To my wife Xiaolin

UNIVERSITY OF NEWCASTLE UPON TYNE

ENGINEERING DESIGN CENTRE

FORMAL SAFETY ANALYSIS METHODS AND THEIR APPLICATION TO THE DESIGN PROCESS

By

Jin Wang B.Eng M.Sc

Thesis submitted for the Degree of Doctor of Philosophy

July, 1994

Acknowledgements

During the course of the research project described in this thesis, many individuals and organisations have provided considerable support without which its successful completion would not have been possible. In particular, the author would like to express his gratitude to the Engineering and Physical Sciences Research Council (EPSRC) (previously known as the U.K. Science and Engineering Research Council) for their financial support of the project, to Dr. P. Sen of the Department of Marine Technology at the Univerity of Newcastle upon Tyne for his stimulating suggestions, constructive comments, enthusiastic encouragement and time spent in charge of the project, and to NEI Clarke Chapman Marine for providing valuable information to the project.

The author would like to take this opportunity to express his sincerest gratitude to his supervisors, T. Ruxton, of School of Engineering and Technology Management at Liverpool John Moores University, and Professor R. V. Thompson, Dean of the Faculty of Engineering at the Univerity of Newcastle upon Tyne, without whose expert supervision the project would not have achieved such a successful conclusion.

During the time that the author has been involved with the research project, he has had the pleasure of working with a number of individuals at the Engineering Design Centre of the Univerity of Newcastle upon Tyne, including Dr. J. B. Yang, Mr. C. R. Labrie, Dr. P. Chawdhry, Mr. I. Applegarth and Dr. M. Guenov. To all these people, the author would like to express his sincere gratitude for their considerable support and friendship.

Last but not least, the author would like to thank Dr. X. Qi for her patience, understanding and support. Finally, the author's parents also deserve special thanks for their support and understanding.

Jin Wang

July, 1994.

Abstract

The work described in this thesis is concerned with formal safety analysis methods and their application to the "design for safety" process of marine and other large Made-To-Order (MTO) products with particular reference to the incorporation of safety aspects into the design process from the initial stages. Large MTO products are complex assemblies of components for which building and testing of prototypes is not usually possible.

This thesis proposes a "design for safety" methodology for large MTO products based upon the general spirit of the recommendations from recent government reports including the Cullen and Carver reports. Such a methodology, consisting of five phases, namely problem definition, risk identification, risk estimation, risk evaluation and design review, is used as the basis for the development of more scientific and objective safety analysis methods and techno-economic modelling techniques applicable to the control of major accidents of large MTO products.

An analysis of the input requirements and the outcomes of the typical safety analysis methods is conducted to identify their possible inter-relationships within the "design for safety" process in order to make full use of the advantages of each method. The selection of these safety analysis methods is discussed in the context of large MTO products. Problems concerned with failure and repair data collection programmes are studied and some typical failure and repair data sources are described.

In order to systematically and effectively identify and estimate risks of large MTO products, an inductive bottom-up Modified Boolean Representation Method (MBRM) is developed to directly make use of the information produced using Failure Mode, Effects and Criticality Analysis (FMECA) to identify and estimate all possible system failure events and respective causes. Such a method can be used to analyse any engineering system which is capable of being broken down into subsystems and components. The overall model and the algorithms are described and tested in association with appropriate computer software.

A modified qualitative reasoning method is developed to describe the behaviour of a large complex system. Such a modelling method can be used for failure propagation

analysis. The proposed qualitative modelling method is further combined with the MBRM to form a flexible mixed safety modelling methodology. In this methodology, the MBRM is used to process the information produced from the qualitative reasoning analysis at the component level to obtain a description of the total system behaviour. This methodology allows a bottom-up safety analysis approach to be taken even in those cases where it is difficult to obtain complete input-output relations for all the components of the system.

Two general simulation models are developed to process the information produced using FMECA and the MBRM. Such simulation models can be used as a quantitative safety analysis tool to simulate system availability, component/subsystem failures, and the probability of occurrence of each identified system failure event. These two models are developed in an Object-Oriented Programming (OOP) environment.

This thesis also presents a new safety analysis and synthesis methodology involving the use of fuzzy set modelling and evidential reasoning, where fuzzy set modelling is used to describe each failure event and an evidential reasoning approach is then employed to synthesise the information produced to assess the safety of the whole system. This subjective reasoning methodology can be used as an alternative approach by safety analysts to carry out analysis particularly in those situations where mostly non-numerical safety data is available or where there is a lack of information regarding distributions of variables for use in probabilistic risk studies.

A techno-economic modelling methodology is also developed to determine where reasonably practicable design actions are required. The proposed methodology brings together risk and cost objectives into the decision making process for the improvement of design aspects and maintenance policies. Information produced using the safety analysis approaches developed in this thesis can be utilised to construct a techno-economic model. Multiple Objective Decision Making (MODM) techniques are then employed to process the constructed model. The results produced can assist designers in developing good compromise designs that take into account risks, their possible consequences, maintenance cost, repair cost and design review cost.

A hydraulic transmission system of an offshore pedestal crane is used to demonstrate the methodologies developed in this thesis.

Finally, the results of the research project are generally summarised and the areas where further effort is seen to be required to improve the developed methodologies are

outlined.

A diagrammatic representation of the work presented in this thesis is shown in Figure 1.

