 Transform the Fuzzy Sets of All Risk Parameters into Belief Structure with the Same Set of Risk Levels

After the fuzzy numbers of all linguistic variables associated with a risk parameter are acquired, the risk level of the parameter may be calculated using the information of these variables. Generally, the evaluation of the risk level may be conducted in a utility decision space, the sets described by the linguistic variables in Figure 6.6 in this case. Consequently, the conditional subjective belief degree distributions (the risk level expressions) given the fuzzy numbers (linguistic variables) of a risk parameter can be expressed as follows:

$$F_i = \{(\beta_{i1}, \text{“good”}), (\beta_{i2}, \text{“average”}), (\beta_{i3}, \text{“fair”}), (\beta_{i4}, \text{“poor”})\}$$

In order to evaluate F_i in terms of the four risk level linguistic variables, it is necessary to map the fuzzy numbers associated with the three basic risk parameters onto the risk level expressions. The approach to compute the fuzzy similarity functions between two fuzzy sets (Equations 6.7 and 6.8) enables this mapping. For example, the similarity degree between C_2 and μ_{Dj}, ($j = 1, 2, 3, 4$) (see Figure 6.7) is calculated as follows:

$$S(F_{C2}, u_{D1}) = \frac{Area1}{Area1 + Area2 + Area3} = 0.125$$

$$S(F_{C2}, u_{D2}) = \frac{Area2}{Area1 + Area2 + Area3} = 0.5$$

$$S(F_{C2}, u_{D3}) = \frac{0}{Area1 + Area2 + Area3} = 0$$

$$S(F_{C2}, u_{D4}) = \frac{0}{Area1 + Area2 + Area3} = 0$$

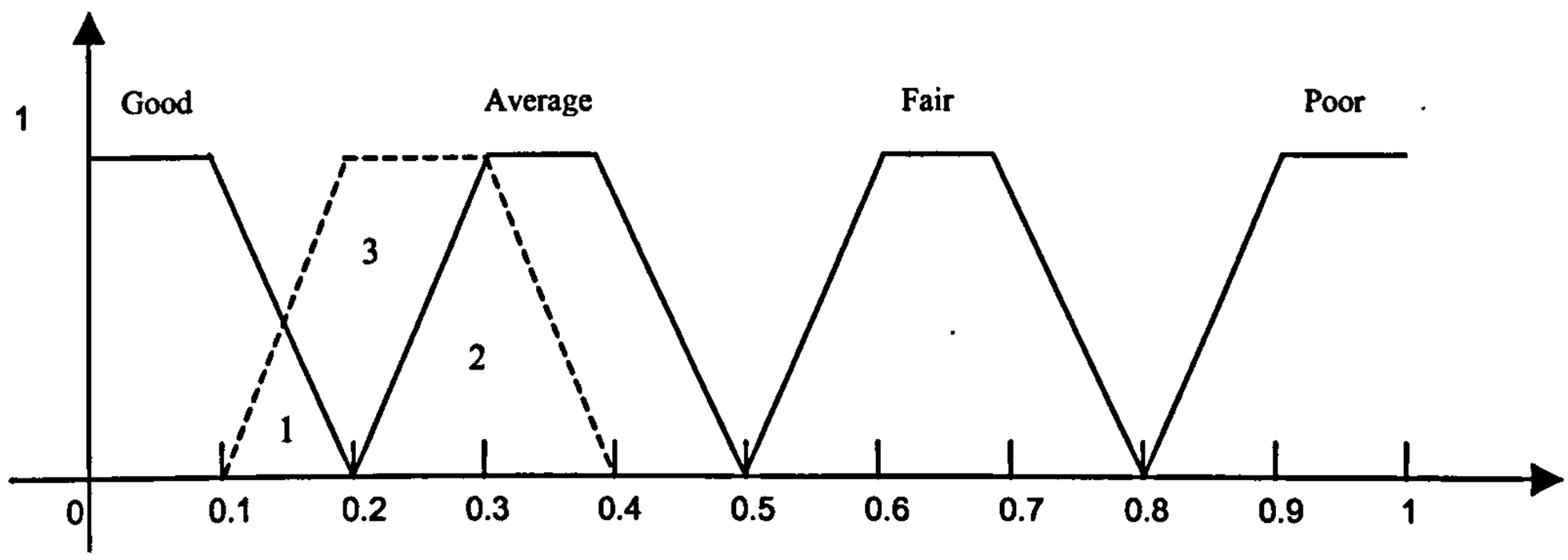


Figure 6.7. Example of the similarity degree between C_2 and μ_{Dj}, ($j = 1, 2, 3, 4$)

Furthermore, using Equation (6.9), $S(F_{C2}, u_{Dj})$ can be normalised as follows:

$$\beta_i^1 = \frac{S(F_{C2}, u_{D1})}{\sum_{j=1}^{4} S(F_{C2}, u_{Dj})} = \frac{0.125}{0.625} = 0.2$$

$$\beta_i^2 = \frac{S(F_{C2}, u_{D2})}{\sum_{j=1}^{4} S(F_{C2}, u_{Dj})} = \frac{0.5}{0.625} = 0.8$$

$$\beta_i^3 = \frac{S(F_{C2}, u_{D3})}{\sum_{j=1}^{4} S(F_{C2}, u_{Dj})} = \frac{0}{0.625} = 0$$

$$\beta_i^4 = \frac{S(F_{C2}, u_{D4})}{\sum_{j=1}^{4} S(F_{C2}, u_{Dj})} = \frac{0}{0.625} = 0$$

In this way, the fuzzy number C_2 can be transformed into the belief structure with the risk level expressions (D_j, $j = 1, 2, 3, 4$) and shown in the following form:

F_{C2} = {(0.2, "good"), (0.8, "average"), (0, "fair"), (0, "poor")}

where F_{C2} presents the conditional risk evaluation given that in three basic risk parameters, only consequence severity is known as "marginal" and no more information is available for the other two parameters.

Using a similar process, F_{Li} (i =1, 2, …, 7), F_{Cj} (j = 1, 2, …, 5), F_{Ek} (k = 1, 2, …, 7) can be obtained respectively in Table 6.6.

Table 6.6. The conditional risk evaluation given individual basic risk parameter

Condition	Conclusion
F_{L1}	{(1, "good"), (0, "average"), (0, "fair"), (0, "poor")}
F_{L2}	{(0.2, "good"), (0.8, "average"), (0, "fair"), (0, "poor")}
F_{L3}	{(0, "good"), (1, "average"), (0, "fair"), (0, "poor")}
F_{L4}	{(0, "good"), (0.5, "average"), (0.5, "fair"), (0, "poor")}
F_{L5}	{(0, "good"), (0, "average"), (1, "fair"), (0, "poor")}
F_{L6}	{(0, "good"), (0, "average"), (0.73, "fair"), (0.27, "poor")}
F_{L7}	{(0, "good"), (0, "average"), (0, "fair"), (1, "poor")}
F_{C1}	{(1, "good"), (0, "average"), (0, "fair"), (0, "poor")}
F_{C2}	{(0.2, "good"), (0.8, "average"), (0, "fair"), (0, "poor")}
F_{C3}	{(0, "good"), (0.5, "average"), (0.5, "fair"), (0, "poor")}
F_{C4}	{(0, "good"), (0, "average"), (0.8, "fair"), (0.2, "poor")}
F_{C5}	{(0, "good"), (0, "average"), (0, "fair"), (1, "poor")}
F_{E1}	{(1, "good"), (0, "average"), (0, "fair"), (0, "poor")}
F_{E2}	{(0.2, "good"), (0.8, "average"), (0, "fair"), (0, "poor")}
F_{E3}	{(0, "good"), (1, "average"), (0, "fair"), (0, "poor")}
F_{E4}	{(0, "good"), (0.5, "average"), (0.5, "fair"), (0, "poor")}
F_{E5}	{(0, "good"), (0, "average"), (1, "fair"), (0, "poor")}
F_{E6}	{(0, "good"), (0, "average"), (0.5, "fair"), (0.5, "poor")}
F_{E7}	{(0, "good"), (0, "average"), (0, "fair"), (1, "poor")}

6.4.4 Use the ER Approach to Capture the Non-linear Relationships between Three Risk Basic Parameters and Construct the Risk Based BRB

The comprehensive risk evaluation of an event is determined by the three basic parameters (risk occurrence likelihood, consequence severity and failure consequence probability) together. Therefore, if the rating on a basic parameter is to some extent evaluated as the risk grade D_j, (j = 1, 2, 3, 4), then the comprehensive risk evaluation would be to some extent estimated as the D_j. Furthermore, the three parameters play

different roles in risk evaluation. In order to represent the relative importance of these parameters, the weights of the parameters, ω_{Li} (i =1, 2, …, 7) = 0.4, ω_{Cj} (j = 1, 2, …, 5) = 0.399 and ω_{Ek} (k = 1, 2, …, 7) = 0.201 require to be incorporated into the evaluation.

Taking such ideas into account, the *ER* approach introduced in Section 3.4 can be used to obtain the comprehensive risk evaluation by synthesising the conditional risk evaluation given the individual risk parameters. For example,

> IF L is "very low" AND C is "negligible" AND E is "highly unlikely", THEN the comprehensive risk evaluation is "good" with a belief degree of β_{11}, "average" with a belief degree of β_{12}, "fair" with a belief degree of β_{13} and "poor" with a belief degree of β_{14}.

β_{1j}, (j = 1, 2, 3, 4) can be calculated as follows:

F_{L1} = {(1, "good"), (0, "average"), (0, "fair"), (0, "poor")} with ω_{L1} = 0.4
F_{C1} = {(1, "good"), (0, "average"), (0, "fair"), (0, "poor")} with ω_{C1} = 0.399
F_{E1} = {(1, "good"), (0, "average"), (0, "fair"), (0, "poor")} with ω_{E1} = 0.201

Using Equations (3.10) – (3.15), each β_{1j}, (j = 1, 2, 3, 4) is computed as the set of (1, 0, 0, 0). Thus, the rule can be formally expressed as follows:

> IF L is "very low" AND C is "negligible" AND E is "highly unlikely", THEN the comprehensive risk evaluation is "good" with a belief degree of 1, "average" with a belief degree of 0, "fair" with a belief degree of 0 and "poor" with a belief degree of 0.

In a similar way, the other rules can be obtained and the risk based *BRB* including 245 rules ($245 = C_7^1 \times C_5^1 \times C_7^1$) can be constructed and shown in Appendix 4.

6.4.5 Analysis of Results

The results obtained for the risk based *BRB* using the proposed *FER* approach are collated with the results obtained from the traditional subjective expert judgement (knowledge based) method (Liu *et al.*, 2005 and Yang *et al.*, 2005) and are given in Appendix 4. From the above results, it is obvious that the subjective belief degrees related to risk evaluation can be reasonably assigned without logical conflicts in the newly constructed *BRB*. This point can be further validated using the analysis associated with specific individual rule, generic grouped rules and the compared rules between the new and old *BRBs*.

For the study of the specific cases, Rules 1, 123 and 245 in Appendix 4 can be chosen to

conduct the analysis. For example, in Rule 1, the risk occurrence likelihood has been assessed as "very low" with a creditability of 100 percent; the consequence severity has been evaluated as "negligible" with complete confidence; and the failure consequence probability has been estimated to a 100 percent belief degree as "highly unlikely". Since the risk evaluation is determined by the information of its three basic parameters, the result of the risk evaluation should be in the best safety situation to a maximum extent according to experts' knowledge. This is in harmony with the result obtained in Rule 1 as follows:

Rule1: IF "very low" and "negligible" and "highly unlikely", THEN {(1, "good"), (0, "average"), (0, "fair"), (0, "poor")}

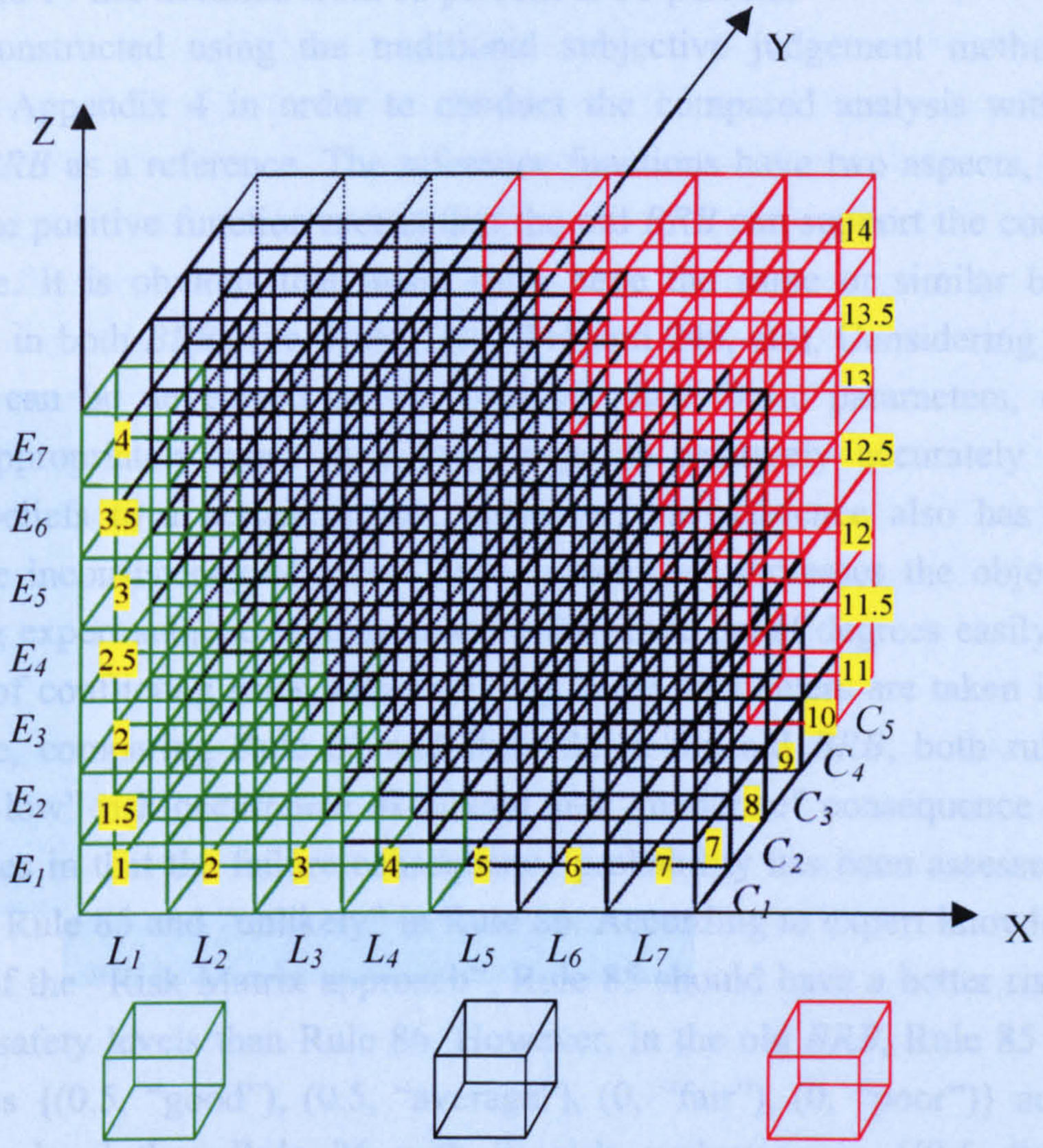
Similarly, the following results have also been acquired to prove the accuracy of the developed *BRB*:

Rule123: IF "average" and "moderate" and "likely", THEN {(0, "good"), (0.5, "average"), (0.5, "fair"), (0, "poor")}

Rule245: IF "very high" and "catastrophic" and "definite", THEN {(0, "good"), (0, "average"), (0, "fair"), (1, "poor")}

As far as the analysis related to the generic grouped rules is concerned, the theoretical basis of the "Risk Matrix approach" (Wang *et al.*, 1999) may be well employed. In risk assessment, it is crucial that important risks can be identified while trivial ones can be disregarded before both of them are forwarded for further complex analysis. The "Risk Matrix approach" just uses quantitative rating of risk parameters to estimate the "Risk Ranking Number" for categorising risks according their importance. An example of the "Risk Matrix approach" and its associated explanatory nodes are given in Figure 6.8, where the categories of three parameters (L, C and E) may be easily connected with the linguistic variables used in the antecedent attributes of the *BRB* and the types of risk levels in the *ALARP* (as low as reasonably practicable) principle may be linked with the linguistic variables used in the conclusion part of the risk evaluation of the *BRB*. For example, L_i (i = 1, 2, ...7) can be considered as "very low", "low", "reasonably low", "average", "reasonably frequent", "frequent" and "very frequent", respectively. The "Insignificant" risks can be connected with the risks with the "good" evaluation. The term, "*ALARP*" may be used to represent the linguistics variables "average" and "fair" and the "Intolerable" is associated with "poor".

Consequently, such an approach can support the validation of the developed *BRB*. For example, observing Figure 6.8, if the risk occurrence likelihood is L_1 and the consequence severity is C_1, then no matter how the failure consequence probability E varies, the risk is in the "insignificant" region. Extending such a statement (fact) to the



*The values can be calculated using the equation $V = i + j + 0.5k - 1.5$ ($(C)j = 1, 2, \ldots, 5$, $(L)i = 1, 2, \ldots, 7$, and $(E)k = 1, 2, \ldots, 7$), where 0.5 means that the importance of the failure consequence probability in determining risk evaluation is half of the other two risk parameters; and the aim of "minus 1.5" is to keep the value of the note with best risk evaluation as 1.

Figure 6.8. Proposed example of "Risk Matrix approach"

development of the risk based *BRB*, if the risk occurrence likelihood has been assessed as "very low" and the consequence severity evaluated as "negligible", then no matter which fuzzy number the failure consequence probability belongs to, the risk should be estimated as "good" to a great extent. The distribution trends of subjective risk beliefs in grouped Rules 1 - 7 ("good" with 88 percent at least) are well reflected with such a result (however, it is not the case of the old *BRB* systems). Compared with the example above, if the consequence severity is evaluated as "marginal" and the other conditions keep unchangeable, then the extent of risk evaluation estimated as "good" should be reduced (because the volume associated with L_1, C_2 and E_k ($k = 1, 2, \ldots, 7$) has less "Insignificant" nodes than the one related to L_1, C_1 and E_k ($k = 1, 2, \ldots, 7$) in Figure 6.8). The results from the *BRB* can effectively respond to such a tendency. Comparing Rule 1 with Rule 8, the extent that the risk evaluation is assessed as "good" has been reduced from 100 percent to 72 percent and the extent that risk evaluation is estimated as "good"

in Rules 7 and 14 has declined from 88 percent to 53 percent.

The *BRB* constructed using the traditional subjective judgement method has been provided in Appendix 4 in order to conduct the compared analysis with the newly developed *BRB* as a reference. The reference functions have two aspects, positive and negative. The positive function means that the old *BRB* can support the construction of the new one. It is obvious that many rules have the same or similar belief degree distributions in both *BRBs* (i.e. Rules 243, 244 and 245, etc). Considering that the risk based *BRB* can be developed on the basis of three basic parameters, experts may therefore, appropriately exert their knowledge to relatively accurately assign their subjective beliefs to a certain extent. However, the reference also has its negative function, the inconsistency of a rule base, which just addresses the objective of this study. Using expert subjective judgement to distribute belief degrees easily enables the occurrence of conflicting rules, although only three parameters are taken into account. For example, comparing Rule 85 and Rule 86 in the old *BRB*, both rules have the "reasonable low" risk occurrence likelihood and "moderate" consequence severity, the difference lies in that the failure consequence probability has been assessed as "highly unlikely" in Rule 85 and "unlikely" in Rule 86. According to expert knowledge and the discussion of the "Risk Matrix approach", Rule 85 should have a better risk evaluation in terms of safety levels than Rule 86. However, in the old *BRB*, Rule 85 with its risk evaluation as {(0.5, "good"), (0.5, "average"), (0, "fair"), (0, "poor")} actually has a worst safety level than Rule 86 with its risk evaluation as {(0.6, "good"), (0.4, "average"), (0, "fair"), (0, "poor")}. Similar situations happen between Rules 127 and 128, Rules 182 and 189, etc. Furthermore, when grouped rules are concerned, some belief distributions in the old *BRB* may be arguable. For example, the extents assigned to "good" in Rules 1 – 7 may reduce too fast according to the "Risk Matrix approach". These limitations are only observed in a three-parameter case study. If the parameters go to ten or more in other decision making problems, the accuracy of the *BRBs* will be arguable and thus, the subjective expert judgement method in the development of *BRBs* based on entire expert judgements is error-intended. Simultaneously, these analyses show that a more accurate and reliable *BRB* can be achieved by the application of the *FER* method.

6.5. Conclusion

The research of using *BRB* expert systems to infer risk based decision making has been widely investigated in recent years and obtained significant academic and industrial achievement. However, few studies have considered the problem of how to develop a rational *BRB* representation system as the reference of such inference. An *FER* method to deal with the inconsistent problem of a *BRB* (for instance, rules are regarded to be inconsistent if they have very similar antecedent parts but possess significant different

consequent parts that conflict with expert knowledge) is promoted in this chapter. In such a method, the expert subjective judgements have been moved to the earliest stage of constructing a *BRB* system, which ensures that the belief degree distributions in the system are as objective as possible and maximally reduces the uncertainties encountered in developing the system. In the methodology, the linguistic variables and their fuzzy membership functions to represent the knowledge of multiple attributes in risk based decision making were first investigated and a new transformation technique was then proposed on the basis of a fuzzy similarity function to assist in connecting each attribute with their utility space. Consequently, the conditional belief degree distributions in the space given the individual antecedent attribute were obtained. The *ER* algorithm was further used to synthesise such conditional belief degrees in a hierarchical order to form rational and consistent *BRBs*.

The results generated from a case study on risk assessment have demonstrated that such a methodology can provide decision makers in *CSCs* with a convenient tool that can be used to deal with the uncertainties resulting from "entirely subjective data". In conclusion, the proposed framework offers great potential in risk based decision making and the method provides both a flexible way to represent and a rigorous procedure to deal with the rational subjective probability distributions in the context of fuzzy expert systems.

Chapter 7 – A Proposed Bayesian Network Model to Risk Assessment

SUMMARY

The problem of developing and sustaining a highly capable risk assessment technique to meet the diverse needs of sophisticated CSCs is extremely onerous and arduous, particularly in view of the plethora of challenges and uncertainties posed by the unavailability and incompleteness of historical failure data, the interaction and dependence of risk factors and the relatively modest level of funding available. One realistic and reliable way to deal with such a situation is to effectively and accurately assess the risk priority so as to ensure that the limited resources and assets are capable of cooperating cohesively together and being distributed to those key risk factors for safety improvement. This goal may be fostered through adopting an appropriate BN approach. This chapter, therefore, proposes a BN-based risk assessment methodology for assisting the CSCs' managers to check, predict and improve the safety and reliability performance of the chains. For any CSC safety-critical application the methodology demonstrates how the BN technique can be used in formalizing reasoning of systematical interactive dependence and incorporating subjective expert judgements to compensate the absence of any objective statistical data. In such a logical framework, adopting BN is shown to realistically deal with the encountered uncertainties whilst at the same time making risk assessment modelling easier to build, check and certainly update. To validate the feasibility of the methodology developed, the risk of terrorists attacking CSCs is studied as an applicable case of interest.

7.1 Introduction

Nowadays, safety is becoming one of the important criteria measuring the efficiency of the design, control and management of *CSC* systems. It is therefore crucial to select a suitable safety policy against the potential vulnerability of the systems. However, such a selection is not straightforward and assessors are often required to contribute to the difficult process of safety management and decision making by providing a predictive link between *RCOs* and system safety response. Furthermore, this link may be a complex causal chain, the entirety of which rarely falls within a single, coordinated research project, considering that *CSCs* are growing systems made up of many sub-systems and sub-functions each of which has been, and may still be treated as a distinct management operation.

Some supply chain risk management models represent attempts to combine the understanding gained from multiple studies into a single framework. Most models do this by endeavouring to simulate all of the physical and managerial processes occurring in the chains at a pre-determined model scale (Chapman *et al.*, 2002; Peck and Jüttner, 2002; Pai *et al.*, 2003; Yang *et al.*, 2004). However, depending on the nature of these processes, the most predictable relationships among different risk variables may emerge at a variety of spatial, temporal or functional scales. Therefore, current safety knowledge might be better represented if each relationship were described at or between the dynamic and interactive levels of detail at which the key risk variables could be identified, rather than at a static and steady scale that is identical for all processes.

Given the diversity of scales at which risks may occur, a serious challenge for risk analysts is to integrate quantitative descriptions of these risks into coherent assessment models. Methodologies are required that allow representation at multiple scales and in a variety of forms, depending on available information. There is also a need to assess how uncertainties in each component of the models translate to uncertainty in the final safety predictions. Finally, such models must be able to be easily updated to reflect evolving safety knowledge and policy needs.

BNs, based on the marriage of a well-defined theory of Bayesian probabilistic reasoning and a networking technique, provide a strong framework for handling uncertainty problems. The networks constitute a class of probabilistic models with strong connections to graph theory (Jensen, 2001), which can be considered as a realistic way of structuring a situation for reasoning uncertainty with an interactive feature. The use of *BNs* may also be capable of combining various pieces of information and making use of expert judgements to compensate the absence of historical statistics and deal with incomplete uncertainty. Since the core technology of *BNs* is maturing and becomes generally available in inexpensive software systems, they have been successfully applied to a variety of problems. Recently, their popularity started to grow among system risk assessors and reliability analysts. Earlier work has examined the parallels between *BNs* and other *QRA* approaches and indicated the potentials of *BNs* in terms of modelling and analysis capabilities (Cagno *et al.*, 2000; Mahadevan and Rebba, 2005).

This chapter proposes a novel *BN*-based risk assessment methodology to investigate the feasibility of applying *BNs* to the risk assessment of *CSCs* and contributes itself to the absence of using *BNs* in the literature of supply chain safety and reliability research. The intention is to emphasize their application as an intuitive risk modelling technique and their potential to offer attractive features not always achievable by other means. The remainder of the chapter is organised as follows. The ensuing section introduces the

background information of *BNs* and their applications in the risk and reliability fields. Section 7.3 examines the development of the novel *BN*-based risk assessment methodology and their specialty in the *CSC* systems. Section 7.4 presents a case study for testing the methodology generated. Finally, Section 7.5 concludes the chapter and indicates the areas for future work.

7.2. Review of *BNs*

7.2.1 Historical Development of BNs

BNs, also known as "Directed acyclic graphs (*DAGs*)", "Bayesian belief networks (*BBNs*)", "probabilistic networks", "causal nets" or "belief nets", constitute a mathematically sound method for representing and reasoning uncertainty with an internally consistent manner. *BNs* initially arose from an attempt to incorporate the probability theory into expert systems, and have an origin and long history in decision analysis (Neapolitan, 1990). In decision theory, the idea of considering the entire model as a construction subject to uncertainty and subjectivity stepped from the game theory of the 1930s and '40s (Shafer, 1990). Games evolved into sequential games against uncontrolled 'nature' and abstractions, such as decision trees were developed. Thus, Bayesian decision theory gained increasing notice and emphasis (Wald, 1950) in the 1950s. The basic Bayesian theory was developed into more applicable level towards the late 1960s (Howard, 1968; North, 1968; Raiffa, 1968).

BNs, the marriage of the Bayesian probability theory and networking techniques, were first developed at Stanford University in the 1970s (McCabe *et al.*, 1998). They fell out of popularity during the 1980s and have experienced resurgence in the 1990s. Conventionally, one of the bottlenecks to practical applications of Bayesian approaches has been the high amount of computation required. However, powerful numerical techniques were not available until the 1980s. According to Shafer and Pearl (1990), the relatively new developments in decision analysis approaches including *BNs* were linked with advances in related computational mathematics available from twenty years ago. The availability of good computing facilities stimulated the fast developments of the *BN* approach and took the focal role for updating the probability information in conditioned networks. In the first half of the 1980s, the concept of *BNs* was originally introduced to the field of expert systems through the work by Pearl (1982) and Spiegelhalter and Knill-Jones (1984). The first real world application of *BNs* was Munin (Andreassen *et al.*, 1989). Since then, *BNs* have spread quickly and been used extensively to model many real world problems (Oliver and Smith, 1990; Ottonello *et al.*, 1992; Burnell and Horvits, 1995; Szolovits and Pauker, 1993; Russell and Norvig, 1995). In particular,

they have been used very successfully in building expert systems to help Artificial Intelligence analysis*, medical diagnosis (Spiegelhalter *et al.*, 1993) and software development (Heckerman *et al.*, 1995). Recently, *BNs* have also led to many new applications of uncertainty modelling, in particular to very complex problems where a large number of variables contribute to overall uncertainty.

7.2.2 Definition of BNs

A complete and rigorous definition of *BNs* can be shown in some of the literature cited (Pearl, 1988; Neapolitan, 1990; Jensen, 1996). This definition focuses on the contents of the networks and describes a *BN* as a *DAG* consisting of nodes, arcs and an associated set of probability tables. Nodes represent *RVs* whose states are usually expressed in discrete numbers or ranges. Directed arcs between pairs of nodes represent dependence between the *RVs*. A *CPT* associated with each node denotes the strength of such causal dependence. The concept is classical and generic, but may need more explanation in this study with just enough rigour and detail that will enable the possibility of easily applying these networks to *CSC* risk assessment problems.

A *BN* model for the *CSC* risk assessment can thus be defined to consist of the following:

a) *Qualitative relationships:*
   ***a set of risk factors as RVs {X_i}**, which can assume discrete values (e.g. false and truth states, soundness and weakness states, etc.);*

   ***a set of directed edges or arcs {E_{ij}}**, between node pairs, which indicate the existence of direct influences between the risk factors, combined in such a way as to form a DAG structure.*

The qualitative relationships can be explained as that given a risk scenario, a *BN* describes graphically the causal relationship between the causes and effects of the scenario. In doing so it also demonstrates conditional independence as to which risk factors are relevant and directly affect a given event and which risk factors are irrelevant – irrelevant in the sense that knowledge regarding these factors becomes redundant once the direct causes are known.

b) *Quantitative relationships:*
   ***a set of root and conditional probabilities {P_i}**, representing root node and parent-child node conditional probabilities, respectively. The precise strength of each parent-child influence relationship is specified in the CPT attached to the child.*

---

* The best general references for the application of *BNs* in the field of *AI* may be the proceedings from the annual *Conference on Uncertainty in Artificial Intelligence* (www.auai.org).

The quantitative relationships enable *BNs* to update the probability distributions. Given a risk situation in *CSCs* and prior probability distributions over the associated risk factors that represent the potential causes resulting in the risk situation, *BNs* provide the capability to update these probability distributions when fresh safety observation is obtained.

c) *Combination relationships:*
***a Joint Probability Distribution (JPD)**, on the basis of which any risk probability query can be answered. The JPDs can be obtained using the combination of qualitative and quantitative relationships.*

When nodes are assigned to each risk factor related to the risk scenario and arcs are drawn toward each node X_i from a select set of "parent" nodes PX_i perceived to be direct causes of X_i, the strengths of these direct dependence can be quantified by assigning each X_i a *CPT* $P(X_i \mid PX_i)$, which depends on subjective judgemental estimation or statistical evidence of the conditional probability of the event $X_i = \langle x \rangle$. The conjunction of these local estimations across the full *DAG* specifies a complete and consistent *JPD*, which over the set of variables $\{X_1, ..., X_n\}$ is given by the product:

$$P(X_1,...,X_n) = \prod_{i=1}^{n} P(X_i \mid PX_i) \tag{7.1}$$

7.2.3 Characteristics of BNs

As one kind of expert system, *BNs*, like rule-based systems, may be developed using expert opinion instead of requiring historical data (Charniak, 1991). This is not always the case for all expert systems. For example, historical data is required to train neural networks, which means that although data is not required for generic algorithms, the development of generic objective functions needs significant resources (McCabe *et al.*, 1998). The major disadvantage of incorporating expert judgements into *BNs* is the general lack of understanding of probability theory so as to fail to precisely probabilistically estimate subjective fuzziness. Such inaccurate subjective estimates of the certainty of an event have been claimed as an unwanted introduction of bias into *BNs* (Tversky and Kahneman, 1974). Research has also shown that significant errors result from the perception of risk depending on the risk-aversion characteristics of the individual (Tversky and Kahneman, 1990).

BNs have a built-in independent characteristic that permits evaluation and propagation of evidence in the networks. Consider nodes *A* and *C* in a serial connection of *BNs*. The nodes are obviously connected and therefore have a dependent relationship. However, if the value of the node *B* between them is known, and there is no other path, then the two

become direction-dependent separated (d-separate), or conditionally independent of each other given the blocking node(s). Once conditionally independent, the probability of one node can be evaluated without consideration of the others, thus providing a basis for overall improvement in computation. As acyclic graphs, *BNs* require that all arrows in the networks must not form a directed cycle or loop. This does not imply that there can only be one path between any two nodes, but it does mean that the path can never be circular when the direction of the arrows is considered. This may constrain *BNs* to model the reality to a certain degree.

BNs are capable of making an intercausal inference operation (Henrion *et al.*, 1991). It is used for updating beliefs with the entry of additional evidence. In the intercausal inference operation, new evidence may be entered at any point in the networks, and the probabilities of the remaining variables are updated. Consequently, the changes from the corresponding marginal probabilities without the new evidence are observed. This enables *BNs* to provide the basis and backing of the *SA* of the influence of any single risk factor to the others or the overall safety system.

Providing great flexibility for accepting input and delivering output, *BNs* have the ability to allow the value of a variable to be entered as a known input or to evaluate the probability of the variable as an output of a system. Consequently, they may accept evidence at any point in the system and likewise, provide output at any point in the system. The ability to adjust variables to be input or output without redesigning the system is not a common characteristic for other expert systems, such as rule-based and neural network systems.

During the development of a knowledge base, the ease of altering variables or states to an existing network is extremely important. The graphical nature of *BNs* allows variables to be added or removed without significantly affecting the remainder of the networks because modifications to the networks may be isolated. Contrarily, additions to neural networks require retraining the networks. It has been also indicated that *BNs* are more effective than rule-based expert systems for capturing knowledge when exceptions to the rules are too important to exclude, but too numerous to express explicitly (Chong and Walley, 1996).

7.2.4 Inference Formulism of BNs

The basis of reasoning under uncertainty in *BNs* is called Bayesian inference formulism, which is developed for the task of computing the probability of each value of a node in a *BN* when other variables' values are known (Jensen, 1996). Bayesian inference can be

defined in the following manner (See Figure 7.1): 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 (probabilistic) dependencies between those variables (Groen and Mosleh, 2001). Suppose one new observation related to one (or more) variable(s) in the models has been obtained from the realistic observable situation. Then the other variables need to be revised and the probabilities or belief values of those variables representing the unobservable situation will happen to change according to their dependent relationships. The reasoning and calculation of the updated probabilities for the system variables based on the new evidence is precisely what Bayesian inference is. The reasoning process relies on the use of Bayes' theorem as its fundamental rule of inference, which makes *BNs* powerful to allow the users to apply their knowledge towards forward or backward reasoning.

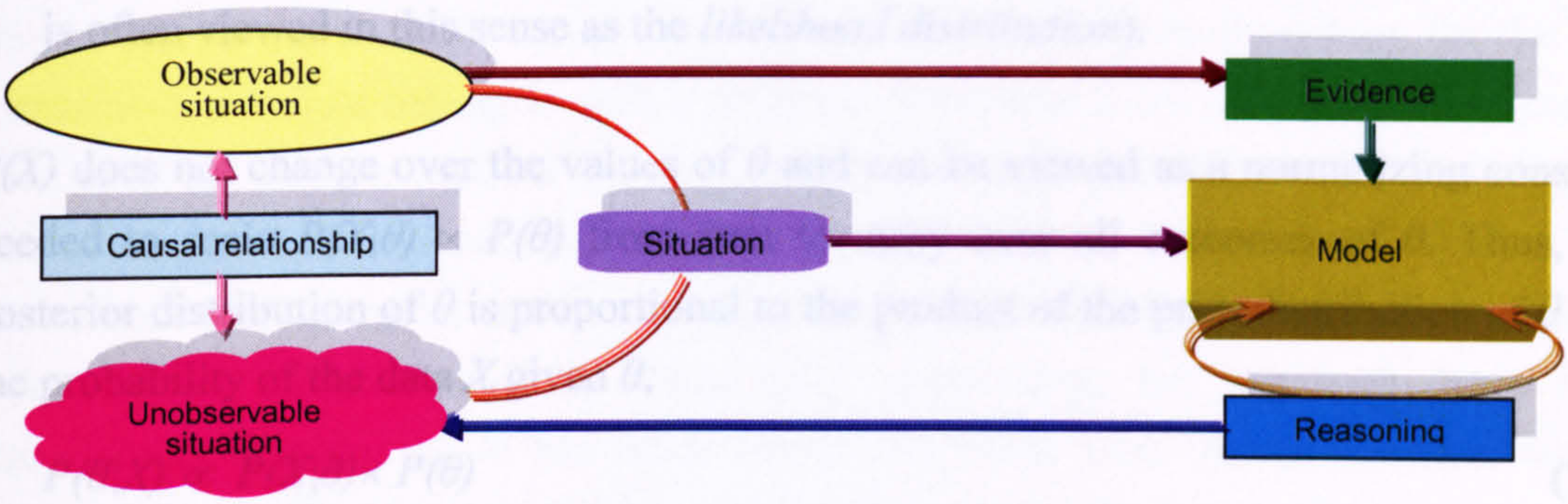


Figure 7.1. Idealised view of Bayesian inference process

Bayes' theorem describes the way that analysts can update their subjective beliefs when new facts are uncovered. The theorem can be stated in words as (Hayes, 1998):

> "The probability distribution of a model parameter, after observation, is proportional to the likelihood of the observation, assuming that the parameter value is true, times the prior probability distribution of the parameter."

or

$$\begin{pmatrix}\textit{Probability of a}\\ \textit{parameter value given}\\ \textit{the observation}\end{pmatrix} = \frac{\begin{pmatrix}\textit{Probability of the}\\ \textit{observation given the}\\ \textit{parameter value}\end{pmatrix} \begin{pmatrix}\textit{Prior probability of}\\ \textit{the parameter value}\end{pmatrix}}{\begin{pmatrix}\textit{Total probability of the}\\ \textit{observation}\end{pmatrix}} \quad (7.$$

The probability of a parameter value given the observation is refereed to as the posterior probability. This distinguishes it from the prior probability held by the analyst prior to the collection and analysis of the observation.

If the model parameter is a discrete variable, then the formal definition of Bayes theorem can be symbolically given as follows:

$$P(\theta|X) = \frac{P(X|\theta) \times P(\theta)}{P(X)} \tag{7.3}$$

where: "|" symbolises conditional probability,

$P(\theta|X)$ represents the posterior probability of θ occurring given the condition that X has occurred,

$P(\theta)$ denotes the prior probability of θ occurring, and this is what causes all the arguments,

$P(X)$ denotes the marginal (total) probability of X occurring, and is effectively constant since the obtained data is at hand, and

$P(X|\theta)$ refers to the conditional probability of X occurring given that θ occurs too (It is often viewed in this sense as the *likelihood distribution*).

$P(X)$ does not change over the values of θ and can be viewed as a normalizing constant needed to scale $P(X|\theta) \times P(\theta)$ from sum to unity over all outcomes of θ. Thus, the posterior distribution of θ is proportional to the product of the prior distribution of θ and the probability of the data X given θ,

$$P(\theta|X) \propto P(X|\theta) \times P(\theta) \tag{7.4}$$

Similarly, the probability that an event B given the condition that an event A occurs is given as:

$$P(B \mid A) = \frac{P(A|B) \times P(B)}{P(A)} \propto P(A \mid B) \times P(B) \tag{7.5}$$

A key aspect of Bayesian inference is the ease with which previous knowledge may be updated as new data/information becomes available. Given a prior probability $P(B)$ and an initial observation A_1, Bayes theorem states that

$$P(B|A_1) \propto P(A_1|B)P(B) \tag{7.6}$$

If a second observation A_2 is made independently of the first then

$$\begin{aligned} P(B|\, A_2, A_1) &\propto P(A_2|B)\, P(A_1|B)P(B) \\ &\propto P(A_2|B)\, P(B|A_1) \end{aligned} \tag{7.7}$$

The expression (7.6) is the same as (7.7) except that $P(B|A_1)$, the posterior probability for B given A, plays the role of the prior distribution $P(B)$ for the second sample. This process can be repeated any number of times, with the posterior probability playing the

role of the prior for the next set of calculations – such that "today's posterior probability is tomorrow's prior" (Lindley, 1970). Furthermore, it can be concluded that the posterior probability of unobservable variables can be continuously updated using the prior probability of all observable ones available. The theorem, therefore, is particularly useful in estimating knowledge about the probability distribution of variables of interest or making reliable predictions where direct observations are unavailable or too complex to be collected.

7.3. *CSC* Risk Assessment with *BNs*

The risk assessment of *CSCs* in essence is a decision making (priority setting) process, in which all potential hazards/threats are identified, the associated risks analysed, calculated and finally presented in terms of importance. Hence, the precise theoretical framework of the decision theory also forms the theoretical methodology for the risk assessment. *BNs* just belong to such a decision theoretical framework, and hence can be used as a risk analysis method and may readily substitute both *FTA* and *ETA* in logical tree analysis. It is noteworthy that the term "important risks" in *BN*-based risk assessment will not mean those risks with high values calculated using some traditional risk analysis methods such as those *QRA* approaches, but represent those risks significantly contributing to the safety level of a whole *CSC* system. In other words, minor changes of the important risks may produce major influences to the system safety. Attention then shifts from an individual viewpoint to an entire perspective. The risk priority assessment, thus, depends on the combination of all risk parameters introduced previously (i.e. *W, P, R, D*) and weight contributing to the safety levels of the whole system. Consequently, an effective assessment can be reduced to two problems on how to improve the judgement accuracy of the likelihood and severity with the uncertainty and how to appropriately reason such dynamic weights for measuring the complex interactive dependence in the system.

In the realm of risk assessment studies, sourcing the most comprehensive historical failure data that can accurately represent the risks estimated is very desirable. However, to realise such desirability is time-consuming, expensive and even unachievable in many circumstances. For example, solely depending on historical failure data makes it impossible to assess the safety and reliability of a modern *CSC* system, where many risks newly emerge from complying with the ever-increasing exploration and application of the latest techniques. As a result, quite a number of risk assessments require to be conducted by the support of human knowledge and experience. Naturally, the research reasonably combining subjective expert judgements and objective statistical data attracts more and more attention from both academic and industrial areas of safety and

reliability. After the introduction of the concept of subjective belief to Bayesian probability theory, *BNs* have been paid particular emphasis on the simultaneous analysis of expert and statistical information, which shows quite attraction to *CSC* risk assessment.

For complex and costly risk management, it is beneficial that all relevant risks are estimated and analysed on an overall basis, treating and assessing them within the same theoretical framework. Following that, different *RCOs* may be consistently compared and the risks can be demonstrated and documented to all stakeholders. This no doubt requires a well-matched solution to deal with the interactive dependence among the risk factors. It is often the case that the interactive dependence concept is neglected in risk assessment studies in order to simplify the analysis that leads to the "satisfying" results. For the sophisticated systems like *CSCs*, where such negligence may cause significant deviations from their realistic safety requirements, more complex interactive dependence expressions such as network structures have to be accounted for. Employing graph and probability theories, *BNs* enable the possibility of the risk analysis with the characteristics of complex interactive dependence using both qualitative and quantitative networking methods. They essentially provide a framework for graphically representing the logical relationships between the risk variables using directed acyclic graphical structures and capturing the uncertainty in the interactive dependence between the variables using the concept of conditional probability.

Proper *BN* structures may result in a reduction of the number of probabilities required initially and at evaluation time, may result in better representations of a true system. Poole *et al.* (1998) have outlined the necessary steps for the development of a well-designed belief network. They include the definition of the relevant variables, the definition of the relationship between the variables, the definition of the states of the variables and the definition of the conditional probabilities of the relationships.

However, such a methodology is too generic to be applied to the current study. Aiming at addressing the characteristics of the risks in *CSCs*, a new risk assessment model is built up on the basis of *BNs*, shown in Figure 7.2. Compared to the generic framework mentioned above, the model has many specialties and merits in the context of risk assessment. They can be concluded as follows:

1. A monitoring system to optimise the *BN* structure to match the reality (qualitative model).
2. A novel hybrid approach of combining fuzzy possibility and Bayesian probability theories to attempt a more accurate probability guess of subjective expert judgements.

3. Two new ranking parameters generated for appropriate decision-making in different risk situations in which the original systems may require to be improved or maintained.
4. A dynamic model for connecting root risk causes and decision support under uncertainties.

All the details associated with the first and second specialties will be explained in this chapter and those related to the third and fourth ones will be described in the next chapter. All of them provide the framework of applying *BNs* to *CSCs'* risk assessment.

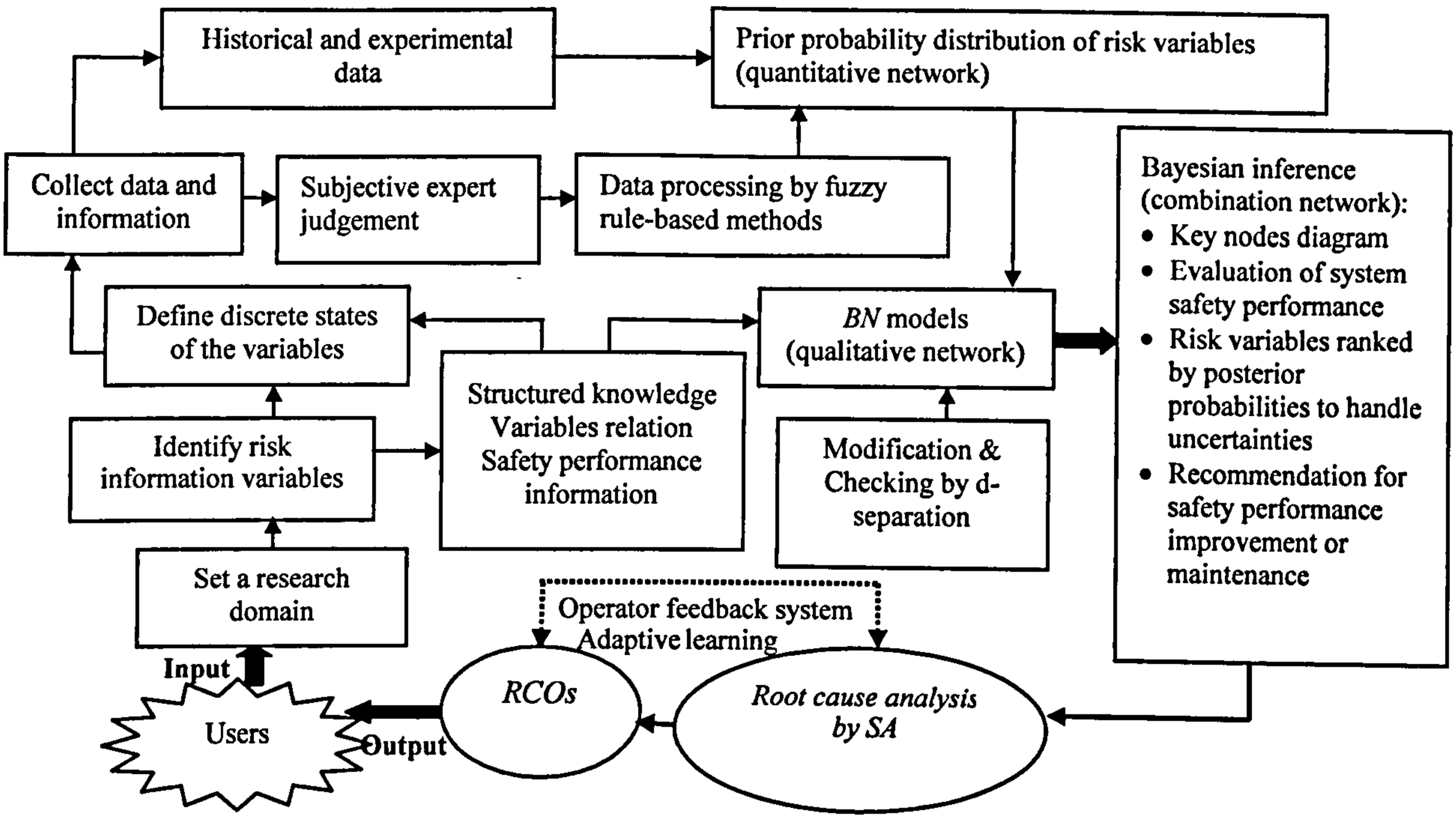


Figure 7.2. The *CSCs*' risk assessment model using *BNs*

7.3.1 Setting the Domain of Risk Assessment (Generating Hypothesis)

The initial research into the *CSCs* risk assessment with *BNs* is to set the domain of risk assessment, in which the targeting events or the variables of interest can be identified and locked. It may be either a kind of risk, such as a fire or transport delay in the chains, or one individual chain including many sub-chains and components. Setting such risk domains is usually difficult considering the risk characteristics, especially the interactive dependence. Therefore, a set of hypotheses is required to make out a specific analysis space. This will be particularly meaningful in collecting historical failure data and developing the conditional probability distributions of the risk variables later. Although it is true that the hypotheses may restrict the simulation of the risk assessment model of real systems, the restriction caused may be reduced because of the fact that in *BNs*, new variables can be allowed for the incorporation into the original model established.

Hypotheses can be built up using brainstorming techniques. Brainstorming is regarded as an essential step in the design of effective simulations of the hypotheses. Through brainstorming sessions, clear statements of the problems are established, the objectives and the desired output characteristics are designed. The techniques themselves strongly depend on the knowledge and expertise of the people involved in the "brainstorming" process, who usually are considered to be the experts in the corresponding areas. This research does not prescribe a standard method of brainstorming as applicable to all risk situations possibly occurring in *CSCs*. The nature and content of the brainstorming session will vary widely on different problems. However, it is particularly noteworthy that in the brainstorming process related to risk assessment, certain safety aspects may be overlooked or overemphasized by the experts as they might be considered "natural" from professional viewpoints, while to a person outside the profession they might be something completely new, thus causing concern. Since by definition the "brainstorming session" ought to be structured to encourage the unfettered thinking and participation of the people involved, the contribution by people with less expertise in the subject would be a positive one, as they might bring up safety issues, which otherwise would have been overlooked (Pillay and Wang, 2003a).

7.3.2 Defining Risk Information Variables

The targeted events represented and supported by hypotheses are usually not directly observable. Therefore, a range of information variables have to be devised which can be observed and which will provide sufficient details to assign the likelihood to the set of hypotheses. In the study of the risk assessment of *CSCs*, such information variables are usually defined as risk causes. In order to better identify the risk causes, one effective way is to simulate the operation of the chains in the domain developed. A *HAZOP* study has great potential in addressing this kind of requirement. It is an inductive technique which is an extended *FMECA* and which can be applied by a multidisciplinary team to stimulate systematic thinking for identifying potential hazards and operability problems, particularly in the process industries (Henley and Kumamoto, 1992). The use of the *HAZOP* study can break down the targeted event system to its identified, logical and manageable levels such as the sub-chain systems, component levels and risk causes for efficient studies, and simultaneously, further confirming that the domain of the study has been correctly set.

7.3.3 Constructing a Qualitative Network Representing the Dependence of the Variables

BNs provide a direct model of the real world environment rather than a model of the reasoning process carried out in many knowledge representation schemes, e.g. neural

networks. After identifying the variables of interest and their corresponding risk information variables, one starts confirming the relationships between them and constructing a qualitative network to represent all *RVs* and their dependencies. The knowledge about the system and intuitive understanding of the various dependencies are then used to construct the causal structure of the *CSC* system. Here the graphical representation becomes very handy. It permits users to directly express the fundamental, qualitative relationships of direct or indirect influence.

A process for obtaining an initial graph can be along the following lines. In the first stage each variable can be found if it is a root cause, which is not directly influence by any other variables. All root causes are then assigned a node each. Because the risk variables are identified in an almost hierarchical way – from a higher level of sub-chains to the component level, the graphical structure will unavoidably have a hierarchical feature. Consequently, the nodes associated with root causes can be defined as level-1 nodes at the first stage. All the variables that are directly influenced by the variables in the level-1 nodes can be discovered and the nodes associated with them can be assigned and defined as level-2 nodes at the second stage. A given node at level-2 has as its parents all those nodes in level-1 that directly influence this particular node. A set of parent-child links is then drawn, which now serve as edges of the graph. In the i^{th} stage all the variables that are directly influenced by variables in the preceding $(i\text{-}1)^{th}$ level can be identified as the level-*i* nodes to be added. The parents of these nodes are identified and the corresponding parent-child links are given. This hierarchical process continues until all the variables have a place in the graph and all parent-child links are accounted for by edges of the graph.

It must be stressed that the nodes in the *level-i* at the i^{th} stage may simultaneously be the *level-(i+j)* nodes at the $(i+j)^{th}$ stage. For example, node *A* represents a root variable, which directly impacts nodes *B* and *C*. At the first stage, node *A* is a *level-1* node and at the second stage, nodes *B* and *C* belong to *level-2*. At the third stage, the variable represented by node *B* directly influences the variable related to node *C*. Therefore, the *level-2* node *C* at the second stage becomes the *level-3* node at the third stage. Another noteworthy point is that the whole process is subjective, because the parents are identified through the subjective judgements of the individuals constructing the graph. The procedure is, however, consistent because in the *BN* formalism, for any node, once the direct influences on it are known, all other potential influences are irrelevant as far as constructing the network is concerned (Das, 2000). The network can then augment these with derived relationships of indirect influences in a consistent manner. To do this, it must be assumed that the subjective judgements of the relationships do not lead to a cycle of influences.

7.3.4 Checking and Modifying the Qualitative Networks

In Section 7.3.3, there are no more considerations of the accuracy in establishing the links and their directions. However, one cannot expect this part of modeling always to go smoothly and right. The initial networks may need some careful verification and modifications. Some links may appear superfluous and some directions may be totally wrong. For this purpose, the concept of d-separation has been developed and introduced for systematic updating of the structure of the networks to ensure that the knowledge of experts can reflect the real world.

The parent-child relationships are identified by the individuals constructing the graph using very simple semantics, namely causality. However, this does not mean that "causality" is an easy concept. It may be very difficult to experience causality and philosophically the concept is not fully understood (Jensen, 2001) so that many humans cannot sensibly organize causal relationships in a knowledge domain. For example, the relationship between "fire" and "temperature" often leads to the debate of whether "fire" causes the increment of "temperature" or vice versa. "Causality" is obviously not a good criterion to measure the effectiveness of the models. When building the structure of *BN* models, assessors need not insist on having links going in a causal direction. On the other hand, they need to check its d-separation properties to ensure that the properties correspond to their perception of the world (Jensen, 2001). Consequently, some possible arguments such as whether various risks favour the less reliable design of logistics units or the vulnerability of the design results in the emergence of the risks, are no longer worrisome. Furthermore, some scientists take the point of view that the networks are not causal models, but models for how information may propagate between events (Jensen, 1996). This, from a foundational viewpoint, might be valid for the way in which the anti-casual links exist in risk based *BNs*.

D-separation (conditional independence) is a very important concept in the Bayesian probability theory, because not only it does assist in modifying the initial networks towards more effective models, but also it provides the basis of inferring the quantitative calculation and combining the probabilities representing uncertainty in *BNs*. It can be well explained by means of the "Bayes Ball" algorithm (Shachter, 1988). Two (sets of) nodes A and B are d-separated (conditionally independent) given a (set of) node(s) C if and only if there is no way for a ball to get from A to B in the graph, where the allowable/unallowable movements of the ball are shown in Figure 7.3. Hidden nodes are nodes whose values are not known, and are depicted as unshaded; observed ones, which are conditioned, are shaded. The dotted arcs indicate the directions of flow of the ball.

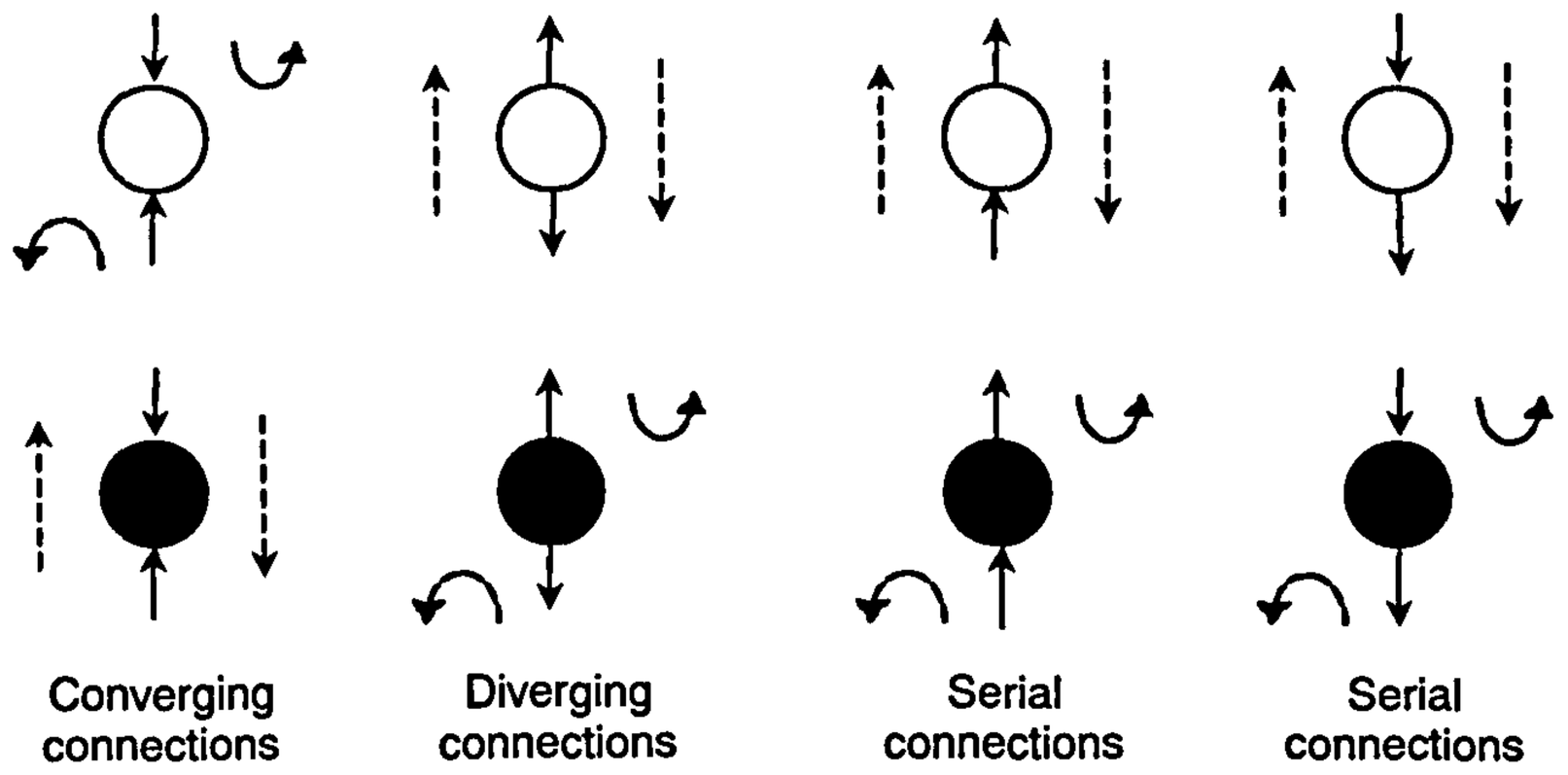
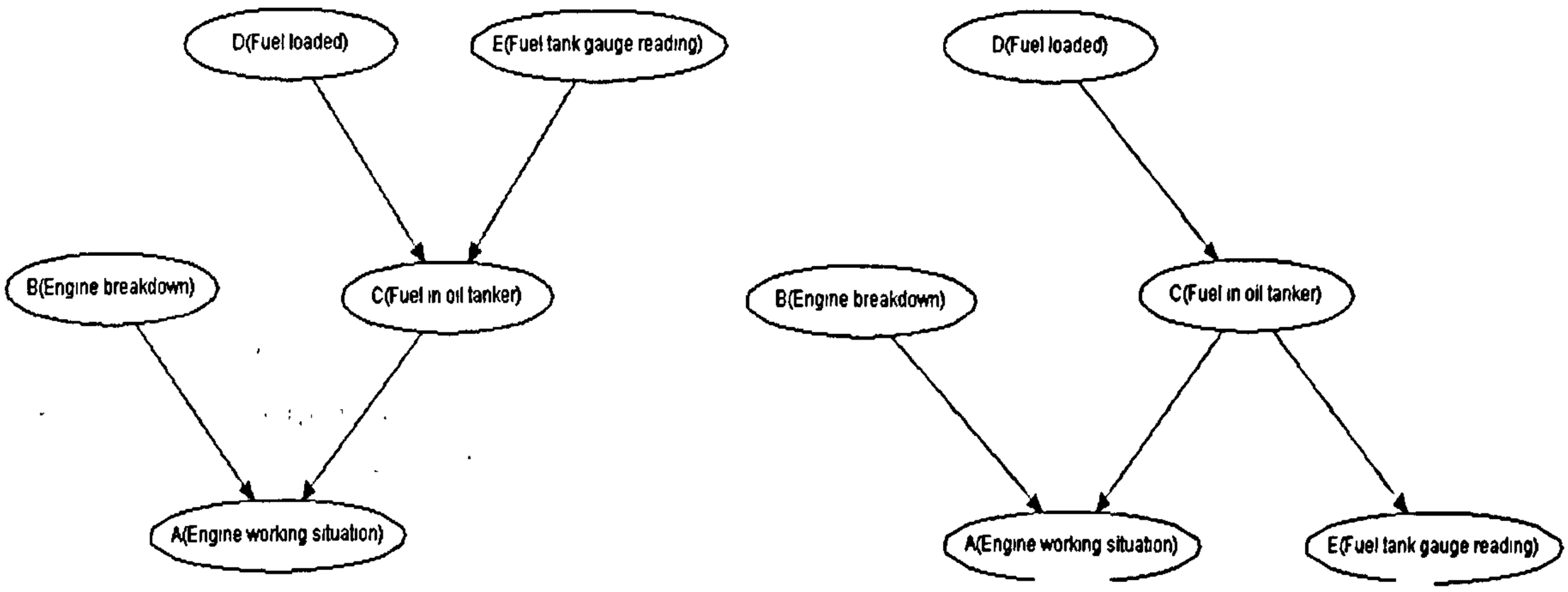


Figure 7.3. The diagram of explaining the concept of D-separation

Firstly consider the first column of Figure 7.3, the converging connections in *BNs*, in which two converging arrows from the nodes A and B point to the node C. If C is hidden, then A and B are conditionally independent, and hence the ball does not pass through, which is indicated by the curved arrows; but if C is observed, then A and B become dependent, and the ball does pass through. Furthermore, other graphs can be analysed in a similar way. In the diverging or serial connections, if C is observed, all balls cannot get though, which indicates that A and B become conditionally independent. Use of the concept of D-separation to check the accuracy of a qualitative *BN* in presenting a realistic situation can be demonstrated in the following example.

Suppose the engine of a containership does not work. The engineers on board analyze two potential reasons – the engine breakdown or lack of fuel. To disclose the truth, the storage of the fuel naturally requires to be checked using two parameters – the record of fuel loaded at the last calling port and fuel tank gauge reading. For this special case, an initial *BN* is built up as shown in Figure 7.4a. Now use the d-separation concept to verify the network. The relationship between nodes B and C is first investigated. Node A is observed (the engine does not work). If node C is found with a new piece of evidence, such as no fuel in the tank, then node B will be affected with a lower probability of breakdown. Therefore, they are dependent and suit the concept of d-separation. The links and directions are sound. However, when a similar analysis is employed to investigate the relationship between nodes D and E, the result is different. With the evidence of node C, the dependent connection between nodes D and E cannot be constructed, which means that there is something wrong with the links and directions. Further careful analysis will assist in identifying their right family relationship shown in Figure 7.4b, in which node C is the parent of node E because the situation of the fuel in the tank decides the fuel tank gauge reading.



a b

Figure 7.4. An example of using D-separation to check qualitative *BNs*

7.3.5 Defining the Discrete States of Risk Variables

A random risk variable representing an uncertain quantity in a *BN* requires a finite number of possible values or states. If the variable is denoted with an uppercase letter (X) and the specific states that the variable might take on are denoted with lowercase letters $<x>$, then the variable states must satisfy the following two criteria in order to be admissible under the *BN* formalism:

- ***Completeness of states.*** For any given *RV X*, the set of variable states $\{<x_i>\}$ must be probabilistically complete, that is, $\sum_i P\{< x_i >\} = 1$, for all i.
- ***Mutually exclusive states.*** For any given *RV X*, its variable states $<x_i>$ must be mutually exclusive (no overlapping between the member set states), which can be described as $P(X = <x_i> \text{ or } X = <x_j>) = P(X = <x_i>) + P(X = <x_j>)$

An additional criterion in analyzing the states of *RVs* is to require them to be in discrete states in order to simplify the practical operations of using *BNs* to risk assessment, although continuous-state variables are certainly allowed by the *BN* mechanism in theory. This may be considered as a drawback of *BNs*, but neither other risk analysis methods such as *FTA* or *ETA* can offer any better alternatives. A consequence of the discretisation is that the result of *BNs* may be sensitive to the selected discretisation, and that the calculations and propagations involved in the evaluation of *BNs* grow exponentially in the number of states of the nodes.

Although variables can be assigned to various states according to their individual characteristics, it is an incontestable fact that in a *BN* for assessing the risk of *CSCs*, many nodes have a common feature, namely risk-based. The criteria used to choose the risk-based nodes are that their conditions can be described using safety degrees and the

use of the safety degree expressions can simultaneously facilitate the simplification and application of risk assessment. Consequently, it is possible to uniformly define the risk-based nodes in a *BN* constructed using two exclusive states, "*Soundness*" and "*Weakness*". The "*Soundness*" represents the probability of being safe of the related nodes and contrarily, the "*Weakness*" responds to the probability of being unsafe of the corresponding nodes. Using such states in a risk-related *BN* is an original and reasonable attempt. Previous work in the risk assessment of using *BNs* has indicated that the most popular states used to define the corresponding risk-based nodes are developed on the basis of the frequency of event occurrence. This is possibly caused by the fact that the "likelihood" nature of the event occurrence frequency well matches the probability requirements in *BNs*. However, the unilateral consideration of the occurrence likelihood as the single criterion of measuring the risk priority could discount the accuracy of making correct decisions.

7.3.6 Determining the Prior Probabilities of the Risk Variables

Once the states of the risk factors are identified, the attention shifts to determining the prior probabilities for specifying the strengths of the direct influences among them. To provide an ordering, the root nodes (the nodes in level-1 described in Section 7.3.3) are initially serialized as $X_1, X_2, \ldots, X_i$. After all the variables in level-1 are exhausted, the nodes in level-2 are taken up from X_{i+1} to X_j. Such a hierarchy is proceeded down until a complete ordering of the form $X_1, X_2, \ldots, X_n$ is obtained. Given any node X_m, let PX_m denote its parents. The prior probabilities are only required locally to be assigned to the bunch of $PX_m \rightarrow X_m$ (parents→child) links as conditional probabilities $P(X_m \mid PX_m)$. For consistency with the axioms of probability one has to ensure that these probabilities address the relation associated with the "*Completeness of States*".

The network formalism then provides the *JPDs* over all the variables through the relation, which is called the chain rule in *BNs*: $P(X_1,\ldots, X_n) = \prod_m P(X_m \mid PX_m)$. These joint probabilities provide the quantitative assessment of the problem domain that has been modelled. In fact, on the basis of the joint probabilities, any $P(S_1 \mid S_2)$, where S_1 and S_2 individually represent a conjunction of a number of instantiated variables, can be inferred.

However, it is often not straightforward to obtain $P(X_m \mid PX_m)$. The Bayesian approach requires much information in the form of prior probabilities. In principle, most values could be acquired through failure database or experimentation. However, the experiments may be difficult to design and conduct correctly and historical data is often

not specified enough for the requirements of the Bayesian approach. In practice, therefore, it is often necessary and important to rely on subjective probabilities provided by expert judgments. Although probability is difficult to define beyond what one might intuitively understand of the term "probable" (likelihood or frequency), the subjective definition can interpret probability as a rational expression of an individual's degree of belief. One argument about this from frequentists is to question the objectivity of the value of assessment because it will be largely impossible to give a same degree-of-belief interpretation for different experts facing a certain problem. However, this does not mean that the classical or frequentist approaches can provide compelling evidence for the objectivity in the risk assessment. Actually, most practical applications of probability entail some form of subjective input. The classical and frequentist notions of probability require a subjective choice of null hypothesis and significant levels (Ludwig, 1996), "plausible symmetries" and "repeated iterations" (Smith, 1984). The traditional *QRA* is therefore no more objective than a *BN* approach. On the other hand, the real strength of one beautiful risk assessment method, as in science, lies not in its objectivity but rather in the way it exposes subjective input (Hayes, 1998).

Because subjective probabilities (beliefs) are based on informed guesses, serious deviations could happen if they are accurately expressed with precise numbers. The difficulty of obtaining point estimates of probabilities in general has been reported (Kahneman *et al.*, 1985; Zimmer, 1983). Moreover, it has been discovered (Zimmer, 1986) that linguistic expressions of probabilistic uncertainty were more accurate than numerical values in estimating the likelihood of multiple attributes through experimental studies. *FST* has been widely used to model such subjective linguistic variables and deal with discrete problems using fuzzy numbers, which more faithfully reflect expert opinion. Actually, a number of psychometric studies have evaluated the claim that fuzzy sets may be used to model qualitative probabilities with generally positive conclusions. Yet, conventional *BNs* can only employ probability expressed as real numbers. To address this issue, the following context presents a novel extension of Bayesian probability approach, which allows subjective probabilities to be appropriately expressed using the combination of fuzzy logic and *D-S* theory. A novel framework for providing logical prior subjective belief degrees is, therefore, developed based on the fuzzy logic and *ER* approaches in Section 5.2. It includes the five steps as follows[•]:

Step 1. Identify influence parameters of risk variables with subjective input.

Step 2. Define the linguistic terms and fuzzy memberships of all influence parameters.

[•] Possible major arguments might come from Steps 3 and 5. The problems on how to effectively assess the influence parameters under multi-state parent conditions and how to ensure the accuracy of subjective probabilities and validate the reliability of transformation functions can be further discussed and dealt with in Section 7.3.8 and Chapter 8.

Step 3. Assess the influence parameters based on multi-state parents and multiple expert judgements.
Step 4. Calculate the possibilities of the risk variables using the *FRB-ER* approaches.
Step 5. Transform the fuzzy possibilities to subjective probabilities using deffuzified methods.

Taking the prior probability analysis of risk-based variables as an example, the framework can be demonstrated using Figure 7.5 in the following context.

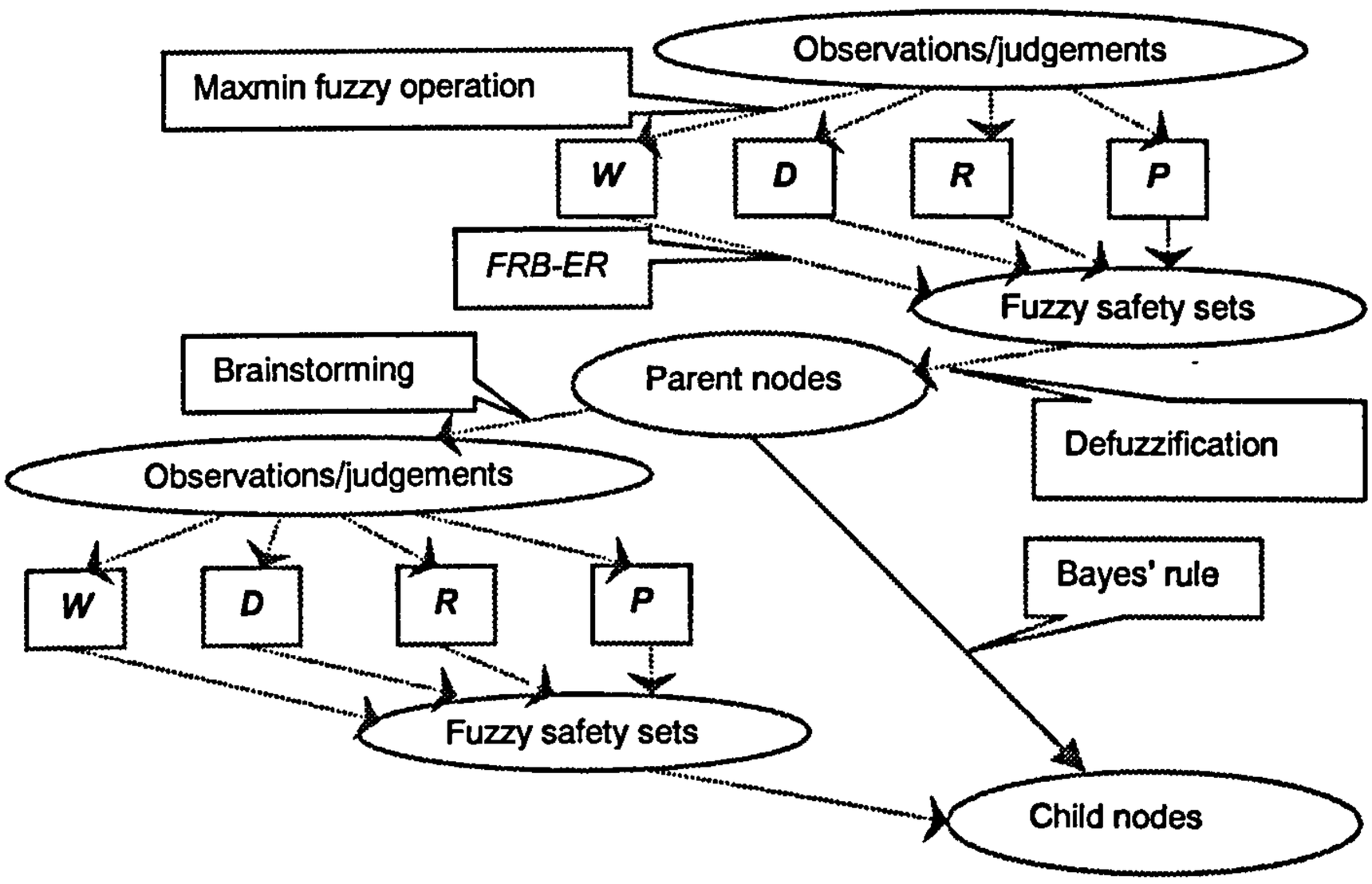


Figure 7.5. An approach to assign conditional probabilities to risk-based nodes

Observing Figure 7.5, it can be shown that it is usually difficult to directly obtain the prior probabilities of the parent and child nodes using Bayesian probability theory. Thus, fuzzy possibility theory is incorporated into the estimate of the prior subjective probabilities of nodes in *BNs*. Having studied the techniques and methods described in Chapters 5 and 6, the influence parameters of risk variables, namely junior risk parameters can be identified as "*W*", "*D*", "*R*" and "*P*", whose indications, linguistic terms and membership functions have been defined and presented in Section 5.2.2. Such risk parameters can be assessed by multiple experts with/without parent conditions and then used to calculate fuzzy safety estimations using the *FRB-ER* approach. The safety estimations are defuzzified to obtain the safety belief degrees distributed to the "*Soundness*" state using the defuzzification method introduced in Section 5.2.6. Here, all observations/judgements from multiple resources can be synthesised to avoid the loss of important information.

7.3.7 Performing the Networks for Risk Diagnosis and Prediction

Once the prior probabilities are appropriately distributed, the next task is to analyse the network constructed to obtain the posterior probabilities of the interested nodes. The objective of using *BNs* is to make the right decision depending on the corresponding posterior probabilities, which can also be explained as the inference of unobservable situations using observable reality. In the context of risk assessment, inferring the posterior probabilities is called risk prediction and diagnosis. Specially, performing a risk-based *BN* is concerned with revising probabilities for a set of risk variables (called the unobserved risk query) when an intervention fixes the values of another set of risk variables (called observed risk evidence). Any risk variables in the network can serve as a query or a piece of evidence under different circumstances, thus allowing forward inference from causes to effects (risk prediction) or backward inference from effects to causes (risk diagnosis). The simplest type of intervention is where a single risk variable is forced to take on a fixed value. The posterior probabilities for the query variables provide the estimates of the casual effects of the evidence.

The state of a risk evidence variable is assumed to be known with certainty and is often termed as an instantiation of the variable. Prior to instantiation, the propagation process yields the marginal distributions (pre-posterior analysis), whereas the query posterior probabilities are calculated with the instantiation of evidence. The magnitude of an effect from an intervention may be viewed as the change from the pre-posterior to posterior probabilities of the query for evidence in terms of their marginal distributions. For a binary variable, the effect can be expressed as

$$\left|P(Query=Yes|Evidence)-P(Query=Yes)\right|.$$

Conceptually, the pre-posterior analysis of a query variable Q_i and its posterior distribution given evidence E_i can be found by exploiting the proportionality relationship, $P(Q_i|E_i) \propto P(Q_i,E_i)$, in which, the joint probability can be computed using the chain rule. However, the required effort of this procedure increases exponentially with the number of variables, which may make the results computationally intensive. Thus, effective inference assisting tools are necessary to perform computations in any work with a large number of risk variables. One of the most popular inference tools is *Hugin* software (Andersen *et al.*, 1990).

The *Hugin* software comes with an easy to use graphical user interface (*GUI*) and provides an applicable programmer's interface (*API*), and hence, it can be used as a robust *BN* programming environment for modelling and inference. The software allows for interactive creation of the network, maintenance of the knowledge bases and

incorporates efficient calculating algorithms such as a junction-tree approach (Jensen *et al.*, 1990) to support the execution of probability calculations. In fact, the adoption of the *BN* approach does not necessarily require the users to have a Bayesian orientation toward statistical analysis (Anderson and Lenz, 2001). While *Hugin* makes it easy to key the input and read the output of the network by providing a graphical representation of the probabilities of each node as a bar graph, the general strategy of using a *Hugin BN* model must be obeyed. It can be given as follows (Wang and Trbojevic, 2006):

- Initially, the nodes of *BNs* must be mapped out (enter evidence for some variables).
- Secondly, the states of the nodes must be defined (observe the effect of the evidence on other variables).
- Thirdly, the probabilities of each state must be determined (explain the new probabilities).

In order to explain the network inference process in a *CSC* setting, a simplified example (Figure 7.6) is given to represent a generic scenario for a queuing problem in container terminals. Most importantly, the aim of this scenario is to clarify how a *BN* actually infers and to demonstrate how the *Hugin* software can be incorporated and assist in simplifying the calculations and making appropriate decisions.

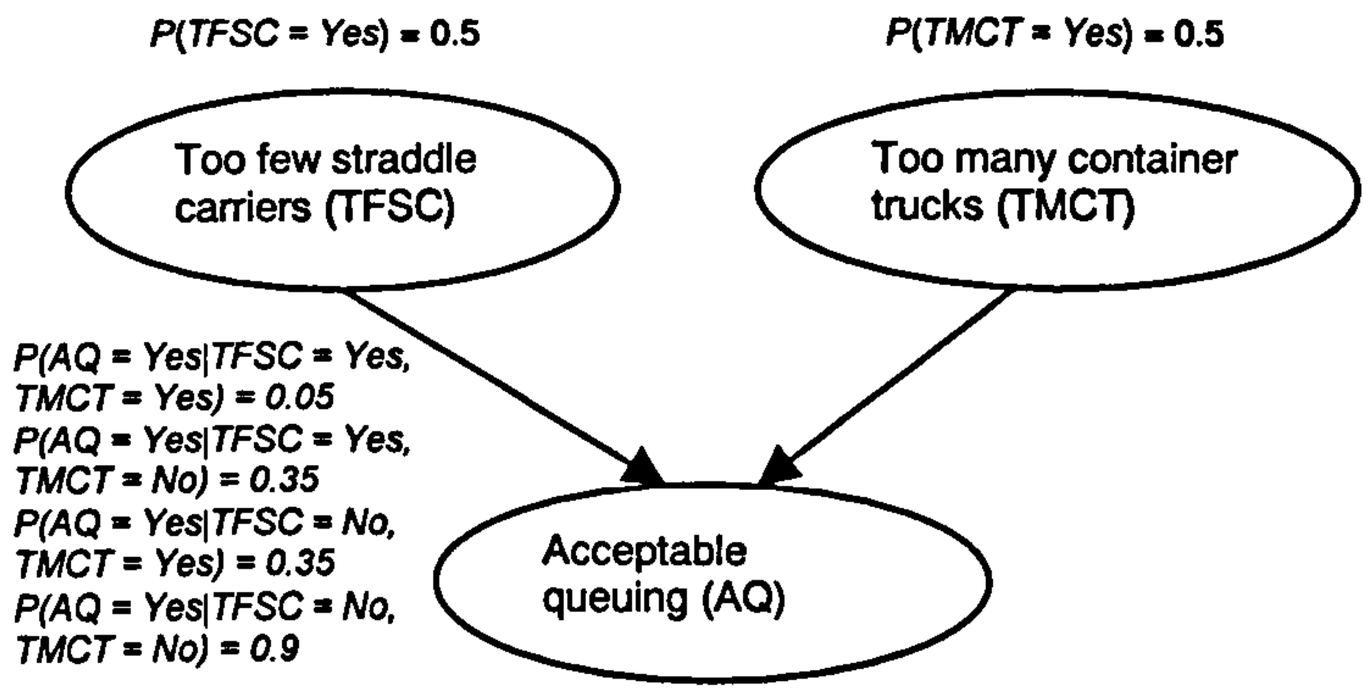


Figure 7.6. A *BN* of analysing a queuing problem in container terminals

Considering the model from the viewpoint of "pure" queuing, the productivity of straddle carriers will not affect the quantity of container trucks, unless the queuing situations are observed. Observing Figure 7.6, the prior probabilities distributed to the variables of "TFSC" and "TMCT" indicate that the situations associated with such events are totally vague so that they provide almost no assistance in making decisions.

The conditional probabilities associated with variable "AQ" are somewhat different from the ones associated with "TFSC" and "TMCT" in nature. This binary node has two binary parents and consequently, there are 8 (2^3) probabilities required and listed. Such

values in the figure suggest that the probability of "AQ = Yes" ranges from unlikely (5%) increasingly to very likely (90%) when conditions change. Such a situation is obviously not beneficial for decision makers to understand the nature of "AQ", especially with the emergence of more parents. An unconditional probability of "AQ" must be obtained using the values of these conditional probabilities. The calculation of the unconditional probability is called marginal probability distributions. To compute marginal probability, the corresponding *JPT* is required. According to the chain rule in *BNs*, the *JPT* of this case can be obtained in Table 7.1.

Table 7.1. The joint probability table of the variables "TFSC", "TMCT" and "AQ"

	TFSC = Yes		TFSC = No		AQ marginal probability
AQ	TMCT = Yes	TMCT = No	TMCT = Yes	TMCT = No	
Yes	0.05×0.5×0.5	0.35×0.5×0.5	0.35×0.5×0.5	0.9×0.5×0.5	0.4125
No	0.95×0.5×0.5	0.65×0.5×0.5	0.65×0.5×0.5	0.1×0.5×0.5	0.5875

The process of computing "AQ" marginal probabilities is called pre-posterior analysis. Given such an analysis, the *BN* can now be used to conduct various types of risk analysis, including risk diagnosis and prediction analysis.

The risk diagnosis analysis is to compute the probabilities of the interested causes in the light of observable evidence of other causes and/or effects. In this case, it can be explained as the calculations of $P(TFSC \mid AQ)$, $P(TMCT \mid AQ)$, $P(TFSC \mid TMCT, AQ)$ and $P(TMCT \mid TFSC, AQ)$. The Bayes' foundational rule can be used in the calculations. For example,

$$P(TFSC = Yes \mid AQ = Yes) = \frac{P(AQ = Yes, TFSC = Yes)}{P(AQ = Yes)}$$

$$= \frac{\sum_{TMCT=Yes} P(AQ = Yes, TFSC = Yes, TMCT = Yes)}{P(AQ = Yes)}$$

$$= \frac{(0.05 \times 0.5 \times 0.5) + (0.35 \times 0.5 \times 0.5)}{0.4125}$$

$$= 0.2424$$

All the other calculations can be carried out in a similar way.

The risk prediction analysis is to calculate the probabilities of interested effects in the light of observable evidence of causes and/or other effects. Here, the risk prediction analysis in this case means attempting to obtain $P(AQ \mid TFSC)$ and $P(AQ \mid TMCT)$. For example,

$$P(AQ = Yes \mid TMCT = Yes) = \frac{P(AQ = Yes, TMCT = Yes)}{P(TMCT = Yes)}$$

$$= \frac{(0.05 \times 0.5 \times 0.5) + (0.35 \times 0.5 \times 0.5)}{(0.05 \times 0.5 \times 0.5) + (0.95 \times 0.5 \times 0.5) + (0.35 \times 0.5 \times 0.5) + (0.65 \times 0.5 \times 0.5)}$$

$$= 0.2$$

However, the nature of "*TMCT*" is fuzzy and its definition is relative so that it is usually difficult to be directly observed. Therefore, a new risk variable "Sound Road Surface (*SRS*)" is incorporated to provide evidence for "*TMCT*". The real aim of the incorporation lies in not repeating the risk prediction analysis, but demonstrating how *BNs* can continue performing themselves when new nodes (evidence) enter into the model without significantly changing the original constructed model. The new *BN* after the entry of the node *SRS* is shown in Figure 7.7.

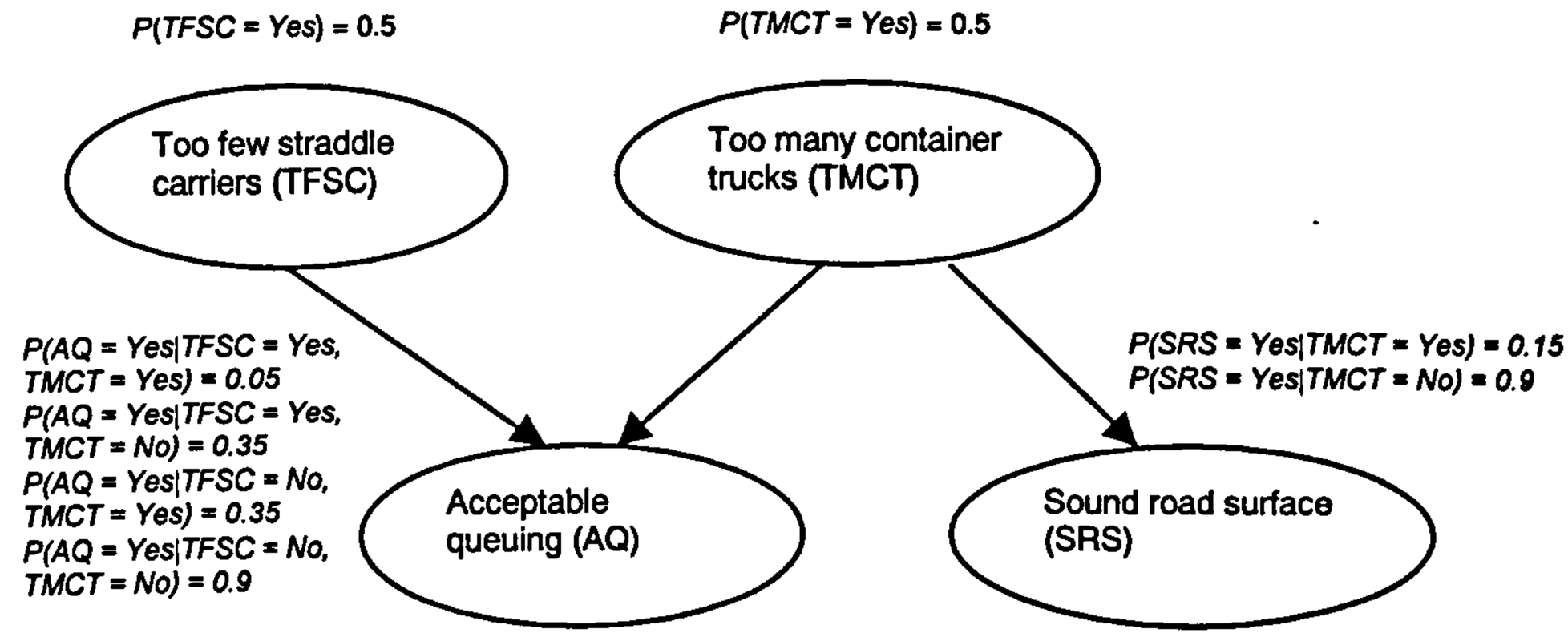


Figure 7.7. The updated *BN* when new nodes are incorporated

In the new *BN* model, the situation of "*SRS*" is obviously easy to be observed and the node "*SRS*" is closely related to the variable "*TMCT*". Therefore, when the evidence is entered into "*SRS*", "*TMCT*" can obtain certain information for further predicting the probability of "*AQ*". If the "*SRS*" observed is in the state "Yes", then the new probability distribution of "*TMCT*" can be calculated using a risk diagnosis analysis.

$$P(TMCT = Yes \mid SRS = Yes) = \frac{P(SRS = Yes \mid TMCT = Yes) \times P(TMCT = Yes)}{P(SRS = Yes)}$$

$$= \frac{P(SRS = Yes \mid TMCT = Yes) \times P(TMCT = Yes)}{P(SRS = Yes \mid TMCT = Yes) \times P(TMCT = Yes) + P(SRS = No \mid TMCT = No) \times P(TMCT = No)}$$

$$= \frac{0.15 \times 0.5}{0.15 \times 0.5 + 0.9 \times 0.5}$$

$$= 0.1429$$

The probability of $P(TMCT = Yes)$ reduces from 50% to 14.29%. Such a change will no doubt affect the probability of $P(AQ)$.

$$P(AQ = Yes) = P(AQ = Yes \mid TMCT = Yes, TFSC = Yes) \times P(TMCT = Yes) \times P(TFSC = Yes) + P(AQ = Yes \mid TMCT = Yes, TFSC = No) \times P(TMCT = Yes) \times P(TFSC = No) + P(AQ = Yes \mid TMCT = No, TFSC = Yes) \times P(TMCT = No) \times P(TFSC = Yes) + P((AQ = Yes \mid TMCT = No, TFSC = No) \times P(TMCT = No) \times P(TFSC = No) = 0.05 \times 0.1429 \times 0.5 + 0.35 \times 0.1429 \times 0.5 + 0.35 \times 0.8571 \times 0.5 \; 0.9 \times 0.8571 \times 0.5 = 0.5643$$

Consequently, it can be predicted that if the road surface is sound, then the probability of queuing being acceptable will be increased from 0.4125 to 0.5643.

It is obvious that even for such four binary variables, the risk diagnosis and prediction analyses have been quite complex and time-consuming. Thus, the *Hugin* software will be applied to compare how effectively it can assist in the simplification of the problem. For example, the risk prediction analysis given that "*SRS*" is true is provided in Figure 7.8.

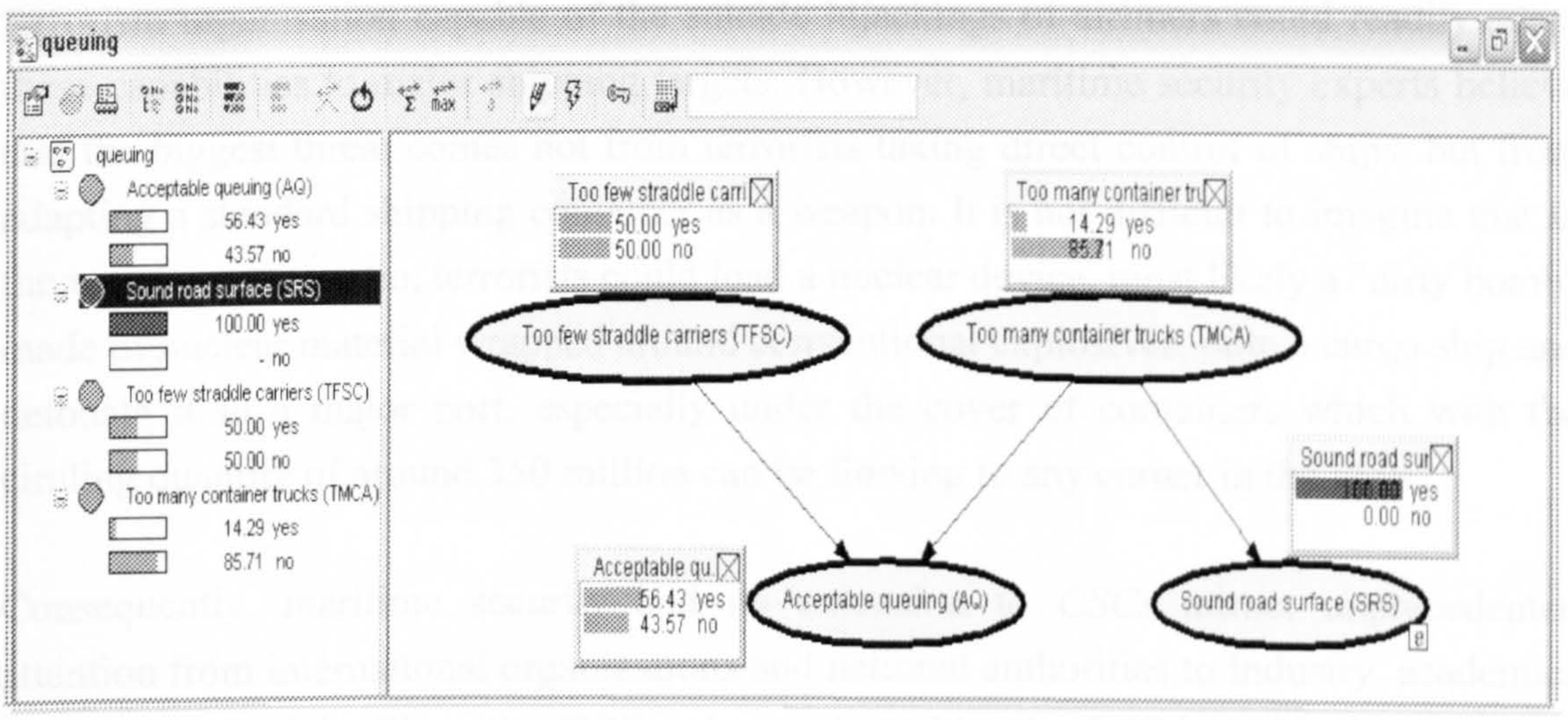


Figure 7.8. The risk prediction analysis of "*AQ*" given "*SRS* =Yes"

7.3.8 SA

The final step is to evaluate the findings and test whether the results and the models can meet the initial objectives or not. *SA* is the process of examining the assumptions and parameters of the models and checking the robustness of the solution to those assumptions. It can be described as "what if analysis" by academics where the implication of alternative conditions to the assumptions is investigated (Samson, 1988). There are two kinds of *SA* proposed in this study, which are individually related to single and multiple risk input prior probability changes. The single risk input related *SA* assists

in this process by slightly changing the probabilities of the risk input nodes in order to observe the state that the model responds to these changes so as to judge the accuracy of the model applied to risk assessment. The range of the lowest and highest possible changing values that each input node can take can be subjectively chosen and the values are considered as the thresholds of the slight probability variation of the risk input nodes. The *SA* associated with multiple risk input prior probability changes is not used for the validation of the model established. It mainly functions on the ranking and prioritization of those key risk factors of influencing the interest node(s) of the research. This will be analysed in the next chapter in detail.

SA is carried out to find the errors made during the risk assessment process. The errors are usually associated with the database, the assessors' probabilistic judgements, the modelling effort and the risk prioritising process itself.

7.4. A Case Study of the Terrorism Threat in *CSCs*

As described previously, there is widespread concern in the international society that a terrorism organisation capable of the suicide hijackings of airliners could readily adapt these capabilities to major shipping targets. However, maritime security experts believe that the biggest threat comes not from terrorists taking direct control of ships, but from adapting a standard shipping container as a weapon. It is not difficult to imagine that in the worst case scenario, terrorists could load a nuclear device, most likely a "dirty bomb" made of nuclear material wrapped around conventional explosives, onto a cargo ship and detonate it in a major port, especially under the cover of containers which with the circling quantity of around 350 million can be flowing to any corner in the globe.

Consequently, maritime security and its extension to *CSCs* attract unprecedented attention from international organizations and national authorities to industry, academics and even the public. Since the *ISPS* code was issued by the *IMO* in 2002, the American government has published two container transport security regulations, *CSI* and *C-TPAT* (*OECD*, 2003). Recently, due to the geopolitical climate requirement the *EU* pushed an urgent security regulation to expand the *ISPS* to further discussion, which aims at ensuring the highest possible levels of security for seamen, ships, ports and the whole intermodal transport chains (*EU*, 2003).

Some risk assessment and management experts have attempted to use traditional risk assessment approaches to deal with the terrorism threats to *CSCs*. Unfortunately, many of such approaches suffer two difficulties. One is related to the quantitative assessment of the risks, more precisely speaking, the challenge lies in failing to obtain information

in an appropriate form (combining the subjective and objective data) suitable as input to a *QRA*. The other is associated with the assessment feasibility and flexibility aiming at dealing with dynamic situations in the chains. Assessment tools are required to have the capability of responding to the terrorism threats (emergency) instantly or at least in a short time constraint and considering (admitting and deleting) different risk information (observations) or parameters to a well suited variety of chains facing different terrorism threats. This case study, using the *BN*-based risk assessment methodology developed in Section 7.3, can deal with such problems and provide a significant contribution in assisting people to better understand the risks and make appropriate anti-terrorism decisions. *BNs*, with their foundational inference rule (Bayes' theorem) and modern computing software (i.e. *Hugin*) make it possible to instantly and dynamically assess the terrorism threats in a friendly interface. Following on from this case is an organization of eight steps closely connected with the methodology.

Step 1: The domain of the terrorism risk research

The interest of this study is focused on one kind of risk, terrorism attacks on physical cargo flows of an assumed targeting *CSC* in its operational process. Therefore, the lines to constrain the research scope are clearly drawn. Firstly, the interest of focus is not a whole supply chain. Secondly, the risk is related to the physical cargo flow of *CSCs*, then those terrorism attacks on the other flows such as the information flow are beyond the research scope. Thirdly, the study only cares about the attacks or threats in the operational process. Finally, any influence resulting from terrorism in economic and managerial aspects will not be admitted here.

Step 2: The risk variables identification

To identify the risk variables related to the terrorism threats in the *CSC*, one analysis of the operational procedure of a container cargo physical flow is required. The normal functioning of the procedure has been reviewed in Section 2.2.1.

A *HAZOP* team formulated can break the process down into appropriate subsystems (nodes). In this study, they are associated with cargo, people, ship, port and inland transportation (See Section 3.4.2). From the viewpoint of security, the five nodes will be further analysed to identify the corresponding risk variables in Table 7.2.

Step 3: Construct a qualitative network

Having analysed the risk factors in the *CSC* with their causes and effects, a qualitative *BN* representing the terrorism threats in the *CSC* can be constructed. Firstly, the root causes in the scenario are identified from Step 2. They include "Intelligence networks", "Checking and supervision", "External", "Internal", "Missile" and "Accessibility", which are not influenced by other risk factors. These root causes are then assigned a node

Table 7.2. The risk factors related to terrorism threats and their causes and results

Risk factors	Causes, effects and their relationships
Cargo	The safety degree of "Cargo" is directly decided by two causes "Intelligence networks" and "Checking and supervision". It will affect the safety of "Containership", "Port" and "Inland transportation".
People	The safety degree of "People" is influenced by "External" and "Internal" persons. It can affect the safety of "Containership", "Port" and "Inland transportation".
Containership	The terrorism threats related to "Containership" will mainly come from two causes: attacking "Bulkhead" and "Engine room". Furthermore, terrorists will use "Missiles" or "hazardous cargo" to carry out the attacks on "Bulkhead" and the attacks on "Engine room" may be implemented by terrorists' hijacking actions.
Port	The combination of "Cargo" and "People" as well as "Containership" can be used to attack valuable port facilities on "Terminal". "Containership" can also take suicide actions to block its "Channel". "Inland transportation" can attack the "Port" directly.
Inland transportation	The "Inland transportation" depends upon its "Accessibility", "Cargo" carried and the "People" driving it.
Supply chain	The risk factors "Containership", "Port" and "Inland transportation" together influence the safety of "Supply chain".

each, and are considered as the level-1 nodes. Secondly, in Table 7.2, the risk factors, which are directly influenced by the root causes, are identified as "Cargo", "People", "Bulkhead" and "Inland transportation". They can be assigned as the level-2 nodes. A series of links are drawn from the level-1 nodes to the level-2 nodes regarding the direct influence relationships. Thirdly, such a process continues until the risk factor "Supply chain" is assigned a node and the links from the nodes "Containership", "Port" and "Inland transportation" are connected. Finally, the qualitative *BN* representing the terrorism threats in the *CSC* is constructed in Figure 7.9.

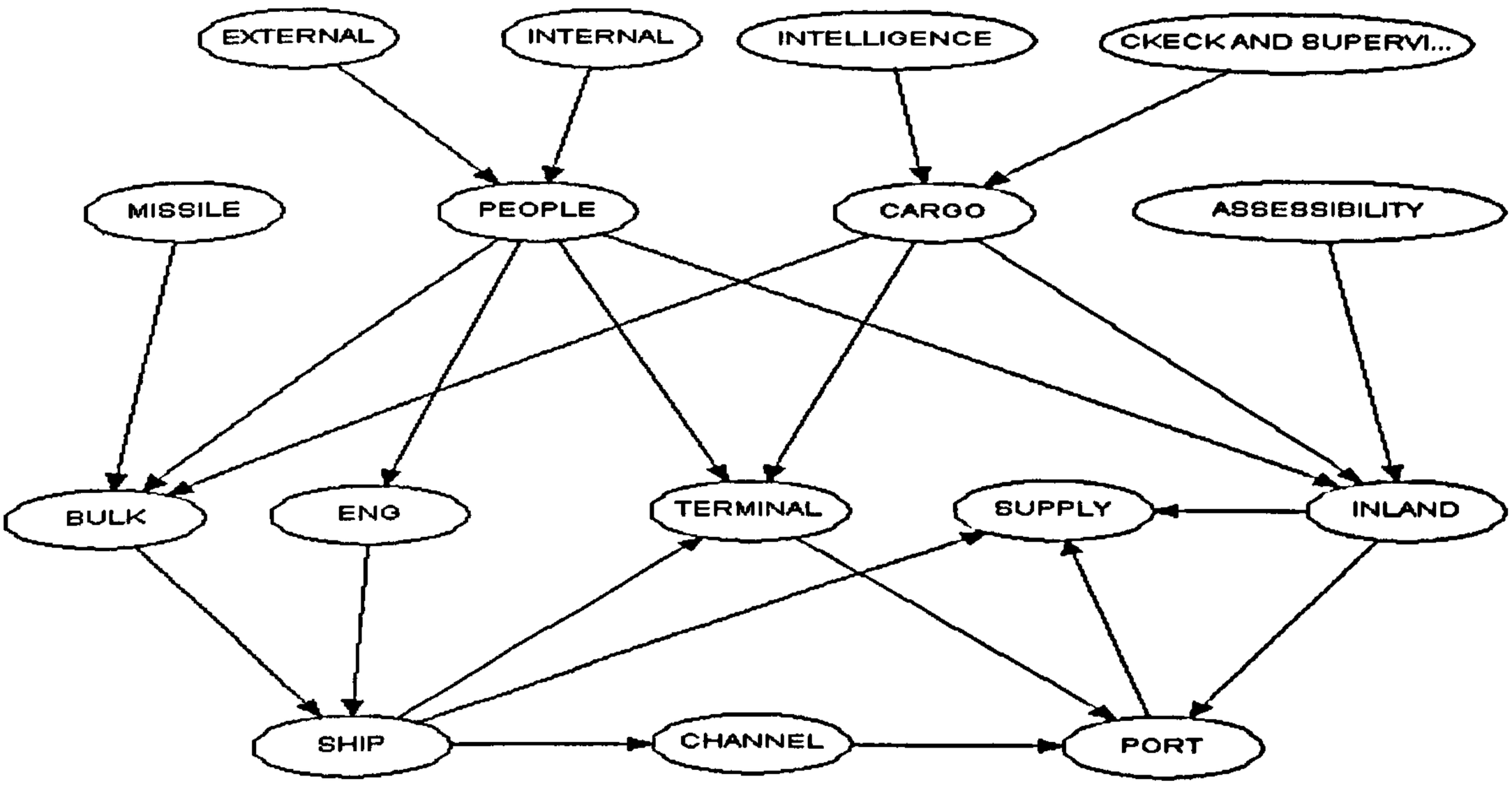


Figure 7.9. The original qualitative *BN* representing the terrorism threats in the *CSC*

Step 4: Check and modify the qualitative network

Using the concept of d-separation to check the network built in Figure 7.9, it is necessary to investigate one node after another starting from the level-1 nodes. Having given an example to demonstrate the practical usage of the concept in checking the accuracy of the network in the methodology, each node with its links in Figure 7.9 is carefully analysed. For example, if the node "Cargo" is given evidence, then the change of the probability distribution of the node "Intelligence network" will affect the node "Checking and supervision" but not affect the nodes "Bulkhead", "Terminal" and "Inland transportation". Such analysis can go smoothly on until the investigation of the nodes "Terminal", "Bulkhead" and "Inland transportation" starts. Such three nodes have a common characteristic, conditional on the nodes "Cargo" and "People". Given evidence to the nodes, the probability distribution changes of the other parent nodes of the three nodes, such as "Missile" and "Accessibility" will directly affect neither the probability of the node "Cargo" nor the one of "People" but the combination of the nodes. Therefore a new node, namely "Car-ple", is incorporated to deal with such a situation, shown in Figure 7.10 (the new node is also called "intermediate variable" in *BNs*). This can be explained using the fact that in normal situations, "Cargo" seldom has the capability to complete a terrorism attack without the assistance of "People".

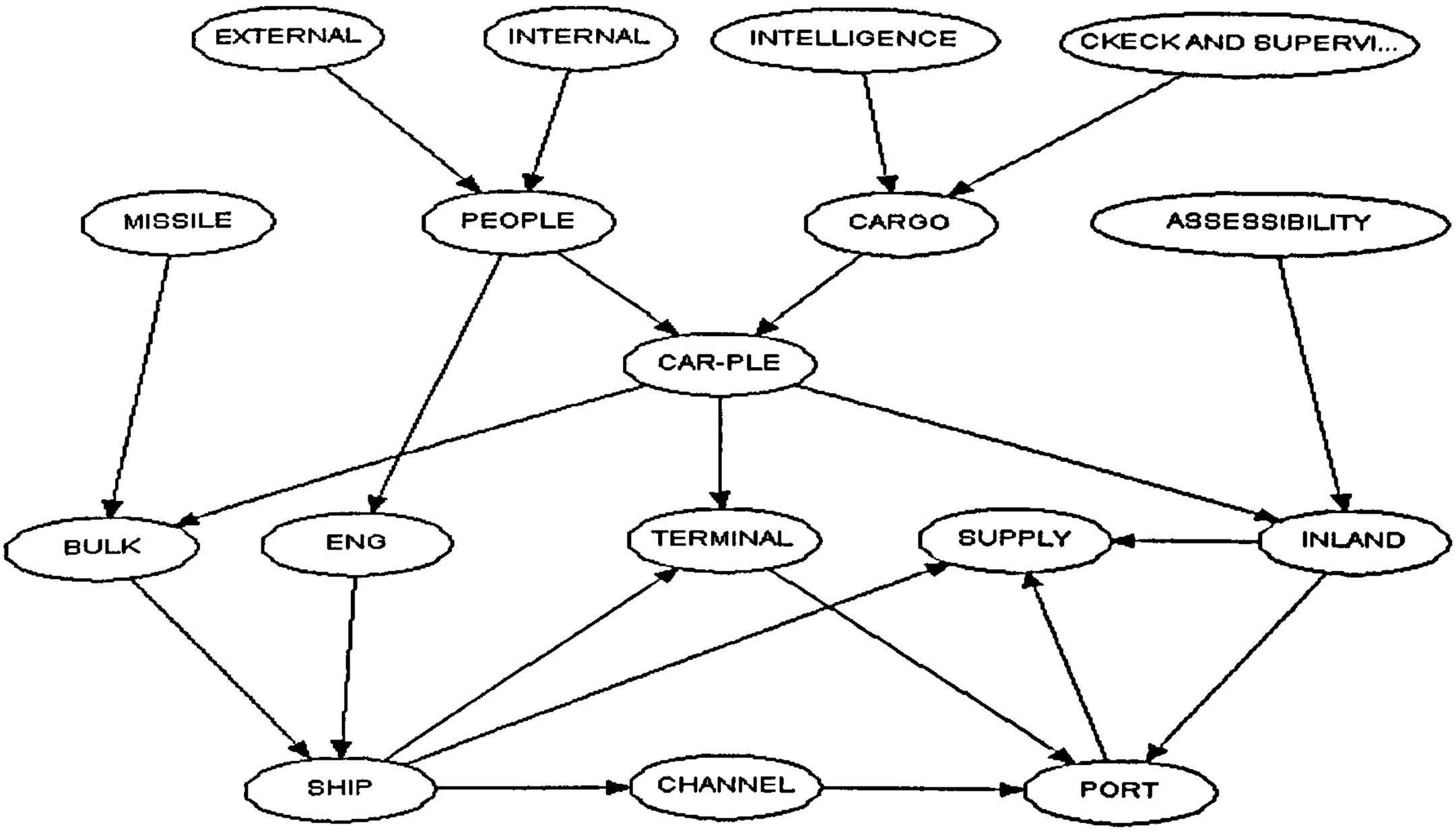


Figure 7.10. The new qualitative network checked using the D-separation concept

Step 5: Define the states of the nodes

This step describes the actual states of the nodes in the network established for the analysis of the terrorism threat associated with the *CSC*. The objective of defining the states of the nodes is to appropriately assign the prior probabilities. In the process, the

modelling aspects of the nodes and the qualitative description of the network through the causal relationship among the variables can also be further consolidated.

The network presented in Figure 7.10 aims at describing the terrorism risks. The nodes in the network can thereby only be explained under the circumstance of terrorism. In other words, the nodes and network can only be properly modelled and understood when a terrorism threat emerges or prepares to emerge. Thus, the threat or attempt of the threat will become the premise for defining the actual states of the nodes.

Assuming that terrorists use/attempt to use "Cargo" to attack the *CSC*, two potential factors may counteract their actions or change their decision. They are "Intelligence network" and "Checking and supervision". If the "Intelligence network" is consummate, the success rate of the terrorism attacks using "Cargo" will be very low. Contrarily, the likelihood of using "Cargo" to attack the *CSC* will significantly increase when the "Intelligence network" is flawed. Thus the "Intelligence network" is modelled as having the states "Flawless" and "Flawed". Similarly, "Checking and supervision" can be modeled into two states: "Checked" and "Ignored". The safety level of the node "People" is affected by the risks of external terrorists' direct attacks and the ones from internal terrorists under the guise of employees. The external people can be categorized into two types, "Friendly" and "Hostile" in the chain. The internal persons may consist of normal employees and some terrorists with spurious identification as working staff, and thus, can be defined as having two states, "Immune" to terrorists and "Infective" by terrorists. The marriage of "Cargo" and "People", "Car-ple", forms the most possible threat to the *CSC*. It may be used to attack the "Bulkhead" of "Containership" when "Internal" terrorists plan the position of the containers with hazardous "Cargo" near the bulkheads chosen between two compartments. It may be used to attack the valuable facilities on container "Terminal" under the assistance of either "External" or "Internal" terrorists. It may also be used to attack "Inland transportation" or more likely to use its flexibility and accessibility to attack any vulnerable places targeted by terrorists. Consequently, the "Bulkhead" can be assigned two states, "Attacked" and "Protected". The "Accessibility" to a targeted valuable place can have two states, "Likely" and "Unlikely". The "Bulkhead" may be stroked by direct "Missile" attacks, which are considered in two conditions, "Yes" and "No". The sinking of the "Bulkhead"-damaged "Containership" or the suicide-taken "Containership" controlled by terrorists "Hijacking" the "Engine room" can threat the "Channel". Thus, the states of the node "Engine room" are "Hijacked" and "Defended". According to the criteria given in Section 7.3.5, all other nodes in the network, "Cargo", "People", "Car-ple", "Containership", "Terminal" and "Channel", "Port", "Inland transportation" and "Supply chain" are identified as the risk-based nodes with the nature of threats. They can be

therefore uniformly defined to have two states, "Soundness" and "Weakness".