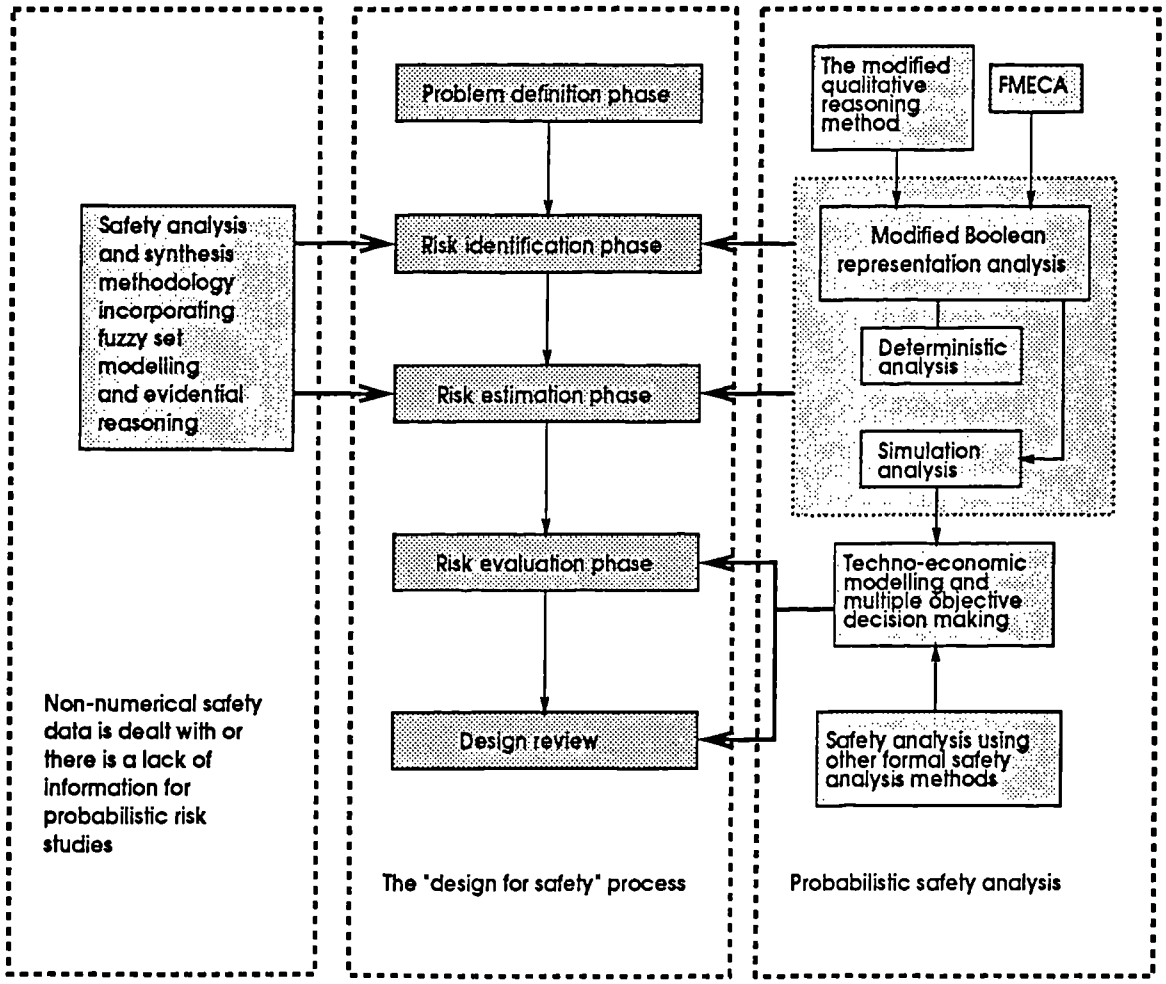


Figure 1 The structure of thesis

Table of Contents

Key Definitions

The following definitions of terms are used in the thesis. Numbers in square brackets represent references.

Availability: The ability of an item (under combined aspects of reliability, maintainability and maintenance support) to perform its required function at a stated instant of time or over a stated period of time [1.5].

Common cause failure: The failure of two or more apparently independent items or systems due to the occurrence of a single event [1.5].

Cost benefit analysis: The identification of the "cost" of reducing risks and comparing this with the likely "benefit" resulting from the risk reduction [1.22].

Criteria: Standards of performance with which actual (measured or estimated) performance may be compared [1.22].

Cut set: A cut set is a collection of basic events; if all these basic events occur, the top event is guaranteed to occur [1.10].

Down time: The time during which an item is not able to perform to specification [1.22].

Failure: The termination of the ability of an item to perform a required function [1.5]. Failures may be unannounced and not detected until the next full test (covert failures), or they may be announced and detected at the instant of occurrence (revealed failures).

Failure mode: A specific manner in which the item under investigation could malfunction [1.5].

Failure rate: For a stated period in the life of an item, the ratio of the total number of failures in a sample to the cumulative time on that sample. The failure rate is to be associated with particular and stated time intervals (or summation of intervals) in the life of the item, and with stated conditions [1.5].

Fault: An accidental condition that causes a functional unit to fail to perform its required function.

Hazard: A physical situation with a potential for human injury, damage to property, damage to the environment or some combination of these [1.10].

Maintainability: The ability of a machine to be maintained in a state which enables it to fulfill its function under conditions of intended use, or restored into such a state, the necessary actions (maintenance) being carried out according to specified practices and using specified means [1.3].

Maintenance: The combinations of all technical and corresponding administrative actions intended to retain an item in, or restore it to, a state in which it can perform its required function [1.5].

Mean time between failures: For a stated period in the life of an item the mean value of the length of time between cumulative failures computed as the ratio of the cumulative time to the number of failures under stated conditions [1.5].

Mean time to failure: For a stated period in the life of an item, the ratio of the cumulative time to failure for a sample to the total number of failures in the sample during the same period under stated conditions [1.5].

Mean time between maintenance: For a stated period in the life of an item the mean value of the length of time between cumulative maintenances computed as the ratio of the cumulative time to the number of maintenance activities under stated conditions.

Prime implicant: Prime implicants are unique failure modes of systems which contain other than simple fault modes connected by AND-OR logic gates, i.e., exclusive OR gates, working states, etc. [1.10]. A prime implicant is the equivalent of a cut set in fault tree analysis but for systems with multiple state variables .

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 [1.10].

Redundancy: The performance of the same overall function by a number of independent means. The means need not be identical [1.5].