Step 6: Assign prior unconditional and conditional probability distributions

This step assigns prior probability distributions to all the nodes and their states introduced above. The prior probabilities of some nodes are obtained based on available data or information. However, for the others (i.e. the risk-based nodes) whose prior probabilities cannot be directly obtained, the subjective expert judgments using the fuzzy logic and *ER* approaches are employed. For example, the basis of the assigned probability distributions of the nodes "Intelligence network", "Checking and supervision", "Engine room" and "Cargo" representing the two different groups above can be stated as follows. For the other nodes, the prior probabilities can be analysed in a similar way and presented in Appendix 5.

Intelligence network: Currently some 90 warships from countries including the UK, Germany, France, Australia, Italy, Japan and Bahrain - under the command of the US Fifth Fleet - are patrolling the waters around the Arabian Peninsula and off the coasts of Pakistan and East Africa for cutting off the most likely escape route and gathering intelligence on the maritime-based logistics network believed to have been developed by terrorists (Felsted and Odell, 2002). This display of naval firepower is concentrated on just one facet of al-Qaeda's use of the shipping industry. Western intelligence agencies suspect the maritime capabilities of the terrorist organisation extend much further. From the viewpoint of securing *CSCs*, the robust degree of the intelligence networks is not perfect. This point can be supported by the facts that a) the phenomenon of stowaways and drug smuggling widely exists; b) the control of the vessels owned by terrorism organizations is not effective (even the guessing scope of the vessel quantity is between 10 and 80) (Felsted and Odell, 2002). Thus the probability distribution of the node "Intelligence network" can be subjectively judged as "Flawless" with 0.8 credibility and "Flawed" with 0.2 belief degree.

Checking and Supervision: Although the American government has attempted to supervise containers' contents and integrity as far upstream in a supply chain as possible in order to reduce the risks probably emerging in the downstream in the chains using the two regulations, *CSI* and *C-TPAT*, in most cases in current practical operations containers are only randomly checked, either physically or using scanners, by import and expert port Customs with a 2-3 percent checking rate individually (normally, import checking is stricter than the export one). Thus, it is reasonable to assume the probabilities of "Checking and supervision" as "Checked" with 0.05 probability (the sum of import and export checking rates) and "Ignored" with 0.95 confidence degree.

Engine room: Compared to the direct attacks on vessels, maritime security experts claim that it is possible for terrorists to imitate/incorporate/employ pirates for hijacking ships to hit other objectives, either ports or vessels. Thus, maritime terrorism alert can/should be lessoned from piracy reports published by the International Maritime Bureau (*IMB*). The *IMB* annual piracy report for 2002 states that in total 370 attacks on shipping at sea worldwide - up from 335 in 2001, there are 25 incidents up from 16 ones in hijackings, but many involved smaller boats, such as tugs, barges and fishing boats. Given this data and considering the amount of containerships sailing in the world, the probability, *P(Engine room = Hijacked | People = Soundness)* = 0 can be reasonably inferred. However, the situation may be significantly altered if the "People" is vulnerable. Experts believe that the probability *P(Engine room" = Hijacked | People = Weakness)* can at least increase 20 percent up from 0.

Cargo: The prior conditional probability distributions require to be acquired using subjective expert judgements. Differing from the subjective estimations discussed above, the subjective probabilities associated with "Cargo" are not straightforward to be judged directly, especially when its states consist of many sub-parameters and are conditioned on two parent nodes simultaneously. Thus, the five-step methodology introduced in Section 7.3.6 is used.

Given the "Flawless" state of the node "Intelligence network" and the "Checked" state of the node "Check and supervision", the observations related to "Cargo" can be described using fuzzy membership functions as follows: ***W*** is a triangular distribution defined by a most likelihood at 0.15, with lower and upper least likelihood at 0 and 0.3; ***D*** is a single deterministic value with 100% certainty at 0.1; ***R*** is a trapezoidal distribution defined by a most likely range between 0.2 to 0.3, with lower and upper least likelihood at 0.1 and 0.4; ***P*** is a closed interval defined by an equally likely range between 0.2 to 0.5. Consequently, using the *FRB-ER* approach, the possiblistic safety distribution of "Cargo" given the conditions can be calculated as *Poss(Cargo | Intelligence network = Flawless, Check and supervision = Checked)* = {0, "Poor", 0, "Fair", 0.084, "Average", 0.916, "Good"}. Based on Equations (5.6) and (5.7), the conditional probability distributions of "Cargo" can be obtained by defuzzifying and transforming the conditional possibilistic safety degrees as follows:

P(Cargo = soundness | Intelligence network = Flawless, Check and supervision = checked) = $0.084 \times 0.5926 + 0.916 \times 1 = 0.96$.

P(Cargo = weakness | Intelligence network = Flawless, Check and supervision = checked) = $1 - 0.96 = 0.04$.

In a similar way, the *CPT* of the node "Cargo" can be computed and shown in Table 7.3.

Table 7.3. The prior conditional probabilities of "Cargo"

Intelligence networks	Flawless		Flawed	
Checking and supervision / Cargo	Checked	Ignored	Checked	Ignored
Soundness	0.96	0.44	0.48	0.02
Weakness	0.04	0.56	0.52	0.98

Step 7: Perform analysis of the network for the posterior probability distributions and conduct risk diagnosis and prediction

The evaluation of the probability of the *CSC* attacked by terrorists needs complex and special calculation and techniques. Thus, the analysis of the *BN* constructed in Figure 7.10, with all prior conditional probability distributions assigned above, is performed with the assistance of the *Hugin* software, as shown in Figure 7.11.

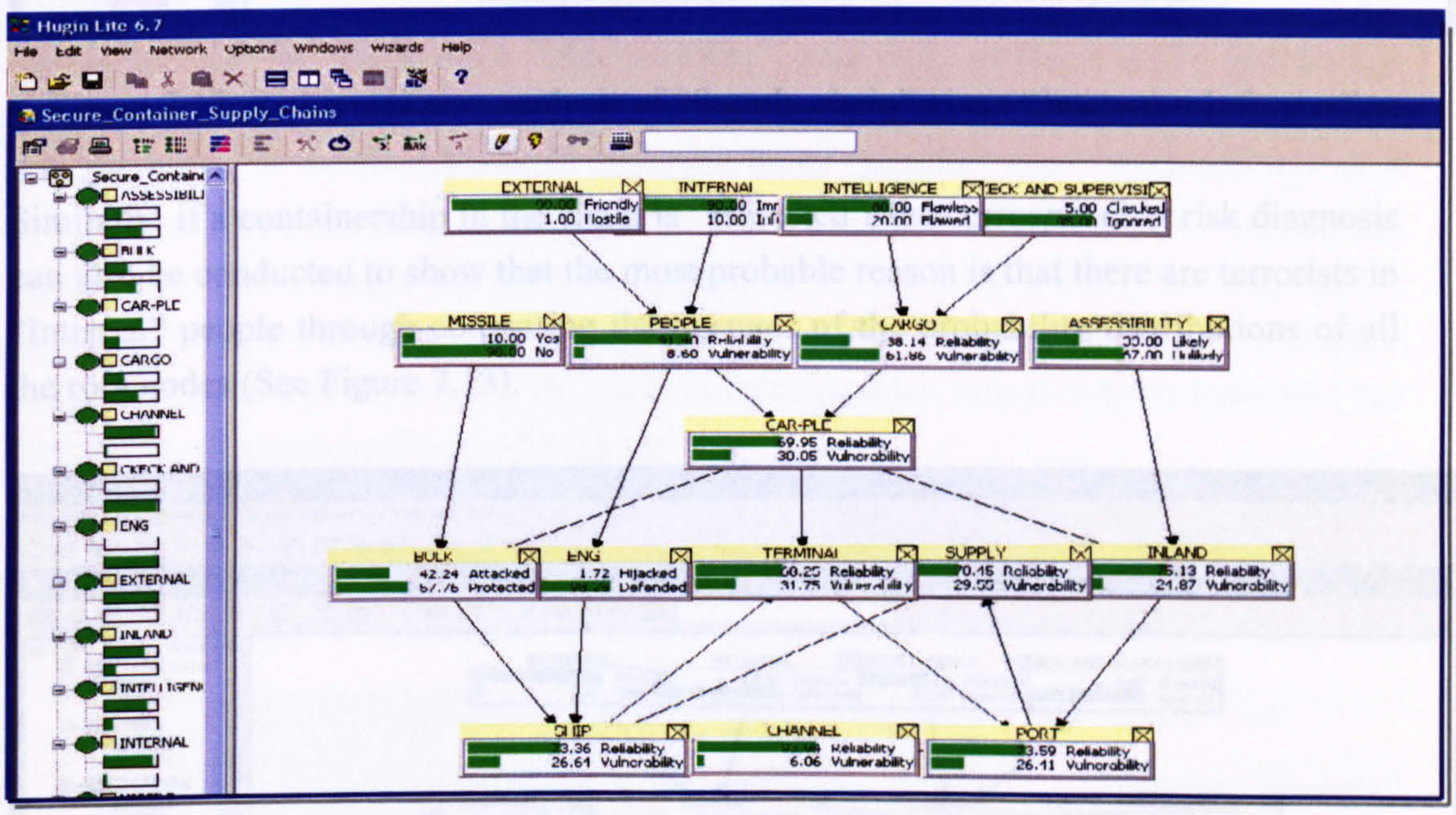


Figure 7.11. The pre-posterior probability distributions using *Hugin* software

In the "run" mode of the software, the initial unobservable pre-posterior probability of the terrorism risks on the *CSC* is obtained as "Soundness" with 0.7045 belief degree and "Weakness" with 0.2955 creditability. Given such an original risk assessment model, any risk diagnosis and prediction in various situations can be inferred. Assume that the condition related to "Internal" people alters and the evidence on the state "Infective" is obtained, as some employees are found to have a close relationship with a terrorism organization. Then the safety level of "Supply chain" can be immediately updated and reassessed as "Soundness" with 0.5915 credibility in Figure 7.12 and a new security plan can be made to ensure the exemption of the chain from terrorism attacks.

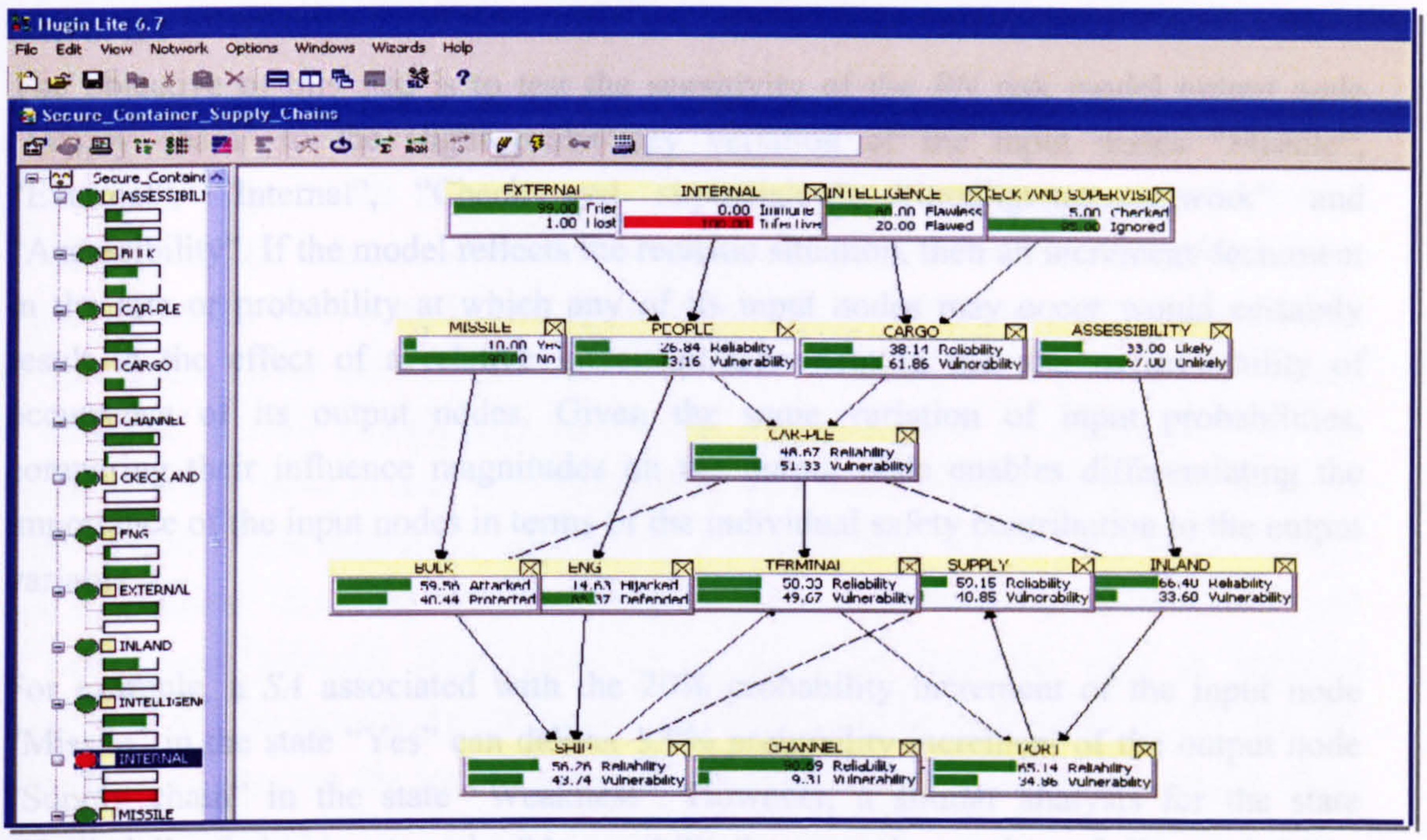


Figure 7.12. Risk prediction analysis of "Supply chain" given "Internal = Infective"

Similarly, if a containership in the chain is "Hijacked", the corresponding risk diagnosis can also be conducted to show that the most probable reason is that there are terrorists in "Internal" people through comparing the changes of the probability distributions of all the root nodes (See Figure 7.13).

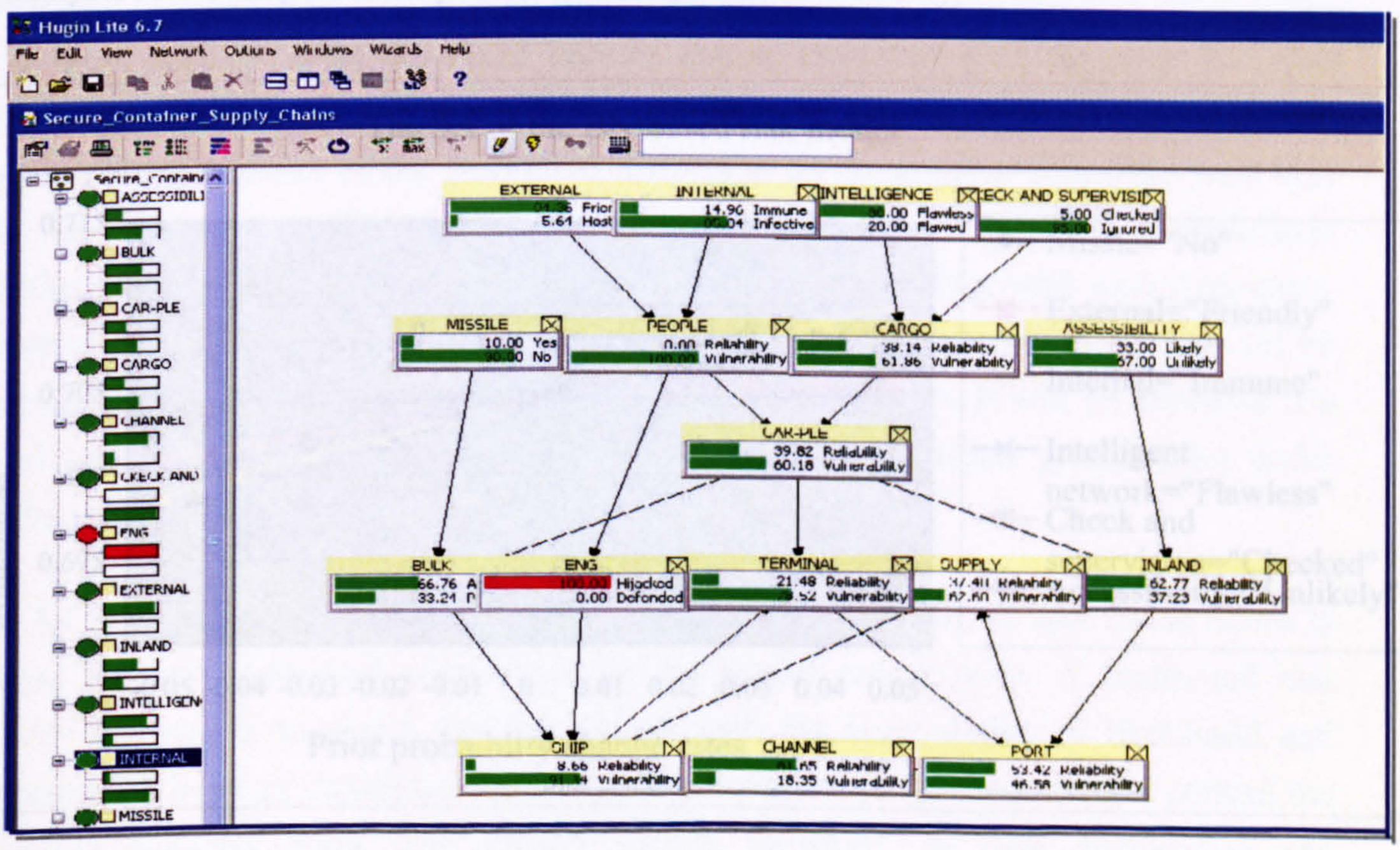


Figure 7.13. Risk diagnosis analysis given "Engine room = Hijacked"

Step 8: SA

The objective of this step is to test the sensitivity of the *BN* risk model output node "Supply chain" to the slight probability variation of the input nodes "Missile", "External", "Internal", "Check and supervision", "Intelligence network" and "Accessibility". If the model reflects the realistic situation, then an increment/decrement in the rate or probability at which any of its input nodes may occur would certainly result in the effect of a relative increment/decrement in the rate or probability of occurrence of its output nodes. Given the same variation of input probabilities, comparing their influence magnitudes on the output node enables differentiating the importance of the input nodes in terms of the individual safety contribution to the output variable.

For example, a *SA* associated with the 20% probability increment of the input node "Missile" in the state "Yes" can deliver 3.9% probability increment of the output node "Supply chain" in the state "Weakness". However, a similar analysis for the state "Unlikely" of the input node "Accessibility" can only produce 2.5% probability increment of the state "Soundness" of the node "Supply chain". Such a result can prove that the output is more sensitive to the input node "Missile" than "Accessibility" and therefore, can be considered more important in making decisions. Figure 7.14 shows the influences of all the input variation on the output. For each input node, the response of the output shows a nearly linear probability distribution with respect to the probability changes of the input. Obviously, the output of the model is sensitive to its input and the analysis result keeps harmony with the reality.

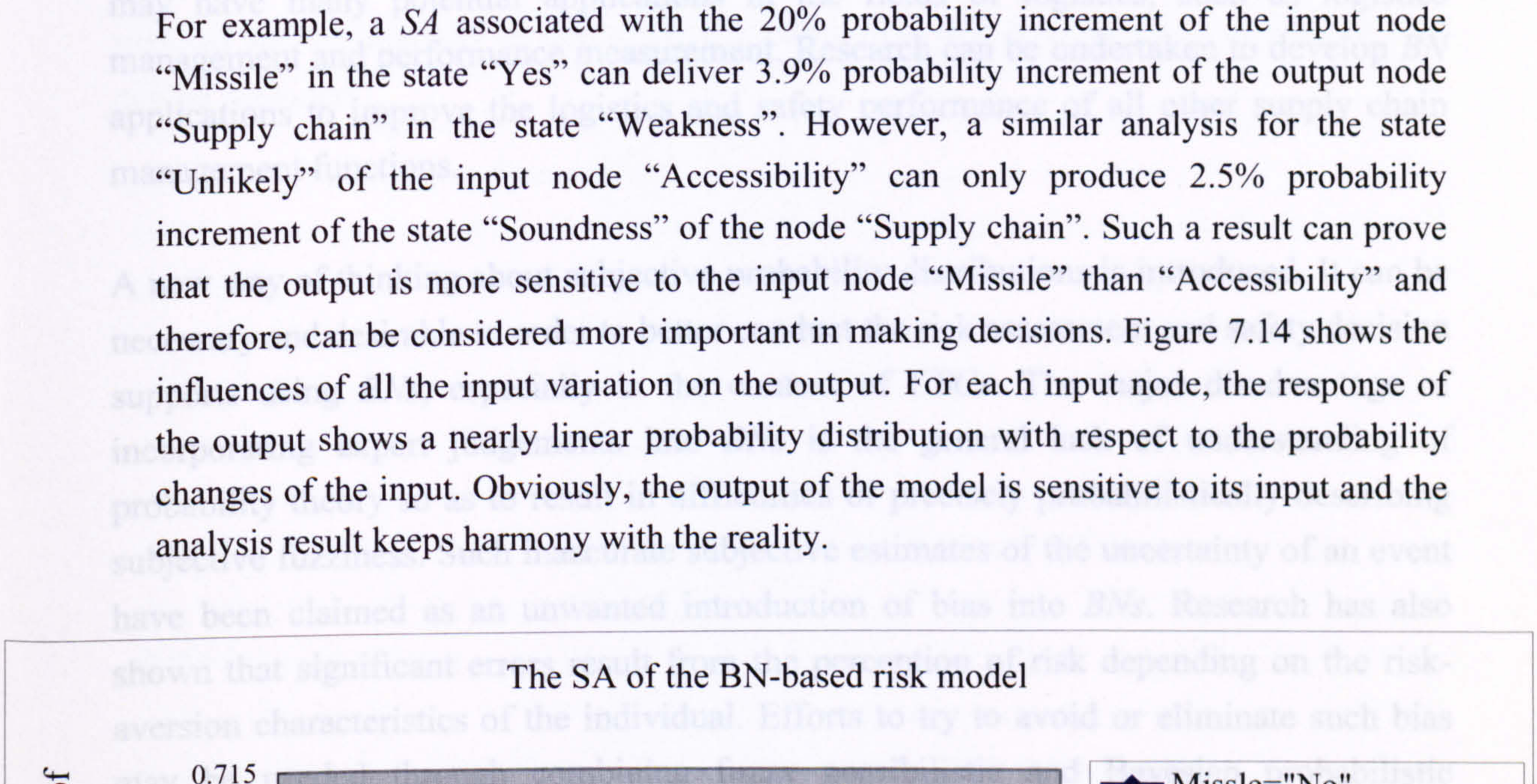


Figure 7.14. The SA of the BN based risk model

7.5 Conclusion and Future Work

This research makes full use of the *BNs*' advantages and further develops and extends the *BNs* technology to the literature of *CSCs* by exploiting a conceptual and sound methodology for the risk assessment of the chains. It describes a risk assessment *BN*, a tool/model initially built to assist risk assessors at *CSC* installations and management to draw inferences about the risks of the chains. The challenges to appropriately assess *CSC* risks lie in their complexity, uncertainty and dependent relationships. *BNs* are naturally effective tools to deal with complexity and interactive dependencies. Because of their flexibility and diagnostic capabilities, *BNs* have been widely used in the context of risk assessment, including broad risk diagnosis and safety based decision making and may have many potential applications in the fields of logistics, such as logistics management and performance measurement. Research can be undertaken to develop *BN* applications to improve the logistics and safety performance of all other supply chain management functions.

A new way of thinking about subjective probability distributions is introduced. It can be necessary and desirable in order to better conduct the risk assessment and safety decision supports using *BNs*, especially in the context of *CSCs*. The major disadvantage of incorporating expert judgements into *BNs* is the general lack of understanding of probability theory so as to result in difficulties of precisely probabilistically describing subjective fuzziness. Such inaccurate subjective estimates of the uncertainty of an event have been claimed as an unwanted introduction of bias into *BNs*. Research has also shown that significant errors result from the perception of risk depending on the risk-aversion characteristics of the individual. Efforts to try to avoid or eliminate such bias may be needed through combining fuzzy possibilistic and Bayesian probabilistic theories. The *FRB-ER* approach may provide a solution of dealing with such a problem. However, the risk parameters under multi-state and multi-parent conditions may not be accurately assessed or estimated even using linguistic variables. It will be desirable if a novel function can be generated to aggregate different conditional probabilities under single-state conditions.

The *SA* is conducted to validate the risk model. The importance of root cause nodes is judged by their individual contribution to the model output node. A traditional risk priority analysis is to assess the risk values with the combination of likelihood and consequence from an individual viewpoint and furthermore, to focus on and control the so-called high-risk areas with greater values. However, in both engineering and managerial systems, whose subsystems and components have interactive relationships, either single consideration of the values of individual risks or their individual impacts on

the node(s) of interest may be inaccurate and incomplete, and it needs to be more systematically analysed from an overall perspective. A new *SA* analysis in *BNs* requires to be carried out to observe the influence of the combination of the input nodes to the output node and furthermore, more reasonable and generic methods of prioritizing risks can be developed.

Additionally, from a vertical viewpoint, future work can also use an *ID* technique to allow analysis and validation of the networks' ability to predict the most effective *CSC* risk management solutions. The use of *ID* in *BNs* can be demonstrated as a decision making tool in the application of *FSA*, either in shipping or supply chain industries, from a more dynamic and feasible risk assessment perspective. The optimisation of safety based decision making by incorporating *ID* techniques into the generated *BNs* can be realized and sequentially an opportunity to harmonize *BNs* with the methodology of *FSA* can be provided.

Chapter 8 – Relative Risk Analysis Using Bayesian Networks and Evidential Reasoning

SUMMARY

BNs provide a unified and consistent framework for analysing and expressing risks and thus, have been widely applied to safety and reliability studies. Yet, most of them focus on using the advances of Bayesian theorem and posterior probabilities to risk prediction and diagnosis (forward and backward inference) and assume that the risk related prior probabilities could be easily obtained from subjective expert judgements if the associated objective historical failure statistics is incomplete or unavailable, although in many circumstances this is not the realistic case. This chapter, therefore, discusses and deals with some of the practical challenges of implementing Bayesian reasoning in relative risk analysis (from a Bayesian view), which is corresponding with those positivism risk analyses from a classical perspective, including risk ranking using the SA of BNs. It emphasizes the introduction of a novel "Noisier or" approach on the basis of an ER algorithm for obtaining the Bayesian prior probability distributions conditioned on multi-state parents. Consequently, analysts can assign subjective probabilities with single condition and synthesise them using the ER algorithm (and its attached computing software – IDS) without adopting the somewhat mathematically sophisticated procedure of specifying prior distributions with multiple ones. An example related to the terrorism threats in CSCs is presented to illustrate the proposed ideas.

8.1. Introduction

Most safety engineers and risk analysts have been trained to analyse risks using the 'classical' approaches, where probability exists independent of analysts – as a quantity characterising the system being studied. The concept of probability is relative frequency-based and the results of the risk analysis provide estimation of objective 'true' probabilities. This view was challenged about 30 years ago, when the need to quantify risks from large technological systems was recognized, resources were expended to produce numerical results (Apostolakis, 1988) and the quantification of the likelihood of rare accidental events could not normally be calculated without employing engineering judgements. It has been evident that the problems of risk quantification cannot be effectively handled using traditional risk analysis methods such as *QRA* in some circumstances.

BNs, as a novel risk analysis-supporting tool, together with its sound fundamental rule of inference – Bayesian theorem, can function well on the simultaneous analysis of expert

and statistical information, an aspect which makes the *BN* approach and its philosophy attractive to risk and reliability studies (Pearl, 1986). Furthermore, the networks constitute a class of probabilistic models with strong connections to graph theory (Jensen, 2001), which forms a powerful framework to allow risk analysts to apply their knowledge towards forward (risk prediction) or backward (risk diagnosis) reasoning. Such advances, together with the emergence of computing software like *Hugin*, stimulate and inspire researchers' interest of using *BNs* in systematical risk analysis (Cagno *et al.*, 2000; Boudali and Dugan, 2005).

Although prior research has greatly increased our understanding that *BNs* have the capability of conducting risk prediction and diagnosis, many of these discussions have been made without a sufficient consideration of the challenges faced when *BNs* are employed in the field of risk assessment, such as Bayesian risk nature, the accuracy and reliability of subjective prior probability distributions and the risk ranking in a networking environment.

This chapter, therefore, is constructed to deal with such challenges by developing a new model for relative risk analysis based on *BNs* and *ER*. For this purpose, the remainder of the chapter is organised as follows. In Section 8.2, the definitions of risks used in *BNs* are reviewed and a new paradigm is presented. In Section 8.3, a novel "*Noisier Or*" approach is generated for subjective prior probability distributions of the child node conditioned on multi-state parents. Section 8.4 demonstrates the necessity of using *SA* to rank risk variables in *BNs*. In Section 8.5, an example is given to validate the methodology. Finally, Section 8.6 concludes the chapter with the main contributions of the model.

8.2. Bayesian Risk Nature

There exist many perspectives on risks, including safety engineering, social science perspectives, risk perception research and economic decision analysis. Traditionally, some of different perspectives have been viewed to represent completely different frameworks, and the exchange of ideas and results has been difficult. For example, the classical view to risks is a positivist view – risk exists objectively and can be measured; or the alternative is a subjectivism view, where risk is primarily a judgement, not a fact. Thus, Aven and Kristensen (2005) developed a common platform to integrate these various perspectives. The basic elements of such a platform are the understanding of risks as comprising the two dimensions: (a) possible consequences and (b) associated uncertainties.

As there are many facets of these dimensions, the framework means a broad perspective

on risks, reflecting for example that there might be different assessments of uncertainties, as well as different views on how these uncertainties should be dealt with. In a Bayesian approach, risk is considered as a way of expressing uncertainty. The Bayesian risks belong to neither positivism nor subjectivism scopes in terms of the capability of evaluating the results of risk assessments. Their position is between the two extremes, positivism and subjectivism, which would probably be the position of most analysts working with risk analysis in a practical context. The Bayesian risks can be called relativism risks. From a networking viewpoint, they are also conditional risks.

The essential feature of the Bayesian thinking to risk analysis is that probability is a measure of expressing uncertainty about the world seen through the eyes of the analysts and based on some historical information and knowledge. Complete knowledge about the world does not exist in most cases, and the analysis provides a tool for dealing with these uncertainties based on coherence using the rules of probability. If sufficient data becomes available, consensus in probability assignments may be achieved, but not necessarily as there are always subjective elements involved in the assessment process. The Bayesian approach means a humble attitude to risk. However, the 'relativism' nature of the Bayesian risks does not only indicate that they can be expressed by both objective and subjective probabilities, but also mean that the Bayesian probability expressing uncertainty can be varied by the entries of different pieces of safety evidence.

From a wider point of view, there might be two ways of thinking about the relativism Bayesian risks: the positivism-relativism Bayesian risks in the sense that there are ways of evaluating the 'goodness' of risk and purely-relativism risks, which are only used in relative risk ranking or *SA*. Further studying such two definitions, one can appreciate the distinction between them by the following explanation: a probability 80% used to express the positivism-relativism Bayesian risks possibly means that failure occurs 8 times out of 10 experimentations given the knowledge mastered in the current situation, while the same probability 0.8 related to the purely-relativism risks may only indicate a relative value without more sense of describing uncertainty, which might only represent a bigger value than 0.6 and be used to risk ranking.

8.3. A Novel "*Noisier Or*" Approach

In constructing a *BN*, the converging connections between nodes are always a headache for both Bayesian statisticians and experienced analysts. They are more difficult to be appropriately handled compared to the diverging and serial connections in *BNs*. This point can be further explained in the discussion of Section 3.1. Many pioneers in the research field associated with *BNs* have generated some novel and effective methods to deal with the problem from both quantitative and qualitative viewpoints, such as "*Noisy*

or" and "*Divorcing*" approaches (Jensen, 2001). They are very effective in distributing subjective Bayesian prior probabilities under the condition of incomplete objective statistics. However, some strong assumptions that these methods depend on hinder their wider applications to risk assessment. Thus, the following context is constructed to explain the necessity of synthesising the amount of incomplete probability distributions; to discuss the philosophy of the "*Noisy or*" approach and its limitations when used to risk analysis; and to originally generate a novel "*Noisier or*" approach to complete the synthesis with less constraints.

8.3.1 The Necessity of the Synthesising Methods

Let A and B be the two children listing all the effects of the single parent C. In order to obtain the probability distributions of each state of every node, the joint probability table $P(A, B, C)$ is needed. According to the Bayesian theorem,

$$P(A, B, C) = P(A|B, C)\, P(B, C) = P(A|B, C)\, P(B|C)\, P(C)$$

Because of the diverging connections, given C, A and B are d-separated. Then,

$$P(A|B, C) = P(A|C)$$

Therefore,

$$P(A, B, C) = P(A|C)P(B|C)\, P(C)$$

which is exactly the chain rule for *BNs*. However, such an inference will not suit the case of the converging connections.

Let A and B be the two parent nodes of their single child C. In order to obtain the joint probability table $P(A, B, C)$, the Bayesian theorem yields:

$$P(A, B, C) = P(C|B, A)\, P(B,A) = P(C|B, A)\, P(A|B)\, P(B)$$

Because of the converging connections, if C is not known, then A and B are d-separated. Therefore,

$$P(A|B) = P(A)$$

and

$$P(A, B, C) = P(C|\, B, A)\, P(A)\, P(B),$$

which suits the chain rule of *BNs*. However in this instance, the rule itself is not friendly enough for human knowledge and may be too specific for any expert, because $P(C|B, A)$ cannot be further decomposed and connected with $P(C|A)$ and $P(C|B)$, which provide more respect to human knowledge or may be easier for historical data collection. This is what the synthesising methods attempt to do.

8.3.2 The "Noisy Or" Approach and Its Extensions

One of effective synthesising methods called "*Noisy or*" is generated with the strong assumptions revealed by a deterministic OR gate, where the child will be present given the presence of any parent and the child will be absent, if and only if all parents are absent. The method itself can be interpreted in the following way. A binary node Y may be conditional upon n binary parent nodes, X_r, where $r = 1, 2, \ldots, n$. In order to assess the 2^n probability values associated with the node Y, a technique called "*Noisy or*" was developed (Pearl, 1986) and successfully used in reliability engineering research (Reed, 1990). In the situation of "*Noisy or*", the probability of Y conditional on n nodes, X_r, $r = 1, 2, \ldots, n$, is estimated as:

$$P(Y|X_1, X_2, \ldots, X_n) = 1 - \prod_{r=1}^{n}(1 - P(Y|X_r)) \tag{8.1}$$

In this equation, $P(Y|X_1)$, $P(Y|X_2)$, ..., $P(Y|X_n)$, are assessed and then used to estimate $P(Y|\ X_1, X_2, \ldots, X_n)$. Its theoretical base is that if any of the parents is present, then the child happens unless an inhibitor prevents it; if all inhibitors are independent, then the combined probabilities are easy to calculate as one minus the product of the appropriate probabilities for the inhibitors.

A standard "*Noisy or*" is correct only if it satisfies the requirement that the possible causes are collectively exhaustive, that is,

$$P(Y = present|X_1, X_2, \ldots, X_n = absent) = 0 \tag{8.2}$$

However, in many real world situations, there are multiple possible causes for the presence of Y, some of which cannot be involved in the model. Therefore, a new model called leaky "*Noisy or*", which considers the probability of Y presence given the absence of $X_1, \ldots, X_n$ as $P_{background}$ is produced as follows (Jensen, 2001; Gerssen, 2004):

$$P(Y|X_1, X_2, \ldots, X_n) = 1 - (1 - P_{background})\prod_{r=1}^{n}(1 - P(Y|X_r)) \tag{8.3}$$

Furthermore, changing the OR property to MAX property, the constraint of the binary states is studied and dealt with by extending the "*Noisy or*" model to a new "*Noisy MAX*" method, shown as follows (Gerssen, 2004):

$$P(Y|X_1, X_2, \ldots, X_n) = \max P(Y|X_r),\ r \in (1, \ldots, n) \tag{8.4}$$

which requires to be conditioned that the nodes are ordinal instead of nominal and the nodes have equal amount of states.

In the process of synthesising incomplete probabilities, the "*Noisy or*" approach and its extensions still reveal certain application problems. For example, the *BN* in Figure 8.1 is established to model the fact that given only food *F*, the probability distribution of people living days, *L* is the set of (0.01, "4-5", 0.25, "3-4", 0.62, "2-3", 0.12, "1-2", 0, "0-1"days) and given water *W*, the probability distribution of people living days, *L* is the set of (0.05, "4-5", 0.75, "3-4", 0.15, "2-3", 0.04, "1-2", 0.01, "0-1"days).

Figure 8.1 can be assumed to have the characteristics of a classical deterministic OR gate, which describes the situation that unless both food and water are not provided, people can live more than 3 days. Consequently, $P(L=Yes \mid F = No, W= No) = 0$. In a similar way, Figure 8.1 can also be assumed to have the characteristics of another classical deterministic OR gate, which describes the condition that unless both food and water are provided, people can live no more than 3 days. Consequently, $P(L=No|F = No, W= No) = 1- (1-0.2) \times (1-0.74) = 0.792$ and $P (L=Yes|F = No, W= No) = 1 - 0.792 = 0.208$, which obviously conflicts with the result above.

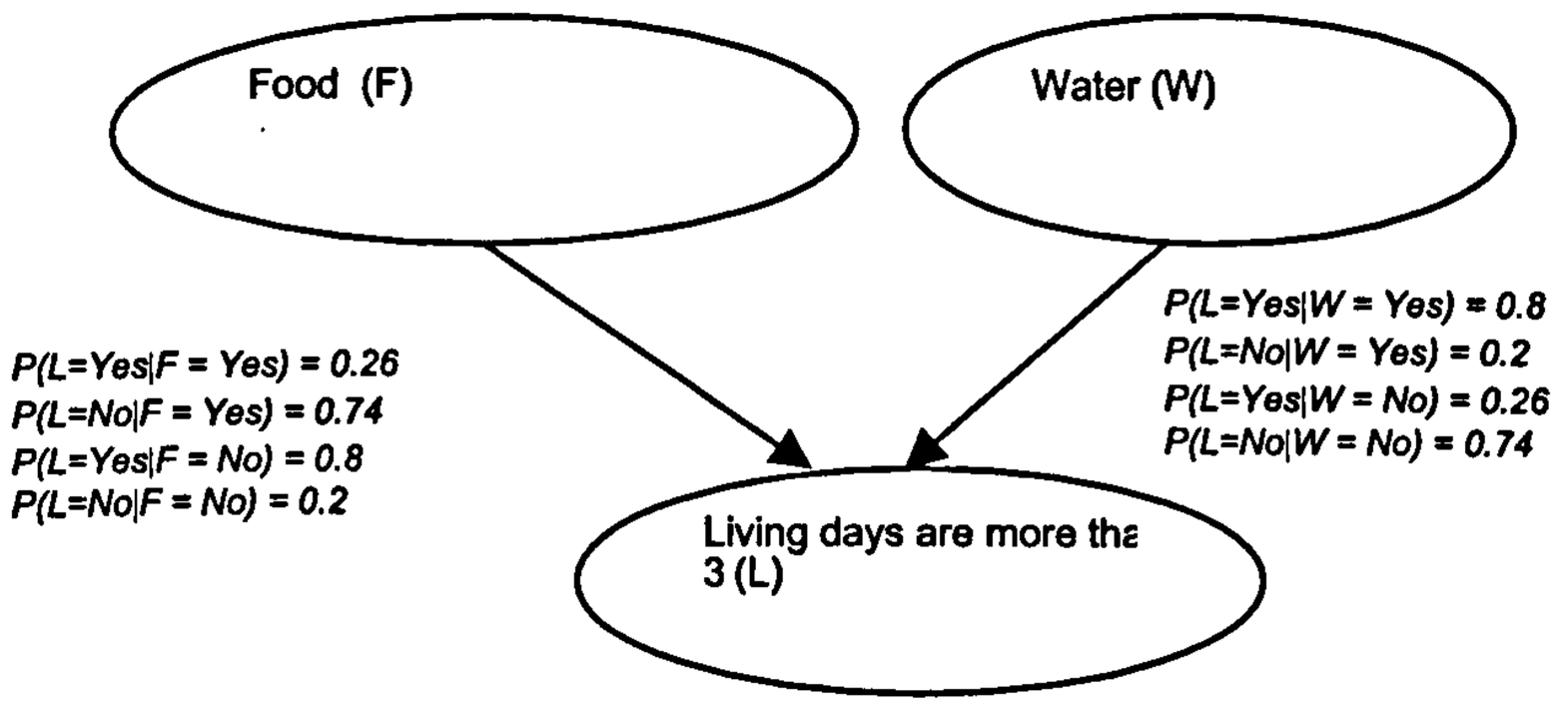


Figure 8.1. A *BN* example to illustrate the shortcomings of the "Noisy or" approach

Another problem is related to the states of the variable, *L*. They need to be changed from five to two states for the application of the "*Noisy or*" approach (all nodes, either *Y* or X_r, are required to be binary variables). However, the probability distributions will vary according to different dividing ways, which may constrain the application of the approach in the context of risk assessment.

8.3.3 A Novel "Noisier Or" Approach

In realistic *BNs* constructed, it is often the case that the parent and child nodes have multiple and different amount states and the prior probabilities are provided by multiple engineering experts. All of these are beyond the capability of the "*Noisy or*" method. Thus, a novel "*Noisier or*" approach is developed and well suited to modelling the probability distributions based on multiple states and multiple experts.

The kernel of this approach is an *ER* algorithm developed on the basis of *D-S* theory, which has been introduced in the previous chapters. In the context of *BNs*, the probabilities assigned into the states of nodes can be considered as the credibility induced by partial evidence. The corresponding uncertainties can be interpreted and inferred as follows:

Let A with L states $\{A_1, A_2, ..., A_L\}$ be the common child of parents B with M states $\{B_1, B_2, ..., B_M\}$ and C with N states $\{C_1, C_2, ..., C_N\}$. Assume that B_i ($i \in M$) represents state i of parent B and C_j ($j \in N$) means state j of parent C. Suppose the set $\{P^i_{A1}, P^i_{A2}, ..., P^i_{AL}\}$ indicates $P(A \mid B_i)$ and the set $\{P^j_{A1}, P^j_{A2}, ..., P^j_{AL}\}$ be $P(A \mid C_j)$, then the set $\{P^{ij}_{A1}, P^{ij}_{A2}, ..., P^{ij}_{AL}\}$ representing $P(A \mid B_i, C_j)$ can be calculated using the following pathway.

Assume that $P(A \mid B_i)$ and $P(A \mid C_j)$ are with the distributed normalized weights w_1 and w_2 ($w_1 + w_2 = 1$) respectively to represent the relative parent-node importance of B and C in determining the combining probability distributions of the child-node, A. Such weights can be calculated and estimated using some well-estimated techniques like *AHP* and pair-wise methods.

Suppose β^i_{Ak} and β^j_{Ak} ($k = \{1, 2, ..., L\}$) are individually degrees to which $P(A \mid B_i)$ and $P(A \mid C_j)$ support the final conclusion that the combined probability distributions are confirmed to the states $\{A_1, A_2, ..., A_L\}$. Then, β^i_{Ak} and β^j_{Ak} can be obtained as follows:

$$\beta^i_{Ak} = w_1 \; P^i_{Ak} \; (k = \{1, 2, ..., L\})$$
$$\beta^j_{Ak} = w_2 \; P^j_{Ak} \; (k = \{1, 2, ..., L\}) \qquad (8.5)$$

Having known that P^{ij}_{Ak} ($k = \{1, 2, ..., L\}$) represents the new prior probability assigned to the sates $\{A_1, A_2, ..., A_L\}$ as a result of synthesising the $P(A \mid B_i)$ and $P(A \mid C_j)$, the *ER* algorithm can be stated as follows (Yang and Xu, 2002):

$$P^{ij}_{Ak} = \frac{K(\beta^i_{Ak}\beta^j_{Ak} + \beta^i_{Ak}w_1 + \beta^j_{Ak}w_2)}{1 - K(w_1 w_2)}$$

$$K = [1 - \sum_{\substack{T=1 \\ R \neq T}}^{L} \sum_{R=1}^{L} \beta^i_{AT}\beta^j_{AR}]^{-1} \qquad (8.6)$$

The above gives the process of calculating the conditional probability of one child node under two parent nodes. If the situation of having three parent nodes occurs, the result obtained from the combination associated with any two parent nodes can be further synthesised with the third one using the above algorithm. In a similar way, the probabilities of one child node under multiple parent nodes can also be assigned. Note

that the "*Noisier or*" approach requires less constraints than the "*Noisy or*" approach in terms of the assumptions required. The new approach does not need to be constrained by the requirements of "a deterministic OR gate" and "independent inhibitors". Its only hidden assumption can be described as that when the prior probability of the child conditioned on one single parent is estimated, assessors have no idea about the status of other parents. In other words, the $P(A|B)$ is evaluated without any knowledge of the states of node C. Furthermore, the relative weights of single probability distributions will be normalized first. If B and C can be considered as two experts and the $P(A \mid B_i)$ and $P(A \mid C_j)$ indicate their individual subjective judgements, the problem of combining single conditional probability distributions from multiple experts can be solved. Such a complex calculation has been simplified by the development of commercially available software, such as *IDS*. Using such a system, the conditional probability distributions given single parent nodes, together with their individual weights, can be easily inputted and transferred into the final synthesised probabilities under multi-state parents automatically.

8.4. A Risk Ranking Technique in a Networking Environment

The aim of many risk analyses is to rank the risk variables on a prioritized list so that assessors can optimize the resource to the key risk areas and maximize the reduction of the risk in a limited cost. Traditionally, such key risk areas are defined as those variables with high values. However, this might not be true in a *BN* case, where the single measurement of risk priority is the influence magnitude to the nodes of interest. Because *BNs* admit the concept of d-separation, many risk variables may have no influence on the probability distributions of the interested variables even if they are in the high-risk areas. Having taken the simple risk diagnosis and prediction analysis into account, many researchers may wrongly use the instantiation of a single risk variable to observe its effect to the nodes of interest and further calculate its priority in risk assessment. This may be very inaccurate, because such analysis obviously ignores the effects of combined risk variables. Thus a new analysis technique appropriately considering the question above is developed to improve the risk priority assessment in a networking environment.

The new risk ranking technique is based on the *SA* in *BNs*. The *SA* in *BNs* refers to analyzing how sensitive the conclusions (the probabilities of the hypothesis/interested variables) are to minor changes. The changes may be variations of the parameters of the model or may be the changes of the evidence (Jensen, 2001). In the context of risk assessment, if e represents the safety evidence entered into a network and H_s and H_r separately denote the hypothesis "*safety-intended*" and "*risk-intended*" states of the focus of interest, *SA* applied to e gives answers to questions such as:

Which piece(s) of e is/are in favor of /against/irrelevant for H_s and H_r?

Which piece(s) of e discriminate(s) H_s from H_r?

The best way to explain the *SA* is to use an example like the following one. Its generic definition is provided later.

> *The engineers on a containership find that its engine does not work. They wonder whether the engine has been faulty or whether the fuel is insufficient. They observe the fuel meter and the record of pumping the fuel at the last calling port. Both results show that the fuel is adequate on board. Consequently, they conclude that the engine has broken down.*

The network for the engineers' reasoning is described in Figure 8.2, where all the nodes have two exclusive states, "*Yes*" and "*No*".

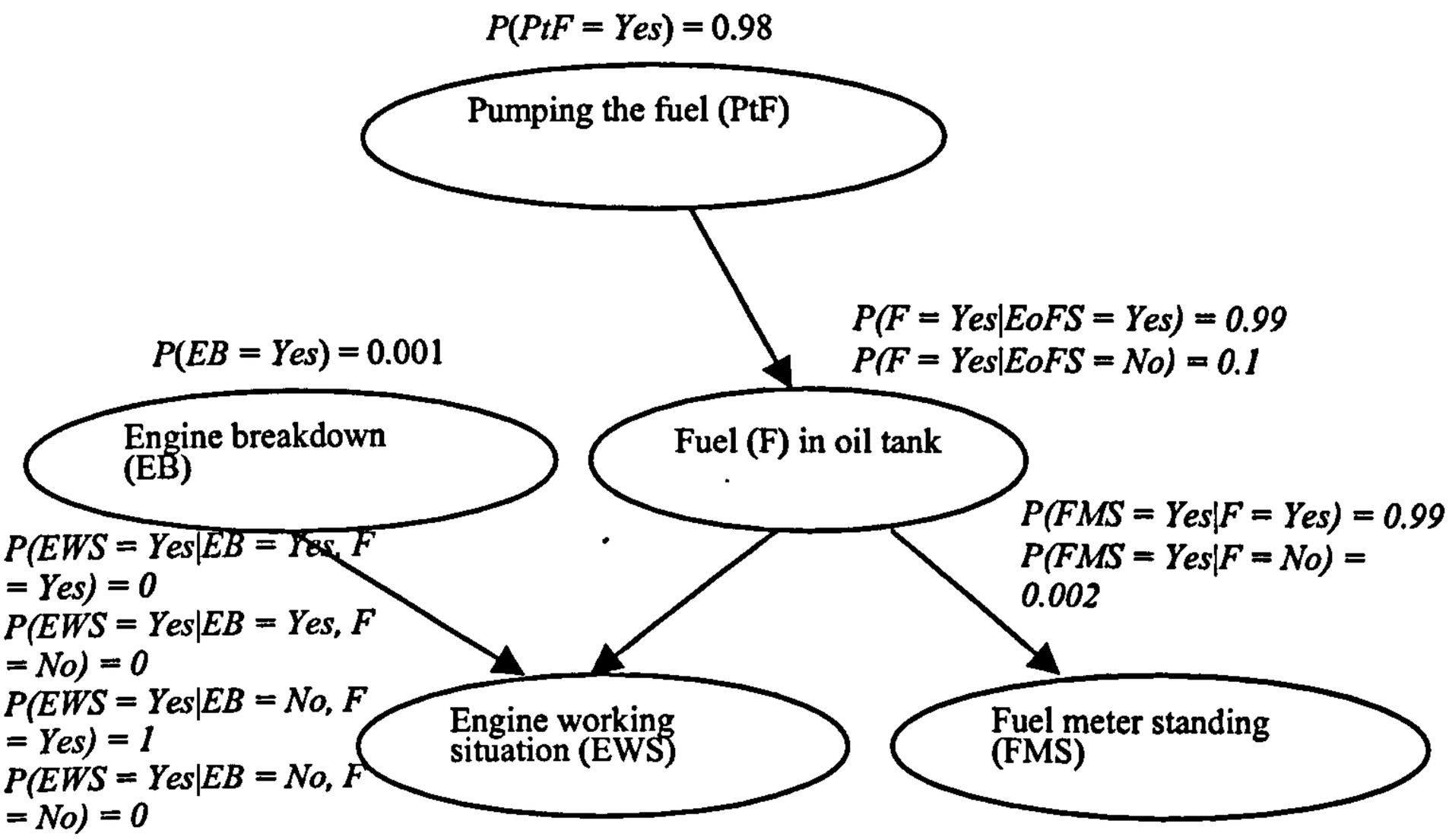


Figure 8.2. The network for demonstrating the engineers' reasoning in the engine breakdown example

The evidence e consists of the three observations $e_{EWS} = No$, $e_{PtF} = Yes$, $e_{FMS} = Yes$, and the hypothesis in focus is H_{EB} = Yes. Performing the network using the *Hugin* software, $P(EB = Yes \mid e) = 0.98$ is obtained. Using risk diagnosis and prediction analysis, $P(EB = Yes \mid EWS = No) = 0.0348$, $P(EB = Yes \mid PtF = Yes) = 0.001$ and $P(EB = Yes \mid FMS = Yes) = 0.001$ can be calculated. Compared to the prior probability of $P(EB = Yes) = 0.001$, neither $e_{PtF} = Yes$ nor $e_{FMS} = Yes$ alone has any impact on the hypothesis, but $e_{EWS} = No$ is not sufficient for the conclusion. Therefore, the immediate decision that $e_{PtF} = Yes$ and $e_{FMS} = Yes$ are irrelevant for the hypothesis is not correct. The fact that the evidence in combination may have a larger impact than the "sum" of the individual impacts must be considered.

Further research will consider the influence of the subsets of the evidence. Their probability computation can be obtained as follows:

$$P(EB = Yes \mid EWS = No, PtF = Yes) = 0.091,$$
$$P(EB = Yes \mid EWS = No, FMS = Yes) = 0.9454,$$
$$P(EB = Yes \mid FMS = Yes, PtF = Yes) = 0.001$$

Consequently, it can be concluded that no single observation is sufficient for the conclusion. Also although *FMS* itself has no impact on the hypothesis, this observation cannot be removed. Moreover, the subset (*EWS = No, FMS = Yes*) can account for almost all the change in the probability for the hypothesis.

Now, the *SA* method to investigate the key risk areas can be defined as follows. Let e be evidence for all potential root risk variables (root causes) which affect the probability distribution of the focus of interest and H be the safety state of the interested leaf node, which may represent a kind of risk or an individual system. Then the analysis of the key risk areas means the investigation of how sensitive the result $P(H \mid e)$ to the particular subset e' of e is. The following three rules are used to define the key risk variables:

Rule 1: **(Relevant risk variables)**
If $P(H \mid e')$ is approximately equal to $P(H \mid e)$, then the evidence e' (subset of e) $\subseteq e$ is *sufficient* and the risk variables associated with them are *relevant*. Note that the term, "approximately" can be made precisely by selecting a threshold θ_1 and requiring that $\left|\frac{P(H|e')}{P(H|e)} - 1\right| < \theta_1$. Note that $\frac{P(H|e')}{P(H|e)}$ is the fraction between the two likelihood ratios.

Rule 2: **(Important risk variables)**
If e' is *sufficient*, but no subset of e' is so, then e' is *minimal sufficient* and $e \backslash e'$ (the other sets in e except e') is *redundant*. If e' is the common subset of all *minimal sufficient* set, then e' is *crucial*; if e' is the common subset of all *redundant* set, then the risk variables associated with them are defined to be *irrelevant* and have lowest priority in risk ranking.
If the probability of H changes too much without e', then it is *important* – to be precise, if $\left|\frac{P(H|e \setminus e')}{P(H|e)} - 1\right| > \theta_2$, where θ_2 is a chosen threshold.

Rule 3: **(Key risk variables)**
If the *BN* is an improvement-needed model, which means the pre-posterior probability distribution of the hypothesis is unacceptable in terms of the safety consideration (that is, the safety degree of the hypothesis is not good enough), then the key risk variables are those related to *minimal sufficient* subsets. The priority of the key risk variables can be obtained through investigating the values of $P(H|e')$. The higher the value is, the more favorable the corresponding key risk variables.

If the *BN* is a maintenance-needed model, which means the pre-posterior probability distribution of the hypothesis is acceptable when its safety levels are taken into account (that is, the safety degree of the hypothesis is good enough), then the key risk variables are those with *crucial e'* or *minimal sufficient e'* if *crucial e'* is not available. The priority of the key risk variables can be obtained through investigating the values of $P(H|e')$. The higher the value is, the more favourable the corresponding key risk variables.

8.5. Case Study

As described previously, there are two difficulties in dealing with terrorism related risk assessment. One is related to the quantitative assessment of the risks and the other is associated with the assessment feasibility and flexibility aiming at dynamic situations in the chains. This case study using the relative risk analysis method can deal with such problems and provide a significant contribution in assisting people to better understand the threats and make appropriate anti-terrorism decisions.

Referred to the methodology of using *BNs* to risk assessment and its corresponding case study in Chapter 7, a sound qualitative *BN* applied to the analysis of terrorism threats in *CSCs* is cited from Figure 7.5, considering that the focus of this chapter is on dealing with some quantitative related challenges. More details about how the qualitative network is constructed and what the nodes mean can be obtained from Section 7.4 and will not be repeated in this chapter.

Taking the advantages of *BNs* into account, the assigned probabilities (See Table 8.1) are for some nodes based on available data/information, while for the other nodes like the risk-based ones, they can be estimated and obtained on the basis of subjective judgements using reliable inference methods such as the *FRB-ER* approach in Chapter 5. However, when subjective judgements are concerned, it may be very difficult for experts to estimate the probabilities conditioned on multi-state parents (the *FRB-ER* method can be more effective and accurate for the assessment under certain circumstances (i.e. the prior probability judgement given individual parents/conditions)). For example, the method can be used to obtain the risk based subjective prior probability *P*(*Cargo*|*Intelligent networks*) as follows:

P(*Cargo*|*Intelligence network* = *Flawless*) = {0, *"Poor"*, 0, "*Fair*", 0, "*Average*", 0.18, "*Good*", 0.82, "*Excellent*"}

P (*Cargo*|*Intelligence network* = *Flawed*) = {0.92, *"Poor"*, 0.08, "*Fair*", 0, "*Average*", 0, "*Good*", 0, "*Excellent*"}

and *P*(*Cargo*|*Check and Supervision*) as follows:

Table 8.1. The prior probability distributions of partial nodes in the *BN*

The prior conditional probabilities of "Cargo"				
Intelligence networks	Flawless		Flawed	
Checking and supervision / Cargo	Checked	Ignored	Checked	Ignored
Soundness	0.96	0.44	0.48	0.02
Weakness	0.04	0.56	0.52	0.98

The prior conditional probabilities of "Supply chains"								
Terminal	Soundness				Weakness			
Inland transportation	Soundness		Weakness		Soundness		Weakness	
Channel / Port	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness
Soundness	0.91	0.66	0.65	0.35	0.63	0.34	0.33	0.14
Weakness	0.09	0.34	0.35	0.65	0.37	0.66	0.67	0.86

P(Cargo|Check and supervision = checked) = {0, "Poor", 0, "Fair", 0, "Average", 0, "Good", 1, "Excellent"}

P(Cargo|Check and supervision = ignored) = {0.89, "Poor", 0.11, "Fair", 0, "Average", 0, "Good", 0, "Excellent"}

However, the *BNs* require the prior probability distribution conditioned on multi-states parents. Thus, using the "*Noisier or*" method, the conditional possibilistic safety degrees of "Cargo" given "Intelligence" and "Check and supervision" can be calculated in the following.

Suppose *P(Cargo|Intelligence network = Flawless)* and *P(Cargo| Check and supervision = checked)* to represent $P(A \mid B_i)$ and $P(A \mid C_j)$ in Section 8.3.3 individually. Given that the nodes "Intelligence network" and "Check and Supervision" are considered to have the same importance to the node "Cargo", $\omega_1 = \omega_2 = 0.5$. Then, for *P(Cargo| Intelligence network = Flawless, Check and supervision = checked)*, the following can be obtained:

$$\beta^{i}_{A1} = \omega_1 \; P^{i}_{A1} = 0.5 \times 0 = 0 \quad \beta^{i}_{A2} = \omega_1 \; P^{i}_{A2} = 0.5 \times 0 = 0$$

$$\beta^{i}_{A3} = \omega_1 \; P^{i}_{A3} = 0.5 \times 0.18 = 0.09$$

$$\beta^{i}_{A4} = \omega_1 \; P^{i}_{A4} = 0.5 \times 0.82 = 0.41$$

$$\beta^{j}_{A1} = \omega_2 \; P^{j}_{A1} = 0.5 \times 0 = 0 \quad \beta^{j}_{A2} = \omega_2 \; P^{j}_{A2} = 0.5 \times 0 = 0$$

$$\beta^{j}_{A3} = \omega_2 \; P^{j}_{A3} = 0.5 \times 0 = 0 \quad \beta^{j}_{A4} = \omega_2 \; P^{j}_{A4} = 0.5 \times 1 = 0.5$$

$$K = [1 - 0.09 \times 0.5]^{-1} = 1.047$$

$$P^{ij}_{A1} = 0 \,, \; P^{ij}_{A2} = 0 \,, \; P^{ij}_{A3} = 0.08 \,, \; P^{ij}_{A4} = 0.92$$

P(Cargo|Intelligence network = Flawless, Check and supervision = checked) = {0, "Poor", 0, "Fair", 0, "Average", 0.08, "Good", 0.92, "Excellent"}

In a similar way, the following conditional probabilities can be calculated as follows:

P(Cargo|Intelligence network = Flawless, Check and supervision = ignored) = {0.45, "Poor", 0.05, "Fair", 0, "Average", 0.07, "Good", 0.43, "Excellent"}

P(Cargo|Intelligence network = Flawed, Check and supervision = checked) = {0.46, "Poor", 0.04, "Fair", 0, "Average", 0, "Good", 0.5, "Excellent"}

P(Cargo|Intelligence network = Flawed, Check and supervision = ignored) = {0.93, "Poor", 0.07, "Fair", 0, "Average", 0, "Good", 0, "Excellent"}

Although such a result has responded to the conditional prior probability distributions in the *BN*, it can still be not entered into the Bayesian inference without further consideration. Obviously, the linguistic terms expressing safety degree function on fuzzy sets may not be used as the mutually exclusive states in the node "Cargo". Thus, further transforming them to a probabilistic "legal identification" admitted by *BNs* may be required.

Having analysed the Bayesian risk nature in Section 8.2, the definition of pure-relativism risks can be employed to conduct the risk ranking analysis here. As a result, each linguistic term expressing safety estimations can provide a safety preferred value according to the defuzzification approach in Equation (5.7) and the combined prior probabilities above can be defuzzified as follows:

P(Cargo = soundness|Intelligence network = Flawless, Check and supervision = checked) = 0.96

P(Cargo = soundness|Intelligence network = Flawless, Check and supervision = ignored) = 0.44

P(Cargo = soundness|Intelligence network = Flawed, Check and supervision = checked) = 0.48

P(Cargo = soundness|Intelligence network = Flawed, Check and supervision = ignored) = 0.02

After assigning all the prior probabilities, the next step is to conduct the *SA* analysis for identifying the key risk variables. Using the *Hugin* software, the pre-posterior probability of the node "Supply chain" facing terrorism threats can be calculated as 0.7. Suppose such a safety degree is not good enough, that is, the network belongs to an improvement-needed model. Then, all root nodes are given their evidence *e*, which will assist in improving the probability of the "*Soundness*" state of "Supply chain". Under such a circumstance, the posterior probability, *P*(*Supply chain*| *e*) can be calculated as {0.89, "*Soundness*", 0.11 "*Weakness*"}. Next, the influence of the subsets *e'* of the evidence *e* will be further analysed and their probability distributions can be obtained in Table 8.2. A threshold is designed as having the value 0.05 so as to investigate *relevant* risk variables.

Table 8.2 Normalised likelihood for the subset evidence

Row (No)	*Missile = No*	*External = Friendly*	*Internal = Immune*	*Intelligence network = Flawless*	*Check and supervision = Checked*	*Accessibility = Unlikely*	*P(Supply chain = Soundness|e')(%)*	*P(Supply chain = Soundness|e') / P(Supply chain = Soundness/e)*
1	1	1	1	1	1	1	88.94	1
2	1	1	1	1	1	0	84.08	0.945
3	1	1	1	1	0	1	79.44	0.893
4	1	1	1	1	0	0	74.92	0.842
5	1	1	1	0	1	1	87.10	0.979
6	1	1	1	0	1	0	82.30	0.925
7	1	1	1	0	0	1	77.81	0.875
8	1	1	1	0	0	0	73.35	0.825
9	1	1	0	1	1	1	87.28	0.981
10	1	1	0	1	1	0	82.47	0.927
11	1	1	0	1	0	1	78.03	0.877
12	1	1	0	1	0	0	73.55	0.827
13	1	1	0	0	1	1	85.48	0.961
14	1	1	0	0	1	0	80.73	0.908
15	1	1	0	0	0	1	76.45	0.86
16	1	1	0	0	0	0	72.03	0.81
17	1	0	1	1	1	1	88.84	0.999
18	1	0	1	1	1	0	83.98	0.944
19	1	0	1	1	0	1	79.36	0.892
20	1	0	1	1	0	0	74.84	0.841
21	1	0	1	0	1	1	87.00	0.978
22	1	0	1	0	1	0	82.20	0.924
23	1	0	1	0	0	1	77.73	0.874
24	1	0	1	0	0	0	73.27	0.824
25	1	0	0	1	1	1	87.19	0.98
26	1	0	0	1	1	0	82.38	0.926
27	1	0	0	1	0	1	77.95	0.876
28	1	0	0	1	0	0	73.48	0.826
29	1	0	0	0	1	1	85.39	0.96
30	1	0	0	0	1	0	80.65	0.907
31	1	0	0	0	0	1	76.37	0.859
32	1	0	0	0	0	0	71.95	0.809
33	0	1	1	1	1	1	86.79	0.976
34	0	1	1	1	1	0	81.96	0.922
35	0	1	1	1	0	1	77.76	0.874
36	0	1	1	1	0	0	73.27	0.824
37	0	1	1	0	1	1	85.04	0.956
38	0	1	1	0	1	0	80.27	0.903
39	0	1	1	0	0	1	76.21	0.857
40	0	1	1	0	0	0	71.78	0.807
41	0	1	0	1	1	1	85.21	0.958
42	0	1	0	1	1	0	80.43	0.904
43	0	1	0	1	0	1	76.42	0.859
44	0	1	0	1	0	0	71.97	0.809
45	0	1	0	0	1	1	83.50	0.939
46	0	1	0	0	1	0	78.79	0.886
47	0	1	0	0	0	1	74.91	0.842
48	0	1	0	0	0	0	70.52	0.793
49	0	0	1	1	1	1	86.70	0.975
50	0	0	1	1	1	0	81.87	0.921
51	0	0	1	1	0	1	77.68	0.873
52	0	0	1	1	0	0	73.19	0.823
53	0	0	1	0	1	1	84.94	0.955
54	0	0	1	0	1	0	80.19	0.902
55	0	0	1	0	0	1	76.14	0.856
56	0	0	1	0	0	0	71.10	0.799
57	0	0	0	1	1	1	85.12	0.957
58	0	0	0	1	1	0	80.35	0.903
59	0	0	0	1	0	1	76.34	0.858
60	0	0	0	1	0	0	71.89	0.808
61	0	0	0	0	1	1	83.41	0.938
62	0	0	0	0	1	0	78.70	0.885
63	0	0	0	0	0	1	74.84	0.841
64	0	0	0	0	0	0	70.45	0.792

"1" in the table indicates that the evidence from risk variables is provided to improve the probability of the state "Soundness" of the "Supply chain".

The *relevant* risk variables can be identified and shaded in Table 8.2. According to ***Rule 1*** in Section 8.4, the 14 shaded rows corresponding with the combinations of the *relevant* risk variables can be defined as *sufficient e'*. From ***Rule 2***, *minimal sufficient* subsets of the evidence can be analysed as follows:

Observing Row 1, all the other 13 shaded rows can be its *sufficient* subsets and thus, Row 1 is not *minimal sufficient.*

Observing Row 5, Rows 13, 21, 29, 37 and 53 can be its *sufficient* subsets and thus, Row 5 is not *minimal sufficient.*

.....

Observing Row 29, no other appropriate row(s) can be its *sufficient* subsets and thus, Row 29 is *minimal sufficient.*

Such an analysis can be carried out throughout the whole 14 shaded *sufficient e'* and three rows are identified to be *minimal sufficient* as follows:

Row 29: (*Missile = No, Check and supervision = Checked and Accessibility = Unlikely*).

Row 53: (*Internal = Immune, Check and supervision = Checked and Accessibility = Unlikely*).

Row 57: (*Intelligence network = Flawless, Check and supervision = Checked and Accessibility = Unlikely*).

Obviously, there are no common subsets of the three *minimal sufficient* sets (no crucial risk variable(s)). Furthermore, the redundant sets of the three *minimal sufficient* sets can be identified and the *irrelevant* risk variable(s) does not exist.

Because the model is assumed to be improvement-needed, the *key* risk areas in the situation are related to all the *minimal sufficient* subsets and can be identified as (***Rule 3***):

"Missile", "Check and supervision" and "Accessibility".

"Internal", "Check and supervision" and "Accessibility".

"Intelligence network", "Check and supervision" and "Accessibility".

Obviously, the *key* risk variables have higher priority than the other ones (i.e. *irrelevant*) in risk analysis. In terms of the *key* risk variables themselves, the priority can be ranked according to their individual contributions to the state "*Soundness*" of the node "Supply chain". Consequently, the risk variables can be prioritised in Table 8.3.

Table 8.3. The risk ranking using the *SA* analysis

Ranks	**Risk variables**
1	"Missile", "Check and supervision" and "Accessibility"
2	"Intelligence network", "Check and supervision" and "Accessibility"
3	"Internal", "Check and supervision" and "Accessibility"

8.6. Conclusion

This chapter generates a novel relative risk analysis model to deal with some practical challenges of using *BNs* to risk assessment. The model applies knowledge-based *BN* construction to allow researchers to appreciate a novel attempt of unifying possibility (i.e. fuzzy logic and *D-S*) and probability (i.e. Bayesian probability) theories by the introduction of the nature of Bayesian risks and "*Noisier or*" approach. The model also provides a new way of thinking about risk ranking in a complex system such as *CSCs*, whose subsystems and components have interactive relationships. It uses the *SA* to investigate the combined influence of multiple risk variables and thus, avoid the possible inaccuracies resulting from the individual viewpoint in traditional risk priority analysis.

Chapter 9 – Hybrid Multiple Attribute Decision Making with Uncertainty

SUMMARY

Safety critical systems often require identifying the "optimal" RCO based on multiple uncertain attributes. While a number of utility theory based techniques such MAUT have been developed to accomplish such an objective, many problems regarding implementation are observed, but not well addressed. They, in particular, are: (1) risk attributes are not always well defined; (2) for a given risk control action, the attribute values may be stochastic rather than deterministic; (3) it is error-intended to assume that all relevant risk attributes are independent; and (4) creating an effective utility function to simultaneously represent the decision makers' preferences to both linguistic and numerical variables may be a difficult task. Consequently, a heuristic two-stage methodology that enables the quantification of the uncertainties related to the risk attributes based on BNs and then uses the fuzzy logic theory to generate novel utility representation functions for selecting the "optimal" safety solution may be an effective and realistic alternative. In the first stage, the role of BNs in MAUT is explained in a complementary way, in which BNs can avoid their application drawbacks resulting from the single risk criterion consideration in risk assessment. Furthermore, given any potential RCO/action, all relevant (sometimes conflicting) decision attributes in the form of the nodes in BNs will produce certain associated attribute values expressed as posterior probabilities, which can be used and combined in a traditional MAUT framework as a reference to rank the set of options/actions. The second step is to focus on the development of novel utility functions, which can appropriately represent the risk results produced above, additive or non-additive and linguistic or numerical. Fuzzy logic is used to take into account crisp values, fuzzy numbers and linguistic variables that are common phenomena in a risk based decision problem. The corresponding fuzzy inference and synthesis operations can be conducted by some well-established decision support techniques such as the ER approach and TOPSIS with the entropy theory, etc. The proposed methodology is illustrated using a container transportation delay related case study.

9.1. Introduction

The benefits of using *BNs* to model the domain of uncertainty are well known (Heckerman *et al.*, 1995; Jensen, 1996), especially after the breakthroughs in algorithms and tools to implement them (Lauritzen, 1988; Pearl, 1988). They also capture non-linear causal relationships between various attributes and predict the effect of the causal

factor changes to the attribute(s) of interest. Therefore, *BNs* provide a powerful decision support tool and are used in a range of real applications concerned with predicting properties of safety critical systems (Faber *et al.*, 2001; Yang *et al.*, 2005c). In most of these applications, the interests are, however, usually focused on the single attribute of the systems, safety or reliability. Although such networks provide important support for risk based decision making, in many circumstances, decisions need to be made on the basis of multiple attributes, such as safety, cost, politics and environmental factors, etc. *BNs* do not allow the incorporating of the notation of preference, which is necessary in such cases. Because they cannot, alone, provide a complete solution for wider decision problems in which a systematic safety assessment exercise inevitably fits, the *BNs* must be complemented by other decision making techniques (Fenton and Neil, 2001) such as those associated with *MAUT* (Keeney and Raiffa, 1976).

If there were only a single attribute with which to make decisions or choose actions, it would not be difficult to solve the decision problems, and the action that returned the 'best' value for the attribute can be chosen. In a risk based decision making context, if safety is really the only attribute on which the decision can be made, then the best action can be chosen straightforwardly with the highest value of safety. Unfortunately, other attributes like cost, functionality and time need to be considered. Inevitably, some of these will be conflicting; the safest system may not be either the cheapest or the one with most functionality. Generally, it is necessary to optimise a number of possibly conflicting attributes. The extensive body of work on *MAUT* (i.e. *MADM*) does provide concrete help for solving such decision problems (Wang *et al.*, 1996). *MADM* includes such well-known techniques as linear programming, the *AHP* (Satty, 1980) and the outranking approach (Roy and Vincke, 1981). However, the *MADM* method and its associated techniques suffer from three critical assumptions (Fenton and Neil, 2001), which may seriously constrain their applications in the risk assessment field:

- The relevant attributes are well defined (for example, for a given action a it is obvious how one can compute $g(a)$ for a given attribute g).
- The relevant attributes are certain (for example, for a given action a and attribute g the value $g(a)$ is deterministic).
- The relevant attributes are independent of each other (for example, for a given action a the value $g(a)$ for a given attribute g has no effect on the value $f(a)$ of another attribute f).

From a non-representational viewpoint, these limitations can be defined as different kinds of uncertainties that arise in decision problems and thus, may be complemented using some uncertain treatment methods such as those related to *BNs* and fuzzy logic (Zadeh, 1965).

A key technical problem to implement the synthesis of *BNs* and *MADM* is how to deal with the risk analysis results from Bayesian inference in the framework of *MADM*. In other words, the kernel of the problem lies in the possibility of developing an appropriate non-additive utility function representing the preferences to the risks usually expressed by linguistic variables. In the framework of *MAUT*, several methods (i.e. the Utility Additive (*UTA*)) have been proposed to build decision makers' utility function representing their preferences. However, such methods can only infer an additive utility function from a set of exemplary decisions using linear programming and thus, do not allow the inclusion of additional information such as an interaction among attributes. A novel method based on the combination of *BFRB* systems and the *ER* algorithm has been introduced to create a non-additive utility function, which permits the modelling of preference structures with interaction between linguistic and numerical variables and uses possibilistic fuzzy linguistic terms to avoid exact point estimations. However, the *ER* approach requires the synthesised sets to be independent. This may constrain its flexibility in a more generic situation.

A novel fuzzy *TOPSIS* method, which can give cardinal order of the *RCOs* with both linguistic and numerical variables, is generated in this study to deal with the problems above. Hwang and Yoon (1981) developed the *TOPSIS* method based on the intuitive principle that the chosen option/alternative should have the shortest distance from the positive-ideal solution and the longest distance from the negative-ideal solution. Although the *TOPSIS* method uses n-dimensional Euclidean distance that by itself could represent some balance between total and individual satisfaction, it assumes that there always exists a performance matrix obtained by the evaluation of all the options in terms of each attribute. Actually, in risk based decision making, such a performance matrix may be difficult to obtain considering that the distance evaluation of some attributes (i.e. safety) expressed by fuzzy numbers may not be straightforward. Additionally, in a Bayesian networking environment, many attributes may have context dependent relationships, which have not been well modelled in the original *TOPSIS* method. Therefore, the definitions of fuzzy ordering and fuzzy similarity (distances) are provided, with which the positive-ideal and negative-ideal solutions can be identified. The entropy theory is introduced, with which the context dependency between attributes can be incorporated into the *MAUT* methodology. Finally, an aggregating function is formulated and it is used as a ranking index.

The remaining part of this chapter is organised as follows. Sections 9.2 and 9.3 are the emphasis of this study and describe the first and second stages of the proposed methodology respectively. In Section 9.2, a six-step framework is proposed to explain the application of *BNs* in *MAUT*. In Section 9.3, The *BERB-ER* and fuzzy *TOPSIS* methods are considered to implement the combination of the attribute values with

various natures obtained from Section 9.2. In Section 9.4 a container delivery delay case study is used to illustrate the methodology. Finally, Section 9.5 concludes that combining *BNs* and *MAUT* with the assistance of fuzzy logic provides a more reasonable and powerful solution for risk based *MADM* under uncertainty.

9.2. Methodology (First Stage): The Application of *BNs* in *MADM*

The interaction between *BNs* and *MADM* has been used in dealing with complex decision making problems. It may either use the utility theory based on *BNs* to form *IDs* (Jensen, 2001) or incorporate the uncertainty treatment ability of *BNs* into the framework of *MADM* (Fenton and Neil, 2001). However, a powerful decision making tool making use of the advantages of both *BNs* and *MADM* is relatively novel in the fields of risk and safety. Therefore, in this study, a risk based decision making model is provided to infer multiple attribute uncertainty and perform risk assessment in a broader context. By doing this, the misunderstandings of the important concepts in making multiple uncertain attribute decisions (i.e. dependency and fuzziness) can be clarified and the limitation of the single risk attribute consideration of *BNs* can also be avoided. The model is the combination of two sub-models: the application of *BNs* in *MADM* and fuzzy based utility methods, which are respectively discussed in this section and the next one. More elements of the model and their relationships are presented in a graphical flowchart (See Figure 9.1).

Once applied to the risk area, the methodologies of *BNs* and *MADM* have many common characteristics. Both studies start with the identification of research objectives and then analyse the attributes/factors influencing the objectives. Next, they both measure these attributes and calculate the analysis results using the measures when actions are taken. Such commonness provides the basis of combining *BNs* and *MADM*. The methodology of applying *BNs* to *MADM* shares the similar philosophy with *GQM* (Goal Question Metric) (Basili and Rombach, 1988; Fenton and Neil, 2001) and is developed to consist of six steps as follows:

- Identify risk based decision problems (objectives) and *RCOs* (actions/functions).
- Identify decision attributes and constraints and analyse risk factors and their causal relationship with the attributes and constraints.
- Connect all risk factors and attributes to form qualitative *BNs*.
- Distribute prior probabilities to model the uncertainties of decision attributes/ criteria.
- Infer the uncertainties given actions and constraints and obtain the posterior probabilities of the decision attributes.
- Construct decision making alternative matrices using the posterior probabilities.

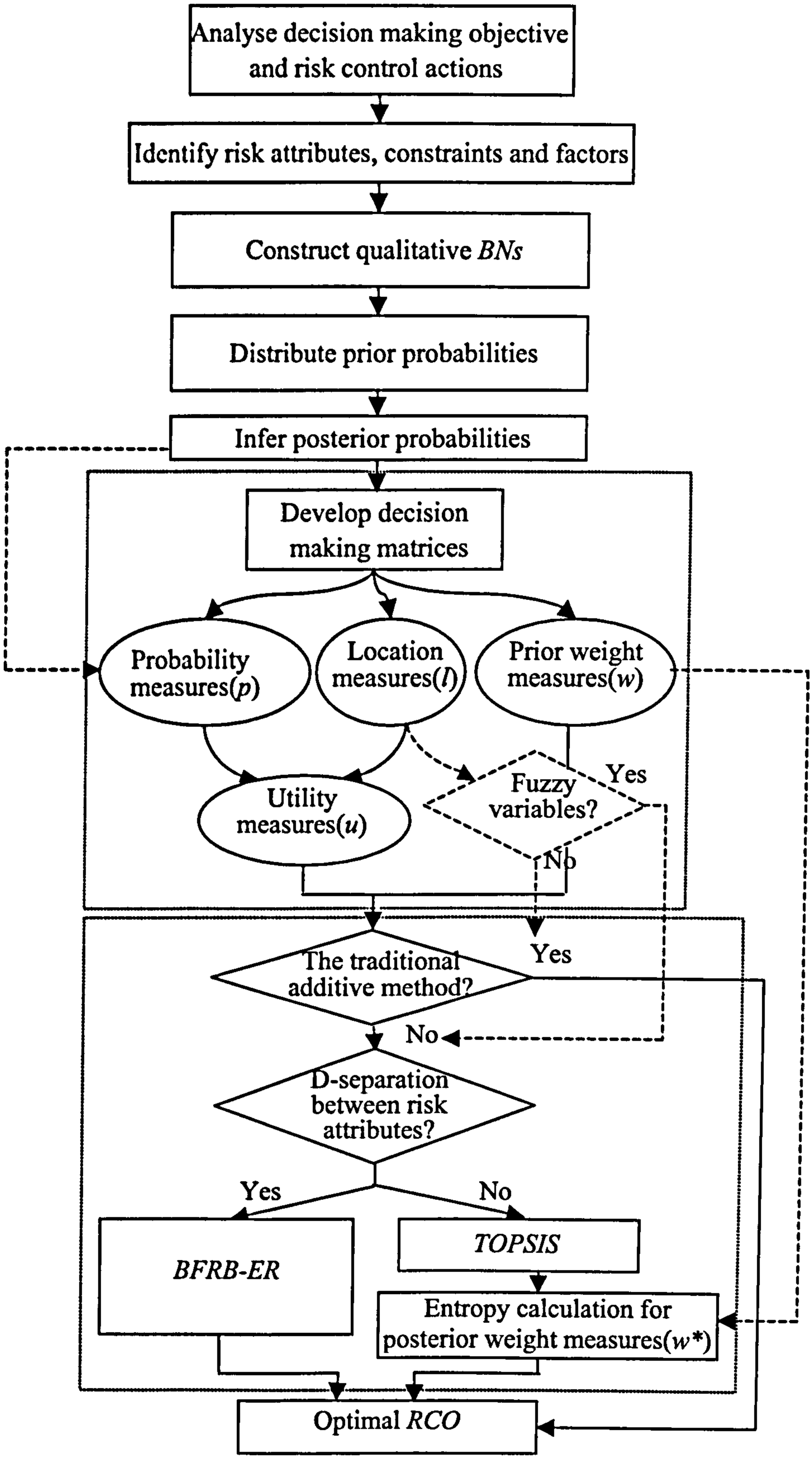


Figure 9.1. The methodology of combining *BNs*, fuzzy logic and *MADM*

9.2.1 Identify Risk Based Decision Problems and RCOs

The first step is concerned with the setting up of clear objectives and functions. The objectives are the targets or goals of a study and the functions are the set of actions that are required in order to achieve the final aim. Obviously, the objectives of dealing with risk based decision making problems are to determine the optimal *RCO* from multiple potential actions or their combinations. Technically, *RCOs* can be obtained using such effective methods as the Chain rule (*PVA*, 1997). However, the objectives are always with respect to particular perspectives. The potential actions are chosen by not only decision makers but also all the stakeholders. Since the stakeholders with various interests may have different or even conflicting perspectives on the same action, it is important to ensure that the stakeholders associated with a particular risk based decision problem can be appropriately considered and accounted. It is a crucial step in scooping and simplifying the problem. Generally, although affected by the decision, a party still ought to be excluded from being considered as a stakeholder if either (Fenton and Neil, 2001):

1. Their viewpoints/needs are not relevant; or
2. Their viewpoints are fundamentally inconsistent with that of the decision makers or accepted stakeholders.

9.2.2 Identify Decision Attributes and Constraints and Analyse Risk Factors and their Causal Relationship with the Attributes and Constraints

Although with the identification of the objective and perspective, risk based decision problems can be expressed using the kind of summary prose, they will not be truly well defined until the following is completely identified and developed:

- The set of possible *RCOs*, which may be identified after appropriate risk analysis.
- The set of decision attributes, which function to distinguish the options.
- The set of constraints, which are usually considered as some realistic conditions and requirements and enter the analysis networks as evidence.
- The set of risk factors, which can connect decision attributes as their media.
- The set of directed acyclic arrows, which represent the causal relationships between the risk factors, attributes and constraints.

Once the set of possible *RCOs* are decided by decision makers, the decision attributes/ criteria, which can be used to distinguish the options, need to be identified. In the risk based decision making context, such attributes often include safety, cost, time, and environmental factors, etc. Whereas traditional *MADM* assumes that all attributes can be measured with certainty and independence, it is clear that any interesting problem will involve key attributes with inherently uncertainty and interactive dependence. Even for

those so called certain and independent attributes, they may only be relatively certain and conditionally independent at one situation and may become uncertain and dependent in another situation. For example, time itself can be considered as one kind of cost and the delay in time truly belongs to risks. *BNs*, as an effective uncertainty treatment method can model the uncertainty and dependence associated with the decision attributes here.

The *BNs* include not only the decision attributes but also other factors that can influence the value of an attribute for a given action. Such factors can be taken as risk factors, which cannot be often controlled by decision makers. These factors, alone with the decision attributes will form the set of nodes in a *BN*, which are connected by the set of directed acyclic arrows for predicting the values of the decision attributes. In the process of predicting the values of the attributes, the changes or requirements of some realistic situations need to be considered as constraints. They may be expressed as the evidence used to fix the state of the nodes in the networks or the changes of structure of the networks. For example, a classical constraint may be that the extremely high cost level for one action is not acceptable no matter how effective or preferred the risk control actions are in terms of their safety contributions.

9.2.3 Connect All Risk Factors and Attributes to Form Qualitative BNs

After identifying all risk factors and decision attributes, one can start to confirm the relationship between them and construct a qualitative *BN* to represent their interactive dependencies. The knowledge about the decision problem and intuitive understanding of the various dependencies are then used to construct the causal structure. Here the graphical representation becomes very handy and permits the decision makers to express the fundamental relationships of direct or indirect influence between decision attributes. The influence relationships expressed in *BNs* have a feature with causality. The concept of d-separation can be used to ensure that the *BN* models correspond with a real-world situation. The previous studies associated with the combination of *BNs* and *MADM* separate certain and uncertain attributes and only consider the latter in a *BN* inference model for simplification (Fenton and Neil, 2001). However, when some constraints are given, the certain attributes may change into uncertain ones and thus, it is desirable that both certain and uncertain attributes are simultaneously represented in one network. This requires the use of the concept of d-separation. Additionally, the definition of d-separation also provides the basis for conducting the entropy calculation to measure the dependence of decision attributes on constraints in Section 9.3.4.

9.2.4 Distribute Prior Probabilities to Model the Uncertainties of Decision Attributes

When the qualitative *BNs* have been built and validated, the prior probabilities to all

nodes of the networks require to be distributed to model the uncertainties of the decision attributes and quantify the *BNs*. In this process, it is necessary to distinguish the different types of uncertainty that arise in decision problems as follows:

- Uncertainty in randomness and dependence.
- Uncertainty in incompleteness.
- Uncertainty in fuzziness.
- Uncertainty in inference.

BNs are designed and constructed as formal graphical languages for representation and communication of decision scenarios requiring reasoning under uncertainty. Their strengths are two-sided. They use the concepts of probability, either classical or subjective to model the uncertainty in randomness and dependency. Furthermore, handy algorithms are developed for analysis of the models and for providing responses to a wide range of requests such as belief updating (uncertainty in inference), which is the key notion of the discussion in the next section. However, they have difficulty in dealing with the uncertainties in incompleteness and fuzziness due to the various characteristics of multiple decision attributes.

It is highly possible in risk based decision making that *BNs* include the "synthetic" attributes that cannot be properly defined without being decomposed into many new converging-connected networks. It has been validated that the converging connections are always a headache and they are more difficult to handle appropriately compared to the diverging and serial connections in *BNs* (Yang *et al.*, 2005c). For any synthetic attribute, it is often the case that given each individual lower level attribute, the conditional probability of the "synthetic" attribute can provide a closer relationship with human knowledge and thus, be relatively easily obtained from either Bayesian statisticians or experienced analysts. In other words, complete conditional probability distributions of the "synthetic" attributes given their all lower level attributes may be too small to be objectively statistic and be too specific to be subjectively judged. Consequently, a "*Noisier or*" approach (Yang *et al.*, 2006) can be used to model the prior probability distributions of the "synthetic" attributes based on multiple lower level attributes and is well suited to treating uncertainty in incompleteness.

In terms of dealing with the fuzziness in prior probability distributions, one can use two different methods to describe the decision attributes or risk factors with various properties. The first method deals with the fuzziness in the meaning of the attribute/factors. It uses linguistic terms to define the states of the nodes representing the attributes/factors and then assigns belief degrees (subjective probability) as the prior probabilities to such states. For example, the prior probability distribution of the node related to the occurrence likelihood (or called *Will*) of a threat-based risk may be "highly

likely" with 0.75 belief degree, "likely" with 0.25 belief degree, "average" with 0 belief degree, "unlikely" with 0 belief degree and "highly unlikely" with 0 belief degree. The second method is used to cope with the fuzziness in data/supporting information of the decision attributes or risk factors. In this case, the states of the nodes associated with the attributes/factors can be clearly defined using crisp number or intervals. However, crisp subjective probabilities (point estimations) cannot be well suited to modelling the prior probability distribution with accuracy but the linguistic description with fuzzy numbers may be used very well to handle this situation. For example, the prior probability distribution of the node related to the occurrence likelihood of a hazard-based risk may be "81-100 times/per year" with the belief degree expressed by "high", "61-80 times/per year" with the belief degree expressed by "low", "41-60 times/per year" with the belief degree expressed by "extremely low", "21-40 times/per year" with the belief degree expressed by "extremely low" and "1-20 times/per year" with the belief degree expressed by "extremely low". In order to update belief and obtain the posterior probabilities of all decision attributes, *BNs* require an effective transformation function between such possibilistic linguistic terms and probabilistic crisp numbers. The transformation function can be developed on the basis of the defuzzification technique such as the one introduced in Equation (5.6). Simultaneously, it is also noteworthy that before being used as the prior probabilities, the crisp numbers obtained by the defuzzification calculations need to be normalised so that their sum can always be equal to one.

9.2.5 Infer the Uncertainties Given Actions and Constraints and Obtain the Posterior Probabilities of the Decision Attributes

Once the qualitative and quantitative *BNs* are appropriately constructed, the next task is to analyse the networks to obtain the posterior probabilities of the decision attributes given risk control actions and constraints from a realistic situation. The objective of using *BNs* in a risk based decision making model is to predict and infer the unobservable situations (uncertainties) related to the decision attributes using the posterior probabilities when observable evidence (alternative risk control actions and constraints) is provided. Such posterior probabilities can be obtained using the Bayes' rule and Chain rule (Jensen, 2001) with the assistance of computing software such as *Hugin*.

Another key point that needs to be discussed in this section is the definition of constraints. The definition of constraints in this newly developed risk based decision making model has been extended from a traditional meaning, where a set of constraints are normally defined as the properties of decision attributes and can also be thought as preferences. For example, one constraint related to one person's height (which is one of the attributes of a special decision problem) may be no less than 165cm. In the domain

of the novel model, constraints can also be used to describe the properties of the risk factors. From the viewpoint of *BNs*, they, together with the pointed *RCO*, can be considered as the intervention (evidence) for the calculation of the posterior probabilities.

9.2.6 Construct Decision Making Alternative Matrices Using the Posterior Probability

In the traditional *MADM* methodology, decision making alternatives (*RCOs*) are normally represented by a $m \times n$ decision matrix, D, where there are m alternatives A_i ($i \in (1,2, ...,m)$) which have n attributes X_j ($j \in (1, 2,..., n)$), as shown in Equation (9.1):

$$D = \begin{array}{c} \\ A_1 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccccc} X_1 & \cdots & X_j & \cdots & X_n \end{array} \\ \begin{bmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1n} \\ \vdots & & \vdots & & \vdots \\ x_{i1} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & & \vdots & & \vdots \\ x_{m1} & \cdots & x_{mj} & \cdots & x_{mn} \end{bmatrix} \end{array} \tag{9.1}$$

It is noteworthy that the attribute value, x_{ij} for option i and attribute j requires to be certain. However this may not be correct in the risk based multiple uncertain attribute decision making modelling. Therefore, the traditional decision making matrices require to be extended to involve more elements (i.e. posterior probability distributions on the states of decision attributes) in order to represent the uncertainties. The new decision making alternative matrices can be developed as follows:

$$D = \begin{array}{c} \\ A_1 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccccccccc} X_1 & & \cdots & & X_j & & \cdots & & X_n \end{array} \\ \begin{bmatrix} (x_{111} & \cdots & x_{1k_1} & \cdots & x_{1l_1}) & \cdots & (x_{1j1} & \cdots & x_{1jk_j} & \cdots & x_{1jl_j}) & \cdots & (x_{1n1} & \cdots & x_{1nk_n} & \cdots & x_{1nl_n}) \\ & & \vdots & & & & \vdots & & & & & & \vdots & & & & \\ (x_{i11} & \cdots & x_{i1k_1} & \cdots & x_{il_1}) & \cdots & (x_{ij1} & \cdots & x_{ijk_j} & \cdots & x_{ijl_j}) & \cdots & (x_{in1} & \cdots & x_{ink_n} & \cdots & x_{inl_n}) \\ & & \vdots & & & & \vdots & & & & & & \vdots & & & & \\ (x_{m11} & \cdots & x_{m1k_1} & \cdots & x_{ml_1}) & \cdots & (x_{mj1} & \cdots & x_{mjk_j} & \cdots & x_{mjl_j}) & \cdots & (x_{mn1} & \cdots & x_{mnk_n} & \cdots & x_{mnl_n}) \end{bmatrix} \end{array} \tag{9.2}$$

where x_{ij} in Equation (9.1) could be any element of the set $(x_{ij1} \quad \cdots \quad x_{ijk_j} \quad \cdots \quad x_{ijl_j})$ in Equation (9.2) with one hundred percent certainty; any element x_{ijk_j} in Equation (9.2) can be connected with its corresponding counterpart from the Bayesian exclusive states of the decision attribute node (X_j) and thus, has been attached a posterior probability as its probabilistic measure; any element x_{ijk_j} requires to be further analysed in order to obtain its location measure; and any decision attribute X_j ($j \in (1, 2,..., n)$) needs to be given its weight measure by decision makers.

The three different measures (probabilistic p, location l and weight w) constitute of the kernel of the extended decision making matrices and become important indicators to rank decision making alternatives. Having studied the probabilistic measures (posterior probabilities) in the previous section, this section focuses on the research of location measures l and weight measures w. Location measures l are used to measure the performance of the decision attribute nodes based on the preference assignments of their exclusive states. There are four types of location measures: linear, bilinear, non-linear and judgemental. In the category of the linear measures, the monotonically increasing and monotonically decreasing measures exist. In the former case where more is better than less, the location measures can be calculated using Equation (9.3) as follows:

$$l_a = (V_a - V_{\min}) / (V_{\max} - V_{\min}) \tag{9.3}$$

where l_a represents the location measure of one state, V_a is its state value, $V_{\min}$ is the value of the state with the minimal value and $V_{\max}$ is the value of the state with the maximal value.

In the latter case where less is better than more the equation of the location measures is

$$l_a = (V_{\max} - V_a) / (V_{\max} - V_{\min}) \tag{9.4}$$

where all symbols have the same meaning with the ones in Equation (9.3).

In the case of the bilinear measures, neither maximum nor the minimum is the preferred value but some mid-point provides the optimum performance measure. If more is better than less, then the equation associated with this kind of measure takes the form of

$$l_a = (V_a - V_{\min}) / (U_{\max} - V_{\min}) \tag{9.5}$$

where all the symbols keep the same meanings with the above except $U_{\max}$, which indicates the value of the state with the highest preference.

On the other hand, if less is better than more, then the function is

$$l_a = (V_{\max} - V_a) / (V_{\max} - U_{\max}) \tag{9.6}$$

where all symbols have the same meaning with the ones in Equation (9.5).

When the performance of the decision attributes measured is not linear, the corresponding location measure function usually adopts a simplified method and can have whatever forms depending on the relation of the states of the attributes to the rate of the performance. Finally, the judgemental measures are purely based on expert

subjective judgement therefore it will be preferred to be expressed using fuzzy numbers based on linguistic variables.

In most cases, measuring the weights of the decision attributes is relatively straightforward considering the fact that many effective weight calculation methods such as an *AHP* technique are available to support and simplify the difficulty of the subjective judgements of decision makers. However, it is important to note that the results obtained (also called prior weights) using such methods are certain and fixed. They are analysed only on the basis of the knowledge, which are mastered by decision makers, but without any information of the constraints given such as the chosen actions or the observed evidence of the risk factors. The direct or indirect relationships between the decision attributes lead to their weight flexibility (weight dependency) conditioned on the constraints. The weight calculation methods cannot explicitly model the propensity for the decision makers' weightings to change once the potential action (*RCO*) is identified. Using the entropy theory, the problem is dealt with appropriately and is detailed in Section 9.3.4.

9.3. Methodology (Second Stage): Novel Utility Methods

Once the decision making alternative matrix is constructed, the next step is to combine the three measures in order to get an overall performance score for ranking decision making alternatives (*RCOs*). Such a task is not straightforward given the uncertainties of location and weight measures. Hence, the following context describes several methods produced to deal with various cases with uncertain location and weight measures.

9.3.1 A Traditional Additive Method Based on Crisp Location Measures

In most applications of the *MADM* technique, overall performance scores can be calculated using a crude multiple attribute utility approach. In such an approach, each attribute is assumed to be measurable on a ratio scale, and hence can be mapped onto a common interval [0, 1], where 0 indicates the "worst" value for the attribute and 1 represents the "best". Consequently, the overall performance scores can be computed using the equation as follows:

$$S_i = \sum_{j=1}^{n} w_j u_{ij} \tag{9.7}$$

where S_i is the overall or composite score of the i^{th} option; w_j is the normalised weight assigned to the j^{th} attribute; u_{ij} is the utility measure of the i^{th} option on the j^{th} attribute.

In the *BN* based *MADM* model, if all location measures are linear or bilinear (in other

words, the location measures can be represented by crisp numbers), then the overall performance scores can be obtained using a novel function which is extended on the basis of Equation (9.7) and includes the probabilistic measures as follows:

$$S_i = \sum_{j=1}^{n} w_j u_{ij} = \sum_{j=1}^{n} w_j \sum_{k_j=1}^{l_j} p_{ijk_j} l_{ijk_j} \tag{9.8}$$

where S_i is the overall or composite score of the i^{th} option; w_j is the normalised weight assigned to the j^{th} attribute; p_{ijk_j} is the probabilistic measure of the k_j^{th} state of the j^{th} attribute given the i^{th} option; l_{ijk_j} is the location measure of such a state; the combination of p_{ijk_j} and l_{ijk_j} is used to represent the utility measure of the i^{th} option on the j^{th} attribute.

The advantage of such an approach lies in its simplicity. However, in terms of accuracy, it is worrisome because not all attributes can be measured on a ratio scale. For example, the utility measures of the attributes whose states require to be located using judgemental measures may be inappropriately represented by crisp numbers. In dealing with a risk based decision making scenario, such attributes widely exist and as a result, appropriate methods that are suitable to modelling the judgemental location measures are required.

9.3.2 BFRB and ER

It has been proven that fuzzy numbers based on linguistic variables can give more consideration to human knowledge than crisp numbers based on point estimations in terms of subjective judgements. Thus, in the risk based multiple uncertain attribute decision making modelling, the states of the attributes which require the use of judgemental location measures can be modelled using fuzzy membership functions (fuzzy numbers). For example, assume the safety attribute X_j ($j \in (1, 2, \ldots, n)$) has four exclusive states – a set of ("poor", "average", "fair" and "good"), whose utility values can be modelled using fuzzy membership functions as the set of (0, 0, 0.3), (0.1, 0.35, 0.6), (0.4, 0.65, 0.9) and (0.7, 1, 1)*.

It is noteworthy that such fuzzy numbers have the difference in nature with the crisp ones representing the ratio scales in Section 9.3.1. While the crisp numbers based on a common interval [0, 1] can be used to represent location measures, the fuzzy ones are obtained/designed from/in different attribute universes (i.e. safety and cost universes) and thus they with the same value but from different attribute universes may indicate completely different location measures. It is therefore required to standardise all fuzzy numbers from different universes onto the same scale. Having known that human

* Also see the discussion related to the fuzzy attributes on Page 42.

preference is often used to model the utility space in *MADM*, a fuzzy common scale based on the human preference universe is developed in Figure 9.2. Such a scale as a generic case can be very suitable to dealing with the difficulties above. For example, if a fuzzy number (0, 0, 0.2) represents the linguistic variable "low" in a cost universe, it can be easily transformed into the fuzzy number with value (0.8, 1, 1) in the common scale using Equation (9.4) (if the three elements of the fuzzy number are separately considered as crisp numbers and then relocated to an interval [0, 1], which is the preference universe of the common scale). When all judgemental location measures on different attributes obtain their corresponding fuzzy numbers, they can be transformed onto the common scale and expressed by the five preference variables using the similarity function between two fuzzy sets (Equation (6.7)). Also, the crisp location measures can be fuzzifed and expressed by the five preference variables. For example, if a crisp location measure has been evaluated as 0.4 on the common interval [0, 1], then it can be equivalently expressed as 0.5 "slightly preferred" and 0.5 "preferred".

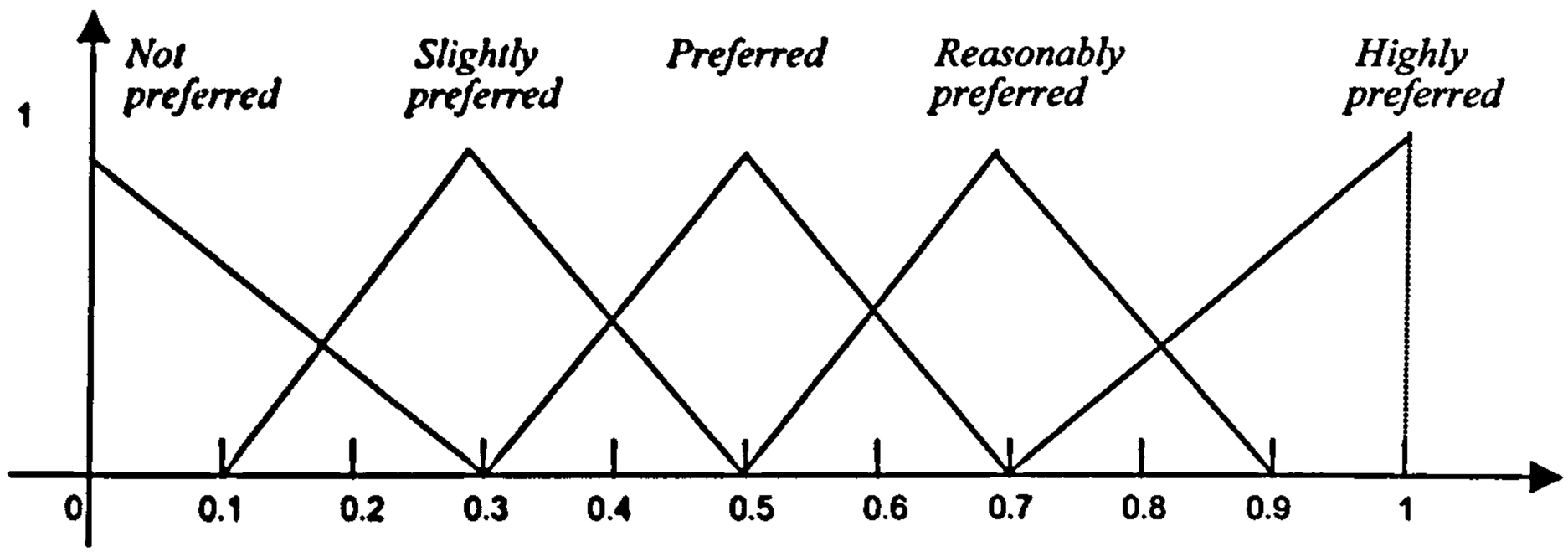


Figure 9.2. The membership functions of the common utility space

To combine the location measures and weight measures, a *BFRB* system can be established using the methodology in Chapter 6. Then using the *FRB-ER* approach proposed in Chapter 5, the probabilistic measures can be incorporated and the overall performance scores can be calculated to rank decision making alternatives (*RCOs*).

9.3.3 TOPSIS

A modified form of the *MADM* methodology known as *TOPSIS* can be adopted to combine the fuzzy and crisp attribute value (Chen and Hwang, 1992) and thus, be able to conduct the aggregation of three measures as an effective tool. The input to the process is the decision making matrix D that is represented by a $m \times n \times l_j$ model in Equation (9.2), where there are m alternatives with n attributes, which have l_j ($j \in (1, 2, \ldots, n)$) states. However, it is obvious that such a model is not convenient for decision makers to identify both positive and negative ideal solutions. Therefore, the probabilistic

and location measures attached on the matrices require to be combined into utility measures using the following equation:

$$u_{ij} = \sum_{k_j=1}^{l_j} p_{ijk_j} l_{ijk_j} \tag{9.9}$$

Consequently, the matrices can be transferred back to a new model similar to Equation (9.1), as shown in Equation (9.10):

$$D = \begin{array}{c} \\ A_1 \\ \vdots \\ A_i \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccccc} X_1 & \cdots & X_j & \cdots & X_n \end{array} \\ \begin{bmatrix} u_{11} & \cdots & u_{1j} & \cdots & u_{1n} \\ \vdots & & \vdots & & \vdots \\ u_{i1} & \cdots & u_{ij} & \cdots & u_{in} \\ \vdots & & \vdots & & \vdots \\ u_{m1} & \cdots & u_{mj} & \cdots & u_{mn} \end{bmatrix} \end{array} \tag{9.10}$$

Note that the attribute utility values u_{ij}, for alternative i and attribute j may be crisp and fuzzy numbers due to the natures of location measures l_{ijk_j}; the crisp attribute utility numbers can be defined as real number $\bar{u}_{ij}$ and the fuzzy attribute utility numbers can be defined as triangular numbers $\tilde{u}_{ij} = (a_{ij}, b_{ij}, c_{ij})$.

In the second step the decision matrix is normalised so that the elements are unit free, which allows for easier comparisons across attributes. A linear scale transformation is used to normalise crisp utility measures as shown in Equation (9.11):

$$\bar{v}_{ij} = \frac{\bar{u}_{ij}}{\bar{u}_j^+}, \text{ when } X_j \text{ is an increasingly ordering attribute}$$

$$\bar{v}_{ij} = \frac{\bar{u}_j^-}{\bar{u}_{ij}}, \text{ when } X_j \text{ is a decreasingly ordering attribute} \tag{9.11}$$

where $\bar{u}_j^+ = \arg\max_i \bar{u}_{ij}$; and $\bar{u}_j^- = \arg\min_i \bar{u}_{ij}$, $i \in (1,2, \ldots,m)$.

The linear scale transformation for fuzzy utility measures is

$$\tilde{v}_{ij} = \frac{\tilde{u}_{ij}}{\tilde{u}_j^+} = \left(\frac{a_{ij}}{c_j^+}, \frac{b_{ij}}{b_j^+}, \frac{c_{ij}}{a_j^+}\right), \text{ when } X_j \text{ is an increasingly ordering attribute}$$

$$\tilde{v}_{ij} = \frac{\tilde{u}_j^-}{\tilde{u}_{ij}} = \left(\frac{a_j^-}{c_{ij}}, \frac{b_j^-}{b_{ij}}, \frac{c_j^-}{a_{ij}}\right), \text{ when } X_j \text{ is a decreasingly ordering attribute} \tag{9.12}$$

where $\tilde{u}_j^+ = \arg\max_i \tilde{u}_{ij}$; and $\tilde{u}_j^- = \arg\min_i \tilde{u}_{ij}$, $i \in (1,2, \ldots,m)$.

The fuzzy data, $\tilde{u}_j^+ = (a_j^+, b_j^+, c_j^+)$ and $\tilde{u}_j^- = (a_j^-, b_j^-, c_j^-)$ can be obtained through a fuzzy ranking technique (Rilett and Rark, 2001) based on two criteria: the fuzzy mean value and the spread of fuzzy numbers (Dubois and Prade, 1987). The underlying assumption is that human intuition would favour a fuzzy number with a higher mean value and a lower spread (higher overall score with less variation). When the means of two fuzzy numbers are equal, the fuzzy number with the lower standard deviation would be preferred. Given a fuzzy number F, its mean and standard deviation are defined by Equations (9.13) and (9.14) (Budois and Prade, 1987; Rilett and Park, 2001), where $S(F)$ is the support (range) of the fuzzy number F.

$$\bar{x}_u(F) = \frac{\int_{S(F)} x u_F(x) dx}{\int_{S(F)} u_F(x) dx} \tag{9.13}$$

$$\sigma_u(F) = \left[\frac{\int_{S(F)} x^2 u_F(x) dx}{\int_{S(F)} x u_F(x) dx} - [\bar{x}_u(F)]^2 \right] \tag{9.14}$$

If all the fuzzy attributes are represented by a triangular distribution, Equation (9.13) and (9.14) can be simplified as follows:

$$\bar{x}_u(F) = \frac{1}{4}(a + 2b + c) \tag{9.15}$$

$$\sigma_u(F) = \frac{1}{80}(3a^2 + 4b^2 + 3c^2 - 2ac - 4ab - 4bc) \tag{9.16}$$

Therefore, for a given attribute j, the value $\tilde{u}_{ij}$ which has the largest generalised mean and the relatively small spread is defined as $\tilde{u}_j^+$; the value $\tilde{u}_{ij}$ which has the smallest mean and the relative large standard deviation is defined as $\tilde{u}_j^-$.

After applying Equations (9.11) and (9.12) to Equation (9.10), a normalized decision matrix V is obtained where the cells v_{ij} contain the normalized attribute values for the i^{th} option on the j^{th} attribute. v_{ij} consists of both fuzzy normalised attribute values $\tilde{v}_{ij}$ and crisp normalised attribute values $\bar{v}_{ij}$.

Next, the positive ideal solution ($\mathbf{IS}^P$), which is the vector involving the highest normalised scores for each attribute and the negative ideal solution ($\mathbf{IS}^N$), which is the vector involving the lowest normalised scores for each attribute can be obtained. Theoretically, either $\mathbf{IS}^P$ or $\mathbf{IS}^N$ containing the best or worst attribute values can be achieved from one special decision making alternative. However, in practice such an alternative is very unusual and thus, is normally considered as a hypothesis and serves as a reference or an anchor point for the decision making comparisons. For both crisp

and fuzzy numbers they can be defined as follows:

$$\mathbf{IS}^P = [v_1^+,\ldots,v_j^+,\ldots,v_n^+]$$
$$\mathbf{IS}^N = [v_1^-,\ldots,v_j^-,\ldots,v_n^-] \tag{9.17}$$

where $v_j^+ = \arg\max_i v_{ij}$; and $v_j^- = \arg\min_i v_{ij}$, $i \in (1,2,\ldots,m)$; if v_{ij} is a set of fuzzy numbers then v_j^+ and v_j^- can be obtained using Equations (9.13) – (9.16).