Abbreviations

ALARP	As Low As Reasonably Practicable
BRM	Boolean Representation Method
CCA	Cause-Consequence Analysis
CFSV	Current Failure State Vector
CRM	Component Relationship Matrix
FMECA	Failure Mode, Effects and Criticality Analysis
DA	Digraph-based Analysis
DSDG	Directed Signed DiGraph
FTA	Fault Tree Analysis
HAZOP	HAZard and OPerability analysis
MBRM	Modified Boolean Representation Method
MCDM	Multiple Criteria Decision Making
MCSM	Minimal Cut Set Matrix
MODM	Multiple Objective Decision Making
MADM	Multiple Attribute Decision Making
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenances
MTBR	Mean Time Between Repairs
MTO	Made-To-Order
OOP	Object-Oriented Programming
PHA	Preliminary Hazard Analysis
PRA	Probabilistic Risk Analysis
QRA	Quantitative Risk Analysis
SRA	Subjective Reasoning Analysis

List of Figures

Reliability: The ability of a machine or components, or equipment, to perform a required function under specified conditions and for a given period of time without failing [1.3].

Repair time: The time during which an item is undergoing diagnosis, repair, checkout and alignment [1.22].

Risk: A combination of the probability and the degree of the possible injury or damage to health in a hazardous situation [1.3].

Risk Assessment: A comprehensive estimation of the probability and the degree of the possible injury or damage to health in a hazardous situation in order to select appropriate safety measures [1.5]

Scenario: The development path of an incident from an initiating event to a cause to a top event.

Top event: Undesired event of an item [1.10].

CHAPTER 1

Introduction

SUMMARY

Following a brief review of the history of safety analysis obtained from within the military and nuclear industries, this chapter describes the concepts of risks, hazards and safety analysis together with ways of reducing risks to employees, the public, the environment and property. Particular emphasis is placed on "design for safety". The objectives, criteria and requirements of "design for safety" are addressed. The levels of "design for safety" are briefly discussed with regard to human behaviour and system design procedures. Difficulties involved in the "design for safety" process of engineering products are discussed with particular reference to large Made-To-Order (MTO) products. Finally, the objectives of this work are described and the extent of this thesis is outlined.

1.1 Historical Developments

Safety and reliability aspects were considered in the process of engineering design relatively late. In the 1930s, as air transportation was developed, the collection of statistical data on the failure rates of various aircraft components, and especially of aircraft engines, was studied for further improvement in design to avoid, wherever possible, further aircraft accidents [1.27]. This was how the first concepts concerning the safety and reliability levels of aircraft came into being. However, before the 1940s, safety design was largely intuitive and based upon specific designers' experience. The Titanic shipwreck also produced an impetus for further investigation into system safety

and reliability [1.27].

During the 1940s, the first predictive reliability models appeared in Germany where the V1 missile project was carried out [1.1]. V1 missiles, during their ultimate development stages, were the first industrial systems for which the safety and reliability were deliberately and successfully defined based upon component performance. In that decade, courses and books on safety and reliability analysis as well as on the related statistical techniques grew in number. Probabilistic safety and reliability analysis methods were also increasingly used.

It was in the 1950s that safety and reliability as a branch of engineering was born in the United States of America. Attention was increasingly centred on safety matters, especially in the aeronautical and nuclear industries. During this decade the use of parameters characterising the reliability of components, such as failure rate and Mean Time Between Failures (MTBF), spread. It was also in the early 1950s that efforts were made to understand and to prevent human error which contributes to system failures.

The 1960s saw the emergence of some new reliability and safety analysis techniques as well as a wider variety of applications. The first analysis of component failures and their effects on system performance and on the safety of property and human beings was performed. As a result, techniques for carrying out such an analysis were rapidly developed, particularly in the aeronautical and aerospace industries. In 1961, Watson of Bell Telephone Laboratories introduced the fault tree concept to assess the reliability of the system designed to control Minuteman missile launching [1.10]. Later, the Boeing company further developed the concept resulting in the fault tree building method which is still in use. The Failure Mode, Effects and Criticality Analysis (FMECA) method [1.12] was also devised in the early 1960s.

Public concern with safety also grew in this decade. For instance, in 1962, after a series of missile accidents, the Air Force in the United States of America called for safety studies. It was at the end of the 1960s that system safety analysis became widespread in the aeronautics and nuclear fields. The awareness of safety concerns became essential to developers in the "high technology" industries. Potential accidents classified in terms of consequences and frequency of occurrence were, for the first time, taken into account in the design process.

Again in the 1960s, it was recognised that integrated studies were necessary to detect and reduce potential hazards of a large engineering product. As a consequence, a large

number of national and international standards regarding safety and reliability were developed. This also happened in the U.K. where similar standards were adopted [1.27].

In the 1970s, a large number of innovations were introduced in industrial safety prediction methods. In the nuclear power industries, accident scenarios were considered covering system failures as well as operator error during tests, maintenance, operations and reactor control. Many new methods were developed during this decade, including the event tree analysis to evaluate accident scenarios. Furthermore, the fault tree analysis, created in the field of aeronautics, was extensively adopted in other "high technology" industries.

The Three Mile Island nuclear accident caused no deaths but dictated a re-evaluation of Probabilistic Risk Analysis (PRA) methods [1.13][1.27]. As a result of the inquiry of this accident, the Commission, set up by the President of the United States, recommended that PRA methods should be increasingly used in the design of large and expensive engineering products. It was also recognised that reliability data, human error and common cause failures played a very important role in the assessment of the safety of large complex projects.

From the end of the 1970s, reliability and safety assessment techniques were widely adopted in the oil, chemical, railway, and car industries, and also for industrial wastewater treatment, i.e., in a great variety of activities and systems with different technological structures. Probabilistic reliability, availability and safety criteria were increasingly used, sometimes to comply with regulations, sometimes as self-imposed goals in the design process. Safety criteria began to play a very important role in product design from the initial design stages. For instance, at the end of the 1970s, the safety analysis of the Canvey Island petrochemical plant in the U.K. led to considerable changes in the design of the plant [1.27].

From 1980 onwards, the number of safety assessment studies increased both in the "high technology" industries and in the other industrial sectors. Possibly the most decisive step in the development of safety analysis methodologies was the publication of "Guide to the Performance of Probabilistic Risk Assessment (PRA) for Nuclear Process Plants" which was produced at the request of the safety authorities [1.19][1.27]. Its objective was to provide the organisations wishing to perform such analyses with the correct procedure. Furthermore in parallel, again at the request of the safety authorities, a significant effort was made to take qualitative as well as quantitative aspects of

human factors into account in safety and reliability analysis [1.13].