The difference between attribute values v_{ij} can be measured using their individual distances to the best and worst values using D_{ij}^+ and D_{ij}^-. For crisp numbers, they can be defined respectively as follows:

$$\overline{D}_{ij}^+ = |\,\overline{v}_{ij} - \overline{v}_j^+\,| \tag{9.18}$$
$$\overline{D}_{ij}^- = |\,\overline{v}_{ij} - \overline{v}_j^-\,| \tag{9.19}$$

For fuzzy data, the difference measures between two fuzzy numbers $\tilde{v}_{ij}(x)$, which is a given *RCO*'s attribute value, and $\tilde{v}_j^+(x)$, which is the best attribute value in the j^{th} chosen attribute set, can be defined as (Zimmemann, 1991; Rilett and Park, 2001):

$$\tilde{D}_{ij}^+(\tilde{v}_{ij},\tilde{v}_j^+) = 1 - \{\sup_x[\tilde{v}_{ij}(x) \wedge \tilde{v}_j^+(x)]\} \tag{9.20}$$

Similarly, the distance $\tilde{D}_{ij}^-$ between $\tilde{v}_{ij}(x)$ and $\tilde{v}_j^-(x)$, which is the worst attribute value in the j^{th} chosen attribute set, can be defined as follows:

$$\tilde{D}_{ij}^-(\tilde{v}_{ij},\tilde{v}_j^-) = 1 - \{\sup_x[\tilde{v}_{ij}(x) \wedge \tilde{v}_j^-(x)]\} \tag{9.21}$$

Both $\tilde{D}_{ij}^+$ and $\tilde{D}_{ij}^-$ are real numbers even though their input is fuzzy sets. In general, $\tilde{D}_{ij}^+$ measures how close each decision making alternative's attribute is to the $\mathbf{IS}^P$ and $\tilde{D}_{ij}^-$ measures how close each decision making alternative's attribute is to the $\mathbf{IS}^N$. Therefore, smaller $\tilde{D}_{ij}^+$ and larger $\tilde{D}_{ij}^-$ are preferred.

The next step is to identify the separation measures S_i^+ and S_i^- for each *RCO* which are related to the difference measures $\tilde{D}_{ij}^+$ and $\tilde{D}_{ij}^-$ with the posterior weights w_j* (more details are provided in the next chapter). The separation measures can be defined as the weighted sum of the difference measures across all attributes for each *RCO* and thus are expressed respectively as follows:

$$S_i^+ = \sum_{j=1}^{n} D_{ij}^+ w_j \text{ to the positive ideal option} \tag{9.22}$$

$$S_i^- = \sum_{j=1}^{n} D_{ij}^- w_j \text{ to the negative ideal option} \tag{9.23}$$

where for a given *RCO* lower value of S_i^+ and higher value of S_i^- are desirable, indicating that the attributes of the i^{th} *RCO* are closer to the $\mathbf{IS}^P$ and further from the $\mathbf{IS}^N$.

In order to rank the *RCOs*, a relative closeness index based on the separation measures is developed as follows:

$$C_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{9.24}$$

The *RCOs* can be ranked in an increasing order of the C_i index. The relative closeness index is essentially a measure of how close the attributes of a particular option are to both the $\mathbf{IS}^P$ and $\mathbf{IS}^N$. The C_i has a range of [0,1] where a value of zero would indicate that the corresponding *RCO* is the worst and equivalent to the $\mathbf{IS}^N$ and a value of one would represent that the corresponding *RCO* is the best and equivalent to the $\mathbf{IS}^P$.

9.3.4 Relative Weight Measures Using Entropy Calculation

While the *TOPSIS* technique deals with utility representations for real and fuzzy numbers as well as caters for dependent relationships between decision attributes, it does not explicitly model the changing propensity of decision attribute weight measures once *RCOs* or constraints are identified. Theoretically, the weight measures of decision attributes can only be precisely calculated and obtained on the basis of the complete knowledge of decision makers, both prior (i.e. historical information, which has been mastered by decision makers) and posterior (i.e. various *RCOs* and constraints observed from different objective situations). However it may not be the case in many real-time applications. Therefore, in this study the definition of prior weight measures is introduced first on the basis of the prior knowledge and then they can be developed into the posterior weight measures with the updated information representing the context dependency of decision attributes using the entropy theory (Zeleny, 1976). Entropy theory is ideal for this application because it can be used to measure the amount of information in the choice set and this information can be used to identify an attribute's relative importance (Relitte and Park, 2001).

The first step is to calculate u_j, the prior utility measure of the j^{th} risk attribute for all *RCOs*. Having known Equation (9.9), u_j can be calculated in a similar way as follows:

$$u_j = \sum_{k_j=1}^{l_j} p_{jk_j} l_{jk_j} \tag{9.25}$$

where p_{jk_j} is the marginal (prior posterior) probabilistic measure of the k_j^{th} state of the j^{th} attribute without the presentation of any *RCO*; l_{jk_j} is the location measure of such a state; the combination of p_{jk_j} and l_{jk_j} is used to represent the prior utility measure of the j^{th} attribute. Next, the posterior utility measures u_{ij} ($i = (1, 2, \ldots, m)$) of the j^{th} risk attribute given each *RCO* and their corresponding constraints can be computed using Equation (9.9). With them, a vector $A_j^{'}$, which characterises the utility measure changes of the j^{th} attribute given all the *RCOs* can be represented as follows:

$$A_j^{'} = \left\| u_{1j} - u_j \right|, \ldots, \left| u_{ij} - u_j \right|, \ldots, \left| u_{mj} - u_j \right\| \; (j \in (1, 2, \ldots, n)) \tag{9.26}$$

where $\left| u_{ij} - u_j \right|$ can be explained as the distances (difference) between two sets (either fuzzy or real numbers) u_{ij} and u_j and thus, always be represented by real numbers given Equations (9.18) – (9.21). Its normalised counterpart is

$$A_j = \left[k_{1j}, \ldots, k_{ij}, \ldots k_{mj} \right] \; (j \in (1, 2, \ldots, n)) \tag{9.27}$$

where $k_{ij} = \dfrac{\left| u_{ij} - u_j \right|}{\max \left| u_{ij} - u_j \right|}$. Note that the normalised variables k_{ij} are used for comparison purposes, although the entropy calculation allows the existence of non-normalised values as well.

The sum of the elements of the normalised vector, $S(A_j)$ is defined as

$$S(A_j) = \sum_{i=1}^{m} k_{ij} \;\; (j \in (1, 2, \ldots, n)) \tag{9.28}$$

The entropy measures of each decision attribute's "contrast intensity" is calculated as follows (Rillett and Park, 2001):

$$e(S(A_j)) = -\frac{1}{\ln m} \sum_{i=1}^{m} \left[\frac{k_{ij}}{S(A_j)} \ln \left(\frac{k_{ij}}{S(A_j)} \right) \right] \tag{9.29}$$

where by definition, the maximum value of $-\sum_{i=1}^{m} \left[\dfrac{k_{ij}}{S(A_j)} \ln \left(\dfrac{k_{ij}}{S(A_j)} \right) \right]$ is obtained as $\ln m$ ($e_{\max} = 1$) when all k_{ij} are identical for a given attribute j.

The total entropy across all decision attributes E, is

$$E = \sum_{j=1}^{n} e(S(A_j)) \tag{9.30}$$

The context dependent weight measures of the j^{th} attribute, w_j^c is inversely related to the entropy measures of the j^{th} attribute, $e(S(A_j))$. Given that the sum of all context dependent weight equals to one ($\sum_{j=1}^{n} w_j^c = 1$), then the weight of the j^{th} attribute can be computed as follows:

$$w_j^c = \frac{1 - e(S(A_j))}{(1 - e(S(A_1))) + \ldots + (1 - e(S(A_j))) + \ldots + (1 - e(S(A_n)))}$$
$$= \frac{1 - e(S(A_j))}{n - E} \tag{9.31}$$

Once the w_j^c is identified, the next step is to determine how to combine the prior weight measures w_j and the context dependent weight measures w_j^c to obtain the posterior weight measures. The combination usually takes additive or productive operations based on different premises and assumptions as well as the characteristics of decision makers. For example, in the assumption of the absence of any prior information, it is possible to use context dependent weight measures to determine the posterior weight measures. Consequently, the posterior weight measures w_j^* can be represented as follow:

$$w_j^* = \frac{w_j + w_j^c}{\sum_{r=1}^{n} (w_r + w_r^c)} \quad j = (1, 2, \ldots, or\ n) \tag{9.32}$$

If the basic premise is that once one of the prior and context dependent weight measures is zero, the posterior weight measures will be considered as zero even if the weight of the other one is measured as one, then the posterior weight measures can be calculated as follows:

$$w_j^* = \frac{w_j w_j^c}{\sum_{r=1}^{n} (w_r w_r^c)} \quad j = (1, 2, \ldots, or\ n) \tag{9.33}$$

which means that any element (w_j or w_j^c) is zero then the attribute it associates with will not work for decision making any more. In the risk based decision making model, the prior weight measures are normally obtained using historical data and decision making requirements. Furthermore, one of the main objectives of using *BNs* to model decision making problems is to emphasise the context dependency between decision attributes. Therefore, Equation (9.33) will be chosen to use in this study.

In general, as the normalised utility measure changes k_{ij} become more distinct and differentiated with respect to the j^{th} attribute, the corresponding contract intensity $e(S(A_j))$ for the given j^{th} attribute decreases. Consequently, the relative weight measure w_j^c related to the j^{th} attribute increases and furthermore, it leads to the increment of the posterior weight measure w_j^*.

9.4. Case Study: A Container Delivery Delay Analysis

9.4.1 Analyse the Case to Combine BNs with MADM

Container transportation delay is a common problem in supply chain management. It may result from various reasons such as transport tool failure, human error, ineffective container control, loose connection between multiple transport modes and external environment factors (i.e. congestion), etc. This section analyses a typical decision scenario for choosing an appropriate container transport mode to prevent a delivery delay in order to demonstrate the described methodology. It is described as follows:

A shipper wants to deliver container cargoes from a place *A* to their consignee in a place *B*. There are three main modes of transport available between *A* and *B*. They are separately container trucks (road), trains (rail) and feeders (shipping).

For the shipper's reason, the departure time is required to be between Monday and Friday. For the consideration of the consignee, the arrival time is as early as possible however not later than the Monday in the next week. With the on-time delivery premise, the shipper and consignee want the delivery to be as cheap and safe as possible. However, simultaneously they also have to take account of certain circumstances and external factors like weather, road traffic congestion and train problems. Such a situation may vary according to status of the consignee. For example, the aim of transporting the containers to *B* (Situation 1) could be to transfer them on a mother ship for another place *C* (Situation 2). In such a case, the arrival time may require to be as late as possible before the loading time of the mother ship, which may be from Thursday to Saturday. Otherwise, the consignee needs to pay the port in *B* more quay rent for storing the containers.

The objective of analysing the decision scenario is to deliver the containers to *B* on the required time (as early as possible in Situation 1 and as late as possible (the least waiting time) in Situation 2). The *RCOs* are chosen on the basis of the main transport modes and the departure time. In terms of time, the flexibility of three transport modes decreases in an order of road, rail and shipping. For simplicity the departure time is considered as discrete five days (from Monday to Friday). Consequently, the *RCOs* can be identified as:

- Container trucks depart on Monday.
- Container trucks depart on Wednesday.
- Container trucks depart on Friday.
- Trains depart on Thursday.
- Container trucks depart on Tuesday.
- Container trucks depart on Thursday.
- Trains depart on Tuesday.
- Feeders depart on Wednesday.

The perspective of the decision problem is associated with not only the shipper but also the stakeholders, both the consignee and possible carriers. While the shipper is interested in the cost of the delivery with on-time delivery, the consignee on the other hand is only interested in not having too much waiting time. Such interests are based on the safety consideration of three transport modes. The possible carriers want to be chosen in order to make profits. Obviously, the carriers are not important stakeholders in this analysis and thus, are excluded from the decision making process.

Having analysed the objective and perspective, the decision problem can be well defined by further researching the concepts of the decision attributes, constraints, risk factors and their causal relationships, as shown in Table 9.1.

Table 9.1. The key concepts

Container delivery delay	
Objective	To deliver the containers from *A* to *B* as early as possible in Situation 1; To deliver the containers in good time to catch the mother ship in Situation 2.
Perspective	Decision maker: the shipper Key stakeholder: the consignee
RCOs	Container trucks depart on Monday. Container trucks depart on Tuesday. Container trucks depart on Wednesday. Container trucks depart on Thursday. Container trucks depart on Friday. Trains depart on Tuesday. Trains depart on Thursday. Feeders depart on Wednesday.
Decision attributes	Arrival time, cost and safety
Constraints	Required time and waiting time
Risk factors (not controlled by decision makers)	Nominal journey time, nominal postponement and adjusted journey time
Causal relationship	The transport mode will influence the cost, safety and nominal journey time, the start time and nominal postponement. The start time will further influence the nominal journey time (for example, the traffic situation on Monday may be worse than the one of Friday). The nominal journey time and nominal postponement determine the adjusted journey time, which together with the start time affects the arrival time. Based on the required time, the arrival time has the waiting time as its child. Such causal relationship will vary in Situation 2, where the waiting time is connected with the cost since the consignee needs to pay for the storage of the containers and the safety considering that too short waiting time leads to the failure of loading the containers on board of the mother vessel.

According to the causal relationship analysis, the qualitative *BNs* for Situations 1 and 2 can be separately developed using the concept of d-separation in Figures 9.3 and 9.4.

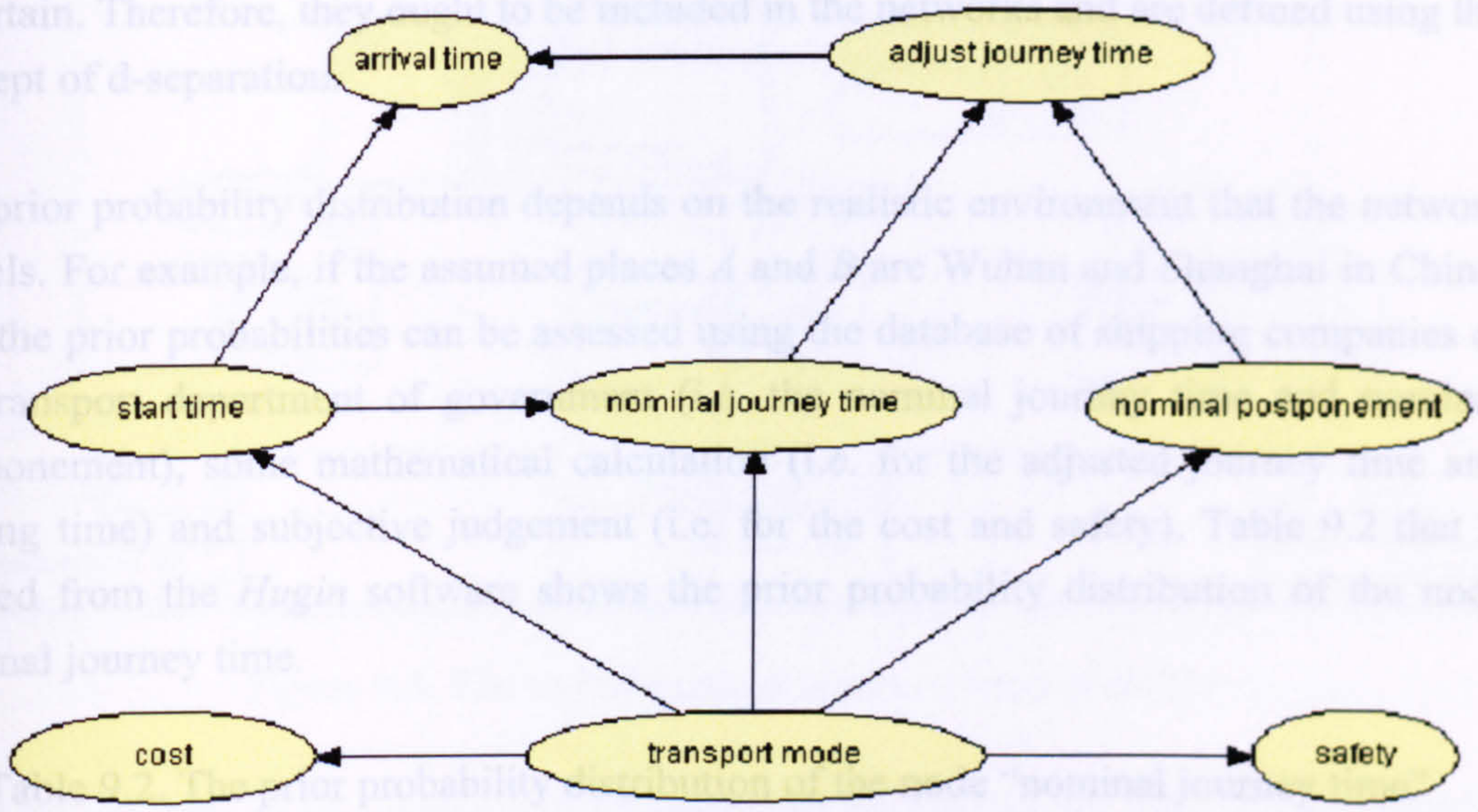


Figure 9.3. The qualitative *BN* for Situation 1

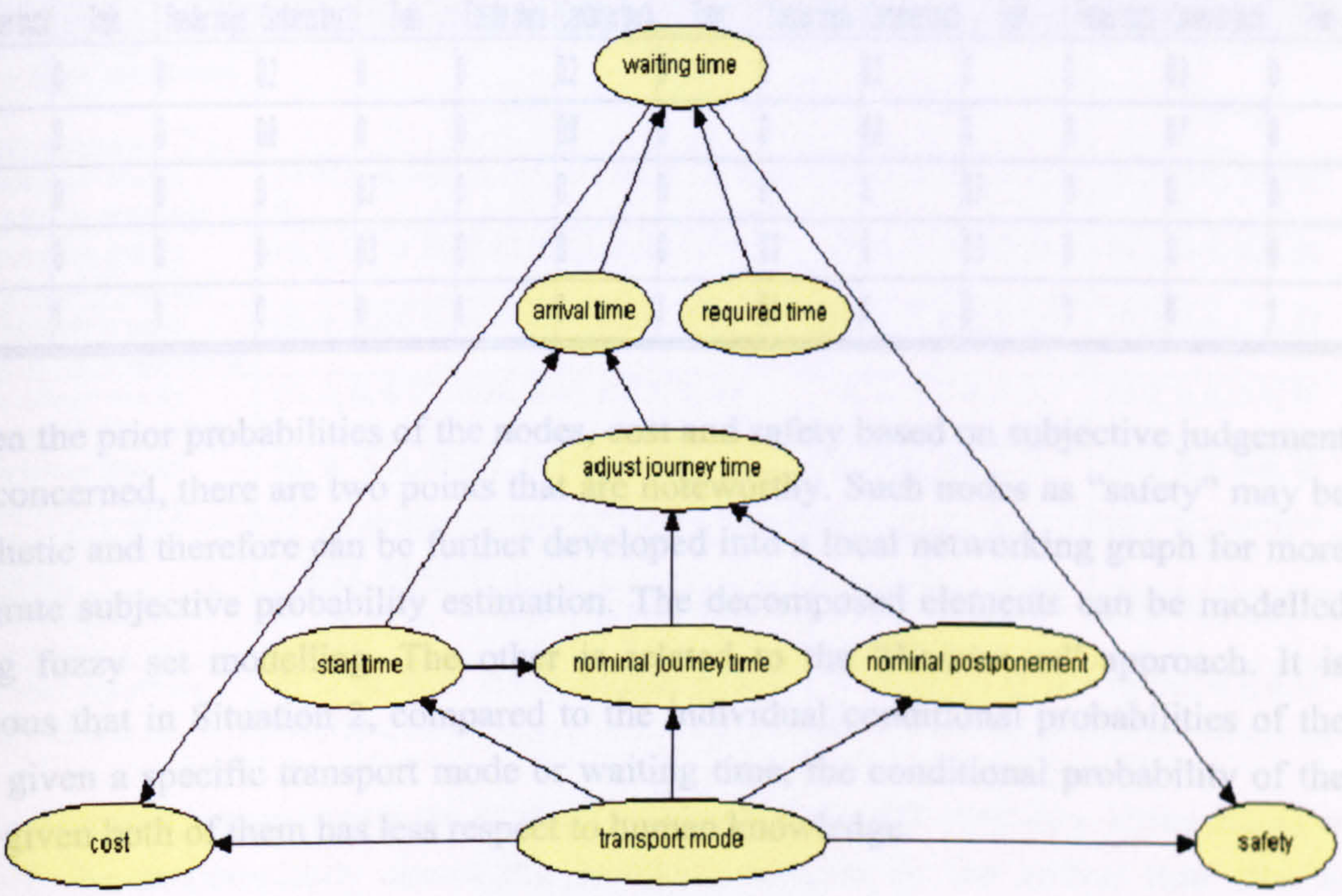


Figure 9.4. The qualitative *BN* for Situation 2

In the analysis of Figure 9.3, once a transport mode is selected, the cost and safety are certain in terms of their utility value - the combination of probabilistic and location measures, because they are conditionally independent of any nodes in the networks.

Such attributes as the cost and safety are normally defined as certain attributes in the previous work and they do not need to be incorporated into the *BN* for simplification. However, in this case, when the situation changes, certain attributes can become uncertain. Therefore, they ought to be included in the networks and are defined using the concept of d-separation.

The prior probability distribution depends on the realistic environment that the network models. For example, if the assumed places *A* and *B* are Wuhan and Shanghai in China, then the prior probabilities can be assessed using the database of shipping companies or the transport department of government (i.e. the nominal journey time and nominal postponement), some mathematical calculation (i.e. for the adjusted journey time and waiting time) and subjective judgement (i.e. for the cost and safety). Table 9.2 that is elicited from the *Hugin* software shows the prior probability distribution of the node nominal journey time.

Table 9.2. The prior probability distribution of the node "nominal journey time"

start time	Monday			Tuesday			Wednesday			Thursday			Friday		
transport m...	Container truck	Train	Feeder ships	Container truck	Train	Feeder ships	Container truck	Train	Feeder ships	Container truck	Train	Feeder ships	Container truck	Train	Feeder ships
0-1day	0.1	0	0	0.2	0	0	0.2	0	0	0.2	0	0	0.3	0	0
1-2days	0.9	0	0	0.8	0	0	0.8	0	0	0.8	0	0	0.7	0	0
2-3days	0	0	0	0	0.7	0	0	0	0	0	0.7	0	0	0	0
3-4days	0	0	0	0	0.3	0	0	0	0.9	0	0.3	0	0	0	0
>(=)4days	0	1	1	0	0	1	0	1	0.1	0	0	1	0	1	1

When the prior probabilities of the nodes, cost and safety based on subjective judgement are concerned, there are two points that are noteworthy. Such nodes as "safety" may be synthetic and therefore can be further developed into a local networking graph for more accurate subjective probability estimation. The decomposed elements can be modelled using fuzzy set modelling. The other is related to the "*Noisier or*" approach. It is obvious that in Situation 2, compared to the individual conditional probabilities of the cost given a specific transport mode or waiting time, the conditional probability of the cost given both of them has less respect to human knowledge.

Once the prior probabilities have been appropriately distributed, the next is to use the *Hugin* software to calculate the values of the risk attributes with certain *RCOs* and constraints. In Figure 9.5, a specified *BN* is provided to represent the probabilistic measures of the decision attributes given the *RCO* that container trucks depart on Monday. They are separately (0.035, 0.365, 0.465, 0.135, 0, 0, 0, 0, 0) for the arrival time, (0, 0, 0, 0.8, 0.2) for the cost and (0.2, 0.4, 0.4, 0) for the safety.

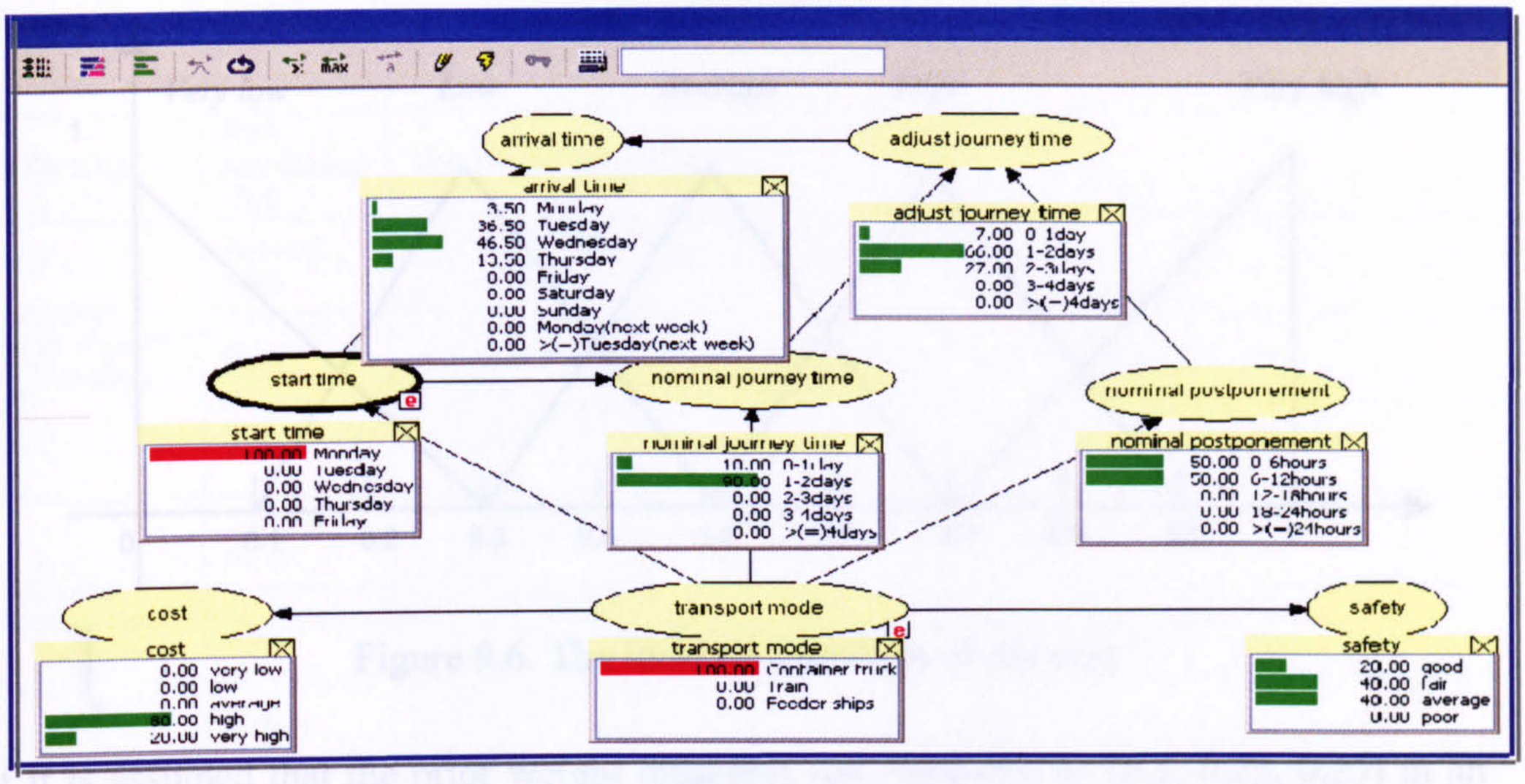


Figure 9.5. The probabilistic measures of one of *RCOs*

In a similar way, all the probabilistic measures can be obtained and described in Table 9.3.

Table 9.3. The probabilistic measures of all *RCOs*

Risk attributes / *Risk control options*	**Arrival time**	**Cost**	**Safety**
Container trucks depart on Monday.	(0.035, 0.365, 0.465, 0.135, 0, 0, 0, 0, 0)	(0, 0, 0, 0.8, 0.2)	(0.2, 0.4, 0.4, 0)
Container trucks depart on Tuesday.	(0, 0.07, 0.38, 0.43, 0.12, 0, 0, 0, 0)	(0, 0, 0, 0.8, 0.2)	(0.2, 0.4, 0.4, 0)
Container trucks depart on Wednesday.	(0, 0, 0.07, 0.38, 0.43, 0.12, 0, 0, 0)	(0, 0, 0, 0.8, 0.2)	(0.2, 0.4, 0.4, 0)
Container trucks depart on Thursday.	(0, 0, 0, 0.07, 0.38, 0.43, 0.12, 0, 0)	(0, 0, 0, 0.8, 0.2)	(0.2, 0.4, 0.4, 0)
Container trucks depart on Friday.	(0, 0, 0, 0, 0.105, 0.395, 0.395, 0.105, 0)	(0, 0, 0, 0.8, 0.2)	(0.2, 0.4, 0.4, 0)
Trains depart on Tuesday.	(0, 0, 0, 0.217, 0.443, 0.2488, 0.0228, 0.0228, 0.0456)	(0, 0.1, 0.9, 0, 0)	(0.6, 0.4, 0, 0)
Trains depart on Thursday.	(0, 0, 0, 0, 0, 0.217, 0.443, 0.2488, 0.0912)	(0, 0.1, 0.9, 0, 0)	(0.6, 0.4, 0, 0)
Feeders depart on Wednesday.	(0, 0, 0, 0, 0, 0.117, 0.2702, 0.1532, 0.4596)	(0.25, 0.75, 0, 0, 0)	(0, 0.2, 0.3, 0.5)

The next step is to calculate the location measures of the risk attributes. Using Equation (9.4), the monotonically decreasing location measures of the arrival time can be obtained as (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0), where "Monday" takes a value 1 and then ">(=)Tuesday(next week)" is linearly distributed a value 0. The judgemental location measures of the safety are defined as ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)). The membership function of the states of the cost can be modelled in Figure 9.6 and thus, their location measures are the set of ((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)).

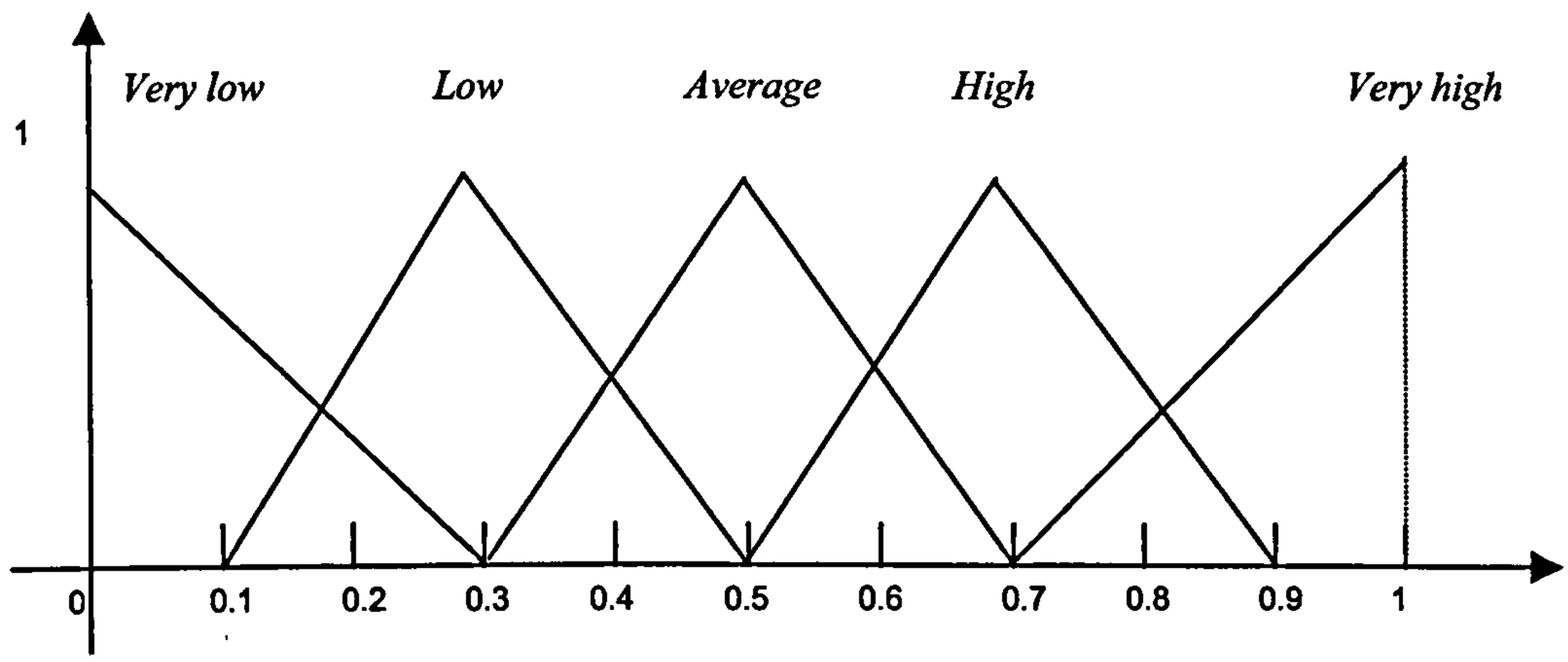


Figure 9.6. The location measures of the cost

If it is assumed that the prior weight measures are computed as (0.5, 0.25, 0.25) in an order of the arrival time, cost and safety using an *AHP* method, then the decision matrix for this case can be represented in Table 9.4 using Equation (9.2).

9.4.2 Novel Utility Representation for Calculating Overall Performance Scores

For the purpose of comparison, the traditional utility function of *MADM* is used to calculate the overall performance values of various *RCOs*. The point estimations of the location measures of the attributes, cost and safety can be subjectively assessed as (1, 0.75, 0.5, 0.3, 0) and (1, 0.75, 0.25, 0) at the common scale [0, 1]. Using Equation (9.7) and its extension, Equation (9.8), the overall performance score of the *RCO* that container trucks depart on Monday can be calculated as follows:

$$S_1 = \sum_{j=1}^{3} w_j u_{1j} = \sum_{j=1}^{3} w_j \sum_{k_j=1}^{lj} p_{1jk_j} l_{1jk_j}$$

$$=(0.035 \times 1 + 0.365 \times 0.875 + 0.465 \times 0.75 + 0.135 \times 0.625) \times 0.5$$
$$+ (0.8 \times 0.3) \times 0.25 + (0.2 \times 1 + 0.4 \times 0.75 + 0.4 \times 0.25) \times 0.25$$
$$= 0.604$$

Similarly, the other overall performance scores of *RCOs* can be computed as follows:

$S_2 = 0.548$
$S_3 = 0.485$
$S_4 = 0.423$
$S_5 = 0.366$
$S_6 = 0.584$
$S_7 = 0.467$
$S_8 = 0.334$

Table 9.4. The decision matrix

***RCOs* (A_i)**	**Risk attributes (X_j)**	**Measurement values (x_{ijk_j})**
Container trucks depart on Monday. (#1)	Arrival time	p = (0.035, 0.365, 0.465, 0.135, 0, 0, 0, 0, 0) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0, 0, 0.8, 0.2) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.2, 0.4, 0.4, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Container trucks depart on Tuesday. (#2)	Arrival time	p = (0, 0.07, 0.38, 0.43, 0.12, 0, 0, 0, 0) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0, 0, 0.8, 0.2) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.2, 0.4, 0.4, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Container trucks depart on Wednesday. (#3)	Arrival time	p = (0, 0, 0.07, 0.38, 0.43, 0.12, 0, 0, 0) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0, 0, 0.8, 0.2) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.2, 0.4, 0.4, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Container trucks depart on Thursday. (#4)	Arrival time	p = (0, 0, 0, 0.07, 0.38, 0.43, 0.12, 0, 0) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0, 0, 0.8, 0.2) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.2, 0.4, 0.4, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Container trucks depart on Friday. (#5)	Arrival time	p = (0, 0, 0, 0, 0.105, 0.395, 0.395, 0.105, 0) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0, 0, 0.8, 0.2) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.2, 0.4, 0.4, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Trains depart on Tuesday. (#6)	Arrival time	p = (0, 0, 0, 0.217, 0.443, 0.249, 0.023, 0.023, 0.045) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0.1, 0.9, 0, 0) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.6, 0.4, 0, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Trains depart on Thursday. (#7)	Arrival time	p = (0, 0, 0, 0, 0, 0.217, 0.443, 0.249, 0.091) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0, 0.1, 0.9, 0, 0) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0.6, 0.4, 0, 0) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25
Feeders depart on Wednesday. (#8)	Arrival time	p = (0, 0, 0, 0, 0, 0.117, 0.27, 0.153, 0.46) l = (1, 0.875, 0.75, 0.625, 0.5, 0.375, 0.25, 0.125, 0) w = 0.5
	Cost	p = (0.25, 0.75, 0, 0, 0) l = (((0, 0, 0.3), (0.1, 0.3, .0.5), (0.3, 0.5, 0.7), (0.5, 0.7, 0.9), (0.7, 1, 1)) w = 0.25
	Safety	p = (0, 0.2, 0.3, 0.5) l = ((0.7, 1, 1), (0.4, 0.65, 0.9), (0.1, 0.35, 0.6), (0, 0, 0.3)) w = 0.25

These scores indicate that the optimal *RCO* is to use container trucks departing on Monday and the second best option is to use trains on Tuesday.

According to Figure 9.3, given a chosen *RCO*, three risk attributes form a diverging connection and thus, show conditionally independent relationships. Considering that using point estimations to deal with the fuzzy nature of the states of the attributes, cost and safety discounts the accuracy of the traditional crude *MADM* method, the *BFRB-ER* method can be employed to rank the options more reasonably and appropriately.

Regarding the *BFRB-ER* method, the first step is to construct a logical *BFRB*. In order to do that, the location measures of the three decision attributes need to be mapped onto the common space, which is the utility function in Figure 9.2. Each measure, either a numerical or fuzzy number, can be mapped on the utility membership function and then described by five preference expressions with belief degrees. For example, the location measure (0.1, 0.3, 0.5) of the state, "*low*", of the attribute, cost, can be first standardised as (0.5, 0.7, 0.9) and then mapped onto the utility scale (shown in Figure 9.7) as follows (using Equations (6.7) – (6.9)):

L_{low} = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (1, "*reasonably preferred*"), (0, "*highly preferred*")}

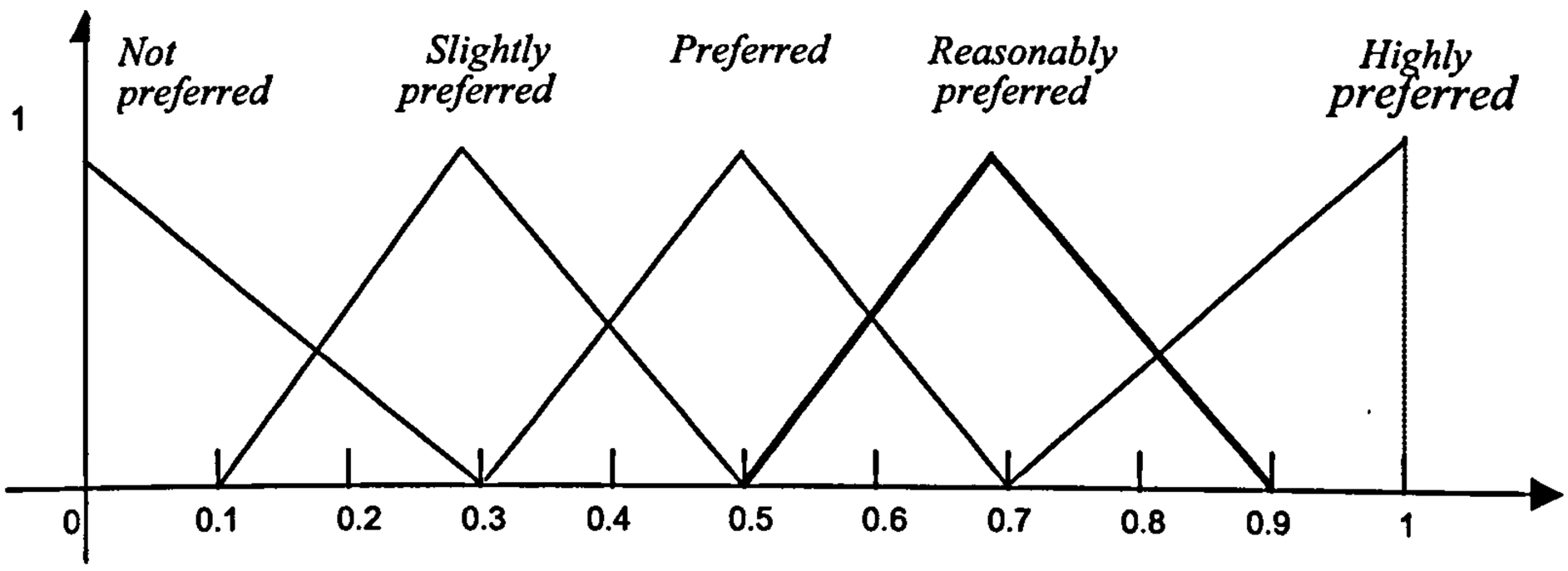


Figure 9.7. Mapping the location measures of the "*low*" state of the cost to the utility scale

Similarly, other location measures represented by the preferred expressions can be computed and obtained as follows:

l_{Monday} = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (1, "*highly preferred*")}

$l_{Tuesday}$ = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0.177, "*reasonably preferred*"), (0.823, "*highly preferred*")}

$l_{Wednesday}$ = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0.818, "*reasonably preferred*"), (0.182, "*highly preferred*")}

$l_{Thursday}$ = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0.375, "*preferred*"),

(0.625, "*reasonably preferred*"), (0, "*highly preferred*")}

l_{Friday} = {(0,"*not preferred*"), (0, "*slightly preferred*"), (1, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

$l_{Saturday}$ = {(0,"*not preferred*"), (0.625, "*slightly preferred*"), (0.375, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

l_{Sunday} = {(0.182,"*not preferred*"), (0.818, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

$l_{Monday(nextweek)}$ = {(0.823,"*not preferred*"), (0.177, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

$l_{\geq Tuesday(nextweek)}$ = {(1,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

$l_{very\ low}$ = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (1, "*highly preferred*")}

$l_{average(cost)}$ = {(0,"*not preferred*"), (0, "*slightly preferred*"), (1, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

l_{high} = {(0,"*not preferred*"), (1, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

$l_{very\ high}$ = {(1,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

l_{good} = {(0,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (1, "*highly preferred*")}

l_{fair} = {(0,"*not preferred*"), (0.034, "*slightly preferred*"), (0.307, "*preferred*"), (0.547, "*reasonably preferred*"), (0.112, "*highly preferred*")}

$l_{average}$ = {(0.112,"*not preferred*"), (0.547, "*slightly preferred*"), (0.307, "*preferred*"), (0.034, "*reasonably preferred*"), (0, "*highly preferred*")}

l_{poor} = {(1,"*not preferred*"), (0, "*slightly preferred*"), (0, "*preferred*"), (0, "*reasonably preferred*"), (0, "*highly preferred*")}

Then using the *ER* approach, together with the weight measures (0.5, 0.25, 0.25) of the three attributes, the arrival time, cost and safety, a *BFRB* including 180 (9 × 5 × 4) rules can be generated. The first 6 rules in such a rule-based system are shown in Table 9.5.

Table 9.5. The partial rules of the new developed *BFRB*

Rules	**Risk attributes**			**Preference estimation (decision making)**				
No	Arrival time	Cost	Safety	Not preferred	Slightly preferred	Preferred	Reasonably preferred	Highly preferred
1	Monday	Very low	Good					1
2	Monday	Very low	Fair		0.006	0.05	0.088	0.856
3	Monday	Very low	Average	0.019	0.912	0.051	0.006	0.833
4	Monday	Very low	Poor	0.167				0.833
5	Monday	Low	Good				0.167	0.833
6	Monday	Low	Fair		0.006	0.058	0.327	0.609

* *The whole structure of the BFRB is given in Appendix 6.*

Once the *BFRB* is constructed, the individual overall performance scores of all *RCOs* can be calculated using the *FRB-ER* approach with the probabilistic measures as input. For example, for the *RCO#1*, its input can be obtained as the set of {(0.035, "*Monday*"), (0.365, "*Tuesday*"), (0.465, "*Wednesday*"), (0.135, "*Thursday*")} for the attribute, arrival time, the set of {(0.8, "*high*"), (0.2, "*very high*")} for the attribute, cost and the set of {(0.2, "*good*"), (0.4, "*fair*"), (0.4, "*average*") for the attribute, safety. Consequently, 24 (4 × 2 × 3) rules will be combined to calculate the overall performance score of the *RCO#1*. They are *Rule 13, Rule 14, Rule 15, Rule 17, Rule 18, Rule 19, Rule 33, Rule 34, Rule 35, Rule 37, Rule 38, Rule 39, Rule 53, Rule 54, Rule 55, Rule 57, Rule 58, Rule 59, Rule 73, Rule 74, Rule 75, Rule 77, Rule 78* and *Rule 79* in Appendix 6. According to the input, their corresponding rule weights can be computed and the overall performance score of the *RCO#1* can be obtained using the *FRB* approach in Chapter 5 as:

S_1 = {(0.04,"*not preferred*"), (0.204, "*slightly preferred*"), (0.069, "*preferred*"), (0.385, "*reasonably preferred*"), (0.302, "*highly preferred*")} ≈ 0.04 × 0 + 0.204 × 0.3 + 0.069 × 0.5 +0.385 × 0.7 + 0.302 × 1 = 0.667

where S_1 means the overall performance score of the *RCO#1* and the symbol "≈" indicates the defuzzification operation using Equation (5.6).

In a similar way, the overall performance scores of the other *RCOs* can be computed as follows:

S_2 = {(0.04,"*not preferred*"), (0.202, "*slightly preferred*"), (0.21, "*preferred*"), (0.436, "*reasonably preferred*"), (0.112, "*highly preferred*")} ≈ 0.583

S_3 = {(0.039,"*not preferred*"), (0.25, "*slightly preferred*"), (0.452, "*preferred*"), (0.212, "*reasonably preferred*"), (0.047, "*highly preferred*")} ≈ 0.496

S_4 = {(0.048,"*not preferred*"), (0.468, "*slightly preferred*"), (0.388, "*preferred*"), (0.058, "*reasonably preferred*"), (0.038, "*highly preferred*")} ≈ 0.413

S_5 = {(0.113,"*not preferred*"), (0.651, "*slightly preferred*"), (0.164, "*preferred*"), (0.036, "*reasonably preferred*"), (0.036, "*highly preferred*")} ≈ 0.339

S_6 = {(0.036,"*not preferred*"), (0.082, "*slightly preferred*"), (0.667, "*preferred*"), (0.115, "*reasonably preferred*"), (0.1, "*highly preferred*")} ≈ 0.539

S_7 = {(0.215,"*not preferred*"), (0.34, "*slightly preferred*"), (0.269, "*preferred*"), (0.054, "*reasonably preferred*"), (0.122, "*highly preferred*")} ≈ 0.396

S_8 = {(0.549,"*not preferred*"), (0.207, "*slightly preferred*"), (0.047, "*preferred*"), (0.155, "*reasonably preferred*"), (0.042, "*highly preferred*")} ≈ 0.236

where each S_j, j = (2, 3, …, 8) represents the overall performance scores of the other *RCOs*. Using the defuzzified values, the *RCO#1* (container trucks depart on Monday) is the optimal decision alternative and the *RCO#2* (container trucks depart on Tuesday) rather than *RCO#6* (trains depart on Tuesday) is the second best option.

The discussion above considers multiple uncertain attribute decision making with the condition that the relationships between attributes are assumed to be independent. The emphasis is focused on dealing with multiplicity, randomness and fuzziness. However, when such a condition is changed and the decision attributes surely have dependencies, the *TOPSIS* with entropy calculation method can be applied and Situation 2 in the case study is used to test the method in the following context.

When container cargos require to be transferred from *B* to *C*, Situation 1 changes to Situation 2, which has been modelled using Figure 9.4. Compared to Figure 9.3, Figure 9.4 has two new nodes, "required time" and "waiting time" and four new links connecting "required time" with "waiting time", "arrival time" with "waiting time", "waiting time" with "cost" and "waiting time" with "safety", which make the three risk attributes not conditionally independent any more even given *RCOs*. Consequently, using *Hugin* software, the prior posterior probability distributions of the risk attributes can be obtained and shown in Figure 9.8.

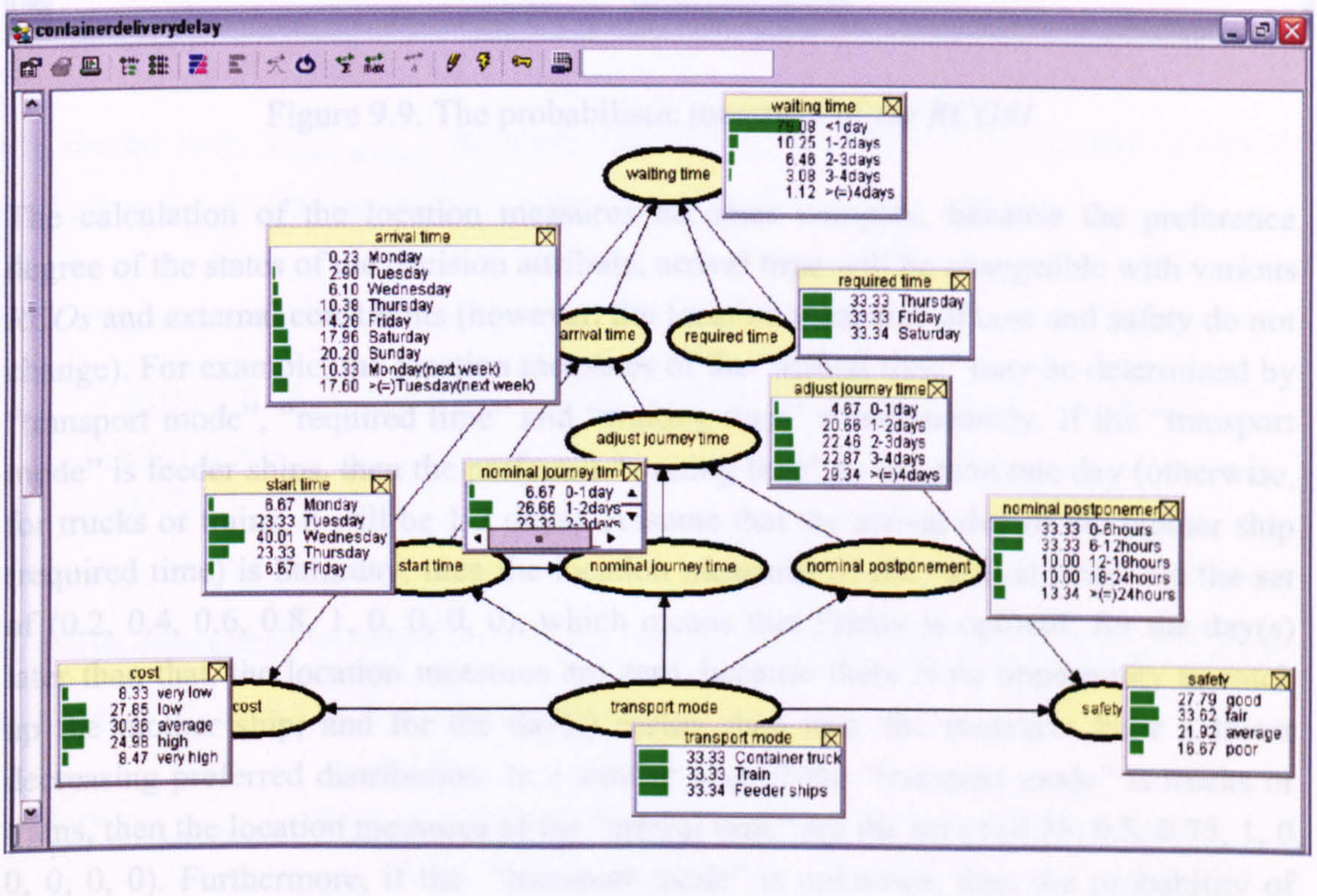


Figure 9.8. The prior posterior probability distribution of the risk attributes

In order to construct the new decision matrix in Situation 2, the probabilistic, location and weight measures require to be reassessed. The estimation of the probabilistic measures based on Bayesian inference software packages is relatively straightforward. For example, given *RCO#1*, the probabilistic measures can be calculated using *Hugin* software in Figure 9.9.

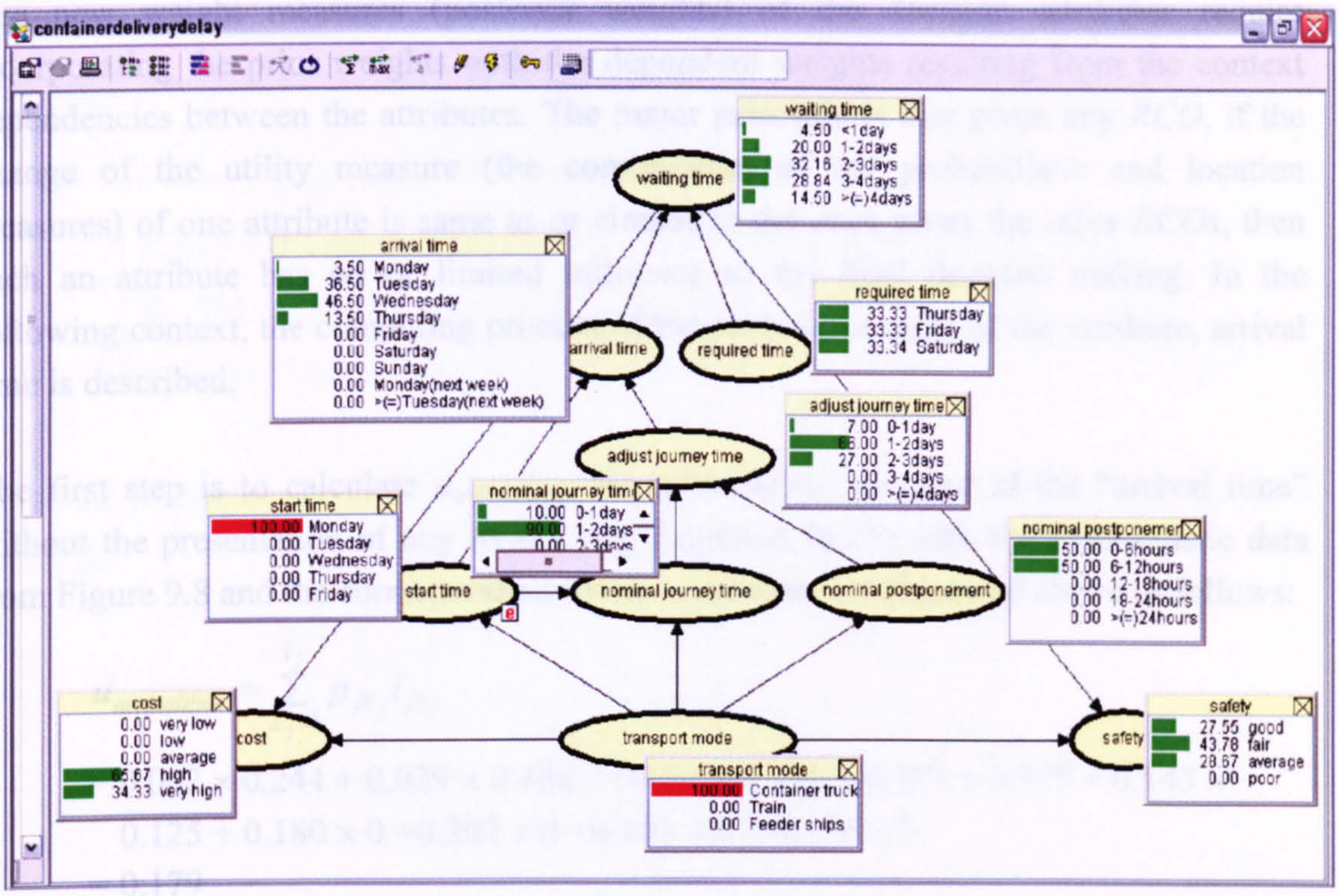


Figure 9.9. The probabilistic measures of the *RCO#1*

The calculation of the location measures becomes complex, because the preference degree of the states of the decision attribute, arrival time will be changeable with various *RCOs* and external constraints (however, the location measures of cost and safety do not change). For example, the location measures of the "arrival time" may be determined by "transport mode", "required time" and "waiting time" simultaneously. If the "transport mode" is feeder ships, then the preferred "waiting time" is less than one day (otherwise, for trucks or trains, it will be 1-2 days). Assume that the arrival day of the mother ship (required time) is Saturday, then the location measures of the "arrival time" are the set of (0.2, 0.4, 0.6, 0.8, 1, 0, 0, 0, 0), which means that Friday is optimal; for the day(s) later than that, the location measures are zero, because there is no opportunity to catch up the mother ship; and for the day(s) earlier than that, the measures have a linear decreasing preferred distribution. In a similar way, if the "transport mode" is trucks or trains, then the location measures of the "arrival time" are the set of (0.25, 0.5, 0.75, 1, 0, 0, 0, 0, 0). Furthermore, if the "transport mode" is unknown, then the probability of using feeders is 0.125 (1 out of 8 *RCOs*) and the probability of using trucks or trains is 0.875. In such a circumstance, the location measures of the "arrival time" belong to the set of (0.2, 0.4, 0.6, 0.8, 1, 0, 0, 0, 0) with a belief degree of 0.125 and the set of (0.25, 0.5, 0.75, 1, 0, 0, 0, 0, 0) with 0.875 credibility. Consequently, the location measures of the "arrival time" without the presentation of *RCOs* are calculated as (0.244, 0.488, 0.731, 0.975, 0.125, 0, 0, 0, 0) (= (0.2, 0.4, 0.6, 0.8, 1, 0, 0, 0, 0) × 0.125 + (0.25, 0.5, 0.75, 1, 0, 0, 0, 0, 0) × 0.875).

The new weight measures (posterior weights) of the decision attributes require incorporating the prior weights with the dependent weights resulting from the context dependencies between the attributes. The major principle is that given any *RCO*, if the change of the utility measure (the combination of the probabilistic and location measures) of one attribute is same as or similar to the ones given the other *RCOs*, then such an attribute has no or limited influence to the final decision making. In the following context, the computing process of the posterior weight of the attribute, arrival time is described.

The first step is to calculate $u_{arrivaltime}$, the prior utility measure of the "arrival time" without the presentation of any *RCO* using Equation (9.25) with the probabilistic data from Figure 9.8 and the corresponding location measure set discussed above as follows:

$$u_{arrivaltime} = \sum_{k_j=1}^{l_j} p_{jk_j} l_{jk_j}$$

$$= 0.002 \times 0.244 + 0.029 \times 0.488 + 0.061 \times 0.731 + 0.104 \times 0.975 + 0.143 \times 0.125 + 0.180 \times 0 + 0.202 \times 0 + 0.103 \times 0 + 0.176 \times 0$$

$$= 0.179$$

In a similar way, $u_{1,arrivaltime}$, the posterior utility measures of the attribute, "arrival time" given the *RCO#1* can be calculated using Equation (9.9) as follows:

$$u_{1,arrivaltime} = \sum_{k_j=1}^{l_j} p_{ijk_j} l_{ijk_j}$$

$$= 0.035 \times 0.25 + 0.365 \times 0.5 + 0.465 \times 0.75 + 0.135 \times 1 + 0 \times 0 + 0 \times 0 + 0 \times 0 + 0 \times 0 + 0 \times 0 + 0 \times 0$$

$$= 0.675$$

where p_{ijk_j} can be obtained as the set of (0.035, 0.365, 0.465, 0.135, 0, 0, 0, 0) using the model established in *Hugin* (see Figure 9.9) and l_{ijk_j} has been analysed previously to be the set of (0.25, 0.5, 0.75, 1, 0, 0, 0, 0, 0).

Similarly, $u_{i,arrivaltime}$ ($i = 2, 3, \ldots, 8$) can be calculated and obtained as follows:

$$u_{2,arrivaltime} = 0.750$$

$$u_{3,arrivaltime} = 0.433$$

$$u_{4,arrivaltime} = 0.070$$

$$u_{5,arrivaltime} = 0$$

$$u_{6,arrivaltime} = 0.217$$

$$u_{7,arrivaltime} = 0$$

$$u_{8,arrivaltime} = 0$$

Consequently, $A'_{attrivaltime}$, which characterises the utility measure changes of the arrival time given the each *RCO* can be represented using Equation (9.26) as follows:

$$A'_{arrivaltime} = \left[\left|u_{1,arrivaltime} - u_{arrivaltime}\right|,\ldots,\left|u_{8,arrivaltime} - u_{arrivaltime}\right|\right]$$

$$= \begin{bmatrix} |0.675-0.179|,|0.750-0.179|,|0.433-0.179|,|0.070-0.179|, \\ |0-0.179|,|0.217-0.179|,|0-0.179|,|0-0.179| \end{bmatrix}$$

$$= [0.496,0.571,0.254,0.109,0.179,0.038,0.179,0.179]$$

Next, the normalising vector of $A'_{attrivaltime}$, $A_{attrivaltime}$ can be calculated using Equation (9.27) as:

$$A_{arrivaltime} = \begin{bmatrix} 0.496/0.571', 0.571/0.571', 0.254/0.571', 0.109/0.571', \\ 0.179/0.571', 0.038/0.571', 0.179/0.571', 0.179/0.571 \end{bmatrix}$$

$$= [0.869,1,0.449,0.190,0.313,0.067,0.313,0.313]$$

Then, according to Equation (9.28), the sum of the elements of the vector is calculated as:

$$S(A_{arrivaltime}) = \sum_{i=1}^{8} k_{i,.arrivaltime} = (0.869 + 1 + 0.449 + 0.190 + 0.313 + 0.067 + 0.313 + 0.313) = 3.514$$

The entropy measure of the risk attribute, arrival time can then be computed using Equation (9.29) as:

$$e(S(A_{arrivaltime})) = -\frac{1}{\ln 8}\sum_{i=1}^{8}\left[\frac{k_{i,arrivaltime}}{S(A_{arrivaltime})}\ln\left(\frac{k_{i,arrivaltime}}{S(A_{arrivaltime})}\right)\right]$$

$$= -\frac{1}{2.079}\times[0.248\times(-1.395)+0.285\times(-1.255)+0.127\times(-2.066)+0.054\times(-2.918)$$
$$+0.089\times(-2.419)+0.019\times(-3.950)+0.089\times(-2.419)+0.089\times(-2.419)]$$

$$= -\frac{1}{2.079}\times(-1.844)$$

$$= 0.887$$

Similarly, the entropy measures of the risk attributes, cost and safety can be separately obtained as*:

$$e(S(A_{cost})) = 0.763$$

$$e(S(A_{safety})) = 0.828$$

---

* The location measures of the attributes, cost and safety are expressed by fuzzy numbers, which are different with the ones of the attribute, arrival time. Thus, the entropy calculation of the risk attribute cost is provided in Appendix 7 for demonstrating its operation with fuzzy numbers.

Using Equation (9.30) to aggregate $e(S(A_{arrivaltime}))$, $e(S(A_{cost}))$ and $e(S(A_{safety}))$ enables the acquirement of the total entropy values across all decision attributes as follows:

$$E = \sum_{j=1}^{3} e(S(A_j)) = 0.887 + 0.763 + 0.828 = 2.478$$

According to Equation (9.31), the context dependent weights of the three attributes can be separately acquired as:

$$w^c_{arrivaltime} = \frac{1 - e(S(A_{arrivaltime}))}{n - E} = \frac{1 - 0.887}{3 - 2.478} = 0.216$$

$$w^c_{cost} = \frac{1 - e(S(A_{cost}))}{n - E} = \frac{1 - 0.763}{3 - 2.478} = 0.454$$

$$w^c_{safety} = \frac{1 - e(S(A_{safety}))}{n - E} = \frac{1 - 0.828}{3 - 2.478} = 0.33$$

Finally, since the prior weights of the risk attributes have been identified as $w_{arrivaltime}$ = 0.5, w_{cost} = 0.25 and w_{safety} = 0.25, the posterior weights can be computed using Equation (9.33) as follows:

$$w^*_{arrivaltime} = \frac{w_{arrivaltime} w^c_{arrivaltime}}{\sum_{r=1}^{3} (w_r w^c_r)} = \frac{0.5 \times 0.216}{0.5 \times 0.216 + 0.25 \times 0.454 + 0.25 \times 0.33} = 0.355$$

$$w^*_{cost} = \frac{w_{cost} w^c_{cost}}{\sum_{r=1}^{3} (w_r w^c_r)} = \frac{0.25 \times 0.454}{0.5 \times 0.216 + 0.25 \times 0.454 + 0.25 \times 0.33} = 0.373$$

$$w^*_{safety} = \frac{w_{safety} w^c_{safety}}{\sum_{r=1}^{3} (w_r w^c_r)} = \frac{0.25 \times 0.33}{0.5 \times 0.216 + 0.25 \times 0.454 + 0.25 \times 0.33} = 0.272$$

Having analysed the three measures (p, l, w) above, one new decision making matrix in the form of Equation (9.10) can be expressed as follows:

$$D = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{array}{c} \begin{array}{ccc} \textit{Arrivaltime} & \textit{Cost} & \textit{Safety} \end{array} \\ \begin{bmatrix} 0.675 & (0.568,0.7,0.934) & (0.396,0.66,0.841) \\ 0.750 & (0.556,0.897,0.928) & (0.375,0.637,0.826) \\ 0.433 & (0.547,0.864,0.923) & (0.353,0.614,0.81) \\ 0.070 & (0.542,0.847,0.921) & (0.342,0.602,0.801) \\ 0 & (0.54,0.841,0.92) & (0.34,0.6,0.8) \\ 0.217 & (0.287,0.487,0.687) & (0.583,0.864,0.961) \\ 0 & (0.28,0.48,0.68) & (0.58,0.86,0.96) \\ 0 & (0.075,0.225,0.45) & (0.11,0.235,0.51) \end{bmatrix} \end{array}$$

where any element u_{ij} has been obtained in the process of computing the posterior weights using Equation (9.9). For example, $u_{1,arrivaltime} = 0.675$ has been obtained above and $u_{1,cost}$ has been calculated to be the set of ((0.568, 0.7, 0.934) in Appendix 7.

From the matrix, $\overline{u}^{+}_{arrivaltime}$; and $\overline{u}^{-}_{arrivaltime}$ can separately be identified as 0.750 and 0. $\widetilde{u}^{+}_{cost}$, $\widetilde{u}^{-}_{cost}$, $\widetilde{u}^{+}_{safety}$ and $\widetilde{u}^{-}_{safety}$ can be calculated as (0.556, 0.897, 0.928), (0.075, 0.225, 0.45), (0.583, 0.864, 0.961) and (0.11, 0.235, 0.51) using Equations (9.13) – (9.16).

Using Equations (9.11) and (9.12), any u_{ij} can be normalised into its counterpart v_{ij}. For example, because cost is a decreasing ordering attribute, $v_{1,cost}$ can be computed as $v_{1,cost} = \frac{\widetilde{u}^{-}_{cost}}{\widetilde{u}_{1,cost}} = \frac{(0.0075,0.225,0.45)}{(0.568,0.7,0.934)} = (0.08,0.321,0.792)$. The matrix can be normalised as:

$$V = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{array}{c} \begin{array}{ccc} \textit{Arrivaltime} & \textit{Cost} & \textit{Safety} \end{array} \\ \begin{bmatrix} 0.9 & (0.08,0.321,0.792) & (0.412,0.764,1.443) \\ 1 & (0.081,0.251,0.809) & (0.39,0.737,1.417) \\ 0.577 & (0.081,0.26,0.823) & (0.367,0.711,1.389) \\ 0.093 & (0.081,0.266,0.83) & (0.356,0.697,1.374) \\ 0 & (0.082,0.268,0.833) & (0.354,0.694,1.372) \\ 0.289 & (0.109,0.462,1.568) & (0.607,1,1.648) \\ 0 & (0.11,0.469,1.607) & (0.604,0.995,1.647) \\ 0 & (0.167,1,6) & (0.114,0.272,0.875) \end{bmatrix} \end{array}$$

Next, $\mathbf{IS}^{P}$ and $\mathbf{IS}^{N}$ are computed using Equations (9.15) – (9.17) as follows:

$$\mathbf{IS}^{P} = [1,(0.167,1,6),(0.607,1,1.648)]$$
$$\mathbf{IS}^{N} = [0,(0.081,0.251,0.809),(0.114,0.272,0.875)]$$

The difference measures between attribute values can be obtained as follows:

$$D^{+}_{ij} = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{array}{c} \begin{array}{ccc} \textit{Arrivaltime} & \textit{Cost} & \textit{Safety} \end{array} \\ \begin{bmatrix} 0.1 & 0.521 & 0.22 \\ 0 & 0.538 & 0.245 \\ 0.423 & 0.53 & 0.27 \\ 0.907 & 0.525 & 0.285 \\ 1 & 0.524 & 0.287 \\ 0.711 & 0.277 & 0 \\ 1 & 0.269 & 0.005 \\ 1 & 0 & 0.831 \end{bmatrix} \end{array}$$

and

$$D_{ij}^{-} = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{array}{c} \begin{array}{ccc} \textit{Arrivaltime} & \textit{Cost} & \textit{Safety} \end{array} \\ \begin{bmatrix} 0.9 & 0.088 & 0.515 \\ 1 & 0 & 0.485 \\ 0.577 & 0.012 & 0.464 \\ 0.093 & 0.02 & 0.45 \\ 0 & 0.022 & 0.447 \\ 0.289 & 0.232 & 0.731 \\ 0 & 0.238 & 0.727 \\ 0 & 0.538 & 0 \end{bmatrix} \end{array}$$

where any element D_{ij} can be calculated using Equations (9.18) – (9.21). For example, $D^{+}_{1,cost} = 1 - \{\sup_x [\mu_{1,cost}(x) \wedge \mu^{+}_{i,cost}(x)]\} = 0.521$, where both $\mu_{1,cost}(x)$ and $\mu^{+}_{i,cost}(x)$ can be represented by their α-cuts as [(0.241α+0.08), (-0.471α+0.792)] and [(0.833α+0.167), (-5α+6)]. Consequently, based on such α-cut representations, the highest degree (α value) of similarity of $\mu_{1,cost}(x)$ and $\mu^{+}_{i,cost}(x)$ is obtained as 0.479.

Having known the posterior weights of the three risk attributes, the separation measures of all *RCOs* can be calculated using Equations (9.22) and (9.23) as follows:

$$S_i^{+} = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{bmatrix} 0.290 \\ 0.267 \\ 0.421 \\ 0.595 \\ 0.629 \\ 0.358 \\ 0.457 \\ 0.581 \end{bmatrix}$$

and

$$S_i^{-} = \begin{array}{c} \\ \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{array} \begin{bmatrix} 0.492 \\ 0.487 \\ 0.336 \\ 0.163 \\ 0.204 \\ 0.388 \\ 0.287 \\ 0.201 \end{bmatrix}$$

Finally, combining S_i^+ and S_i^- enables the calculation of the *RCO* ranking index C_i using Equation (9.24).

$$C_i = \begin{matrix} \#1 \\ \#2 \\ \#3 \\ \#4 \\ \#5 \\ \#6 \\ \#7 \\ \#8 \end{matrix} \begin{bmatrix} 0.629 \\ 0.646 \\ 0.444 \\ 0.215 \\ 0.245 \\ 0.520 \\ 0.386 \\ 0.257 \end{bmatrix}$$

9.4.3 Rank RCOs and Analyse the Results

Compared to all overall performance scores based on the three approaches above, the *RCOs* can be ranked in different orders, as shown in Table 9.6.

Table 9.6. Ranking *RCOs* using various utility combination approaches

Various methods / *Risk control options*	Situation 1 (Independent)		Situation 2 (Dependent)
	Traditional crude approach	***BFRB-ER***	***Fuzzy TOPSIS* and entropy**
RCO#1	***1*** (0.604)	***1*** (0.667)	***2*** (0.629)
RCO#2	***3*** (0.548)	***2*** (0.583)	***1*** (0.646)
RCO#3	***4*** (0.485)	***4*** (0.496)	***4*** (0.444)
RCO#4	***6*** (0.423)	***5*** (0.413)	***8*** (0.215)
RCO#5	***7*** (0.366)	***7*** (0.339)	***7*** (0.245)
RCO#6	***2*** (0.584)	***3*** (0.539)	***3*** (0.520)
RCO#7	***5*** (0.467)	***6*** (0.396)	***5*** (0.386)
RCO#8	***8*** (0.334)	***8*** (0.236)	***6*** (0.257)

In Situation 1, the results obtained for the *RCO* ranking using the *BFRB-ER* approaches are collated with the results obtained from the traditional crude *MADM* approach. From the table, using the traditional approach, the second best option is that trains depart on Tuesday (*RCO*#6) and the option that trains depart on Thursday (*RCO*#7) is better than the option that container trucks depart on Thursday (*RCO*#4). However, such conclusions are based on the subjective point estimation of location measures. Compared to point estimation, the fuzzy linguistic description to location measures can be more reliable and accurate in terms of subjective judgement. Using the *BFRB-ER* methods, it can be obtained that the second best option is *RCO*#2, *RCO*#4 is better than *RCO*#7. Based on the same departure time, container trucks have priority over trains and feeders from an overall decision making viewpoint.

In Situation 2, the effects of the dependent relationships established between decision attributes and the weighting coefficient introduced by the entropy calculation can be clearly seen in the results obtained. The ranking ordering of *RCOs* #1, #2, #4, #7 and #8 has been changed. An interesting phenomenon is that the ranks of the train and feeder related *RCOs* move forward. The entropy modification reduces the relative importance of the decision attribute, arrival time and increases the one of the cost and safety. This has shown that container trucks have more advantage with regard to the arrival time, while the trains and feeders have priority on the cost and safety. Additionally, it is noteworthy that the rank of *RCO*#2 is higher than the one of *RCO*#1. The main reason is that compared to *RCO*#2, *RCO*#1 has less preference in terms of arrival time in this case. Furthermore, it is for the first time that *RCOs* #4, #5 and #8 are ranked in such an order as *RCO*#8>*RCO*#5>*RCO*#4. This can be explained as that since the containers cannot arrive on time no matter which *RCO* is chosen from them, decision makers can only select the cheapest and safest way to deliver in order to catch the next mother ship available.

9.5. Conclusion

BNs enable risk diagnosis and prediction to be made using its sound uncertainty inference foundation. However, they cannot be allowable to involve multiple attributes and fuzzy uncertainty expressions (the possibilistic concept), which are extremely important to make wider risk based decisions. This chapter therefore develops a novel methodology by synthesising *BNs*, *MAUT* and fuzzy logic to provide a complete solution for *MADM* under uncertainty. The framework consists of two components: the combination of *BNs* and *MADM* and the generation of novel fuzzy utility representations.

The advantages (contributions) of such a methodology focus on the following:

- Extending traditional decision making measures from utility and weight to probabilistic, location and weight measures, which are suitable to modelling uncertainties, either fuzziness or randomness.
- Using the *BN* mechanism to infer a probabilistic measure in order to model randomness.
- Using linguistic variables based on fuzzy logic to more accurately describe location measures.
- Using the entropy theory to incorporate dependent weights measures with prior weights and obtain the modified posterior weight measures.
- Using the *BFRB-ER* approach to unify Bayesian output with fuzzy logic reasoning.
- Using the fuzzy *TOPSIS* technique to avoid the conflicts resulting from crisp and fuzzy location measures and solve the attribute dependence problem.
- Using the combination of the *Hugin* and *IDS* software to realise real time decision making under dynamic conditions.

Apart from such strengths, such a methodology shows some disadvantages, which need to be further considered in the future work. In risk assessment and management, the occurrence of any disaster requires the experience of certain pathways from incidents to accidents. Correspondingly, an effective *RCO* usually includes several sequential control measurement elements. When a hazardous event evolves into an accident like a chain, the control measurements are distributed in an order: if the first action does not work properly, then the following ones can be activated. Clearly, the methodology is not suitable for modelling sequential decision making problems. A modified *ID* may show potentials in dealing with such time sequent problems. Furthermore, more studies such as treating different local utility functions and developing an effective additive algorithm for the application of the *MEU* theory require further research. Another important consideration is the creation of an adapted computing support tool for the fuzzy *TOPSIS* approach using computing languages, which can be combined with *Hugin* and *IDS* and help the implement of real-time decision making with dependent attributes.

Chapter 10 – Conclusions and Future Research

SUMMARY

This chapter briefly summarises that the risk assessment and decision making approaches and techniques in all previous chapters would be of benefit in CSC safety design, operation and management. The areas, which require more effort to be paid for the improvement of the developed approaches, are outlined.

10.1 Research Contribution

Containerisation is a necessary trend in the global trade and international transportation. *CSCs* are playing an increasingly important role in the process of facilitating economic development. The optimal performance of the chains requires multiple 'success' factors to be considered. One of them is safety, which becomes particularly important in the post 9-11 era. However, the findings from the literature review have revealed that there are few conceptual risk assessment methodologies available in *CSC* systems and the risk assessment of the systems is closely associated with a high level of uncertainty and dependency. Thus, the previous chapters of this thesis have described a modified *FSA* framework in *CSC* safety design, operation and management and also a range of risk assessment and risk based decision making approaches. The framework has been developed in a generic sense to be applicable to deal with both engineering and managerial problems. It provides the basis for the generation of the various risk analysis methods and decision making procedures. In summary, these methods and techniques can be concluded as follows:

1) Combining the fuzzy set and *ER* approaches to analyse the threat-based risks, in which safety data is insufficient, incomplete or unavailable (Chapter 3).
2) Using a novel fuzzy continuous set technique to synthesise the hazard-based and threat-based risk estimations (Chapter 4).
3) Applying the *FRB* and *ER* approaches to incorporate more risk parameters into risk calculation and estimations (Chapter 5).
4) Using the *FER* method to justify the belief degree distributions in fuzzy rule bases (Chapter 6).
5) Generating a *BN*-based risk analysis model to deal with the dependent relationships between risk variables (Chapter 7).
6) Creating a novel "*Noisier or*" approach to enable more reasonable subjective probability distributions in the *BN*-based risk model (Chapter 8).
7) Producing a *BN-MAUT* risk based decision making technique to model multiple uncertain attributes in the process of *RCO* selection (Chapter 9).

Obviously, all the approaches and methods proposed in this thesis are developed on the basis of certain application (conditional) situations, which means that one has no absolute superiority than the others. For example, for only dealing with hierarchical threat-based risk analysis, Method 1 may be the most appropriate and for prioritising the interactive risk parameters with sufficient safety data, it will be desirable to use Method 5.

Additionally, it is particularly noteworthy that the combination of some methods can produce more powerful supporting tools in *CSC* risk assessment and decision making and obtain more appropriate recommendations. For example, the combination of Methods 5 and 6 enables the delivery of a new *BN*-based risk analysis framework and can be used to rank the priority of risk parameters from a new perspective using the concept of *SA*. Furthermore, the comparison between Methods 3 and 5 and discussion of their individual strengths and weaknesses can demonstrate that any safety model does not have the exclusive advantages to describe risks. Of course, such a comparison can also help improve the assessors' confidence in terms of obtaining accurate analysis results. For example, the two methods have been simultaneously applied to assess the risk related to a terrorism threat against port and obtain a consistent result.

Based on these methods, the major research contributions focus on both academic and practical aspects. The challenges to appropriately assess *CSC* risks are associated with uncertainty. The fuzzy logic and Bayesian probability inferences are two major uncertainty reasoning theories. Because of their flexibility and prediction capabilities, both fuzzy logic and *BNs* have shown much potential in the field of risk assessment including broad risk analysis, risk prediction and risk based decision making. The various methods developed on the basis of the two theories can be considered as the contribution to the absence of the literature of risk and reliability studies in the context of *CSCs* and the transference of the knowledge of uncertainty treatment to the area of risk assessment. Although in certain cases, it could be time consuming to conduct risk analysis of *CSCs* using some of the described methods, it is believed that the methods possess enormous potential as valuable aids and effective alternatives to assist the *CSC* managers in developing continuity safety planning and will gain increased usage in *CSC* operation and management. It is also believed that these methods can be tailored to the practical applications of dealing with the safety problems in the other industries, especially in situations where a high level of uncertainty exists. The implementation of the described approaches could have a highly beneficial effect in real life. More specific description can be provided as follows:

- The *FSA* methodology for *CSCs* provides new insights that should be of particular interest to practitioners and academics. The use of the fuzzy set and *ER* methods in

Chapter 3 can effectively help carry out the safety assessment of *CSCs* particularly in those situations where *QRA* is not applicable due to incomplete data. The fuzzy set approach employs fuzzy membership functions to model the uncertainty from subjective discrete estimation. Additionally, the application of *FTA* as a hierarchical diagram and the consideration of a new measure parameter "*Recall difficulty*" in fuzzy safety analysis are unique and innovative.

- It is desirable to identify the vulnerability in the chains from two different views of threats and hazards in Section 3.3.2. In the use of traditional hazard identification techniques, it is very difficult to satisfy the requirements of the threat-based risk assessment. Furthermore, these threat-based risks widely exist and attract more attention from the managers of the chains. Therefore, the definition of vulnerability can provide more effective help to carry out the chains' risk assessment from a practical viewpoint. An interesting insight is that although the vulnerability nature is not necessarily connected with its origin, they certainly have close relationships: most hazard-based risks in the chains originate from the internal vulnerability and those threat-based risks are more associated with the external factors of the chains.

- Although the *FRB* method has been well established in the risk assessment context, its applications in analysing threat-based risks, especially with the consideration of belief degrees in the conclusion part of rules, are relatively new. Furthermore, in order to make fuzzy output more logical and sensitive to its fuzzy input, a reasonable belief degree distribution algorithm generated in Chapter 6 on the basis of the combination of a fuzzy set mapping technique and the *ER* approach is desirable.

- There is a common concern in the research associated with *BNs* that some subjective probabilities used, mostly due to unavailable historical data, result in academic bias. A *BFRB* method may be well suited to dealing with subjective guess or judgements. However, based on fuzzy logic theory, the method usually provides possibilistic output, which is incompatible with *BNs*. Therefore, it is beneficial to transform the fuzzy possibilistic output into the Bayesian probabilistic mode in Chapter 7 using the novel state categories "Soundness" and "Weakness" in order to produce more powerful risk based uncertainty treatment and decision making tools.

- In modelling realistic safety scenarios using *BNs*, the converging connections are more popular than diverging and serial connections. This point can be supported by many widely used hierarchical risk analysis approaches such as *FTA*. Thus, some Bayesian modelling techniques are developed to try to implement reasonable estimations of conditional probability distributions given multiple parents, such as the "*Noisy or*" and "divorcing" techniques. Unfortunately, such methods have many

constraints in dealing with the conditional probability combination of multi-state parents. A novel "*Noisier or*" technique has been developed in Chapter 8 to have the capability of dealing with such a problem with less limitations and enabled the wider applications of *BNs* in a generic risk mode.

- A new way of thinking about risk ranking is introduced in Section 8.4. In either engineering or managerial systems, whose subsystems and components have interactive relationships, considering the effect values of individual risk variables as the criterion of prioritising their importance may be inaccurate and incomplete. A *SA* analysis in *BNs* is introduced to investigate the combined influences of the multiple attributes thus providing a more systematical analysis from an overall perspective.

- *BNs* cannot be allowed to incorporate the notation of preference and thus fail to involve multiple decision attributes, which are extremely important to make wider risk based decisions. *MAUT* is incorporated to implement *BN*-based *MADM* by developing an innovative model with three parameters, probability, location and weight measures in Chapter 9. The three parameters extended from the traditional decision making measures, utility and weight are more suitable to modelling uncertainties from the dependent decision attributes in the networks. The incorporation of *MAUT* into *BNs* on the basis of some well-established techniques such as fuzzy logic, *ER*, *TOPSIS* and entropy calculations can deliver a holistic solution for *MADM* with uncertainty. The utilisation of a fuzzy logic approach in the solution may also give a reference to investigate new development directions for the combination of the fuzzy possibilistic and Bayesian probabilistic theories.

10.2 Limitations of Research and Future Research

Although the research attempts to provide a comprehensive analysis related to the risk assessment and decision making of *CSCs*, due to the time and column constraints, the current study does not refer more problem analyses, which may be necessary and desirable in further investigation. They can be identified as:

1) It would be useful if some *QRA* with objective data from realistic risk scenarios could be incorporated, especially in further validating the feasibility of the *BN* based risk model.
2) It would be useful if more test cases are applied to the described risk assessment and decision making approaches in order to further demonstrate their applicability.
3) It would be useful if more powerful and flexible risk modelling and decision making tools based on uncertainty treatment methods are developed to facilitate the modified *FSA* methodology in *CSCs*.

4) It would be useful if more computing software can be developed to simulate the calculation process of the described approaches and realise the smooth communications from risk input to output.

Aiming at dealing with the limitations displayed above, the current research can be extended in the following directions:

- Collision has been identified as one of the most dangerous risk categories in containership navigation. Such a hazard may become more worrisome when it is combined with the 'frequent' occurrence of human error on the bridge. The emergence of mistakes or wrong behaviours results from multiple factors such as complex sea environment, dynamic containership meeting situations and the physical and mental status of navigators, etc. Currently anti-collision measures are usually adopted on the basis of navigation regulations and navigators' experience. Since it is highly possible to take the wrong anti-collision measures when containerships meet, it will be beneficial if a risk prediction/*RCO* optimisation model is designed using the methodology in Chapter 7. This will simulate the ship route situations and provide a reasonable anti-collision suggestion. Such a model can be developed into a real-time anti-collision control-supporting tool on the basis of the *Hugin* software. When all evidence related to collision is identified as input to the tool, it can produce an optimal decision making option as a reference for navigators to take suitable anti-collision measures and then, reduce the occurrence likelihood of human error. Such a model can be first designed in a limited sea area, such as a channel or port and then extended or popularised to a wider domain according to a specific requirement. The corresponding data in a limited area can be effectively collected or mined using both historical data and simulators. Furthermore, such a real case study can facilitate the applications of the approaches introduced in this thesis.

- The traditional *FRB* risk assessment technique has been widely applied due to the capability of combining different parameters to obtain an overall risk estimation. However, a drawback occurs as the technique is applied in circumstances where there are multiple parameters to be evaluated, which are described by multiple linguistic terms. This will easily lead to the requirement of constructing an extensive rule base and the occurrence of intensive computing. Therefore, a risk prediction model incorporating *FST* and Artificial Neural Network (*ANN*) capable of resolving the problem encountered may be proposed to simplify the *FRB* related construction and calculations in risk assessment. It is believed that the model can provide reliable risk prediction results when relatively comprehensive training data is provided to cover the potential situations that future risk assessment may confront as much as possibly.

- *BNs* can be well used to predict consequences of a hazard and diagnose its causes based on observable safety evidence. This is an important development as it helps to quantify the uncertainties, infer the interactive dependencies of risk factors and support safety based decisions in the process of risk assessment. However, the conventional *BNs* established in the field of safety/reliability are usually based on the assumption that the probabilities, which enter into their assessments, are known as real numbers. In many realistic settings like *CSCs*, where risks often result from threats, this assumption is of questionable validity since the failure data from which the probabilities must be estimated is usually incomplete, imprecise or not totally reliable. Due to the lack of historical or experimental data, prior input into *BNs* often relies on subjective probabilities based on expert judgements. However, such subjective probabilities are based on informed guesses from experts with various backgrounds and epistemologies. Thus, it will be very difficult to give a same degree-of-belief interpretation with precise numbers for different experts facing a certain problem. To address this issue, a novel *FBN* modelling method, which allows the expression of subjective probabilities as fuzzy numbers through combing fuzzy logic and Bayesian probability theories may be worth being further investigated. The new method is believed to be able to more faithfully reflect expert opinion so as to effectively facilitate the application of *BNs* in the context of risk assessment of *CSCs*.

- The risk assessment of complex *CSC* systems is a process that synthesises many risk analyses of subsystems and components. Such a process unavoidably has a hierarchical feature. Thus, the combination of hierarchical graphs and *BNs*, namely hierarchical *BNs* (*HBNs*) may be developed through extending the conventional *BN* methodology. It can be hoped to provide an expressive power by allowing a node in the network to represent an individual *BN*. *HBNs* can describe the knowledge in a structured way, leading to more realistic probabilistic models. Furthermore, The analysis in Section 1.4 has pointed out that the *CSC* systems have time-related dependency, which means that potential models should discretize the time line and associate a *RV* (node) to each time interval (point). Thus, a Temporal *BN* (*TBN*) may be obtained by generating a *BN* for a specific time and repeating the same structure for each time over the period of interest. Early work on the *TBNs*, Dynamic *BNs* (*DBNs*), Modifiable Temporal *BNs* (*MTBNs*), Temporal Node *BNs* (*TNBNs*) and Net of Irreversible Events in Discrete Time (*NIEDT*) can provide sound literature and the development basis of this new proposal.

- Future work may also be able to extend *BNs* to *IDs* and further allow analysis and validation of the networks' ability to predict the most effective *CSC* risk management solutions. The use of *IDs* in *BNs* may be demonstrated, together with

the comparison with the *CBA* and decision-making techniques employed in *FSA*. It may not need to detail a finer quantitative comparison, but rather validates the hypothesis that *BNs* and their practical implications may become a better decision making tool in the application of *FSA* from a dynamic and feasible risk assessment perspective. As a result, the optimisation of safety based decision making by incorporating *ID* techniques into the generated *BNs* is expected to realise and sequentially an opportunity to harmonize *BNs* with the methodology of *FSA* may be obtained. Furthermore, in risk assessment and management, the occurrence of any disaster requires the experience of certain pathways from incidents to accidents. Correspondingly, an effective *RCO* usually includes several sequential control measurement elements. A modified *ID* shows potentials in and is also believed to have ability to contribute itself to dealing with such dynamic time sequent problems.

- Final but not least consideration may be associated with the development or adoptions of some computing support tools using computing languages. Many methods and techniques developed in this thesis require the support of a variety of software packages. For example, a new computing programme edited to simulate the algorithms of the fuzzy *TOPSIS* approach in Chapter 9 can be combined with *Hugin* and *IDS* and help to realise real-time decision making/*RCO* selection with dependent decision attributes. A new software tool may be explored on the basis of the *FRB-ER* approach in Chapter 5 and provide a friendly and easily used interface for many assessors to automatically obtain risk output, either in a probabilistic or possibilistic mode, when input related to the risk parameters in the antecedent part is provided.

References:

An, M., Wang, J. and Ruxton, T. (2000), "The Development of Fuzzy Linguistic Risk Levels for Risk Analysis of Offshore Engineering Products Using Approximate Reasoning Approach", *19th International Conference on Offshore Mechanics and Arctic Engineering*, Feb. 14-17, USA.

Andersen, D.R., Sweeney, D.J. and Williams, T.A. (2003), *An Introduction to Management Science: Quantitative Approaches to Decision Making*, South-Western, Ohio, USA.

Andersen, R.D. and Lenz, R.T. (2001), "Modelling the Impact of Organizational Change: A Bayesian Network Approach", *Organizational Research Methods,* Vol. 4, No. 2, pp. 112-130.

Andersen, S.K., Olesen, K.G., Jensen, F.V. and Jensen, F. (1990), "Hugin – A Shell for Building Belief Universes for Expert Systems", *Reading in Uncertainty*, Shafer, G. and Pearl, J. (eds.), Morgan Kaufmann, pp. 332-337.

Andreassen, S., Jensen, F.V., Andersen, S.K., Falck, B., Kjæul ff, U., Woldbye, M., Sœnsen, A., Rosenfalck, A. and Jens en, F. (1989), "MUNIN – An Expert EMG Assistant", *Computer-aided Electromyography and Expert Systems,* Desmedt, J.E. (eds.), Elsevier Science Publishers, Amsterdam, pp. 255-277.

Andrews, J.D. and Moss, T.R. (2002), *Reliability and Risk Assessment*, Professional Engineering Publishing Ltd, London and Bury St Edmunds, UK.

Ang, A.H.S. and Tang, W.H. (1984), *Probability Concepts in Engineering Planning and Design*, John Wiley &Sons, UK.

Apostolakis, G., Farmer, F.R. and van-Otterloo, R.W. (1988), "The Interpretation of Probability in Probability Safety Assessments", *Reliability Engineering & System Safety*, Vol. 23, pp. 247-252.

Aven, T. and Kristensen, V. (2005), "Perspectives on Risk: Review and Discussion of the Basis for Establishing a Unified and Holistic Approach", *Reliability Engineering & System Safety*, Vol. 90, No. 1, pp. 1-14.

Ballou, R.H. (1987), *Basic Business Logistics*, Prentice-Hall International, Englewood Cliffs, NJ, USA.

Bangash, Y. (1983), "Containment Vessel Design and Practice", *Progress-in-Nuclear-Energy*, Vol. 11, No. 2, pp. 107-181.

Barker, G.C., Talbot, N.L.C. and Peck, M.W. (2002), "Risk Assessment for Clostridium Botulinum: A Network Approach", *International Biodeterioration & Biodegradation,* Vol. 50, pp. 167-175.

Basili, V.R. and Rombach, H.D. (1988), "The TAME Project: towards Improvement-Oriented Software Environments", *IEEE Transaction on Software Engineering*, Vol. 14, No. 6, pp. 758-773.

Bell, P.M. and Badiru, A.B. (1996), "Fuzzy Modelling and Analytic Hierarchy Processing to Quantify Risk Levels Associated with Occupational Injures – Part I: The Development of Fuzzy-Linguistic Risk Levels, *IEEE Transactions on Fuzzy Systems,* Vol. 4, No. 2, pp. 124-131.

Ben-Daya, M. and Raouf, A. (1993), "A Revised Failure Mode and Effects Analysis Model", *International Journal of Quality and Reliability Management*, Vol. 3, No. 1, pp. 43-47.

Bendixen, L.M., O'Neil, J.K. and Little, A.D. (1984), "Chemical Plant Risk Assessment Using HAØP and Fault Tree Methods", *Plant/Operations Progress*, Vol. 3, No. 3, pp. 179-184.

Beynon, M., Curry, B. and Morgan, P. (2000), "The Dempster-Shafer Theory of Evidence: An Alternative Approach to Multicriteria Decision Modelling", *OMEGA-International Journal of Management Science*, Vol. 28, pp. 37-50.

Bobbio, A., Portinale, L., Minichino, M. and Ciancamerla, E. (2001), "Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks", *Reliability Engineering & System Safety,* Vol. 71, No. 3, pp. 249-260.

Bojadziev, G. and Bojadziev, M. (1995), *Fuzzy Sets, Fuzzy Logic, Application*, World Scientific, Singapore.

Bordogna, G., Fedrizzi, M. and Pasi, G. (1997), "A Linguistic Modelling of Consensus in Group Decision Making Based on OWA Operators", *IEEE - Systems, Man and Cybernetics*, Vol. 27, pp. 126-132.

Bortolan, G. and Degani, R. (1985), "A Review of Some Methods for Ranking Fuzzy Subsets", *Fuzzy sets and Systems*, Vol. 15, pp. 1-19.

Boudali, H. and Dugan, J.B. (2005), "A Discrete-time Bayesian Network Reliability Modelling and Analysis Framework", *Reliability Engineering & System Safety*, Vol. 87, pp. 337-349.

Bouissou, M. and Bon, J.L. (2003), "A New Formalism that Combines Advantages of Fault-Trees and Markov Models: Boolean Logic Driven Markov Process", *Reliability Engineering & System Safety*, Vol. 82, No. 2, pp. 149-163.

Bowles, J.B. and Pelaez, C.E. (1995), "Fuzzy Logic Prioritisation of Failures in a System Failure Mode, Effects and Criticality Analysis", *Reliability Engineering and System Safety*, Vol. 50, pp. 203-213.

Bruk, I.V. and El'Yanov, V.D. (1975), "Performance Study of Loose-linked Automatic Lines", *Machines and Tolling*, Vol. 46, No. 4, pp. 50-53.

BS 4778 (1986), *Glossary of Terms Used in Quality Assurance*, BSI Handbook 22, British Standards Institution, UK.

Buchanan, B.G. and Shortliffe, E.H. (1984), *Rule-Based Expert Systems*, Addison-Wesley, Reading, USA.

Buckley, J.J. and Eslami, E. (2002), *An Introduction to Fuzzy Logic and Fuzzy Sets*, Physica-Verlag, Heidelberg, NY, USA.

Burnell, L. and Horvitz, E. (1995), "Structure and Chance: Melding Logic and Probability for Software Debugging", *Communications of the ACM*, Vol. 38, No. 3, pp. 31-41.

Burns, H.T., Cordire, P. and Eriksson, T. (2003), *Security Risk Assessment and Control*, Perpetuity Press Ltd., Leicester, UK.

Cagno, E., Caron, M., Mancini, M. and Ruggeri, F. (2000), "Using AHP in Determining the Prior Distributions on Gas Pipeline Failures in a Robust Bayesian Approach", *Reliability Engineering & System Safety,* Vol. 67, No. 3, pp. 275-284.

Carr, C.H. and Truesdale, T.A. (1992), "Lessons from Nissan's British Suppliers", *International Journal of Operations and Production Management*, Vol. 12, No. 2, pp. 49-57.

Cavinato, J.L. (1992), "A Total Cost/value Model for Supply Chain Competitiveness", *Journal of Business Logistics,* Vol. 13, No. 2, pp. 285-301.

Chadwin, M.L., Pope, J.A. and Talley, W.K. (1999), *Ocean Container Transportation, an Operation Perspective*, Taylor &rancis, NY, USA.

Chapman, P., Christopher, M., Jüttner, U., Peck, H. and Wilding, R. (2002), "Identifying and Managing Supply-Chain Vulnerability", *Logistics & Transport Focus*, Vol. 4, No. 4, pp. 17.

Charniak, E. (1991), "Bayesian Networks without Tears", *Artificial Intelligence Magazine*, Vol. 12, No. 4, pp. 55-63.

Chen, C.B. and Klien, C.M. (1997), "A Simple Approach to Ranking a Group of Aggregated Fuzzy Utilities," *IEEE Transactions on System, Man, Cybernetics - Part B: Cybernetics,* Vol. 27, No. 1, pp. 26-35.

Chen, C.T. (2001), "Fuzzy Approach to Select the Location of the Distribution Center", *Fuzzy Sets and Systems*, Vol. 118, No. 1, pp. 65-73.

Chen, S.J. and Hwang, C.L. (1992), *Fuzzy Multiple Attribute Decision making,* Springer, Berlin, Germany.

Cheng, C.H. and Lin, Y. (2002), "Evaluating the Best Main Battle Tank Using Fuzzy Decision Theory with Linguistic Criteria Evaluation", *European Journal Operational Research*, Vol. 142, pp. 174-186.

Cheng, T.C.E. (1990), "A State-of-the-art Review of Just-in-time Production", *Advanced Manufacturing Engineering*, Vol. 2, No. 2, pp. 90-102.

Cheng, S.J. and Huang, C.L. (1992), *Fuzzy Multiple Attribute Decision-Making: Methods and Applications*, Springer-Verlag, Berlin, Germany.

Chicken, J.C. and Posner, T. (1998), *The Philosophy of Risk*, Thomas Telford Publishing, London, UK.

Chong, H.G. and Walley, W.J. (1996), "Rule-based Versus Probabilities Approaches to the Diagnosis of Faults in Wastewater Treatment Processes", *Artificial Intelligence in Engineering*, Vol. 1, pp. 265-273.

Christopher, K. (2005), " Coalition for Secure Ports: Container Cargo Secure", *Annual Spring Conference of American Association of Port Authorities*, April 5, Washington D.C., USA, available at (Dec. 5, 2006), (*http://www.secureports.org/speeches/chris_koch_aapa_040505.html*).

Christopher, M. and Lee, H. (2004), "Mitigating Supply Chain Risk through Improved Confidence", *International Journal of Physical Distribution and Logistics Management,* Vol. 34, No. 5, pp. 388-398.

CLSCM (2003), *Creating Resilience Supply Chains: A Practical Guide*, Cranfield University Press, Bedford, UK.

Coyle, J.J., Bardi, E.J. and Langley, C.J. (1996), *The Management of Business Logistics*, West Publishing Company, MN, USA.

Cutter, S.L. (1996), "Vulnerability to Environmental Hazards", *Progress in Human*

Geography, Vol. 20, pp. 529-539.

Darbra, R.M. and Casal, J. (2004), "Historical Analysis of Accidents in Seaports", *Safety Science*, Vol. 42, pp. 85-98.

Das, B. (2000), "Representing Uncertainties Using Bayesian Networks", *Technical Report, DSTO-TR-0918,* Defence Science &T echnology Organisation Electronics and Surveillance Research Laboratory, Salisbury, Australia.

Dempster, A.P. (1967), "Upper and Lower Probabilities Induced by a Multivalued Mapping", *Annals of Mathematical Statistics*, Vol. 38, pp. 325-339.

Dempster, A.P. (1968), "A Generation of Bayesian Inference", *Journal of the Royal Statistical Society-Serire B*, Vol. 13, pp. 205-247.

De Jager, P. and Bergeon, R. (1997), *Managing '00: Surviving the Year 2000 Computing Crisis*, John Wiley &Sons, NY, USA.

De Korvin, A. and Shipley, M.F. (1993), "A Dempster-Shafer Based Approach to Compromise Decision Making with Multiattributes Applied to Product Selection", *IEEE Transactions on Engineering Management*, Vol. 40, No. 1, pp. 60-67.

Denoex, T. (1999), "Reasoning with Imprecise Belief Structures", *International Journal of Approximate Reasoning*, Vol. 20, pp. 79-111.

Deshpande, A.W. (1999), "Application of Fuzzy Set Theory to Environmental Engineering Systems", *BISC Seminar*, Oct. 7, National Environmental Engineering Research Institute (NEERI), India.

De Souza, S.E. and Ocha, P.M. (1992), "State Space Exploration in Markov Models", *ACM SIGMETRICS Performance Evaluation Review,* Vol. 20, No. 1, pp. 152.

Diehl, M. and Haimes, Y.Y. (2004), "Influence Diagrams with Multiple Objectives and Tradeoff Analysis", *IEEE Transactions on Systems Man and Cybernetics Part A – Systems and Humans*, Vol. 34, No. 3, pp. 293-304.

Dixon P., (1964), "Decision Tables and Their Applications", *Computer and Automation*, Vol. 13, No. 4, pp. 376-386.

DNV (2000), "Scoping Study for a Formal Safety Assessment of Ballast Water Management", for Maritime and Coastguard Agency (MCA), *Det Norske Veritas (DNV) Job No. C305018, Revision 1.*

Drucker, P.F. (1990), "The Emerging Theory of Manufacturing", *Harvard Business Review*, Vol. 68, No. 3, pp. 94-102.

Dubois, D. and Prade, H. (1987), Mean Value of a Fuzzy Num ber," *Fuzzy Sets and Systems*, Vol. 24, No. 3, pp. 279-300.

Duckstein, L. (1994), "Elements of Fuzzy Set Analysis and Fuzzy Risk", *Decision Support Systems in Water Resources Management*, Nachtnebel, H.P. (eds.), UNESCO press, Paris, France.

Edwards, W. (1954), "The Theory of Decision Making", *Psychological Bulletin*, Vol. 50, pp. 380-417.

Edwards, W. (1961), "Behavioral Decision Theory", *Annual Review of Psychology*, Vol. 12, pp. 473-498.

Edwards, W. and Newman, J.R. (1982), *Multiattribute Evaluation*, (*Pager series on*

Quantitative Application in the Social Sciences, 07-026), Sage University, London, UK.

Erkut, E and Verter, V. (1998), "Modeling of Transport Risk for Hazardous Materials", *Operations Research*, Vol. 46, No. 5, pp. 625-642.

Evans, J.R. (1993), *Applied Production and Operations Management*, West Publishing Company, MN, USA.

EU (2003), "Fight against Terrorism: Security of European Maritime Transport to be Strengthened", *European Commission Press Release-IP/03/651*, Brussels, Belgium.

Faber, M.H., Kroon, I.B., Kragh, E., Bayly, D.B. and Decosemaeker, P. (2001), "Risk Assessment of Decommissioning Options Using Bayesian Networks", *20th Offshore Mechanics and Arctic Engineering Conference,* June 3-8, Rio de Janeiro, Brazil.

Fairplay (2004), *Ports and Terminals Guide 2003-2004*, Fairplay Publication Ltd., London, UK.

Felsted, A. and Odell, M. (2002), "Agencies Fear Extent of Al-Qaeda's Sea Network", *Finance Time Special Report*, available at (Dec. 5, 2006), (*http://specials.ft.com/attackonterrorism/FT3U47PPYXC.html*).

Fenton, N. and Neil, M. (2001), "Making Decisions: Using Bayesian Nets and MCDA", *Knowledge-Based Systems*, Vol.14, pp. 307-325.

Fishburn, P.C. (1968), "Utility Theory", *Management Science*, Vol. 14, pp. 335-378.

Fishburn, P.C. (1991), "Nontransitive Preferences in Decision Theory", *Journal of Risk and Uncertainty*, Vol. 4, pp.113-134.

Frankel, E.G. (1988), *Systems Reliability and Risk Analysis*, Kluwer Academic Publishers, NY, USA.

Friedman, F. and Savage, L. (1952), "The Expected-Utility Hypothesis and The Measurability of Utility", *Journal of Political Economy*, Vol. 60, pp. 463-474.

Friis-Hansen, A. (2001), "Bayesian Networks as a Decision Support Tool in Marine Application", *PhD Thesis,* Technical University of Denmark, Lyngby, Denmark.

FSI of IMO (1999-2002), "Casualty Statistics and Investigations", *IMO FSI Circles*, FSI 3/Circ. 1-3, London, UK.

Fullwood, R.R. (2000), *Probabilistic Safety Assessment in Chemistry and Nuclear Industries*, Butterworth-Heinemann Publishers, Woburn, MA, USA.

Ganesan, S. (1994), "Determinants of Long-term Orientation in Buyer-seller Relationships'', *Journal of Marketing*, Vol. 58, No. 2, pp. 1-19.

Garg, D., Narahari, Y. and Viswanadham, N. (2003), "Design of Six Sigma Supply Chains", *Proceedings - IEEE International Conference on Robotics and Automation*, pp. 1737-1742.

Garrick, B.J., Hall, J.E., Kilger, M., McDonald, J.C., O'Toole, T., Probst, P.S., Parker, E.R., Rosenthal, R., Trivelpiece, A.W., Arsdale, L.A. and Zbroski, E .L. (2005), "Confronting the Risks of Terrorism: Making the Right Decisions", *Reliability Engineering & System Safety*, Vol. 86, No. 2, pp. 129-176.

Garrote, L., Molina, M. and Blasco, G. (2003), "Application of Bayesian Networks to Real-time Flood Risk Estimation", *Geophysical Research Abstracts*, Vol. 5, pp. 13171.

Gerssen, S. (2004), "Bayesian Networks in Credit Rating", *Master Thesis*, Faculty of Information Technology and Systems, Delft University of Technology, Netherlands.

Gilchrist, W. (1993), "Modelling Failure Modes and Effects Analysis", *International Journal of Quality and Reliability Management,* Vol. 10, No. 5, pp. 16-23.

Groen, F.J. and Mosleh, A. (2001), *Principles of Uncertain Evidence in the Context of a Failure Rate Assessment Problem*, University of Maryland, MD, USA.

Golter, J. and Hawryl, P. (1998), "Circle of Risk", available at (Jun 29, 1998), (*http://www.year2000.com/achieve/Nfcirclesrisk.html*).

Ha, J.S. and Seong, P.H. (2004), "A Method for Risk-informed Safety Significance Categorization Using the Analytic Hierarchy Process and Bayesian Belief Networks", *Reliability Engineering & System Safety,* Vol. 83, No. 1, pp. 1-15.

Halebsky, M. (1989), "System Safety Analysis Techniques as Applied to Ship Design," *Marine Technology*, Vol. 26, No. 3, pp. 245-251.

Halliwell, J. and Shen, Q. (2002), "Towards a Linguistic Probability Theory", *Proceedings of the 11th International Conference on Fuzzy Sets and Systems* (*FUZZ-IEEE '02*), May 12-17, HI, USA, Vol. 1, pp. 596-601.

Halliwell, J., Keppens, J. and Shen, Q. (2003), "Linguistic Bayesian Networks for Reasoning with Subjective Probabilities in Forensic Statistics", *Proceedings of the 9th International Conference on Artificial and Intelligence and Law*, June 24-28, Edinburgh, UK.

Hammarkvist, K.O., Håkansson and H., Mattsson, L.G. (1982), *Marknadsföring för konkurrenskraft*, IVA, MTC och Liber Förlag, Stockholm .

Hammer, H. (1992), "The Economics of Flexible Manufacturing Systems Contingent upon Operating and Service Personnel", *European Production Engineering*, Vol. 16, No. 3, pp. 38-41.

Harris, R. (1998), *Introduce to Decision Making*, available at (Dec 5, 2006), (*http://www.virtualsalt.com/crebook5.htm*).

Hay, E.J. (1987), "Any Machine Setup Time Can Be Reduced by 75 Per cent", *Industrial Engineering*, August, pp. 62-66.

Hayes, K.R. (1998), "Bayesian Statistical Inference in Ecological Risk Assessment", *Technical Report No.17,* Centre for Research on Introduced Marine Pests, Australia.

He, A.Y., Han, Y.Q., Wang, H.W. and Mei, Q. (2002), "Using Bayesian Belief Networks to Evaluate Credit Guarantee Risk", *1st International Conference on Machine Learning and Cybernetics*, Nov. 4-5, Beijing, China.

Heckerman, D., Mamdani, E.H., and Wellman, M. (1995), "Real-World Applications of Bayesian Networks", *Communications of ACM,* Vol. 38, No. 3, pp. 24-26.

Henley, E.J. and Kumamoto, H. (1992), *Probabilistic Risk Assessment*, IEEE Press, NY, USA.

Henrion, M., Breese, J.S. and Horvitz, E.J. (1991), "Decision Analysis and Expert Systems", *Artificial Intelligence Magazine*, Vol. 12, No. 4, pp. 64-91.

Holicky, M. and Schleich, J.B. (2000), "Estimation of Risk under Fire Design Situation", *2nd International Conference on Computer Simulation: Risk Analysis and Hazard Mitigation,* Oct. 11-12, Bologna Wit Press, Italy.

Howard, R.A. (1968), "The Foundations of Decision Analysis", *IEEE Transactions on Systems, Science and Cybernetic,* No. 4, pp. 211-219.

Howard, R.A. and Matheson, J. (1981), "*Influence Diagrams*". *Readings on The Principles and Applications of Decision Analysis*. Howard, R. and Matheson, J. (eds.) (1984), Strategic Decisions Group, CA, USA.

HSE (2003), *Major Hazard Incident Database,* HSE Bootle Headquarter Library, Liverpool, UK.

Huang, W.C., Teng, J.Y., Hung, M.J. and Kou, M.S. "Port Competitiveness Evaluation by Fuzzy Multicriteria Grade Classification Model", *Journal of Marine Science and Technology*, Vol. 11, No. 1, pp. 53-60.

Hudson, L.D., Ware, B.S., Laskey, K.B. and Mahoney, S.M. (2001), "An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners", *Technical Report*, Department of Systems Engineering and Operations Research, George Mason University, Virginia, USA.

Hwang, C.L. and Yoon, KP. (1981), *Multiple Attribute Decision-Making: Methods and Applications*, Springer-Verlag, NY, USA.

IACS (2001), "Formal Safety Assessment of Bulk Carriers - Fore-End Watertight Integrity", *MSC/74/5/X,* submitted by International Association of Classification Societies (IACS), Agenda Item 5, London, UK.

Imai, M. (1990), "Kaizen Wave Circles the Globe", *Tokyo Business Today*, May.

IMO (1997), "Formal Safety Assessment: Trial Application to High Speed Passenger Catamaran Vessels", *Final Report, DE 41/INF.7,* submitted by International Maritime Organization (IMO) UK, IMO Sub-Committee on Ship Design and Equipment, 41st Session, Agenda Item 5, London, UK.

IMO (1998a), "Trial Application of Formal Safety Assessment to Dangerous Goods on Passenger/Ro-Ro Vessels", *MSC69/INF.24*, submitted by International Maritime Organization (IMO), Finland.

IMO (1998b), "Formal Safety Assessment Study on the Effects of Introducing Helicopter Landing Area (HLA) on Cruise Ships", *MSC69/INF.31,* submitted by International Maritime Organization (IMO), Italy.

IMO (1999-2005), *Casualty Statistics and Investigations 1998–2003*. FSI 3/Circ.1-6, London, UK.

IMO (2001), "Formal Safety Assessment of Life Saving Appliances for Bulk Carriers", *MSC 74/5/5*, submitted by Norway and ICFTU.