In the 1980s, reliability, availability, maintainability and safety assessment techniques tended to be adopted on a wide scale to control and to manage major industrial hazards. This gave birth to an actual distinct engineering discipline (safety) which, like others used in engineering design, involves concepts, measurable quantities and mathematical tools as well as methods for measuring and predicting these quantities [1.27]. As computers became more and more widely used in engineering design, more and more safety and reliability analysis techniques such as event tree and fault tree analyses were implemented through different codes of practice. Expert systems were also widely used together with the computerised safety and reliability assessment tools to conveniently and effectively predict the safety and reliability of engineering systems or products.

Also in the 1980s, the importance of failure and repair data collection programmes was realised [1.27]. Both the marine classification societies and other authorities showed great interest in collecting failure and repair data, obtained either by laboratory tests or from field reports, which was used to compile failure and repair data banks. Examples of such data banks are Lloyds Data Bank and System Reliability Service Data Bank managed by the United Kingdom Energy Authority.

Traditionally, safety analysis has been primarily used in many industries for verification purposes. However, this approach fails when large and complex engineering products with significant elements of novelty are designed. For such products, safety aspects should be more systematically integrated into the design process from the initial stages.

More recently, interest in the improvement of the safety of large engineering products through quantitative safety analysis from the initial design stages is growing considerably, both within industries and within the authorities. Some of the large companies and organisations have used quantitative safety analysis techniques to a considerable extent and some have only used qualitative methods due to the fact that many quantitative safety analysis methods are still insufficiently developed to contribute to major improvement in the safety of engineering products. In the 1990s, the need for the development of more objective, flexible and effective safety analysis methods has been identified, and the use of cost-benefit analysis and formal decision making techniques in the design process is demanded in order to achieve an optimal safety of a product within both technical and economic constraints [1.32].

1.2 Safety Analysis

1.2.1 What is Safety Analysis?

Reliability analysis and safety analysis are different concepts although there is a considerable overlap (and often confusion) between them. They both refer to the studies of process and equipment failures or operability. Reliability analysis of an item involves studying its characteristics expressed by the probability that it will perform a required function under stated conditions for a stated period of time. An item could be a piece of equipment, a component, a subsystem, or a system. If such an analysis is extended to involve the study of the consequences of the failures of the item in terms of possible damage to property or injury/death of people, the study is referred to as safety analysis.

System safety analysis is devoted to the prevention or control of risks of a product. A risk is defined as the measure of the occurrence of a hazard and its associated effects or consequences. A hazard could be a condition such as high voltage, an event such as a contact with high voltage, or a result such as death from the electric shock.

Safety analysis as used for the assessment of risks associated with an engineering system or product may be summarised to answer the following four questions:

i. What can go wrong?

ii. What are the effects and consequences?

iii. How often will they happen?

iv. What measures need to be undertaken to reduce the risks and how can this be achieved?

To answer above questions it is necessary to examine an actual or proposed design to identify and assess potentially hazardous situations and associated risks in order to provide a rational basis for determining where risk reduction measures are required.

Although reduction of risks to employees, the public, the environment and property can be achieved through other ways such as safety training and the application of sound engineering standards with respect to design, manufacturing, installation, commissioning, operations, and maintenance aspects, safety analysis is increasingly recommended to estimate the safety of a product in order to take proper measures to

reduce risks to a minimum by the improvement of design aspects, maintenance policies and similar actions. It is realised that safety aspects should be incorporated into the design process. Actually, incorporation of safety into the design process from the early stages, that is, "design for safety", may be the most effective way to reduce or eliminate potential serious risks of large MTO products. This is particularly so as large MTO products are complex assemblies of components for which building and testing of prototypes can often be impractical, and hence analytical tools must be used.

1.2.2 **Design for Safety**

"Design for safety" is a process aimed at minimising personnel injury or death, product damage or destruction, or degradation of the environment and mission performance [1.1]. It provides a systematic approach to the identification and control of high risk areas [1.30].

When an engineering product is designed, "design for safety" is required to be carried out to identify all possible failure conditions and to assess how often they may happen and how serious the possible consequences may be. This is achieved by applying various system safety analysis methods in the design process.

The assessment of probability of occurrence of a system failure event is a matter of judgement, usually based very much on the experience of similar products. However, when there is no such experience it may be difficult to make this kind of judgement. This is particularly true in the development of a Made-To-Order (MTO) product which is specially ordered by a customer [1.30]. As a consequence, quantitative probability analysis techniques rather than experience-based techniques are usually recommended to make a judgement of such a failure probability.

Consequence analysis is not an exact science [1.7] since it varies greatly with the value placed on a human life or a loss of any kind. Over the past years, experience has been obtained and calculation methods have been developed to produce a specification of the magnitude of a failure consequence. There is no doubt that development and improvement of consequence analysis techniques will be increasingly seen in the coming years.

"Design for safety" through the full quantification of consequences and probabilities of hazards can provide figures describing risks. When risks, either qualified or quantified, are judged to be not acceptable with respect to the corresponding criteria, the design

may need to be rearranged or modified by the provision of a set of protection systems, alarm systems, or more reliable components, for example, to reduce risks (i.e., reduce the frequencies of unacceptable system failure events and/or the magnitudes of the respective consequences) to an acceptable level. Cost-benefit analysis may also be beneficially applied to make full use of the available technical and economic sources to produce an optimal safe product.

1.2.3 **Criteria and Requirements for "Design for Safety"**

It is usually very difficult to determine the acceptable safety level of a system. One basis for judgement used in British law is that the product should be designed to be as safe as is reasonably practicable. However, that poses the question — what is reasonably practicable? It may be assumed that the whole subject of criteria of "design for safety" depend on the answers to the following three basic questions [1.22].

i. What is "design for safety".

ii. What is the effect of "design for safety".

iii. What is the time period of concern.

The answers to these questions may change with time or the particular problem in hand. However, "design for safety" would have the general objectives of improvement in safety and reliability utilising technological advances within economic constraints. Modern methods of safety analysis enable the risks to be more easily identified and an estimation of the magnitudes to be more confidently determined. Control systems, sensors, alarm devices and protection systems provide the means to determine disturbance conditions and necessary actions. The criteria of "design for safety" of engineering systems can generally be described as follows:

i. Safety devices and protection systems are the principal contributors to system safety.

ii. Safety devices, control systems and protection systems should be designed to have lower failure rates than the system being protected.

iii. The sources assigned to the improvement of the system safety should be optimally utilised to control high risk areas.

iv. "Design for safety" should not, in general, be in conflict with the general design process, and it should be consistent with the engineering design framework.

1.2.4 **Levels of "Design for Safety"**

Generally, levels of "design for safety" can be classified with regard to two aspects, i.e., the human behaviour and the system design procedures. Such levels are studied as follows:

1.2.4.5 Human Behaviour

It has been postulated that there are three levels of human behaviour in controlling or supervising tasks of "design for safety" as shown in Figure 1.1 [1.21]. These three levels are:

i. Skill-based.

ii. Rule-based.

iii. Knowledge-based.

The information produced at each of these levels can be used in decision making in the "design for safety" process. Each of these levels is briefly discussed as follows:

Skill-based

Skill-based "design for safety" deals with safety problems at the lowest level. This requires little conscious attention — that is, it is automatic. For an experienced safety analyst, determining where some safety devices need to be provided in a design according to experience falls into this category.

Rule-based

With rule-based behaviour more mental effort is required. Examples of rules include BS 327 and BS 1957 which can be used as a design guide in the design of cranes.

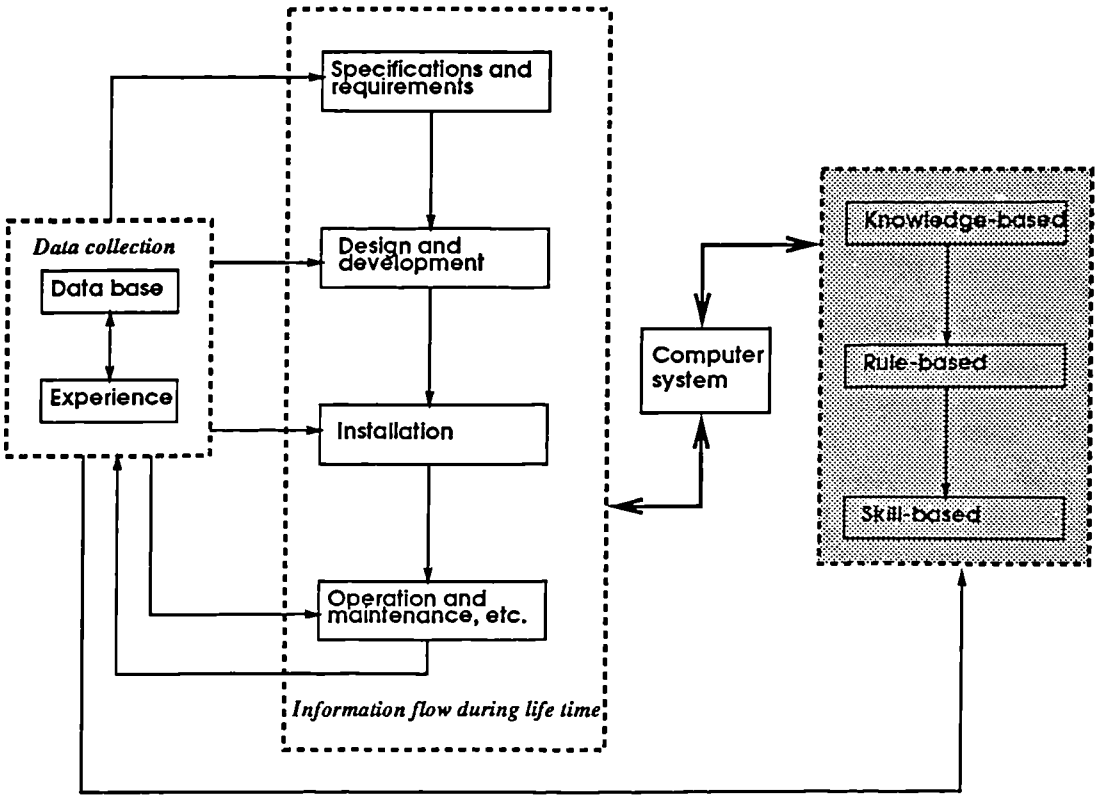


Figure 1.1 The three levels of human behaviour in controlling or supervising tasks of "design for safety"

Knowledge-based

The structure of the knowledge-based behaviour is an evaluation of the situation and planning of proper sequences of actions to pursue the goal. The activity depends on fundamental knowledge of the processes, functions and structure of the system. Therefore, knowledge-based "design for safety" involves higher level thinking, typically using fundamental principles, functional relationships and knowledge to identify and assess risks and determine what measures should be taken to control risks.

It is interesting to note that as experience is gained the "design for safety" of engineering systems may move from knowledge-based to rule-based to skill based. When a MTO product is designed, knowledge-based actions may be essential to cover all the aspects of the design since experience may not be available.

1.2.4.2 System Design Procedures

As previously described, "design for safety" involves the use of a set of alarm devices, protection systems and more reliable components designed to increase safety on the basis of the information obtained from experience or produced using formal safety analysis methods. This is usually achieved by applying a three-level approach to the "design for safety" process [1.2].

Level I

Within level I, the definition of safety objectives is required. It is important that these objectives be realistic. Once a tentative set of objectives is obtained, consideration should be given within level I to identify the system functions required to satisfy each objective. The purpose of specifying system functions is to clarify the objectives.

Level II

As the design moves from level I to level II, decisions requiring more detailed analysis and less philosophical reasoning will be encounted. The system will be divided into subsystems. Safety analysis is carried out at the subsystem level, and safety systems such as alarm devices and protection systems may then be determined and used to reduce or eliminate significant system failure events where

required.

Level III

At level III, more details of the system "design for safety" are produced. Safety analysis may be progressed to the component level. The procedures used in level II may be repeatedly applied at this level.