IMO (2002), *International Ship and Port Facility Security Code,* IMO Publications, London, UK.

ISL (2003), "General Cargo and Container Shipping", *Shipping Statistics and Market Review (SSMR)*, Vol. 47. pp.1-7.

Jain, P. and Agoino, A.M. (1990), "Stochastic Sensitivity Analysis Using Fuzzy Inference Diagrams", *Uncertainty in Artificial Intelligence*, Schachter, R.D., Levitt, T.S., Kanal, L.N. and Lemmer, J.F. (eds.), North-Holland, Amsterdam, Netherlands, pp. 79-92.

James, H.L. (1996), "Managing Information Systems Security: A Soft Approach", *Proceedings of the Information Systems Conference of New Zealand*, New Zaland.

Jensen, F.V. (1996), *An Introduction to Bayesian Networks*, University College London Press, London, UK.

Jensen, F.V. (2001), *Bayesian Network and Decision Graphs,* Springer-Verlag, NY, USA.

Jensen, F.V., Lauritzen, S.L. and Olesen, K.G. (1990), "Bayesian Updating in Causal Probabilistic Networks by Local Computations", *Computational Statistics, Quarterly 4*, pp. 269-282.

Johnson, J.C. and Wood, D.F. (1993), *Contemporary Logistics*, Macmillan Publishing Company, NY, USA.

Kahneman, D., Slovic, P. and Tversy, A. (1985), *Judgement under Uncertainty: Heuristics and Biases,* Cambridge University Press, Cambridge, UK.

Kapoor, V. and Tak, S.S. (2003), "Framework of a Fuzzy Multiple Criteria Model for Facilities Planning", *Proceedings of the Artificial Neural Networks in Engineering Conference*, Nov. 2-5, St. Loius, USA.

Kardes, E. and LuxhØ J.T. (2004), "A Hier archical Probabilistic Approach for Risk Assessments of an Aviation Safety Product Portfolio", available at (Dec 5, 2006), (*http://coewww.rutgers.edu/ie/research/working_paper/paper%2004-013.pdf*).

Karowski, W. and Mital, A. (1986), "Potential Applications of Fuzzy Sets in Industrial Safety Engineering", *Fuzzy Sets and Systems*, Vol. 19, pp. 105-120.

Keeney, R.L. and Raiffa, H. (1976), *Decision with Multiple Objectives*, John Wiley, NY, USA.

Keeney, R.L. and Raiffa, H (1993), *Decision with Multiple Objectives: Preferences and Value Trade-offs*, Cambridge University Press, Cambridge, UK.

Keller, A.A. and Kara, Z(1989), "Further Applications of Fuzzy Logic to Reliability Assessment and Safety Analysis", *Microelectronics and Reliability*, Vol. 29, No. 3, pp. 105-120.

Keogh, J. (1997), *Solving the Year 2000 Problem*, Academic Press, London, UK.

King, J.L. (2001), *Operational Risk: Measurement and Modelling*, John Wiley &Sons Inc., Chichester, UK.

Khan, F.I., Sadig, R. and Haddara, M.M. (2004), "Risk-Based Inspection and Maintenance (RBIM) Multi-Attribute Decision-Making with Aggregative Risk Analysis", *Process Safety and Environmental Protection*, Vol. 82, No. 6, pp. 398-411.

Khouja, M. and Booth, D.E. (1995), "Fuzzy Clustering Procedure for Evaluation and Selection of Industrial Robots", *Journal of Manufacturing Systems*, Vol. 14, No. 4, pp. 244-251.

Kjærulff, U.B. and Madsen, A.L. (2005), *Probabilistic Networks - An Introduction to Bayesian Networks and Influence Diagrams*, available at (Dec 5, 2006), (*http://www.cs.auc.dk/~uk/papers/pgm-book-I-05.pdf*).

Knight, F.H. (1921), *Risk, Uncertainty and Profit*, Houghton Mifflin Company, MA, USA.

Korhonen, P., Moskowitz, H., Wallenius, J. and Zionts, S. (1986) "An Interactive Approach to Multiple Criteria Optimization with Multiple Decision-Makers," *Naval Research Logistics Quarterly*, Vol. 33, pp. 589-602.

Kramer, M.A. and Palowitch, B.L. (1987), "A Rule Based Approach to Fault Diagnosis Using the Signed Directed Graph", *AIChE Journal*, Vol. 33, No. 7, pp. 1067-1077.

Kuusela, H., Spence, M.T. and Kanto, A.J. (1998), Expertise Effects on Pre-choice Decision Processes and Final Outcomes: A Protocol Analysis," *European Journal of Marketing,* Vol. 32, No. 5/6, pp. 559-576.

Kuo, C. (1998), *Managing Ship Safety*, LLP, London.

Kuo, W. and Zo, M.J. (2003), *Optimal Reliability Modeling: Principles and Applications*, John Wiley &Sons, Hoboken, New Jersey.

Labib, A.W. (1998), "A Logistics Approach to Managing the Millennium Information Systems Problem", *Logistics Information Management*, Vol. 11, No. 5, pp. 285.

Lambert, D.M., Cooper, M.C. and Pagh, J.D. (1998), "Supply Chain Management Implementation Issues and Research Opportunities", *International Journal of Logistics Management,* Vol. 9, No. 2, pp.1-19.

Langseth, H. (2002), "Bayesian Networks with Applications in Reliability Analysis", *PhD Thesis,* Department of Mathematical Sciences, Norwegian University of Science and Technology, Norway.

Laurizen, S.L. and Spiegelhalter, D.J. (1988), "Local Computations with Probabilities on Graphical Structures and Their Application to Expert Systems", *Journal of Royal Statistical Society B*, Vol. 50, No. 2, pp. 157-224.

LCP and CLSCM (2003), *Understanding Supply Chain Risk: A Self-Assessment Workbook*, Cranfield University Press, Bedford, UK.

Lee, B.H. (2001), "Using Bayes Belief Networks in Industrial FMEA Modelling and Analysis", *International Symposium on Product Quality and Integrity,* January 22-25, Philadelphia, USA, Part 1, pp. 7-15.

Lloyds Register (1978-2004), *Lloyd's Maritime Information Services (LMIS) Casualty Database*, Lloyd's Shipping Publication, London, UK.

Li, Y. and Liao, W. (2004), "Decision Support for Risk Analysis on Dynamic Alliance", *Decision Support Systems (in Press, Corrected Proof, Available online 18 December 2004).*

Liang, G.S. (1999), "Fuzzy MCDM Based on Ideal and Anti-ideal Concepts", *European Journal of Operational Research,* Vol. 112, No. 3, pp. 682-691.

Linares, P. (2002), "Multiple Criteria Decision Making and Risk Analysis as Risk Management Tools for Power Systems Planning", *IEEE Transactions on Power Systems*, Vol. 17, No. 3, pp. 895-900.

Lindley, D.V. (1970), "Bayesian Analysis in Regression Problems", *Bayesian Statistics*, Meyer, D.L. and Collier, R.O. (eds.), F.E. Peacock Publication, Itasca, Illinois, USA, pp. 38.

Liu, J., Yang, J.B., Wang, J., Sii, H.S. and Wang, Y.M., (2004), "Fuzzy Rule-based Evidential Reasoning Approach for Safety Analysis", *International Journal of General Systems*, Vol. 23, No. 2-3, pp. 183-204.

Lois, P., Wang, J., Wall, A. and Ruxton, T. (2004), "Formal Safety Assessment of Cruise Ships", *Tourism Management*, Vol. 25, pp. 93-109.

Lopez, D.M.R. (1990), *Approximate Reasoning Models*, Ellis Harwood Ltd, Chichester, UK.

Loughran, C., Pillay, A., Wang, J., Wall, A. and Ruxton, T. (2002), "A Preliminary Study of Fishing Vessel Safety", *Journal of Risk Research*, Vol. 5, No. 1, pp. 3-21.

Lovell, D.R., Rosario, B., Nirajan, M., Prager, R.W., Dalton, K.J., Derom, R. and Chalmers, J. (1997), "Design, Construction and Evaluation of Systems to Predict Risk in Obstetrics", *International Journal of Medical Informatics,* Vol. 46, pp. 159-173.

Ludwig, D. (1996), "Uncertainty and the Assessment of Extinction Probabilistic", *Ecological Applications,* Vol. 6, No. 4, pp. 1067-1076.

Mahadevan, S. and Rebba, R. (2005), "Validation of Reliability Computational Models Using Bayes Networks", *Reliability Engineering & System Safety,* Vol. 87, pp. 223-232.

Marsh, W. and Bearfield, G. (2000), "Using Bayesian Networks to Model Accident Causation in the UK Railway Industry", *7th International Conference on Probabilistic Safety Assessment and Management (PSAM 7),* June 14 -18, Berlin, Germany.

Mattsson, S.A. (2000), *Effektivisering Av Materialflöden I Supply Chains*, Acta Wexionensia, Samhällsvetenskap, VäjöUniversitet, Växjö

MCA (1996), "FSA of Shipping", *Trial Application to HSC,* Research Project, Phase 2, pp. 6.

McCabe, B., AbouRizk, M.S., Member ASCE and Randy, G. (1998), "Belief Networks for Construction Performance Diagnostics", *Journal of Computing in Civil Engineering*, Vol. 12, No. 2, pp. 93-100.

McDaniels, T.L. (1995), "Using Judgments in Resource Management: A Multiple Objective Analysis of a Fisheries Management Decision", *Operations Research*, Vol. 43, No, 3, pp. 415.

Military Standard (1969), "Department of Defence; System Safety Program Requirements", *MIL-STD-882*, USA.

Military Standard (1999), "Department of Defence, Military Standards;System Safety Program Requirements", *MIL-STD-882D*, USA.

Min, H. (1994), "International Supplier Selection: A Multi-attribute Utility Approach", *International Journal of Physical Distribution & Logistics Management*, Vol. 24, No. 5, pp. 24-33.

Modarres, M. (1993), *What Every Engineer Should Know about Reliability and Risk Analysis*, Marcel Dekker Inc., NY, USA.

Monden, Y. (1994), *Tokyo Production System: An Integrated Approach to Just-In-Time*, Second edition, Institute of Industrial Engineers, Chapman and Hall, London, UK.

Morgan, M.G. and Henrion, M. (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk Assessment and Policy Analysis*, Cambridge University Press, Cambridge, UK.

MSA (1993), "Formal Safety Assessment", *MSC66/14*, submitted by the UK to IMO Maritime Safety Committee, London, UK.

Murphy, K. (1998), "A Brief Introduction to Graphical Models and Bayesian Networks", available at (Dec 5, 2006),
(*http://www.cs.ubc.ca/~murphyk/Bayes/bayes.html*).

Murphy, C.K. (2000), "Combining Belief Functions When Evidence Conflicts", *Decision Support Systems*, Vol. 29, pp. 1-9.

Murray, J.T. and Murray, M.J. (1996), *The Year 2000 Computing Crisis: A Millennium Date Conversion Plan*, Computing McGraw-Hill, NY, USA.

Nakajima, S. (1989), *TPM Development Program: Implementing Total Productive Maintenance*, Productivity Press, MA, USA.

Narahari, Y., Viswanadham, N. and Bhattacharya, R. (2000), "Design of Synchronized Supply Chains: A Six Sigma Tolerancing Approach", *Proceedings - IEEE International Conference on Robotics and Automation*, pp. 1151-1156.

Neapolitan, R.E. (1990), *Probabilistic Reasoning in Expert System: Theory and Algorithms*, John Willey &Sons, Inc., NY, USA.

NGA (2004), *World Port Index – PUB.150*, available at (Nov 21, 2003), (*http://164.214.12.145/pubs/pubs_j_wpi_sections.html*).

Noble, J. (2004), "Surviving the Damage", *Marine Engineers Review*, February, pp. 11.

Norris, J.R. (1998), *Markov Chains, Statistical and Probabilistic Mathematics: Series 2*, Cambridge University Press, UK.

North, D.W. (1968), "A Tutorial Introduction to Decision Theory", *IEEE Transactions on System, Science and Cybernetic*, Vol. 4, pp. 201-210.

OECD (2003), "Security in Maritime Transport: Risk Factors and Economic Impact", *Maritime Transport Committee of OECD Report*, France.

Ohno, T. (1988), *Toyota Production System: Beyond Large Scale Production*, Productivity Press, MA, USA.

Öer, A.I. and Majumder, J. (2006), "A Case-based Decision Support System for Flooding Crises Onboard Ships", *Quality and Reliability Engineering International*, Vol. 22, No. 1, pp. 59-78.

Oliver, R.M. and Smith, J.Q. (1990), *Influence Diagrams, Belief Nets and Decision Analysis*, Wiley, Chichester, UK.

Ong, G.G. (2002), "Pre-empting Maritime Terrorism in Southeast Asia", *Viewpoints of ISESA*, available at (Dec 5, 2006), (*http://www.iseas.edu.sg/viewpoint/ggonov02.pdf*).

Ottonello, C., Peri, M., Regazzoni, C. and Tesei, A. (1992), "Integration of Multisensor Data for Vercrowding Estimation", *IEEE International Conference on Systems, Man and Cybernetics*, NY, USA, pp. 791-196.

Pai, R.R., Kallepalli, V.R., Caudill, R.J. and Zhou, M.C. (2003), "Methods to wards Supply Chain Risk Analysis", *System Security and Assurance*, Vol. 5, pp. 4560-4565.

Pan, H.P. and McMichael, D. (1998), "Fuzzy Causal Probabilistic Networks – A new Ideal and Practical Inference Engine", *Proceeding of the 1st International Conference on Multisource-Multisensor Data Fusion, FUSION 98*, July, Las Vegas, USA.

Pan, H.P. and 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.

Parker, D.B. (1998), *Fighting Computer Crime - A New Framework for Protecting Information*, John Wiley &Sons, NY, USA.

Pate-Cornell, M.E. (1996), "Uncertainties in Risk Analysis: Six Levels of Treatment", *Reliability Engineering & System Safety,* Vol. 54, pp. 95-111.

Patrick, L.A. (2002), "Lost Earnings Due to the West Coast Port Shutdown - Preliminary Estimate", *Working paper 2002-10, Anderson Economic Group LLC,* USA.

Pearl, J. (1982), "Reverend Bayes on Inference Engines: A Distributed Hierarchical Approach", *National Conference on Artificial Intelligence,* pp. 133-136.

Pearl, J. (1986), "Fusion, Propagation and Structuring in Belief Networks", *Artificial Intelligence,* Vol. 29, pp. 241-288.

Pearl, J. (1988), *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann Publishers Inc., CA, USA.

Peck, H. and Jüttner, U. (2002), "Risk Management in Supply-Chain", *Logistics & Transport Focus*, Vol. 4, No. 10, pp. 17-22.

Perry, W.E. (1985), *Management Strategies for Computer Security*, Butterworth-Heinemann, MA, USA.

Platts, K.W., Probert, D.R. and Cãz, L. (2002), "Make vs. Buy Decisions: A Process Incorporating Multi-Attribute Decision-Making", *International Journal of Production Economics*, Vol. 77, No, 11, pp. 247-257.

Pillay, A. and Wang, J. (2003a), *Technology and Safety of Marine Systems*, Elsevier Science Publishers, Oxford, UK.

Pillay, A. and Wang, J. (2003b), "A Risk Ranking Approach Incorporating Fuzzy Set Theory and Grey Theory," *Engineering Reliability & System Safety*, Vol. 79, No. 1, pp. 61-67.

Pillay, A., Wang, J., Wall, A., Ruxton, T. and Loughran, C. (2003), "Formal Safety Assessment of Fishing Vessels: Risk and Maintenance Modelling", *World Marine Technology Conference*, Oct. 17-20, San Francisco, CA, USA.

Poole, D.L., Mackworth, A. and Goebel, R.G. (1998), *Computational Intelligence: A Logical Introduction,* Oxford University Press, NY, USA.

PVA (1997), *A Guide to Improving the Safety of Passenger Vessel Operations by Addressing Risk*, Arlington, pp. 1-28.

Ragland, B. (1996), *A Five-Step Disaster Prevention Plan*, Computing McGraw-Hill, NY, USA.

Raiffa, H. (1968), *Decision Analysis*, Addison-Wesley, Reading, MA, USA.

Raymond, G.G. (2005), "The Malacca Straits and the Threat of Maritime Terrorism", *Power and Interest News Report*, available at (Dec 5, 2006), (*http://www.pinr.com/report.php?ac=view_printable&report_id=352&language_id=1*).

Reed, D.A. (1990), "Reliability of Multi-component Assemblages", *Reliability Engineering & System Safety,* Vol. 27, pp. 167-178.

Rilett, L.R. and Park, D. (2001), "Incorporating Uncertainty and Multiple Objectives in Real-Time Route Selection", *Journal of Transportation Engineering*, Vol. 127, No. 6, pp. 531-539.

Roberts, F.S. (1979), *Measurement Theory with Applications to Decision Making, Utility, and the Social Sciences*, Addison-Wesley, Reading, MA, USA.

Ronza, A., Fĕez, S., Darbra, R.M., Carol, S., Vlchez, J.A. and Casal, J. (2003), "Predicting the Frequency of Accidents in Ports Areas by Developing Event Trees from Historical Analysis", *Journal of Loss Prevention in the Process Industries*, Vol. 16, pp. 551-560.

Roubens, M. (1996), "Choice Procedures in Fuzzy Multicriteria Decision Analysis Based on Pairwise Comparisons", *Fuzzy Sets and Systems*, Vol. 84, pp. 135-142.

Roy, B. and Vincke, P. (1981), "Multicriteria Analysis: Survey and New Directions", *European Journal of Operational Research*, Vol. 8, pp. 207-218.

Rushton, A., Oxley, J. and Croucher, P. (2000), *The Handbook of Logistics and Distribution Management*, Institute of Logistics and Transport, Kogan Page Limited, London, UK, pp. 6.

Russell, S. and Norvig, P. (1995), *Artificial Intelligence: A Modern Approach*, Prentice-Hall, Englewood Cliffs, NJ, USA.

Saaty, T.L. (1980), *The Analytic Hierarchy Process*, University of Pittsburgh, USA.

Saaty, T.L. (1987), "Risk – Its Priority and Probability: the Analytic Hierarchy Process", *Risk Analysis*, Vol. 7, No, 2, pp. 147-158.

Samson, D. (1988), *Managerial Decision Analysis*, Richard D. Irwin Inc., Homewood, USA.

Sandler, G.H. (1963), *System Reliability Engineering*, Prentice-Hall, Englewood Cliffs, NJ, USA.

Santa-Fe Institute (2001), *Working Definitions of Robustness*, available at (Dec 5, 2006): (*http://discuss.santafe.edu/robustness/stories/storyReader$9*).

Sarma, K.C. and Adeli, H. (2000), "Fuzzy Discrete Multicriteria Cost Optimization of Steel Structures", *Journal of Structural Engineering*, Vol. 126, No. 11, pp. 1339-1347.

Schmucker, K.J. (1984), *Fuzzy Sets, Natural Language Computations and Risk Analysis*, Computer Science Press, Rockville, MA, USA.

SERENE consortium (1999), *SERENE (SafEty and Risk Evaluation using Bayesian Nets): Method Manual*, ESPRIT Project 22187, available at (Dec 5, 2006), (*www.hugin.com/serene*).

Shachter, R.D. (1988), "Probabilistic Inference and Influence Diagram", *Operations Research*, Vol. 36, No. 4, pp. 589-604.

Shachter, R.D. and Peot, M.A., (1992), "Decision Making Using Probabilistic Inference Methods", *Proceedings of the 8th Conference on Uncertainty in AI*, Stanford University, Jul 17-19, CA, USA, pp. 276-283.

Shafer, G. (1976), *A Mathematical Theory of Evidence*, Princeton University Press, Princeton, USA.

Shafer, G. (1990), "Decision Making", *Readings in Uncertain Reasoning*, Shafer, G. and Pearl, J. (eds.), Morgan-Kaufmann, San Mateo, CA, USA, pp. 61-67.

Shafer, G. and Pearl, J. (1990), *Readings in Uncertain Reasoning*, Morgan-Kaufmann, San Mateo, CA, USA.

Shingo, S. (1985), *A Revolution in Manufacturing: the SMED System,* Productivity Press, MA, USA.

Shipley, M.F., De Korvin, A. and Omer, K. (2001), "A Fuzzy Logic-Based Decision Model to Satisfy Goals for Successful Product/Service Introduction", *European Journal of Operational Research*, Vol. 135, No. 1, pp. 209-219.

Shrinath, L.S. (1991), *Reliability Engineering,* Affiliated East-West Press Private Limited, New Delhi, India.

Sifder, S.P. and Smeltzer, L.R. (1997), "Risk Assessment in the Supply Chain", *Annual Meeting of the Decision Science Institute*, Vol. 3, Part 3, pp. 1476.

Sii, H.S., Wang, J. and Ruxton, T. (2001), 'A Fuzzy-logic-based Approach to Subjective Safety Modelling for Maritime Products," *Journal of UK Safety and Reliability Society*, Vol. 21, No. 2, pp. 65-79.

Sii, H.S. and Wang, J. (2002), "Safety Assessment of FPSOs – The Process of Modelling System Safety and Case Studies", *Report of the Project – "The Application of Approximate Reasoning Methodologies to Offshore Engineering Design" (EPSRC GR/R30624 and GR/R32413)*, Liverpool John Moores University, Liverpool, UK.

Singh, D and Tiong, R.L.K. (2000), "A Fuzzy Decision Framework for Contractor Selection", *Journal of Construction Engineering and Management*, Vol. 131, No. 1, pp. 62-70.

Siponen, M.T. and Baskerville, R. (2001), "A New Paradigm for Adding Security into IT Development Methods", *Advances in Information Security Management and Small Systems Security*, Kluwer Academic Publishers, NY, USA.

Skjong, R. and Wentworth, B. (2000), "Formal Safety Assessment of Life Saving Appliances for Bulk Carriers", *DNV Report 2000-0539 (Also available as IMO document MSC/74/5/5),* Oslo, Norway.

Smith, A.F.M. (1984), "Present Position and Potential Developments: Some Personal Views Bayesian Statistics", *Journal of the Royal Statistical Society A*, Vol. 147, pp. 245-259.

Sonmez, M. (2002), "Investigation Into Utility Based Methods and Evidential Reasoning Approach for Complex Decision Analysis", *PhD Thesis*, University of Manchester, Manchester, UK.

Speigelhalter, D.J., Dawid, D.J., Lauritzen, S.L. and Cowell, R.G. (1993), "Bayesian Analysis in Expert Systems", *Statistical Science*, Vol. 8, pp. 219-283.

Spiegelhalter, D.J. and Knill-Jones, R.P. (1984), "Statistical and Knowledge-based Approaches to Clinical Decision-support Systems", *Journal of the Royal Statistical society: Series A,* Vol. 147, pp. 35-37.

Spouge, J.R. (1998), "Formal Safety Assessment of Helicopter Landing Area on Passenger Ships as a Safety Measure - Additional Information", *DNV Report 98-2047*, Oslo, Norway.

Sugimori, Y., Kusunoki, K., Cho, F. and Uchikawa, S. (1977), "Toyota Production System and Kanban System: Materialization of Just-in-time and Respect-for-human System'', *International Journal of Production Research*, Vol. 15, No. 6, pp. 553-564.

Sullivan, K.J., Dugan, J.B. and Coppit, D. (1999). "The Galileo Fault Tree Analysis Tool", *29th Annual International Symposium on Fault-Tolerant Computing*, pp. 232-235.

Svensson, G. (2000), "A Conceptual Framework for the Analysis of Vulnerability in Supply Chains", *International Journal of Physical Distribution and Logistics Management*, Vol. 30, No. 9, pp. 731-749.

Svensson, G. (2002), "A Conceptual Framework of Vulnerability in Firms' Inbound and Outbound Logistics Flows", *International Journal of Physical Distribution and Logistics Management*, Vol. 32, No. 2, pp. 110-134.

Svensson, G., (2004), "Key Areas, Causes and Contingency Planning of Corporate Vulnerability in Supply Chains: A Qualitative Approach", *International Journal of Physical Distribution and Logistics Management*, Vol. 34, No. 9, pp. 728-748.

Szolovits, P. and Pauker, S.G. (1993), "Categorical and Probabilistic Reasoning in Medicine Revisited", *Artificial Intelligence*, Vol. 59, pp. 167-180.

Talluri, S. and Narasimhan, R. (2003), "Vendor Max-min Evaluation with Performance Variability: A Max-min Approach", *European Journal of Operational Research*, Vol. 146, No. 3, pp. 543-552.

Thomas, M.U. (2002), "Supply Chain Reliability for Contingency Operations", *Annual Reliability and Maintainability Symposium*, pp. 61-67.

Timmerman, P. (1981), "Vulnerability, Resilience and the Collapse of Society", *Institute of Environmental Studies*, University of Toronto, Toronto, Canada.

Tummala, V.M.R. and Leung Y.H. (1995), "A Risk Management Model to Assess Safety and Reliability Risks", *International Journal of Quality and Reliability Management*, Vol. 13, No. 8, pp. 53-62.

Tversky, A. and Kahneman, D. (1974), "Judgment under Uncertainty: Heuristics and Biases", *Science*, Vol. 185, pp. 1124-1131.

Tversky, A. and Kahneman, D. (1990), "Judgment under Uncertainty: Heuristics and Biases", *Readings in Uncertain Reasoning*, Shafer, G. and Pearl, J. (eds.), Morgan Kaufmann Publishers Inc., San Mateo, CA, USA.

UK P&Cl ub (1999), *Analysis of Major Claims – Ten Years Trends in Maritime Risk*, London, UK.

Ulrich, W.M. and Hayes, I.S. (1997), *The Year 2000 Software Systems Crisis: the Challenge of the Century*, Yourdon Press Computing Series, NY, USA.

Vaidya, O.S. and Kumar, S. (2003), "Dependency and its Predictions for Systems and its Components", *International Journal of Quality & Reliability Management*, Vol. 20, No. 9, pp. 1096-1116.

Vivalda, C. (2000), "Formal Safety Assessment of High Speed Craft", *Ship Design Conference 2000*, Sep. 5-6, Aalesund, Norway.

Von Winterfeldt, D. (1982), "Setting Standards for Offshore Oil Discharges: A Regulatory Decision Analysis", *Operations Research*, Vol. 14, pp. 247-256.

Vouros, G. (2000), "Representing, Adapting, and Reasoning with Uncertain, Imprecise and Vague Information", *Expert Systems with Applications*, Vol. 19, pp. 167-192.

Wald, A. (1950), *Statistical Decision Functions*, Wiley, NY, USA.

Wang, J. (1997a), "A Subjective Methodology for Safety Analysis of Safety Requirements Specifications", *IEEE Transactions on Fuzzy Systems*, Vol. 5, No. 3, pp. 418-430.

Wang, J. and Foinikis, P. (2001), "Formal Safety Assessment of Containerships", *Marine Policy*, Vol. 25, No. 2, pp. 143-157.

Wang, J. and Lin, Y. (2003), "A Fuzzy Multicriteria Group Decision Making Approach to Select Configuration Items for Software Development", *Fuzzy Sets and Systems*, Vol. 134, No. 3, pp. 343-363.

Wang, J. Pillay, A. Wall, A. and Ruxton, T. (1999), "The Latest Development in Ship Safety Assessment", *Proceeding of the 4th International Conference on Reliability, Maintainability and Safety (ICRMS '99)*, Shanghai, China. pp. 711-719.

Wang, J. and Ruxton T. (1998), "A Design for Safety Methodology of Large Engineering Systems", *Journal of Engineering Design*, Vol. 9, pp. 159-170.

Wang, J. and Trbojevic, V.M. (2006), *Design for Safety of Large Marine and Offshore Engineering Products*, Institute of Marine Engineering, Science and Technology (IMarEST), London, UK.

Wang, J., Yang, J.B. and Sen, P. (1995), "Safety Analysis and Synthesis Using Fuzzy Set Modelling and Evidential Reasoning", *Reliability Engineering & System Safety*, Vol. 47, No. 3, pp. 103-118.

Wang, J., Yang J.B. and Sen P. (1996), "Multi-person and Multi-attribute Design Evaluations Using Evidential Reasoning Based on Subjective Safety and Cost Analyses", *Reliability Engineering & System Safety*, Vol. 52, pp. 113-128.

Wang, L.X(1997b), *A Course in Fuzzy Systems and Control*, Prentice-Hall, NJ, USA.

Warman, A.R. (1992), "Organizational Computer Security Policy: the Reality", *European Journal of Information Systems*, Vol. 1, No. 5, pp. 305-10.

Weichselgartner, J. (2001), "Disaster Mitigation: the Concept of Vulnerability Revisited", *Disaster Prevention and Management,* Vol. 10, No. 2, pp. 85-94.

Willems, A., Janssen, M., Verstegen, C. and Bedford, T. (2005), "Expert Quantification of Uncertainties in a Risk Analysis for an Infrastructure Project", *Journal of Risk Research*, Vol. 8, No. 1, pp. 3-17.

IX H. (1997), "Valuation-Based System s for Decision Analysis by Using Belief Functions", *Decision Support Systems*, Vol. 20, pp. 165-184.

Yager, R.R. (1981), "A New Methodology for Ordinal Multiobjective Decision Based on Fuzzy Sets", *Decision Science*, Vol. 12, pp. 589-600.

Yager, R.R. (1992), "On the Specificity of a Possibility Distribution", *Fuzzy Sets and Systems*, Vol. 50, pp. 279-292.

Yager, R.R. (1995), "An Approach to Ordinal Decision Making", *International Journal of Approximate Reasoning*, Vol. 12, pp. 237-261.

Yang, J.B. (2001), "Rule and Utility Based Evidential Reasoning Approach for Multiattribute Decision Analysis under Uncertainties", *European Journal of Operational Research*, Vol. 131, No. 1, pp. 31-61.

Yang, J.B., Deng, M. and X, D.L. (2001), "Nonlinear Regression to Estimate Both Weights and Utilities via Evidential Reasoning for MADM", *Processing 5th International Conference, Optimization: Techniques and Applications*, Dec. 15-17, Hong Kong.

Yang, J.B., Liu, J., Wang, J., Sii, H.S. and Wang, Y.M. (2005), "Belief Rule-base Inference Methodology Using the Evidential Reasoning Approach – *RIMER*", *IEEE Transactions on Systems, Man and Cybernetics – Part A: Systems and Humans*, Vol. 36, no. 2, pp. 266-285.

Yang, J.B. and Singh, M. (1994), "An Evidential Reasoning Approach for Multiple Attribute Decision Making with Uncertainty", *IEEE Transaction on Systems, Man and Cybernetics*, Vol. 24, No. 1, pp. 1-18.

Yang, J.B. and Sen, P. (1994), "A General Multi-Level Evaluation Process for Hybrid MADM with Uncertainty", *IEEE Transaction on Systems, Man and Cybernetics*, Vol. 34, No. 10, pp. 1458-1473.

Yang, J.B. and Sen, P. (1996), "Preference Modelling by Estimating Local Utility Functions for Multiobjective Optimisation", *European Journal of Operational Research*, Vol. 95, pp. 115-138.

Yang, J.B. and Sen, P. (1997), "Multiple Attribute Design Evaluation of Complex Engineering Products Using the Evidential Reasoning Approach", *Journal of Engineering Design*, Vol. 8, No. 3, pp. 211-230.

Yang, J.B. and X, D.L. (2000), "An Introduc tion to an Intelligent Decision System: IDS", *Proceedings of the 42nd Annual Conference of the UK Operational Research Society*, Sep. 12-14, Swansea, UK.

Yang, J.B. and X, D.L. (2002), "On the Ev idential Reasoning Algorithm for Multiple 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, Z., Wang, J., Bonsall, S., Fang, Q.G. and Yang, J.B. (2004), "A Subjective Risk Analysis Approach for Container Supply Chains", *Proceeding of the 10th Annual Conference of CACSUK '04*, Sep. 18, Liverpool, UK.

Yang, Z., Bonsall, S., Alan, W . and Wang, J. (2005b), "Reliable Container Line Supply Chains – A New Risk Assessment Framework for Improving Safety Performance", *WMU Journal of Maritime Affairs,* Vol. 4, No. 1, pp. 107-122.

Yang, Z., Bonsall, S., Fang, Q.G. and W ang, J. (2005a), "Formal Safety Assessment of Container Liner Supply Chains", *European Safety and Reliability Conference '05.* June 27-30, Tri City, Poland.

Yang, Z., Bonsall, S ., Fang, Q.G. and Wang, J. (2005c), "Risk Assessment of Container Supply Chains Using Bayesian Networks", *4th International Conference of Quality and Reliability*, Aug 9-11, Beijing, China.

Yang, Z., Bonsall, S., Fang, Q.G. and W ang, J. (2006), "Relative Risk Analysis Using Bayesian Networks and Evidential Reasoning", *European Reliability and Safety Conference '06*, Sep. 18-22, Estoril, Portugal.

Yen, J. (1990), "Generalizing the Demspter-Shafer Theory to Fuzzy Sets", *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 20, No. 3, pp. 559-570.

Zdeh, L.A. (1965), "Fuzzy Sets", *Information and Control*, Vol. 8, No. 3, pp. 338-353.

Zadeh, L.A. (1975), "The Concept of a Linguistic Variable and its Application to Approximate Reasoning", *Information Science*, Vol. 8, No. 2, pp. 301-353.

Zadeh, L.A. (1984), "Fuzzy Probabilities", *Information Processing Management*, Vol. 20, pp. 363-372.

Zadeh, L.A. (1985), "Syllogistic Reasoning in Fuzzy Logic and its Application to Usuality and Reasoning with Dispositions," *IEEE Transaction on Systems, Man and Cybernetics*, Vol. 15, pp. 754-763.

Zeleny, M. (1976), "The Attribute-Dynamic Attitude model (ADAM)", *Management Science*, Vol. 23, No. 1, pp. 12-26.

Zhang, H., Li, H. and Tan, C.M. (2004), "Fuzzy Discrete-event Simulation for Modeling Uncertain Activity Duration", *Engineering, Construction and Architectural Management*, Vol. 11, No. 6, pp. 426-437.

Zhang, Q., Chen, J.H., He, Y.Q., Ma, J. and Zhou, D.N. (2003), "Multiple Attribute Decision Making: Approach Integrating Subjective and Objective Information", *International Journal of Manufacturing Technology and Management*, Vol. 5, No. 4, pp. 338-361.

Zimmer, A.C. (1983), "Verbal vs. Numerical Processing of Subjective Probabilities", *Decision Making under Uncertainty*, Scholz, R.W. (eds.), North-Holland, Amsterdam, Netherlands.

Zimmer, A.C. (1986), "What Uncertainty Judgements Can Tell about the Underlying Subjective Probabilities", *Uncertainty in Artificial Intelligence*, Kanal, L.N. and Lemmer, J.F. (eds.), North-Holland, Amsterdam, Netherlands.

Zimmermann, H.J. (1991), *Fuzzy Set Theory and its Application*, Norwell, MA, Kluwer.

Zimmermann, H.J. (2000), "An Application-oriented View of Modelling Uncertainty", *European Journal of Operational Research*, Vol. 122, pp. 190-199.

Appendix 1. Research Deliverables Arising from this Research

1) **Yang, Z.L.**, Bonsall, S., Fang, Q.G., Yang, J.B. and Wang, J. (2004), "A Subjective Risk Analysis Approach for Container Supply Chains", *Proceeding of the 10th Annual Conference of CACSUK '04*, Sep. 18, Liverpool, UK (Given the Best Paper Award by the Conference Programmer Committee). *Also see*
Yang, Z.L., Bonsall, S., Fang, Q.G., Yang, J.B. and Wang, J. (2005), "Subjective Risk Assessment of Container Supply Chains", *International Journal of Automation and Computing*, Vol. 1, pp. 20-28.

2) **Yang, Z.L.**, Bonsall, S., Wall, A. and Wang, J. (2005), "Reliable Container Liner Supply Chains", *WMU Journal of Maritime Affairs*, Vol. 4, No. 1, pp. 107-122.

3) Fang, Q.G., **Yang, Z.L.**, Wang, J. and Hu, S.P. (2005), "FSA and Its Application to the Prevention of Human Error in Ship Operations Using Navigation Simulators", *International Workshop on Automation, Computing and Manufacturing '05*, March 29-30, Beijing, China.

4) Fang, Q.G., **Yang, Z.L.**, Hu, S.P. and Wang, J. (2005), "Formal Safety Assessment and Application of the Navigation Simulators for Preventing Human Error in Ship Operations", *Journal of Marine Science and Application,* Vol. 4, No. 3, pp.5-12.

5) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2005), "Formal Safety Assessment of Container Line Supply Chains", *European Safety and Reliability conference '05*, June 27 – 30, Tri City, Poland. *Also see*
Yang, Z.L., Wang, J., Bonsall, S, and Fang, Q.G. (2005), "Formal Safety Assessment of Container Line Supply Chains", *Archives of Transport, Journal of Polish Academy of Science,* Vol. 17, No.3/4, pp. 255-274.

6) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2005), "Risk Assessment of Container Supply Chains Using Bayesian Networks", *the 4th International Conference on Quality and Reliability*, Aug. 9-11, Beijing, China.

7) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2005), "Risk Assessment of Container Supply Chains Using the Methods of Uncertainty Treatment", *Journal of UK Safety and Reliability Society,* Vol. 26, No. 1, pp. 29-38.

8) **Yang, Z.L.**, Bonsall, S., Fang, Q.G., Yang, J.B. and Wang, J. (2005), "Fuzzy Risk Assessment of Container Supply Chains", *Fuzzy Sets and Systems (Accepted subject to revision).*

9) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2005), "Risk Assessment of Container Supply Chains Using Bayesian Networks", *Reliability Engineering & System Safety (Revision).*

10) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2006), "Relative Risk Assessment Using Bayesian Networks and Evidential Reasoning", *European Safety and Reliability conference '06*, Sep. 18-22, Estoril, Portugal.

11) **Yang, Z.L.**, Bonsall, S., Fang, Q.G. and Wang, J. (2006), "Maritime Security: Assessment and Management", *Proceeding of the 7th International Association of Maritime Universities (IAMU) Annual General Assembly (AGA)*, Oct. 16-18, Dalian, China.

Appendix 2. References for the Economic Estimation of *RCOs*[*]

Although fuzzy cost assessment (qualitative method) requires less detailed data than precise *CBA* (quantitative assessment), a certain amount of relative data as qualitative estimation references is still necessary in order to determine the cost levels of *RCOs*. Thus, the following *RCOs* are analysed to define the references for their economic considerations.

AIS

AIS systems can be used to monitor the movements of ships that are suspected. The cost for an AIS transponder ranges from $10,000 to 20,000 and therefore the total cost to equip the entire current containership fleet (2905 containerships until Jan 2003) is approximately $43.6 million. To avoid using a vessel as weapon to attack ports, the total cost of AIS systems should be calculated on the basis of the whole international commercial fleet with a value about $649.3 million. This amount, however, should not be seen as the security cost of taking this measure *per se* given that AIS requirements were already in place for navigation safety before MSC 76. In terms of the security-based cost associated with AIS, it only covers the cost for the ISPS-related security elements, which can be applied to upgrade the original systems to a more sophisticated and advanced level to satisfy the ISPS requirements. Additional AIS-related costs are associated with the development of shore-based facilities and the maintenance costs. The costs at the associated shore-based facilities are generally built and operated by governments as an extension of their navigation roles. The costs are quite different in different countries since the facilities are not required under the SOLAS regulations. Taking into accounting all such factors, the costs for AIS systems can be estimated as:

Investment costs: "*Average*" Maintenance costs: "*Low*"

Ship identification number

Although the costs for this measure might be deducted by scheduled re-painting operations during the vessels' dry-docking, this expense is still estimated to be around $5,000 per ship (OECD, 2003). The total related costs are around $14.5 million for the containerships fleet and $216.4 million for the entire commercial fleet, which means the costs for this measure can be estimated as:

Investment costs: "*High*" Maintenance costs: "*Nil*"

Ship alert system

The USCG estimates that such a system will cost approximately $2,000 a piece and

---

[*] Much information and data related to this cost analysis comes from the report produced by OECD (2003) and the research conducted by USCG (http://www.uscg.mil/uscg.shtm).

simultaneously, maintenance costs will require $100 per piece per year (OECD, 2003). The safety measure investment costs related to containerships arrive at $5.8 million and $86.5 million for the international commercial fleet. Yearly maintenance costs spending on the containership fleet and total commercial ship fleet are $290,000 and $4.3 million, respectively. The investment and maintenance costs for this measure are estimated as:

Investment costs: "*Moderately high*" Maintenance costs: "*Average*"

Designating specific security officers

The USCG assesses the cost for a shipping company security officer (CSO) to be $150,000 per year for a large American-based company (controlling 10 or above containerships) and $37,500 per year for a small American-based company (owing less than 10 containerships) (OECD, 2003). In this thesis, three problems will be considered and analysed. One is that a large company in the international liner shipping sector are generally competing against each other in the international job market and facing a similar labour cost. The second is that the concentrating tendency in liner shipping has dramatically increased. Thirdly, precise estimates of the number of container liner shipping companies, either large or small, are difficult to make given that, for a reason of liability, many vessels are owned by one-ship companies. Many of these companies, however, are effectively controlled by the same operator. To the authors' knowledge, it is reasonable to assume that there are 30 - 50 large liner shipping lines (for this study, the average number – 40 can be taken) acting in the international liner shipping trade. Because of this, the costs estimated only for *CSOs* in large container liner shipping companies have arrived at $6 million per year. Furthermore, based on the USCG figure, the maintenance costs, namely training fees, of *CSOs* are $3,500 per person per year and consequently the total maintenance costs for large companies are $135,000 per year. The costs for this measure will undoubtedly be extremely high if the security officers for other small liner shipping companies, the 2814 worldwide commercial ports and unaccountable inland logistics companies are also taken into account. Therefore, the estimation of the costs for this measure can be shown as:

Investment costs: "*Extremely high*" Maintenance costs: "*High*"

Carrying out containership and port security assessment

A comprehensive containership security assessment requires to outline preventative counter-measures to potential security risks. Such a work can usually be completed by classification societies or other security assessment service organizations with a period of 3 eight-hour working days. Based on the charging rate provided by the USCG – $100 per hour (OECD, 2003), the total containership fleet for developing security assessment can be estimated as about $6.98 million.

According to the USCG, a high-standard port facility security assessment requires

$8,000 initially and $400 per year thereafter and while the costs for a lower-standard port facility are $4,000 and $100, respectively. In terms of the number of port facilities in a word-wide scope, many authorities or organizations have made their estimations. The *World Port Index* (National Geospatial-intelligence Agency, (NGA), 2004) pointed out that there are more than 6 000 ports in the world. The figure, however, takes both commercial and military ports into account and has little significance for this study. *The US Department of Transport* identified at least 3970 ports in the world in the "schedule K" of its USDOT listing of world ports (OECD, 2003). However not all these ports are involved in international trade. *Fairplay/Lloyds Register* (2004) counted 2814 port authorities worldwide, who are operating 6,500 port facilities from a conservative estimation perspective. Such a figure is considered to be a more reasonable representation of the universe of ports and their facilities involved in international trade. Out of this figure, the authors have identified over 430 highly automated container handling facilities. Approximately, half of these facilities are controlled by the top 40 container ports, which handled 63% of total international seaborne container transportation in terms of goods loaded in 2001 (OECD, 2003). These facilities are global competitors and will seek a high standard of compliance with the ISPS code, therefore face higher security assessment costs. On the other hand, the other half of the facilities are with a comparatively low standard and as a result pay less security costs. Thus the estimated costs of undertaking container port facility security assessment are around $2.6 million initially and $107,500 annually. In subjective terms, the investment and maintenance costs are estimated as:

Investment costs: 0.5 "*Average*" and 0.5 "*Moderately low*"

Maintenance costs: "*Low*"

Adequate security equipment

The tasks to estimate the costs of security equipment in a container liner supply chain will be extremely complicated given the great variability of their costs from country to country and from port to port. The containership security equipment, however, can be effectively estimated considering liner shipping as an international industry. Therefore, this research will carefully analyse the containership security equipment and provide a reference to the estimation of cost level of this measure.

Complying with the guidance shown in part "B" of the ISPS code, one can get an idea of the general equipment that the IMO rules imply. In this study, the security equipment for containerships can be listed in Table A1 and estimated for each item in terms of both initial investment and annual maintenance costs.

Given the total number of the worldwide containership fleet – 2905 in Jan. 2003 (ISL, 2003), the total containership security equipment costs $49.1 million initially and annual

Table A1. Cost analyses of containership security equipments

Item	Initial investment costs			Annual maintenance costs	
	Number	Cost/item (USD)	Sub-total cost (USD)	Cost/item (USD)	Sub-total cost (USD)
Hand-held metal detector	2	200	400	10	20
Hand-held radio	5	200	1,000	10	50
Lock	10	300	3,000	15	150
Light	5	400	2,000	20	100
Auto-intrusion alarm	5	500	2,500	25	125
Portable vapour detector (for explosives)	1	8,000	8,000	400	400
Total			16,900		845

Source: OECD Maritime Transport Committee

$2.5 million thereafter. Based on such a reference and also considering more expensive equipment required for other sectors in the chain (i.e. CCTV and gates for port facilities), the entire costs of this measure will be extremely high and are subjectively estimated as:

Investment costs: "*Extremely high*" Maintenance costs: "*High*"

96-hour advance notification of arrival of vessels

Although the cargo manifest filling requirement involves some data processing time and software, overall costs for this measure should not be too significant. The *USCG's* estimate for annual maintenance costs is approximately $6.7 million (OECD, 2003). The subjective estimation for this measure can be obtained as:

Investment costs: "*Very low*" Maintenance costs: "*Average*"

24-hour advance manifest rule

The requirements of this rule have imposed costs on carriers who must field sufficient clerical/data entry staff to handle bookings. Some carriers have also expressed fears that the rule would reduce their flexibility to accept last-minute bookings. The costs stemming from the early manifest requirements are also associated with shippers. The shippers must pay for port space for containers shipped in advance of the 24-hour deadline. Actually, shippers are building buffer periods in their logistics operations to account for the rule. The buffer period often extends beyond the 24-hour period given that carriers require shippers to provide data even earlier so that they have time to re-key and transmit the data to the American customs. All of the above factors have led some analysts to predict that the overall cost of the 24-hour rule will be in the order of $5-10 billion per year. (CI-Online, 2003) The costs are estimated as:

Investment costs and Maintenance costs: "*Extremely high*"

Appendix 3. Safety Rule-Base with Belief Structure

Rule No	Antecedent attribute (input)				Safety estimate (output)			
	W	D	R	P	Poor	Fair	Average	Good
1	Very weak	Negligible	Easy	Unlikely				1
2	Very weak	Negligible	Easy	Average			0.1	0.9
3	Very weak	Negligible	Easy	Likely			0.15	0.85
4	Very weak	Negligible	Easy	Definite			0.2	0.8
5	Very weak	Negligible	Average	Unlikely			0.1	0.9
6	Very weak	Negligible	Average	Average			0.2	0.8
7	Very weak	Negligible	Average	Likely			0.25	0.75
8	Very weak	Negligible	Average	Definite			0.3	0.7
9	Very weak	Negligible	Difficult	Unlikely			0.15	0.85
10	Very weak	Negligible	Difficult	Average			0.25	0.75
11	Very weak	Negligible	Difficult	Likely			0.3	0.7
12	Very weak	Negligible	Difficult	Definite			0.35	0.65
13	Very weak	Negligible	Extremely Difficult	Unlikely			0.2	0.8
14	Very weak	Negligible	Extremely Difficult	Average			0.3	0.7
15	Very weak	Negligible	Extremely Difficult	Likely			0.35	0.65
16	Very weak	Negligible	Extremely Difficult	Definite			0.45	0.55
17	Very weak	Moderate	Easy	Unlikely			0.3	0.7
18	Very weak	Moderate	Easy	Average			0.5	0.5
19	Very weak	Moderate	Easy	Likely			0.55	0.45
20	Very weak	Moderate	Easy	Definite			0.6	0.4
21	Very weak	Moderate	Average	Unlikely			0.5	0.5
22	Very weak	Moderate	Average	Average			0.7	0.3
23	Very weak	Moderate	Average	Likely			0.75	0.25
24	Very weak	Moderate	Average	Definite			0.8	0.2
25	Very weak	Moderate	Difficult	Unlikely			0.55	0.45
26	Very weak	Moderate	Difficult	Average			0.75	0.25
27	Very weak	Moderate	Difficult	Likely			0.8	0.2
28	Very weak	Moderate	Difficult	Definite			0.9	0.1
29	Very weak	Moderate	Extremely Difficult	Unlikely			0.6	0.4
30	Very weak	Moderate	Extremely Difficult	Average			0.8	0.2
31	Very weak	Moderate	Extremely Difficult	Likely			0.9	0.1
32	Very weak	Moderate	Extremely Difficult	Definite			1	
33	Very weak	Critical	Easy	Unlikely		0.2	0.5	0.3
34	Very weak	Critical	Easy	Average		0.2	0.7	0.1
35	Very weak	Critical	Easy	Likely		0.35	0.65	
36	Very weak	Critical	Easy	Definite		0.6	0.4	
37	Very weak	Critical	Average	Unlikely		0.2	0.7	0.1
38	Very weak	Critical	Average	Average		0.3	0.7	
39	Very weak	Critical	Average	Likely		0.5	0.5	
40	Very weak	Critical	Average	Definite		0.65	0.35	
41	Very weak	Critical	Difficult	Unlikely		0.35	0.65	
42	Very weak	Critical	Difficult	Average		0.5	0.5	
43	Very weak	Critical	Difficult	Likely		0.6	0.4	
44	Very weak	Critical	Difficult	Definite		0.7	0.3	
45	Very weak	Critical	Extremely Difficult	Unlikely		0.5	0.5	
46	Very weak	Critical	Extremely Difficult	Average		0.55	0.45	
47	Very weak	Critical	Extremely Difficult	Likely		0.6	0.4	
48	Very weak	Critical	Extremely Difficult	Definite		0.7	0.3	
49	Very weak	Catastrophic	Easy	Unlikely		0.3	0.7	
50	Very weak	Catastrophic	Easy	Average		0.35	0.65	
51	Very weak	Catastrophic	Easy	Likely		0.4	0.6	
52	Very weak	Catastrophic	Easy	Definite		0.5	0.5	
53	Very weak	Catastrophic	Average	Unlikely		0.35	0.65	
54	Very weak	Catastrophic	Average	Average		0.4	0.6	
55	Very weak	Catastrophic	Average	Likely		0.5	0.5	
56	Very weak	Catastrophic	Average	Definite		0.7	0.3	
57	Very weak	Catastrophic	Difficult	Unlikely		0.4	0.6	
58	Very weak	Catastrophic	Difficult	Average		0.5	0.5	
59	Very weak	Catastrophic	Difficult	Likely		0.7	0.3	

60	Very weak	Catastrophic	Difficult	Definite		0.9	0.1	
61	Very weak	Catastrophic	Extremely Difficult	Unlikely		0.5	0.5	
62	Very weak	Catastrophic	Extremely Difficult	Average		0.7	0.3	
63	Very weak	Catastrophic	Extremely Difficult	Likely		0.9	0.1	
64	Very weak	Catastrophic	Extremely Difficult	Definite		1		
65	Weak	Negligible	Easy	Unlikely			0.05	0.95
66	Weak	Negligible	Easy	Average			0.2	0.8
67	Weak	Negligible	Easy	Likely			0.25	0.75
68	Weak	Negligible	Easy	Definite			0.3	0.7
69	Weak	Negligible	Average	Unlikely			0.2	0.8
70	Weak	Negligible	Average	Average			0.35	0.65
71	Weak	Negligible	Average	Likely			0.4	0.6
72	Weak	Negligible	Average	Definite			0.45	0.55
73	Weak	Negligible	Difficult	Unlikely			0.25	0.75
74	Weak	Negligible	Difficult	Average			0.4	0.6
75	Weak	Negligible	Difficult	Likely			0.45	0.55
76	Weak	Negligible	Difficult	Definite			0.5	0.5
77	Weak	Negligible	Extremely Difficult	Unlikely			0.3	0.7
78	Weak	Negligible	Extremely Difficult	Average			0.45	0.55
79	Weak	Negligible	Extremely Difficult	Likely			0.5	0.5
80	Weak	Negligible	Extremely Difficult	Definite			0.55	0.45
81	Weak	Moderate	Easy	Unlikely			0.4	0.6
82	Weak	Moderate	Easy	Average			0.6	0.4
83	Weak	Moderate	Easy	Likely			0.75	0.25
84	Weak	Moderate	Easy	Definite			0.7	0.3
85	Weak	Moderate	Average	Unlikely			0.6	0.4
86	Weak	Moderate	Average	Average			0.8	0.2
87	Weak	Moderate	Average	Likely			0.9	0.1
88	Weak	Moderate	Average	Definite			1	
89	Weak	Moderate	Difficult	Unlikely			0.65	0.35
90	Weak	Moderate	Difficult	Average			0.9	0.1
91	Weak	Moderate	Difficult	Likely			1	
92	Weak	Moderate	Difficult	Definite		0.1	0.9	
93	Weak	Moderate	Extremely Difficult	Unlikely			0.7	0.3
94	Weak	Moderate	Extremely Difficult	Average			1	
95	Weak	Moderate	Extremely Difficult	Likely		0.1	0.9	
96	Weak	Moderate	Extremely Difficult	Definite		0.2	0.8	
97	Weak	Critical	Easy	Unlikely		0.2	0.6	0.2
98	Weak	Critical	Easy	Average		0.2	0.8	
99	Weak	Critical	Easy	Likely		0.4	0.6	
100	Weak	Critical	Easy	Definite		0.45	0.55	
101	Weak	Critical	Average	Unlikely		0.2	0.8	
102	Weak	Critical	Average	Average		0.25	0.75	
103	Weak	Critical	Average	Likely		0.45	0.55	
104	Weak	Critical	Average	Definite		0.65	0.35	
105	Weak	Critical	Difficult	Unlikely		0.4	0.6	
106	Weak	Critical	Difficult	Average		0.5	0.5	
107	Weak	Critical	Difficult	Likely		0.6	0.4	
108	Weak	Critical	Difficult	Definite		0.7	0.3	
109	Weak	Critical	Extremely Difficult	Unlikely		0.45	0.55	
110	Weak	Critical	Extremely Difficult	Average		0.65	0.35	
111	Weak	Critical	Extremely Difficult	Likely		0.7	0.3	
112	Weak	Critical	Extremely Difficult	Definite		0.8	0.2	
113	Weak	Catastrophic	Easy	Unlikely		0.3	0.6	0.1
114	Weak	Catastrophic	Easy	Average		0.35	0.65	
115	Weak	Catastrophic	Easy	Likely		0.5	0.5	
116	Weak	Catastrophic	Easy	Definite		0.6	0.4	
117	Weak	Catastrophic	Average	Unlikely		0.35	0.65	
118	Weak	Catastrophic	Average	Average	0.2	0.1	0.65	
119	Weak	Catastrophic	Average	Likely	0.3	0.2	0.5	
120	Weak	Catastrophic	Average	Definite	0.2	0.5	0.3	
121	Weak	Catastrophic	Difficult	Unlikely		0.5	0.5	
122	Weak	Catastrophic	Difficult	Average	0.3	0.2	0.5	
123	Weak	Catastrophic	Difficult	Likely	0.4	0.3	0.3	
124	Weak	Catastrophic	Difficult	Definite	0.5	0.4	0.1	
125	Weak	Catastrophic	Extremely Difficult	Unlikely		0.6	0.4	