1.3 Difficulties Involved in "Design for Safety"

Although, in recent years, quantitative safety assessment techniques have been increasingly developed and applied by both design engineers and safety researchers, there are still some problems for these techniques to be widely applied to provide ultimate answers to safety based decision making in the design process. In order to effectively use these techniques, to develop more objective and efficient safety analysis methods and to integrate "design for safety" into the design process from the initial stages, it is necessary to describe the difficulties involved in the "design for safety" process. Such difficulties are briefly addressed as follows:

i. In many cases only limited data is available on component failures and repairs as well as on system failures and repairs for which statistical accuracy is often poor. In some cases, it may be difficult to obtain any such data, especially when human error is involved. This may be particularly true for MTO products.

ii. The safety of an engineering product is affected by many factors such as design, manufacturing, installation, commissioning, operations and maintenance as shown in Figure 1.2. Therefore, it may be extremely difficult to precisely construct a mathematical model for the product to describe its behaviour and to carry out "design for safety".

iii. A fully quantified safety analysis entails considerable work and therefore is costly. The scope and depth of "design for safety" may be very difficult to define.

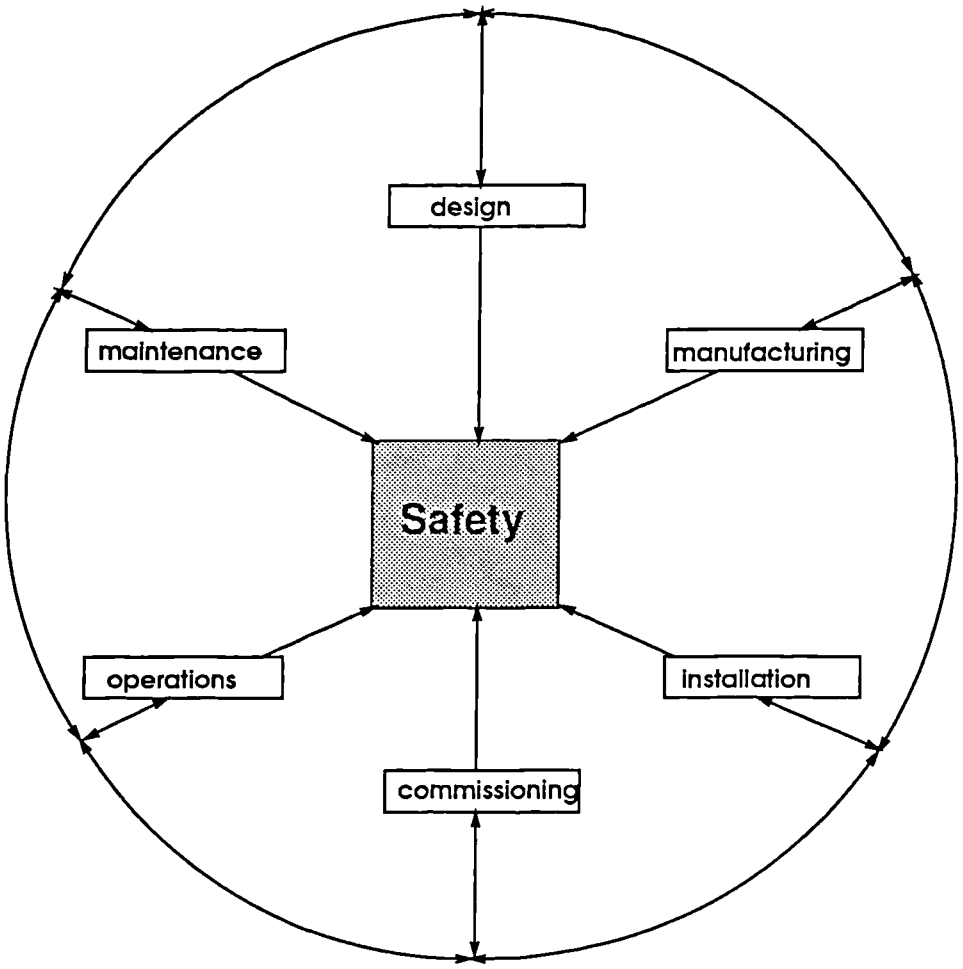


Figure 1.2 The factors affecting the safety of an engineering product

iv. The quantification of effects and consequences of hazards involves great uncertainty, even in those cases where the physical processes are clearly understood.

v. An analytical exercise associated with the quantification of risks involves a large number of assumptions, estimates, judgements and opinions which are often subjective. Therefore, it may need considerable skill for a safety analyst to interpret the results produced.

vi. It is extremely difficult to set up absolute criteria for safety acceptability since safety is only one of the important factors in the appraisal of the acceptability of an industrial activity.

1.4 Objectives

"Design for safety" should be carried out in a systematic way in parallel with other design processes to aid decision making on a product design from the initial stages. It includes a wide range of activities. The inherent purpose of the systematic use of these activities is to accurately predict the safety characteristics of an engineering product, to control the high risk areas, to maximise system safety and minimise its life cycle cost.

The work in this thesis deals with such activities. The objectives of this work are outlined as follows:

i. To identify the needs in the process of designing large MTO products with respect to safety aspects.

ii To construct a "design for safety" methodology in order to objectively and effectively incorporate safety aspects into the design process from the initial stages.

iii. To study typical safety analysis methods and to investigate their interrelations with regard to each stage of the "design for safety" process.

iv. To synthesise the typical safety analysis methods to form more flexible and efficient mixed safety assessment tools in order to make full use of the advantages of such methods.

v. To develop novel safety analysis methods to meet the challenge imposed by the increasing complexity of engineering products and the increasing public concern on safety.

vi. To develop a techno-economic modelling philosophy to integrate safety analysis and cost modelling in order to obtain optimal system safety within both technical and economic constraints.

vii. To identify further research areas which are required to be explored and exploited in the future.

1.5 Scope of the Work

It is quite obvious that the safety analysis methodologies described and developed in this work are of fairly general nature and can therefore theoretically be applicable to the design of a wide range of large engineering products such as marine cranes, offshore platforms, vessels and different types of marine vehicles. The developed methodologies in this work can also be used to effectively and efficiently incorporate and quantify safety as an integral part of the process of designing large MTO products, especially for those with a comparatively high level of innovation.

Chapter 2 studies the engineering design methodologies and "design for safety" methodology for large Made-To-Order (MTO) products. Following a survey of current "design for safety" status in engineering design, a "design for safety" methodology is proposed to address the needs identified by both the Cullen report and the Carver report [1.24]. The proposed "design for safety" methodology is studied together with the engineering design process of large MTO products and is used as a basis for further development of formal safety assessment procedures and safety-based decision making modelling techniques.

In Chapter 3, the concepts of qualitative and quantitative safety analysis, and bottom-up and top-down event-based safety analysis approaches are described. The typical safety analysis methods are outlined and discussed with respect to each phase of the proposed "design for safety" framework. An analysis of the input requirements and the outcomes of these methods is carried out to identify their possible inter-relationships in order to make full use of their advantages. The selection of these safety analysis methods is also

studied with respect to the characteristics of the particular product.

In Chapter 4, an inductive bottom-up safety modelling and assessment methodology is developed in a general way. In this methodology, the Modified Boolean Representation Method (MBRM) is developed to directly process the information produced using Failure Mode, Effects and Criticality Analysis (FMECA) in order to identify the system failure events and respective causes. This inductive bottom-up methodology can be applied to the "design for safety" process of engineering products involving multiple state variables and with feedback loops.

In Chapter 5, a modified qualitative reasoning approach is developed on the basis of the qualitative reasoning approaches used in the Artificial Intelligence (AI) field. The developed approach is also combined with the MBRM to form a mixed safety modelling methodology. In this methodology, the MBRM is used to process the information produced from qualitative reasoning analysis at the component level to produce a description of the total system behaviour. This developed methodology allows a bottom-up approach to be taken even in those cases where it is difficult to obtain complete input-output relations for all the components of a system.

In Chapter 6, two simulation models are developed to process the information produced using FMECA, MBRM as well as other safety analysis methods described and developed in Chapters 3, 4 and 5. The system availability, component/system failures, and the probability of occurrence of each undesired system failure event can be simulated on the basis of these two models.

The safety of a large product is affected by so many factors that great uncertainty exists in safety analysis. Generally, these problems of uncertainty can be treated using two principal types of method involving probability and possibility, respectively. The safety analysis methods developed in Chapters 3, 4, 5 and 6 are usually classified as the probablistic type and have been widely applied in various engineering environments. In some circumstances, however, possibility analysis, which often involves fuzzy sets and evidential reasoning, may prove to be a worthwhile alternative for system safety analysis. Therefore, in Chapter 7, the applications of fuzzy set theory and approximate modelling are explored. A hierarchical framework incorporating fuzzy set modelling and evidential reasoning is developed to assess the safety of a system. Such a reasoning framework provides the safety analyst with a rational tool to make full use of the information generated at the lowest level in design in order to evaluate the safety of the

whole system. This tool can be used as an alternative approach for safety analysts to carry out analysis particularly in those situations where distributions of variables for use in probabilistic risk studies are difficult or impossible to obtain.

To incorporate safety into the design process of a large engineering product from the initial stages, a techno-economic analysis may be needed. Therefore, in Chapter 8, a techno-economic modelling approach is developed to bring together the cost of undesired top event-caused consequences, maintenance cost, repair cost and design review cost in the decision making process for the improvement of design aspects and maintenance policies. Information produced using the safety analysis methods developed in this work is used to construct such techno-economic models. Multiple Objective Decision Making (MODM) techniques are then utilised to optimise the system design aspects and maintenance policies in terms of life-cycle cost and safety.

Finally, conclusions and recommendations are presented in Chapter 9.

REFERENCES - CHAPTER 1

[1.1] Bazovesky I., *Reliability theory and practice,* Prentice Hall, Englewood Cliffs, N.J., 1961.

[1.2] Brown D. B., *Systems analysis & design for safety,* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.

[1.3] *BS EN 292: Safety of machinery - Basic concepts, general principles for design, part 1: basic terminology methodology; part 2: technical principles and specification.* 1991.

[1.4] *BS 1957: Specification for power-driven mobile cranes,* 1979.

BS 327, *Specification for power driven derrick cranes,* 1964.

[1.5] *BS 4778, Glossary of terms used in quality assurance,* BSI Handbook 22, British Standards Institution, 1986.

[1.6] *BS 5760: Part 1, 2, 3: Reliability of systems, requirements and components,* 1979.

[1.7] Cox A. P., *Risk analysis in process industries,* 4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication Series No. 33 Vol.1, 1983, G2-G7.

[1.8] Halebsky M., *System safety engineering as applied to ship design,* Marine Technology, Vol.26, No.3, July 1989, 245-251.

[1.9] Health and Safety executive, *Canvey: an investigation of potential hazards from operations in the Canvey Island Thurock Area,* Her Majesty's Stationary Office, London, 1978.

[1.10] Henley E. J., Kumamoto H., *Probabilistic risk assessment,* IEEE Press, New York, 1992.

[1.11] Hope S., *The CONCAWE report on methodology for hazard analysis and risk assessment,* 4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication Series No. 33 Vol.1, 1983, B1-B7.

[1.12] IEEE Std 352-1975, *IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems,* (An American National Standard), IEEE Press, ANSI N41-4-1976, 1975.

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

[1.14] Labrie C. R., *Design for safety: design methodology,* Research Report, EDCN/SAFE/RESC/12/1, Engineering Design Centre, University of Newcastle upon Tyne, June 1992, 29 pages.

[1.15] Levine S., Stetson F., *Applying the lessons of PRA (Probabilistic Risk Assessment), an American perspective Nuclear Engineering Internation,* 1984.

[1.16] LR Reliability Data, *Pump system reliability data,* Lloyds Register of Shipping, 1982.

[1.17] LR Report, *Pump system reliability data,* Lloyds Register of Shipping, 1982.

[1.18] *NRC statement on risk assessment and the reactor safety report (Wash-1400),* in light of the risk assessment review group report US/NRC, 1979.

[1.19] PRA procedure guide. *A guide to the performance of probabilistic risk assessments for nuclear power plants,* NUREG/CR 2300-1983.