126	Weak	Catastrophic	Extremely Difficult	Average	0.2	0.5	0.3	
127	Weak	Catastrophic	Extremely Difficult	Likely	0.5	0.4	0.1	
128	Weak	Catastrophic	Extremely Difficult	Definite	0.6	0.4		
129	Average	Negligible	Easy	Unlikely			0.3	0.7
130	Average	Negligible	Easy	Average			0.5	0.5
131	Average	Negligible	Easy	Likely			0.55	0.45
132	Average	Negligible	Easy	Definite			0.6	0.4
133	Average	Negligible	Average	Unlikely			0.5	0.5
134	Average	Negligible	Average	Average			0.7	0.3
135	Average	Negligible	Average	Likely			0.75	0.25
136	Average	Negligible	Average	Definite			0.8	0.2
137	Average	Negligible	Difficult	Unlikely			0.55	0.45
138	Average	Negligible	Difficult	Average			0.75	0.25
139	Average	Negligible	Difficult	Likely		0.2	0.8	
140	Average	Negligible	Difficult	Definite		0.3	0.7	
141	Average	Negligible	Extremely Difficult	Unlikely			0.6	0.4
142	Average	Negligible	Extremely Difficult	Average			0.8	0.2
143	Average	Negligible	Extremely Difficult	Likely		0.3	0.7	
144	Average	Negligible	Extremely Difficult	Definite		0.4	0.6	
145	Average	Moderate	Easy	Unlikely			0.75	0.25
146	Average	Moderate	Easy	Average			0.9	0.1
147	Average	Moderate	Easy	Likely		0.05	0.95	
148	Average	Moderate	Easy	Definite		0.1	0.9	
149	Average	Moderate	Average	Unlikely			0.9	0.1
150	Average	Moderate	Average	Average			1	
151	Average	Moderate	Average	Likely		0.1	0.9	
152	Average	Moderate	Average	Definite		0.15	0.85	
153	Average	Moderate	Difficult	Unlikely		0.05	0.95	
154	Average	Moderate	Difficult	Average		0.1	0.9	
155	Average	Moderate	Difficult	Likely		0.25	0.75	
156	Average	Moderate	Difficult	Definite		0.3	0.7	
157	Average	Moderate	Extremely Difficult	Unlikely		0.1	0.9	
158	Average	Moderate	Extremely Difficult	Average		0.15	0.85	
159	Average	Moderate	Extremely Difficult	Likely		0.3	0.7	
160	Average	Moderate	Extremely Difficult	Definite		0.4	0.6	
161	Average	Critical	Easy	Unlikely		0.35	0.35	0.3
162	Average	Critical	Easy	Average		0.35	0.55	0.1
163	Average	Critical	Easy	Likely		0.55	0.35	0.1
164	Average	Critical	Easy	Definite		0.5	0.5	
165	Average	Critical	Average	Unlikely		0.35	0.55	0.1
166	Average	Critical	Average	Average		0.3	0.7	
167	Average	Critical	Average	Likely		0.5	0.5	
168	Average	Critical	Average	Definite	0.1	0.35	0.55	
169	Average	Critical	Difficult	Unlikely		0.55	0.35	0.1
170	Average	Critical	Difficult	Average		0.5	0.5	
171	Average	Critical	Difficult	Likely		0.7	0.3	
172	Average	Critical	Difficult	Definite	0.1	0.55	0.35	
173	Average	Critical	Extremely Difficult	Unlikely		0.5	0.5	
174	Average	Critical	Extremely Difficult	Average	0.1	0.35	0.55	
175	Average	Critical	Extremely Difficult	Likely	0.1	0.55	0.35	
176	Average	Critical	Extremely Difficult	Definite	0.3	0.35	0.35	
177	Average	Catastrophic	Easy	Unlikely		0.3	0.7	
178	Average	Catastrophic	Easy	Average		0.4	0.6	
179	Average	Catastrophic	Easy	Likely		0.55	0.45	
180	Average	Catastrophic	Easy	Definite	0.1	0.5	0.4	
181	Average	Catastrophic	Average	Unlikely		0.4	0.6	
182	Average	Catastrophic	Average	Average	0.3		0.7	
183	Average	Catastrophic	Average	Likely	0.35	0.1	0.55	
184	Average	Catastrophic	Average	Definite	0.5		0.5	
185	Average	Catastrophic	Difficult	Unlikely		0.55	0.45	
186	Average	Catastrophic	Difficult	Average	0.35	0.1	0.55	
187	Average	Catastrophic	Difficult	Likely	0.35	0.3	0.35	
188	Average	Catastrophic	Difficult	Definite	0.55	0.1	0.35	
189	Average	Catastrophic	Extremely Difficult	Unlikely	0.1	0.5	0.4	
190	Average	Catastrophic	Extremely Difficult	Average	0.5		0.5	
191	Average	Catastrophic	Extremely Difficult	Likely	0.55	0.1	0.35	

192	Average	Catastrophic	Extremely Difficult	Definite	0.7		0.3	
193	Strong	Negligible	Easy	Unlikely		0.2	0.1	0.7
194	Strong	Negligible	Easy	Average		0.25	0.25	0.5
195	Strong	Negligible	Easy	Likely		0.4	0.1	0.5
196	Strong	Negligible	Easy	Definite		0.4	0.2	0.4
197	Strong	Negligible	Average	Unlikely		0.25	0.25	0.5
198	Strong	Negligible	Average	Average		0.25	0.4	0.35
199	Strong	Negligible	Average	Likely		0.45	0.25	0.3
200	Strong	Negligible	Average	Definite		0.4	0.6	
201	Strong	Negligible	Difficult	Unlikely		0.4	0.1	0.5
202	Strong	Negligible	Difficult	Average		0.45	0.25	0.3
203	Strong	Negligible	Difficult	Likely		0.6	0.1	0.3
204	Strong	Negligible	Difficult	Definite		0.6	0.4	
205	Strong	Negligible	Extremely Difficult	Unlikely		0.4	0.2	0.4
206	Strong	Negligible	Extremely Difficult	Average		0.4	0.6	
207	Strong	Negligible	Extremely Difficult	Likely		0.6	0.4	
208	Strong	Negligible	Extremely Difficult	Definite	0.1	0.6	0.3	
209	Strong	Moderate	Easy	Unlikely		0.25	0.45	0.3
210	Strong	Moderate	Easy	Average		0.25	0.65	0.1
211	Strong	Moderate	Easy	Likely		0.45	0.45	0.1
212	Strong	Moderate	Easy	Definite		0.4	0.6	
213	Strong	Moderate	Average	Unlikely		0.25	0.65	0.1
214	Strong	Moderate	Average	Average		0.2	0.8	
215	Strong	Moderate	Average	Likely		0.4	0.6	
216	Strong	Moderate	Average	Definite	0.1	0.25	0.65	
217	Strong	Moderate	Difficult	Unlikely		0.45	0.45	0.1
218	Strong	Moderate	Difficult	Average		0.4	0.6	
219	Strong	Moderate	Difficult	Likely		0.6	0.4	
220	Strong	Moderate	Difficult	Definite	0.15	0.4	0.45	
221	Strong	Moderate	Extremely Difficult	Unlikely		0.4	0.6	
222	Strong	Moderate	Extremely Difficult	Average	0.1	0.25	0.65	
223	Strong	Moderate	Extremely Difficult	Likely	0.15	0.4	0.45	
224	Strong	Moderate	Extremely Difficult	Definite	0.3	0.25	0.45	
225	Strong	Critical	Easy	Unlikely		0.65	0.1	0.25
226	Strong	Critical	Easy	Average		0.65	0.2	0.15
227	Strong	Critical	Easy	Likely		0.8	0.1	0.1
228	Strong	Critical	Easy	Definite		0.8	0.2	
229	Strong	Critical	Average	Unlikely		0.65	0.2	0.15
230	Strong	Critical	Average	Average		0.65	0.35	
231	Strong	Critical	Average	Likely		0.8	0.2	
232	Strong	Critical	Average	Definite	0.15	0.65	0.2	
233	Strong	Critical	Difficult	Unlikely		0.8	0.1	0.1
234	Strong	Critical	Difficult	Average		0.8	0.2	
235	Strong	Critical	Difficult	Likely		0.95	0.05	
236	Strong	Critical	Difficult	Definite	0.15	0.8	0.05	
237	Strong	Critical	Extremely Difficult	Unlikely		0.8	0.2	
238	Strong	Critical	Extremely Difficult	Average	0.15	0.65	0.2	
239	Strong	Critical	Extremely Difficult	Likely	0.15	0.8	0.05	
240	Strong	Critical	Extremely Difficult	Definite	0.25	0.65	0.1	
241	Strong	Catastrophic	Easy	Unlikely		0.6	0.4	
242	Strong	Catastrophic	Easy	Average	0.2	0.4	0.4	
243	Strong	Catastrophic	Easy	Likely	0.25	0.55	0.2	
244	Strong	Catastrophic	Easy	Definite	0.4	0.4	0.2	
245	Strong	Catastrophic	Average	Unlikely	0.2	0.4	0.4	
246	Strong	Catastrophic	Average	Average	0.35	0.25	0.4	
247	Strong	Catastrophic	Average	Likely	0.35	0.4	0.25	
248	Strong	Catastrophic	Average	Definite	0.5	0.25	0.25	
249	Strong	Catastrophic	Difficult	Unlikely	0.25	0.55	0.2	
250	Strong	Catastrophic	Difficult	Average	0.35	0.45	0.2	
251	Strong	Catastrophic	Difficult	Likely	0.3	0.6	0.1	
252	Strong	Catastrophic	Difficult	Definite	0.5	0.4	0.1	
253	Strong	Catastrophic	Extremely Difficult	Unlikely	0.4	0.4	0.2	
254	Strong	Catastrophic	Extremely Difficult	Average	0.5	0.25	0.25	
255	Strong	Catastrophic	Extremely Difficult	Likely	0.5	0.4	0.1	
256	Strong	Catastrophic	Extremely Difficult	Definite	0.7	0.2	0.1	
257	Very strong	Negligible	Easy	Unlikely		0.3	0.3	0.4

258	Very strong	Negligible	Easy	Average		0.3	0.5	0.2
259	Very strong	Negligible	Easy	Likely		0.5	0.4	0.1
260	Very strong	Negligible	Easy	Definite		0.5	0.5	
261	Very strong	Negligible	Average	Unlikely		0.3	0.5	0.2
262	Very strong	Negligible	Average	Average		0.35	0.65	
263	Very strong	Negligible	Average	Likely		0.5	0.5	
264	Very strong	Negligible	Average	Definite	0.2	0.3	0.5	
265	Very strong	Negligible	Difficult	Unlikely		0.5	0.4	0.1
266	Very strong	Negligible	Difficult	Average		0.5	0.5	
267	Very strong	Negligible	Difficult	Likely		0.65	0.35	
268	Very strong	Negligible	Difficult	Definite	0.2	0.5	0.3	
269	Very strong	Negligible	Extremely Difficult	Unlikely		0.5	0.5	
270	Very strong	Negligible	Extremely Difficult	Average	0.2	0.3	0.5	
271	Very strong	Negligible	Extremely Difficult	Likely	0.2	0.5	0.3	
272	Very strong	Negligible	Extremely Difficult	Definite	0.4	0.3	0.3	
273	Very strong	Moderate	Easy	Unlikely		0.35	0.65	
274	Very strong	Moderate	Easy	Average	0.15	0.15	0.7	
275	Very strong	Moderate	Easy	Likely	0.2	0.3	0.5	
276	Very strong	Moderate	Easy	Definite	0.35	0.15	0.5	
277	Very strong	Moderate	Average	Unlikely	0.15	0.15	0.7	
278	Very strong	Moderate	Average	Average		0.6	0.4	
279	Very strong	Moderate	Average	Likely	0.35	0.15	0.5	
280	Very strong	Moderate	Average	Definite	0.2	0.6	0.2	
281	Very strong	Moderate	Difficult	Unlikely	0.2	0.3	0.5	
282	Very strong	Moderate	Difficult	Average	0.35	0.15	0.5	
283	Very strong	Moderate	Difficult	Likely	0.35	0.3	0.35	
284	Very strong	Moderate	Difficult	Definite	0.55	0.15	0.3	
285	Very strong	Moderate	Extremely Difficult	Unlikely	0.35	0.15	0.5	
286	Very strong	Moderate	Extremely Difficult	Average	0.2	0.6	0.2	
287	Very strong	Moderate	Extremely Difficult	Likely	0.55	0.15	0.3	
288	Very strong	Moderate	Extremely Difficult	Definite	0.4	0.6		
289	Very strong	Critical	Easy	Unlikely		0.7	0.3	
290	Very strong	Critical	Easy	Average	0.2	0.5	0.3	
291	Very strong	Critical	Easy	Likely	0.2	0.65	0.15	
292	Very strong	Critical	Easy	Definite	0.4	0.45	0.15	
293	Very strong	Critical	Average	Unlikely	0.2	0.5	0.3	
294	Very strong	Critical	Average	Average	0.35	0.35	0.3	
295	Very strong	Critical	Average	Likely	0.35	0.55	0.1	
296	Very strong	Critical	Average	Definite	0.55	0.35	0.1	
297	Very strong	Critical	Difficult	Unlikely	0.2	0.65	0.15	
298	Very strong	Critical	Difficult	Average	0.35	0.55	0.1	
299	Very strong	Critical	Difficult	Likely	0.3	0.7		
300	Very strong	Critical	Difficult	Definite	0.5	0.5		
301	Very strong	Critical	Extremely Difficult	Unlikely	0.4	0.45	0.15	
302	Very strong	Critical	Extremely Difficult	Average	0.55	0.35	0.1	
303	Very strong	Critical	Extremely Difficult	Likely	0.5	0.5		
304	Very strong	Critical	Extremely Difficult	Definite	0.7	0.3		
305	Very strong	Catastrophic	Easy	Unlikely	0.5	0.25	0.25	
306	Very strong	Catastrophic	Easy	Average	0.65	0.1	0.25	
307	Very strong	Catastrophic	Easy	Likely	0.7	0.2	0.1	
308	Very strong	Catastrophic	Easy	Definite	0.8	0.1	0.1	
309	Very strong	Catastrophic	Average	Unlikely	0.65	0.1	0.25	
310	Very strong	Catastrophic	Average	Average	0.6	0.4		
311	Very strong	Catastrophic	Average	Likely	0.7	0.3		
312	Very strong	Catastrophic	Average	Definite	0.85	0.15		
313	Very strong	Catastrophic	Difficult	Unlikely	0.7	0.2	0.1	
314	Very strong	Catastrophic	Difficult	Average	0.7	0.3		
315	Very strong	Catastrophic	Difficult	Likely	0.75	0.25		
316	Very strong	Catastrophic	Difficult	Definite	0.9	0.1		
317	Very strong	Catastrophic	Extremely Difficult	Unlikely	0.8	0.1	0.1	
318	Very strong	Catastrophic	Extremely Difficult	Average	0.85	0.15		
319	Very strong	Catastrophic	Extremely Difficult	Likely	0.9	0.1		
320	Very strong	Catastrophic	Extremely Difficult	Definite	1			

Appendix 4. Risk Based *BRB*

Rules	**Antecedent attributes**			**Risk evaluation (using the *FER* method)**				**Risk evaluation (using subjective judgement)**			
No	Risk occurrence likelihood	Consequence severity	Failure consequence probability	Good	Ave rage	Fair	Poor	Good	Ave rage	Fair	Poor
1	very low	negligible	highly unlikely	1				1			
2	very low	negligible	unlikely	0.91	0.09			0.8	0.2		
3	very low	negligible	reasonably unlikely	0.88	0.12			0.7	0.2	0.1	
4	very low	negligible	likely	0.88	0.06	0.06		0.3	0.7		
5	very low	negligible	reasonably likely	0.88		0.12		0.1	0.9		
6	very low	negligible	highly likely	0.88		0.06	0.06	0.1	0.8	0.1	
7	very low	negligible	definite	0.88			0.12		1		
8	very low	marginal	highly unlikely	0.72	0.28			0.9	0.1		
9	very low	marginal	unlikely	0.54	0.46			0.8	0.1		
10	very low	marginal	reasonably unlikely	0.49	0.51			0.7	0.3		
11	very low	marginal	likely	0.51	0.42	0.07		0.5	0.5		
12	very low	marginal	reasonably likely	0.53	0.32	0.15		0.4	0.6		
13	very low	marginal	highly likely	0.53	0.32	0.08	0.07	0.2	0.8		
14	very low	marginal	definite	0.53	0.32		0.15	0.1	0.9		
15	very low	moderate	highly unlikely	0.62	0.19	0.19		0.8	0.2		
16	very low	moderate	unlikely	0.45	0.35	0.2		0.7	0.3		
17	very low	moderate	reasonably unlikely	0.4	0.4	0.2		0.6	0.4		
18	very low	moderate	likely	0.4	0.3	0.3		0.2	0.6	0.2	
19	very low	moderate	reasonably likely	0.4	0.2	0.4			0.5	0.5	
20	very low	moderate	highly likely	0.41	0.2	0.31	0.08		0.3	0.7	
21	very low	moderate	definite	0.42	0.21	0.21	0.16		0.1	0.9	
22	very low	critical	highly unlikely	0.62		0.3	0.08		1		
23	very low	critical	unlikely	0.46	0.12	0.33	0.08		0.9	0.1	
24	very low	critical	reasonably unlikely	0.42	0.16	0.34	0.08		0.7	0.3	
25	very low	critical	likely	0.4	0.08	0.44	0.08		0.3	0.7	
26	very low	critical	reasonably likely	0.39		0.53	0.08		0.2	0.8	
27	very low	critical	highly likely	0.4		0.44	0.16			0.4	0.6
28	very low	critical	definite	0.41		0.33	0.26			0.3	0.7
29	very low	catastrophic	highly unlikely	0.62			0.38		0.8	0.2	
30	very low	catastrophic	unlikely	0.47	0.12		0.41		0.6	0.4	
31	very low	catastrophic	reasonably unlikely	0.42	0.16		0.42		0.3	0.7	
32	very low	catastrophic	likely	0.42	0.08	0.08	0.42		0.2	0.8	
33	very low	catastrophic	reasonably likely	0.42		0.16	0.42			1	
34	very low	catastrophic	highly likely	0.4		0.08	0.52			0.4	0.6
35	very low	catastrophic	definite	0.38			0.62			0.2	0.8
36	low	negligible	highly unlikely	0.72	0.28			0.8	0.2		
37	low	negligible	unlikely	0.54	0.46			0.7	0.3		
38	low	negligible	reasonably unlikely	0.49	0.51			0.6	0.4		
39	low	negligible	likely	0.51	0.42	0.07		0.3	0.7		
40	low	negligible	reasonably likely	0.53	0.32	0.15		0.2	0.8		
41	low	negligible	highly likely	0.53	0.32	0.08	0.07	0.1	0.9		
42	low	negligible	definite	0.53	0.32		0.15		1		
43	low	marginal	highly unlikely	0.31	0.69			0.8	0.2		
44	low	marginal	unlikely	0.16	0.84			0.7	0.3		
45	low	marginal	reasonably unlikely	0.13	0.87			0.6	0.4		
46	low	marginal	likely	0.14	0.8	0.06		0.3	0.7		
47	low	marginal	reasonably likely	0.15	0.72	0.13		0.2	0.8		
48	low	marginal	highly likely	0.15	0.72	0.07	0.06	0.1	0.9		
49	low	marginal	definite	0.15	0.72		0.13	0.1	0.8	0.1	
50	low	moderate	highly unlikely	0.23	0.58	0.19		0.7	0.3		
51	low	moderate	unlikely	0.1	0.73	0.17		0.3	0.7		
52	low	moderate	reasonably unlikely	0.07	0.77	0.16			0.6	0.4	
53	low	moderate	likely	0.07	0.67	0.26			0.5	0.5	
54	low	moderate	reasonably likely	0.07	0.57	0.36			0.2	0.8	
55	low	moderate	highly likely	0.07	0.58	0.28	0.07		0.1	0.9	

56	low	moderate	definite	0.08	0.59	0.19	0.14			1	
57	low	critical	highly unlikely	0.26	0.33	0.33	0.08		0.8	0.2	
58	low	critical	unlikely	0.11	0.5	0.31	0.08		0.6	0.4	
59	low	critical	reasonably unlikely	0.08	0.53	0.31	0.08		0.2	0.8	
60	low	critical	likely	0.08	0.42	0.42	0.08			0.6	0.4
61	low	critical	reasonably likely	0.08	0.31	0.53	0.08			0.5	0.5
62	low	critical	highly likely	0.08	0.32	0.44	0.16			0.3	0.7
63	low	critical	definite	0.08	0.33	0.33	0.26			0.2	0.8
64	low	catastrophic	highly unlikely	0.26	0.33		0.41		0.6	0.4	
65	low	catastrophic	unlikely	0.11	0.5		0.39		0.1	0.9	
66	low	catastrophic	reasonably unlikely	0.08	0.53		0.39			0.9	0.1
67	low	catastrophic	likely	0.08	0.44	0.08	0.4			0.7	0.3
68	low	catastrophic	reasonably likely	0.08	0.34	0.16	0.42			0.3	0.7
69	low	catastrophic	highly likely	0.08	0.32	0.08	0.52			0.3	0.7
70	low	catastrophic	definite	0.08	0.3		0.62			0.2	0.8
71	reasonably low	negligible	highly unlikely	0.62	0.38			0.8	0.2		
72	reasonably low	negligible	unlikely	0.43	0.57			0.7	0.3		
73	reasonably low	negligible	reasonably unlikely	0.38	0.62			0.6	0.4		
74	reasonably low	negligible	likely	0.4	0.52	0.08		0.3	0.7		
75	reasonably low	negligible	reasonably likely	0.42	0.42	0.16		0.1	0.9		
76	reasonably low	negligible	highly likely	0.42	0.42	0.08	0.08		1		
77	reasonably low	negligible	definite	0.42	0.42		0.16		0.9	0.1	
78	reasonably low	marginal	highly unlikely	0.21	0.79			0.8	0.2		
79	reasonably low	marginal	unlikely	0.08	0.92			0.7	0.3		
80	reasonably low	marginal	reasonably unlikely	0.06	0.94			0.6	0.4		
81	reasonably low	marginal	likely	0.06	0.88	0.06		0.2	0.8		
82	reasonably low	marginal	reasonably likely	0.07	0.8	0.13			1		
83	reasonably low	marginal	highly likely	0.07	0.8	0.07	0.06		0.9	0.1	
84	reasonably low	marginal	definite	0.07	0.8		0.13		0.8	0.2	
85	reasonably low	moderate	highly unlikely	0.14	0.68	0.18		0.5	0.5		
86	reasonably low	moderate	unlikely	0.03	0.81	0.16		0.6	0.4		
87	reasonably low	moderate	reasonably unlikely		0.84	0.16		0.4	0.6		
88	reasonably low	moderate	likely		0.75	0.25			0.7	0.3	
89	reasonably low	moderate	reasonably likely		0.65	0.35			0.4	0.6	
90	reasonably low	moderate	highly likely		0.66	0.27	0.07			1	
91	reasonably low	moderate	definite		0.68	0.18	0.14			0.6	0.4
92	reasonably low	critical	highly unlikely	0.16	0.42	0.34	0.08		1		
93	reasonably low	critical	unlikely	0.03	0.58	0.31	0.08		0.7	0.3	
94	reasonably low	critical	reasonably unlikely		0.62	0.3	0.08		0.5	0.5	
95	reasonably low	critical	likely		0.5	0.42	0.08			1	
96	reasonably low	critical	reasonably likely		0.39	0.53	0.08		0.1	0.2	0.7
97	reasonably low	critical	highly likely		0.4	0.44	0.16		0.1	0.1	0.8
98	reasonably low	critical	definite		0.41	0.33	0.26			0.1	0.9
99	reasonably low	catastrophic	highly unlikely	0.16	0.42		0.42		1		
100	reasonably low	catastrophic	unlikely	0.03	0.58		0.39		0.3	0.7	
101	reasonably low	catastrophic	reasonably unlikely		0.62		0.38		0.1	0.9	
102	reasonably low	catastrophic	likely		0.53	0.07	0.4			0.5	0.5
103	reasonably low	catastrophic	reasonably likely		0.42	0.16	0.42			0.3	0.7
104	reasonably low	catastrophic	highly likely		0.4	0.08	0.52			0.2	0.8
105	reasonably low	catastrophic	definite		0.38		0.62			0.1	0.9
106	average	negligible	highly unlikely	0.62	0.19	0.19		0.1	0.9		
107	average	negligible	unlikely	0.44	0.36	0.2			0.8	0.2	
108	average	negligible	reasonably unlikely	0.4	0.4	0.2			0.7	0.3	
109	average	negligible	likely	0.4	0.3	0.3			0.5	0.5	
110	average	negligible	reasonably likely	0.4	0.2	0.4			0.3	0.7	
111	average	negligible	highly likely	0.41	0.2	0.31	0.08		0.2	0.8	
112	average	negligible	definite	0.42	0.21	0.21	0.16		0.0	0.95	
113	average	marginal	highly unlikely	0.23	0.58	0.19			1		
114	average	marginal	unlikely	0.1	0.73	0.17			0.8	0.2	
115	average	marginal	reasonably unlikely	0.07	0.77	0.16			0.5	0.5	
116	average	marginal	likely	0.07	0.67	0.26			0.3	0.7	
117	average	marginal	reasonably likely	0.07	0.57	0.36			0.2	0.8	
118	average	marginal	highly likely	0.07	0.58	0.28	0.07		0.1	0.9	
119	average	marginal	definite	0.08	0.59	0.19	0.14			1	

120	average	moderate	highly unlikely	0.14	0.43	0.43			1		
121	average	moderate	unlikely	0.02	0.58	0.4			0.9	0.1	
122	average	moderate	reasonably unlikely		0.61	0.39			0.8	0.2	
123	average	moderate	likely		0.5	0.5			0.5	0.5	
124	average	moderate	reasonably likely		0.39	0.61				1	
125	average	moderate	highly likely		0.41	0.52	0.07			0.9	0.1
126	average	moderate	definite		0.43	0.43	0.14			0.8	0.2
127	average	critical	highly unlikely	0.14	0.19	0.59	0.08		0.8	0.2	
128	average	critical	unlikely	0.03	0.33	0.57	0.07		1		
129	average	critical	reasonably unlikely		0.36	0.57	0.07		0.2	0.8	
130	average	critical	likely		0.26	0.67	0.07			1	
131	average	critical	reasonably likely		0.16	0.77	0.07			0.5	0.5
132	average	critical	highly likely		0.18	0.68	0.14			0.3	0.7
133	average	critical	definite		0.19	0.58	0.23			0.2	0.8
134	average	catastrophic	highly unlikely	0.16	0.21	0.21	0.42		0.8	0.2	
135	average	catastrophic	unlikely	0.03	0.36	0.2	0.41		0.6	0.4	
136	average	catastrophic	reasonably unlikely		0.4	0.2	0.4		0.5	0.5	
137	average	catastrophic	likely		0.3	0.3	0.4			0.5	0.5
138	average	catastrophic	reasonably likely		0.2	0.4	0.4			0.4	0.6
139	average	catastrophic	highly likely		0.2	0.29	0.51			0.2	0.8
140	average	catastrophic	definite		0.19	0.19	0.62			0.15	0.85
141	reasonably frequent	negligible	highly unlikely	0.62		0.38			1		
142	reasonably frequent	negligible	unlikely	0.47	0.12	0.41			0.8	0.2	
143	reasonably frequent	negligible	reasonably unlikely	0.42	0.16	0.42			0.6	0.4	
144	reasonably frequent	negligible	likely	0.4	0.08	0.52			0.3	0.7	
145	reasonably frequent	negligible	reasonably likely	0.38		0.62			0.1	0.9	
146	reasonably frequent	negligible	highly likely	0.4		0.52	0.08			1	
147	reasonably frequent	negligible	definite	0.42		0.42	0.16			0.9	0.1
148	reasonably frequent	marginal	highly unlikely	0.26	0.33	0.41			0.8	0.2	
149	reasonably frequent	marginal	unlikely	0.11	0.5	0.39			0.5	0.5	
150	reasonably frequent	marginal	reasonably unlikely	0.08	0.53	0.39			0.3	0.7	
151	reasonably frequent	marginal	likely	0.08	0.42	0.5			0.1	0.9	
152	reasonably frequent	marginal	reasonably likely	0.08	0.3	0.62				1	
153	reasonably frequent	marginal	highly likely	0.08	0.32	0.52	0.08			0.9	0.1
154	reasonably frequent	marginal	definite	0.08	0.34	0.42	0.16			0.8	0.2
155	reasonably frequent	moderate	highly unlikely	0.14	0.18	0.68			0.5	0.5	
156	reasonably frequent	moderate	unlikely	0.03	0.32	0.65			0.4	0.6	
157	reasonably frequent	moderate	reasonably unlikely		0.35	0.65			0.2	0.8	
158	reasonably frequent	moderate	likely		0.25	0.75			0.1	0.9	
159	reasonably frequent	moderate	reasonably likely		0.16	0.84				1	
160	reasonably frequent	moderate	highly likely		0.17	0.77	0.06		0.2	0.7	0.1
161	reasonably frequent	moderate	definite		0.18	0.68	0.14			0.8	0.2
162	reasonably frequent	critical	highly unlikely	0.13		0.8	0.07		0.7	0.3	
163	reasonably frequent	critical	unlikely	0.03	0.10	0.8	0.07		0.5	0.5	
164	reasonably frequent	critical	reasonably unlikely		0.13	0.8	0.07		0.1	0.9	
165	reasonably frequent	critical	likely		0.06	0.88	0.06			0.8	0.2
166	reasonably frequent	critical	reasonably likely			0.94	0.06			0.5	0.5
167	reasonably frequent	critical	highly likely			0.87	0.13			0.4	0.6
168	reasonably frequent	critical	definite			0.79	0.21			0.3	0.7
169	reasonably frequent	catastrophic	highly unlikely	0.16		0.42	0.42		0.6	0.4	
170	reasonably frequent	catastrophic	unlikely	0.03	0.13	0.42	0.42		0.5	0.5	
171	reasonably frequent	catastrophic	reasonably unlikely		0.16	0.42	0.42		0.2	0.8	
172	reasonably frequent	catastrophic	likely		0.08	0.52	0.4		0.1	0.8	0.1
173	reasonably frequent	catastrophic	reasonably likely			0.62	0.38			0.9	0.1
174	reasonably frequent	catastrophic	highly likely			0.5	0.5			0.4	0.6
175	reasonably frequent	catastrophic	definite			0.38	0.62			0.3	0.7
176	frequent	negligible	highly unlikely	0.62		0.28	0.1		0.8	0.2	
177	frequent	negligible	unlikely	0.46	0.12	0.31	0.11		0.5	0.5	
178	frequent	negligible	reasonably unlikely	0.42	0.16	0.31	0.11		0.3	0.7	
179	frequent	negligible	likely	0.4	0.08	0.41	0.11		0.1	0.9	
180	frequent	negligible	reasonably likely	0.39		0.5	0.11			0.8	0.2
181	frequent	negligible	highly likely	0.4		0.4	0.2			0.5	0.5
182	frequent	negligible	definite	0.41		0.3	0.29			0.4	0.6
183	frequent	marginal	highly unlikely	0.26	0.33	0.3	0.11		0.8	0.2	

184	frequent	marginal	unlikely	0.11	0.49	0.29	0.11		0.5	0.5	
185	frequent	marginal	reasonably unlikely	0.08	0.53	0.28	0.11		0.3	0.7	
186	frequent	marginal	likely	0.08	0.42	0.39	0.11		0.1	0.9	
187	frequent	marginal	reasonably likely	0.08	0.31	0.5	0.11		0.1	0.8	0.1
188	frequent	marginal	highly likely	0.08	0.32	0.4	0.2		0.8	0.8	0.2
189	frequent	marginal	definite	0.08	0.33	0.3	0.29			0.6	0.4
190	frequent	moderate	highly unlikely	0.14	0.19	0.56	0.11		0.8	0.2	
191	frequent	moderate	unlikely	0.03	0.33	0.54	0.1		0.4	0.6	
192	frequent	moderate	reasonably unlikely		0.36	0.54	0.1		0.3	0.7	
193	frequent	moderate	likely		0.26	0.64	0.1			0.9	0.1
194	frequent	moderate	reasonably likely		0.17	0.74	0.09			0.8	0.2
195	frequent	moderate	highly likely		0.18	0.65	0.17			0.7	0.3
196	frequent	moderate	definite		0.18	0.55	0.27		0.5	0.5	
197	frequent	critical	highly unlikely	0.13		0.69	0.18		0.3	0.6	0.1
198	frequent	critical	unlikely	0.03	0.10	0.69	0.18		0.2	0.7	0.1
199	frequent	critical	reasonably unlikely		0.13	0.69	0.18			0.8	0.2
200	frequent	critical	likely		0.06	0.77	0.17			0.5	0.5
201	frequent	critical	reasonably likely			0.85	0.15			0.3	0.7
202	frequent	critical	highly likely			0.76	0.24		0.1	0.1	0.8
203	frequent	critical	definite			0.66	0.34			0.2	0.8
204	frequent	catastrophic	highly unlikely	0.15		0.28	0.57		0.5	0.5	
205	frequent	catastrophic	unlikely	0.03	0.12	0.28	0.57		0.2	0.6	0.2
206	frequent	catastrophic	reasonably unlikely		0.15	0.28	0.57			0.7	0.3
207	frequent	catastrophic	likely		0.07	0.38	0.55			0.5	0.5
208	frequent	catastrophic	reasonably likely			0.47	0.53			0.4	0.6
209	frequent	catastrophic	highly likely			0.36	0.64			0.3	0.7
210	frequent	catastrophic	definite			0.25	0.75			0.2	0.8
211	highly frequent	negligible	highly unlikely	0.62			0.38		0.8	0.2	
212	highly frequent	negligible	unlikely	0.47	0.12		0.41		0.5	0.5	
213	highly frequent	negligible	reasonably unlikely	0.42	0.16		0.42		0.3	0.7	
214	highly frequent	negligible	likely	0.42	0.08	0.08	0.42		0.3	0.5	0.2
215	highly frequent	negligible	reasonably likely	0.42		0.16	0.42		0.1	0.6	0.3
216	highly frequent	negligible	highly likely	0.4		0.08	0.52			0.4	0.6
217	highly frequent	negligible	definite	0.38			0.62			0.3	0.7
218	highly frequent	marginal	highly unlikely	0.26	0.33		0.41		0.6	0.4	
219	highly frequent	marginal	unlikely	0.11	0.5		0.39		0.5	0.5	
220	highly frequent	marginal	reasonably unlikely	0.08	0.53		0.39		0.4	0.6	
221	highly frequent	marginal	likely	0.08	0.43	0.09	0.4		0.1	0.7	0.2
222	highly frequent	marginal	reasonably likely	0.08	0.34	0.16	0.42			0.9	0.1
223	highly frequent	marginal	highly likely	0.08	0.32	0.08	0.52			0.7	0.3
224	highly frequent	marginal	definite	0.08	0.3		0.62			0.6	0.4
225	highly frequent	moderate	highly unlikely	0.16	0.21	0.21	0.42		0.7	0.3	
226	highly frequent	moderate	unlikely	0.03	0.37	0.2	0.4		0.5	0.5	
227	highly frequent	moderate	reasonably unlikely		0.4	0.2	0.4		0.2	0.6	0.2
228	highly frequent	moderate	likely		0.3	0.3	0.4			0.5	0.5
229	highly frequent	moderate	reasonably likely		0.2	0.4	0.4			0.4	0.6
230	highly frequent	moderate	highly likely		0.2	0.29	0.51			0.3	0.7
231	highly frequent	moderate	definite		0.19	0.19	0.62			0.2	0.8
232	highly frequent	critical	highly unlikely	0.15		0.32	0.53		0.5	0.5	
233	highly frequent	critical	unlikely	0.03	0.12	0.32	0.53		0.2	0.6	0.2
234	highly frequent	critical	reasonably unlikely		0.15	0.32	0.53		0.1	0.5	0.4
235	highly frequent	critical	likely		0.07	0.42	0.51			0.4	0.6
236	highly frequent	critical	reasonably likely			0.51	0.49			0.2	0.8
237	highly frequent	critical	highly likely			0.39	0.61			0.1	0.9
238	highly frequent	critical	definite			0.28	0.72				1
239	highly frequent	catastrophic	highly unlikely	0.12			0.88		0.5	0.3	0.2
240	highly frequent	catastrophic	unlikely	0.02	0.1		0.88			0.5	0.5
241	highly frequent	catastrophic	reasonably unlikely		0.12		0.88			0.4	0.6
242	highly frequent	catastrophic	likely		0.06	0.06	0.88			0.2	0.8
243	highly frequent	catastrophic	reasonably likely			0.12	0.88			0.15	0.85
244	highly frequent	catastrophic	highly likely			0.04	0.96			0.05	0.95
245	highly frequent	catastrophic	definite				1				1

Appendix 5. The Prior Probability Distributions in the BN

The probability distribution of "Intelligence network"	
State	Probability
Flawless	0.8
Flawed	0.2
The probability distribution of "Checking and supervision"	
States	Probabilities
Checked	0.05 (the sum of import and export checking)
Ignored	0.95
The probability distribution of "External"	
States	Probabilities
Friendly	0.99
Hostile	0.01
The probability distribution of "Internal"	
States	Probabilities
Immune	0.9
Infective	0.1
The probability distribution of "Missile"	
States	Probabilities
Yes	0.1
No	0.9
The probability distribution of "Accessibility"	
States	Probabilities
Likely	0.33
Unlikely	0.67

The probability distribution of "Engine room"

People / Engine room	Soundness	Weakness
Hijacked	0	0.2
Defended	1	0.8

The prior conditional probabilities of "Bulkhead"

Missile	Yes		No	
Car-ple / Bulkhead	Soundness	Weakness	Soundness	Weakness
Attacked	0.905	0.999	0.097	0.991
Protected	0.095	0.001	0.903	0.009

The prior conditional probabilities of "Cargo"

Intelligence networks	Flawless		Flawed	
Checking and supervision / Cargo	Checked	Ignored	Checked	Ignored
Soundness	0.96	0.44	0.48	0.02
Weakness	0.04	0.56	0.52	0.98

The prior conditional probabilities of "People"

External	Friendly		Hostile	
Internal / People	Immune	Infective	Immune	Infective
Soundness	0.99	0.27	0.56	0.11
Weakness	0.01	0.73	0.44	0.89

The prior conditional probabilities of "Car-ple"

Cargo	Soundness		Weakness	
People / Car-ple	Soundness	Weakness	Soundness	Weakness
Soundness	1	0.59	0.56	0.28
Weakness	0	0.41	0.44	0.72

The prior conditional probabilities of "Containerships"

Bulkhead	Attacked		Protected	
Engine / room	Hijacked	Defended	Hijacked	Defended

Containerships				
Soundness	0.07	0.39	0.12	1
Weakness	0.93	0.61	0.88	0

The prior conditional probabilities of "Channel"

Containerships / Channel	Soundness	Weakness
Soundness	0.99	0.8
Weakness	0.01	0.2

The prior conditional probabilities of "Terminal"

Containerships	Soundness		Weakness	
Car-ple / Terminal	Soundness	Weakness	Soundness	Weakness
Soundness	0.95	0.52	0.41	0.01
Weakness	0.05	0.48	0.59	0.99

The prior conditional probabilities of "Inland Transportation"

Accessibility	Unlikely		Likely	
Car-ple / Inland transportation	Soundness	Weakness	Soundness	Weakness
Soundness	1	0.56	0.62	0.27
Weakness	0	0.44	0.38	0.73

The prior conditional probabilities of "Port"

Terminal	Soundness				Weakness			
Inland transportation	Soundness		Weakness		Soundness		Weakness	
Channel / Port	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness
Soundness	0.91	0.66	0.65	0.35	0.63	0.34	0.33	0.14
Weakness	0.09	0.34	0.35	0.65	0.37	0.66	0.67	0.86

The prior conditional probabilities of "Supply chains"

Terminal	Soundness				Weakness			
Inland transportation	Soundness		Weakness		Soundness		Weakness	
Channel / Port	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness	Soundness	Weakness
Soundness	0.91	0.66	0.65	0.35	0.63	0.34	0.33	0.14
Weakness	0.09	0.34	0.35	0.65	0.37	0.66	0.67	0.86

Appendix 6. A New Developed *BFRB* for Decision Making

Rules	**Risk attributes**			**Preference estimation (decision making)**				
No	Arrival time	Cost	Safety	Not preferred	Slightly preferred	Preferrec	Reasonably preferred	Highly preferred
1	Monday	Very low	Good					1
2	Monday	Very low	Fair		0.006	0.05	0.088	0.856
3	Monday	Very low	Average	0.019	0.091	0.051	0.006	0.833
4	Monday	Very low	Poor	0.167				0.833
5	Monday	Low	Good				0.167	0.833
6	Monday	Low	Fair		0.006	0.058	0.327	0.609
7	Monday	Low	Average	0.022	0.109	0.061	0.209	0.599
8	Monday	Low	Poor	0.2			0.2	0.6
9	Monday	Average	Good			0.167		0.833
10	Monday	Average	Fair		0.007	0.27	0.105	0.618
11	Monday	Average	Average	0.22	0.107	0.276	0.007	0.588
12	Monday	Average	Poor	0.2		0.2		0.6
13	Monday	High	Good		0.167			0.833
14	Monday	High	Fair		0.204	0.06	0.107	0.629
15	Monday	High	Average	0.022	0.334	0.059	0.007	0.579
16	Monday	High	Poor	0.2	0.2			0.6
17	Monday	Very high	Good	0.167				0.833
18	Monday	Very high	Fair	0.196	0.007	0.06	0.107	0.631
19	Monday	Very high	Average	0.228	0.109	0.061	0.007	0.596
20	Monday	Very high	Poor	0.437				0.563
21	Tuesday	Very low	Good				0.073	0.927
22	Tuesday	Very low	Fair		0.006	0.051	0.193	0.75
23	Tuesday	Very low	Average	0.019	0.094	0.053	0.098	0.736
24	Tuesday	Very low	Poor	0.172			0.091	0.737
25	Tuesday	Low	Good				0.285	0.715
26	Tuesday	Low	Fair		0.006	0.055	0.46	0.479
27	Tuesday	Low	Average	0.022	0.105	0.059	0.339	0.475
28	Tuesday	Low	Poor	0.193			0.33	0.477
29	Tuesday	Average	Good			0.172	0.091	0.737
30	Tuesday	Average	Fair		0.006	0.266	0.222	0.505
31	Tuesday	Average	Average	0.022	0.107	0.276	0.112	0.483
32	Tuesday	Average	Poor	0.2		0.2	0.106	0.494
33	Tuesday	High	Good		0.172		0.091	0.737
34	Tuesday	High	Fair		0.201	0.059	0.226	0.514
35	Tuesday	High	Average	0.022	0.333	0.059	0.11	0.476
36	Tuesday	High	Poor	0.2	0.2		0.106	0.494
37	Tuesday	Very high	Good	0.172			0.091	0.737
38	Tuesday	Very high	Fair	0.193	0.007	0.059	0.226	0.515
39	Tuesday	Very high	Average	0.228	0.109	0.061	0.113	0.49
40	Tuesday	Very high	Poor	0.438			0.1	0.462
41	Wednesday	Very low	Good				0.426	0.574
42	Wednesday	Very low	Fair		0.006	0.054	0.606	0.334
43	Wednesday	Very low	Average	0.022	0.105	0.059	0.483	0.331
44	Wednesday	Very low	Poor	0.193			0.474	0.333
45	Wednesday	Low	Good				0.712	0.288
46	Wednesday	Low	Fair		0.005	0.046	0.846	0.103
47	Wednesday	Low	Average	0.019	0.093	0.052	0.742	0.094
48	Wednesday	Low	Poor	0.172			0.734	0.094
49	Wednesday	Average	Good			0.193	0.474	0.333
50	Wednesday	Average	Fair		0.006	0.253	0.619	0.122
51	Wednesday	Average	Average	0.002	0.107	0.275	0.49	0.106
52	Wednesday	Average	Poor	0.2		0.2	0.491	0.109
53	Wednesday	High	Good		0.193		0.474	0.333
54	Wednesday	High	Fair		0.191	0.056	0.629	0.124
55	Wednesday	High	Average	0.022	0.332	0.059	0.483	0.105

56	Wednesday	High	Poor	0.2	0.2		0.491	0.109
57	Wednesday	Very high	Good	0.193			0.474	0.333
58	Wednesday	Very high	Fair	0.183	0.006	0.056	0.631	0.124
59	Wednesday	Very high	Average	0.227	0.108	0.061	0.497	0.107
60	Wednesday	Very high	Poor	0.438			0.46	0.102
61	Thursday	Very low	Good			0.211	0.352	0.437
62	Thursday	Very low	Fair		0.006	0.282	0.503	0.209
63	Thursday	Very low	Average	0.022	0.106	0.301	0.376	0.195
64	Thursday	Very low	Poor	0.2		0.225	0.375	0.2
65	Thursday	Low	Good			0.2	0.622	0.178
66	Thursday	Low	Fair		0.005	0.243	0.734	0.018
67	Thursday	Low	Average	0.019	0.095	0.267	0.619	
68	Thursday	Low	Poor	0.178		0.2	0.622	
69	Thursday	Average	Good			0.465	0.349	0.186
70	Thursday	Average	Fair		0.006	0.513	0.463	0.018
71	Thursday	Average	Average	0.02	0.097	0.542	0.341	
72	Thursday	Average	Poor	0.186		0.465	0.349	
73	Thursday	High	Good		0.2	0.225	0.375	0.2
74	Thursday	High	Fair		0.191	0.283	0.505	0.021
75	Thursday	High	Average	0.02	0.325	0.291	0.363	
76	Thursday	High	Poor	0.2	0.2	0.225	0.375	
77	Thursday	Very high	Good	0.2		0.225	0.375	0.2
78	Thursday	Very high	Fair	0.183	0.006	0.284	0.506	0.021
79	Thursday	Very high	Average	0.222	0.106	0.299	0.373	
80	Thursday	Very high	Poor	0.437		0.211	0.352	
81	Friday	Very low	Good			0.563		0.437
82	Friday	Very low	Fair		0.006	0.676	0.102	0.215
83	Friday	Very low	Average	0.021	0.103	0.681	0.006	0.188
84	Friday	Very low	Poor	0.2		0.6		0.2
85	Friday	Low	Good			0.6	0.2	0.2
86	Friday	Low	Fair		0.006	0.658	0.315	0.021
87	Friday	Low	Average	0.021	0.103	0.68	0.196	
88	Friday	Low	Poor	0.2		0.6	0.2	
89	Friday	Average	Good			0.833		0.167
90	Friday	Average	Fair		0.005	0.894	0.084	0.017
91	Friday	Average	Average	0.017	0.084	0.894	0.005	
92	Friday	Average	Poor	0.167		0.833		
93	Friday	High	Good		0.2	0.6		0.2
94	Friday	High	Fair		0.197	0.68	0.103	0.02
95	Friday	High	Average	0.02	0.315	0.659	0.006	
96	Friday	High	Poor	0.2	0.2	0.6		
97	Friday	Very high	Good	0.2		0.6		0.2
98	Friday	Very high	Fair	0.188	0.006	0.681	0.103	0.022
99	Friday	Very high	Average	0.215	0.103	0.676	0.006	
100	Friday	Very high	Poor	0.437		0.563		
101	Saturday	Very low	Good		0.352	0.211		0.437
102	Saturday	Very low	Fair		0.373	0.299	0.106	0.222
103	Saturday	Very low	Average	0.02	0.507	0.284	0.006	0.183
104	Saturday	Very low	Poor	0.2	0.375	0.225		0.2
105	Saturday	Low	Good		0.375	0.225	0.2	0.2
106	Saturday	Low	Fair		0.363	0.291	0.325	0.021
107	Saturday	Low	Average	0.02	0.505	0.283	0.192	
108	Saturday	Low	Poor	0.2	0.375	0.225	0.2	
109	Saturday	Average	Good		0.349	0.465		0.186
110	Saturday	Average	Fair		0.341	0.542	0.097	0.02
111	Saturday	Average	Average	0.019	0.463	0.513	0.006	
112	Saturday	Average	Poor	0.186	0.349	0.465		
113	Saturday	High	Good		0.622	0.2		0.178
114	Saturday	High	Fair		0.618	0.268	0.095	0.019
115	Saturday	High	Average	0.018	0.734	0.243	0.005	
116	Saturday	High	Poor	0.178	0.622	0.2		
117	Saturday	Very high	Good	0.2	0.375	0.225		0.2
118	Saturday	Very high	Fair	0.195	0.376	0.301	0.106	0.022

119	Saturday	Very high	Average	0.209	0.503	0.282	0.006	
120	Saturday	Very high	Poor	0.437	0.352	0.211		
121	Sunday	Very low	Good	0.102	0.46			0.438
122	Sunday	Very low	Fair	0.108	0.497	0.06	0.108	0.227
123	Sunday	Very low	Average	0.124	0.631	0.056	0.006	0.183
124	Sunday	Very low	Poor	0.333	0.474			0.193
125	Sunday	Low	Good	0.109	0.491		0.2	0.2
126	Sunday	Low	Fair	0.105	0.483	0.059	0.332	0.021
127	Sunday	Low	Average	0.124	0.629	0.056	0.191	
128	Sunday	Low	Poor	0.333	0.474		0.193	
129	Sunday	Average	Good	0.109	0.491	0.2		0.2
130	Sunday	Average	Fair	0.106	0.49	0.275	0.107	0.022
131	Sunday	Average	Average	0.122	0.619	0.253	0.006	
132	Sunday	Average	Poor	0.333	0.474	0.193		
133	Sunday	High	Good	0.094	0.734			0.172
134	Sunday	High	Fair	0.093	0.743	0.052	0.093	0.019
135	Sunday	High	Average	0.103	0.846	0.046	0.005	
136	Sunday	High	Poor	0.288	0.712			
137	Sunday	Very high	Good	0.333	0.474			0.193
138	Sunday	Very high	Fair	0.332	0.483	0.059	0.105	0.021
139	Sunday	Very high	Average	0.334	0.606	0.054	0.006	
140	Sunday	Very high	Poor	0.574	0.426			
141	Monday (nextweek)	Very low	Good	0.463	0.1			0.437
142	Monday (nextweek)	Very low	Fair	0.49	0.113	0.061	0.108	0.228
143	Monday (nextweek)	Very low	Average	0.515	0.226	0.059	0.007	0.193
144	Monday (nextweek)	Very low	Poor	0.737	0.091			0.172
145	Monday (nextweek)	Low	Good	0.494	0.106		0.2	0.2
146	Monday (nextweek)	Low	Fair	0.476	0.11	0.059	0.333	0.022
147	Monday (nextweek)	Low	Average	0.514	0.226	0.059	0.201	
148	Monday (nextweek)	Low	Poor	0.737	0.091		0.172	
149	Monday (nextweek)	Average	Good	0.494	0.106	0.2		0.2
150	Monday (nextweek)	Average	Fair	0.483	0.112	0.276	0.107	0.022
151	Monday (nextweek)	Average	Average	0.505	0.222	0.266	0.007	
152	Monday (nextweek)	Average	Poor	0.737	0.091	0.172		
153	Monday (nextweek)	High	Good	0.477	0.33			0.193
154	Monday (nextweek)	High	Fair	0.475	0.339	0.059	0.105	0.022
155	Monday (nextweek)	High	Average	0.479	0.46	0.005	0.006	
156	Monday (nextweek)	High	Poor	0.715	0.285			
157	Monday (nextweek)	Very high	Good	0.737	0.091			0.172
158	Monday (nextweek)	Very high	Fair	0.736	0.098	0.053	0.094	0.019
159	Monday (nextweek)	Very high	Average	0.751	0.193	0.05	0.006	
160	Monday (nextweek)	Very high	Poor	0.927	0.073			
161	≥Tuesday (nextweek)	Very low	Good	0.563				0.437
162	≥Tuesday (nextweek)	Very low	Fair	0.595	0.007	0.061	0.109	0.228
163	≥Tuesday (nextweek)	Very low	Average	0.631	0.107	0.06	0.007	0.195
164	≥Tuesday (nextweek)	Very low	Poor	0.833				0.167
165	≥Tuesday (nextweek)	Low	Good	0.6			0.2	0.2
166	≥Tuesday (nextweek)	Low	Fair	0.579	0.007	0.059	0.334	0.021
167	≥Tuesday (nextweek)	Low	Average	0.629	0.107	0.06	0.204	
168	≥Tuesday (nextweek)	Low	Poor	0.833			0.167	
169	≥Tuesday (nextweek)	Average	Good	0.6		0.2		0.2
170	≥Tuesday (nextweek)	Average	Fair	0.588	0.007	0.276	0.107	0.022
171	≥Tuesday (nextweek)	Average	Average	0.618	0.105	0.27	0.007	
172	≥Tuesday (nextweek)	Average	Poor	0.833		0.167		
173	≥Tuesday (nextweek)	High	Good	0.6	0.2			0.2
174	≥Tuesday (nextweek)	High	Fair	0.599	0.209	0.061	0.109	0.022
175	≥Tuesday (nextweek)	High	Average	0.609	0.327	0.058	0.006	
176	≥Tuesday (nextweek)	High	Poor	0.833	0.167			
177	≥Tuesday (nextweek)	Very high	Good	0.833				0.167
178	≥Tuesday (nextweek)	Very high	Fair	0.833	0.006	0.051	0.091	0.019
179	≥Tuesday (nextweek)	Very high	Average	0.857	0.088	0.5	0.005	
180	≥Tuesday (nextweek)	Very high	Poor	1				

Appendix 7. The Entropy Calculation for the Risk Attribute, Cost

The prior utility measure of the risk attribute, cost, u_{cost}, can be calculated using Equation (9.25) as follows:

$$u_{cost} = \sum_{k_j=1}^{l_j} p_{jk_j} l_{jk_j}$$

$$= 0.083 \times (0, 0, 0.3) + 0.279 \times (0.1, 0.3, 0.5) + 0.304 \times (0.3, 0.5, 0.7)$$
$$+ 0.25 \times (0.5, 0.7, 0.9) + 0.085 \times (0.7, 0.7, 1)$$
$$= (0.303, 0.47, 0.687)$$

In a similar way, $u_{i,cost}$, the posterior utility measure of the attribute, cost given the i^{th} *RCO* can be calculated using Equation (9.9) as follows:

$$u_{\#1,cost} = (0.568, 0.7, 0.934)$$
$$u_{\#2,cost} = (0.556, 0.897, 0.928)$$
$$u_{\#3,cost} = (0.547, 0.864, 0.923)$$
$$u_{\#4,cost} = (0.542, 0.847, 0.921)$$
$$u_{\#5,cost} = (0.54, 0.841, 0.92)$$
$$u_{\#6,cost} = (0.287, 0.487, 0.687)$$
$$u_{\#7,cost} = (0.28, 0.48, 0.68)$$
$$u_{\#8,cost} = (0.075, 0.225, 0.45)$$

Consequently, A'_{cost}, which characterises the utility measure changes of the cost given the each *RCO* can be represented using Equations (9.26) and Equations (9.18) – (9.21) as follows:

$$A'_{cost} = \left[\left|u_{\#1,cost} - u_{cost}\right|,\ldots,\left|u_{\#8,cost} - u_{cost}\right|\right]$$
$$= [0.659,0.765,0.738,0.722,0.716,0.041,0.024,0.625]$$

Next, the normalising vector of A'_{cost}, A_{cost} can be calculated using Equation (9.27) as:

$$A_{cost} = [0.861,1,0.965,0.944,0.936,0.054,0.031,0.817]$$

Then, according to Equation (9.28), the sum of the elements of the vector is calculated as:

$$S(A_{cost}) = \sum_{i=1}^{8} k_{i,.cost} = (0.861 + 1 + 0.965 + 0.944 + 0.936 + 0.054 + 0.031 + 0.817) = 5.608$$

The entropy measure of the risk attribute, cost can then be computed as:

$$e(S(A_{cost})) = -\frac{1}{\ln 8}\sum_{i=1}^{8}\left[\frac{k_{i,cost}}{S(A_{cost})}\ln\left(\frac{k_{i,cost}}{S(A_{cost})}\right)\right]$$

$$= -\frac{1}{2.079}\times[0.154\times(-1.874)+0.178\times(-1.724)+0.172\times(-1.76)+0.168\times(-1.782)$$
$$+0.167\times(-1.79)+0.01\times(-4.643)+0.006\times(-5.198)+0.146\times(-1.926)]$$
$$= -\frac{1}{2.079}\times(-1.586)$$
$$= 0.763$$