[1.20] Ruxton T., *Information engineering for ship operation,* Proceeding of Maritime Communications and Control Conference, IMarE, London, 21-23 November 1990.

[1.21] Ruxton T., *Safety analysis required for safety assessment in the shipping industries,* Presented to NECJB, Institute of Marine Engineers and the Royal Institute of Naval Architects, December 1992.

[1.22] Ruxton T., Wang J., *Advances in marine safety technology applied to marine engineering systems,* Proceeding of First Joint Conference on Marine Safety and Environment, Delft, The Netherlands, June 1992, 421-432.

[1.23] Sen P., Labrie C. R., Wang J., Ruxton T., Chan J., *A general design for safety framework for large made-to-order engineering products,* Proceeding of First Newcastle International Conference on Quality and Its Applications, Newcastle, September 1993, 499-505.

[1.24] Shooman M. L., *Probabilistic reliability: an engineering approach,* 2nd ed., Robert E. Krieger Publishing Company, Florida, 1990.

[1.25] Smith D. J., *Reliability and maintainability and perspective,* Second Edition, Macmillan Publishers Ltd, 1985.

[1.26] Smith D. J., *Reliability, maintainability and risk,* Forth Edition, Butterworths-Heinemann Ltd, 1992.

[1.27] Villemeur A., *Reliability, availability, maintainability and safety assessment,* John Wiley & Sons, England, 1992.

[1.28] Wang J., *Design for safety: a general review in marine field,* EDCN/SAFE/RESC/1/1, Engineering Design Centre, University of Newcastle upon Tyne, February 1991, 60 pages.

[1.29] Wang J., *Design for safety,* EDCN/SAFE/RESC/8/2, Engineering Design Centre, University of Newcastle upon Tyne, March 1992, 31 pages.

[1.30] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12

[1.31] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), Vol.105, 1993, 21-34.

[1.32] Wang J., Yang. J. B., Sen P., *Techno-economic modelling for design and maintenance optimisation based on safety analysis,* Submitted February 1994 to: Quality and Reliability Engineering International, (Research Report, EDCN/SAFE/RESC/19/2, Engineering Design Centre, University of Newcastle upon Tyne, February 1994).

[1.33] Yannoutsos P., *Implementation of reliability engineering in the marine field - physics of exhaust valves failure due to high temperature corrosion,* Ph.D Thesis, Department of Marine Technology, University of Newcastle upon Tyne, November 1989.

CHAPTER 2

Design for Safety Methodology

SUMMARY

As indicated in the last chapter, both the Cullen report [2.8] of the Piper Alpha disaster and the Carver report [2.12] on ship safety have recommended that safety should be incorporated into the design process from the initial stages and that more scientific and objective approaches are required to be developed in order to control major accidents, to demonstrate safety by design and to describe the operational requirements of large marine and by implication other Made-To-Order (MTO) products effectively and efficiently.

In this chapter, the characteristics of large MTO products are described and their design process is studied together with a proposed MTO product design framework. After investigating the current "design for safety" status of large MTO products, a "design for safety" methodology is proposed in a generic sense and discussed in the context of the general design process. The proposed "design for safety" methodology could form the basis for the further development of safety assessment procedures and safety-based decision-making modelling techniques. The phases in the proposed "design for safety" methodology are studied together with their objectives and requirements. Finally, concluding remarks are given.

2.1 Introduction

As described in Chapter 1, system "design for safety" provides a systematic approach to the identification and control of high risk areas, and it should be integrated into the design process from the initial stages to reduce or eliminate major hazards. However, due to the complexity of the safety assessment of marine and other large Made-To-Order (MTO) products and the lack of clear and complete guidance for a "design for safety" methodology, "design for safety" has not been specifically integrated into the design process for such products. It is worth noting that deficiencies in MTO products are usually corrected only after accidents have occurred, and few organised "design for safety" programmes devoted to MTO products have been implemented. Many accidents, even those involving human error, could have been prevented with greater attention to safety in the initial design stages. There is therefore a perceived need for a "design for safety" methodology for MTO products in order to improve their safety.

As "design for safety" is a part of the overall design process, design methodologies of MTO products are studied first.

2.2 Engineering Design Methodologies for Made-To-Order (MTO) Products

2.2.1 Made-To-Order (MTO) Products

A Made-To-Order (MTO) product is an expensive, large and complex engineering structure, made up of many subsystems which must be carefully integrated to form a complete working system. Each MTO product may be a unique commission ordered by a customer for a specific purpose and location. The efficient design process for a MTO product is a key procedure to allow alternatives to be generated and compared.

MTO product design is a broad-based activity. The design process combines creativity, empiricism, theory and practice, while the range of influencing factors and diversity of applications require the latest technology to be utilised.

MTO products add the following difficulties to the general design process.

- The non-existence of historical data on design aspects. This is particularly true for original design problems and design solutions.

- The impracticability of full-scale experimentation with many design aspects.
- Difficulty of replacing or modifying them once on location and in operation.

2.2.2 Engineering Design Methodologies

Engineering design is a creative process, which begins with a requirement, and defines a system and the methods of its realisation so as to satisfy the requirement [2.10].

Three broad categories of design, which are related to the design of various marine and other large MTO products, have been identified as follows [2.6]:

i. *Original design:* which involves producing an original solution for a system to carry out a new task.

ii. *Adaptive design:* which involves adapting a known system to a changed task.

iii. *Variant design:* which involves varying the size and/or arrangement of certain aspects of the chosen system, the function and the solution principle remaining the same.

Patterns within each individual category above and various engineering disciplines can be identified and analysed to form a series of steps for organising and guiding an engineering design. Such a framework is referred to as an engineering design methodology [2.7].

The benefits of engineering design methodologies are obvious. These include rapid and direct generation and evaluation of design solutions. A rational and systematic framework can make the work of an engineering design more efficient and effective.

It is widely recognised that two types of model, which are the descriptive and prescriptive types, are generally available for representing the creative process of a MTO product design [2.6]. Both types of model are offered as a rational, systematic framework simplifying the process of design and increasing the effectiveness and efficiency of the design engineer. The descriptive type of model describes how a design is done by the design engineer. It is important to make the distinction that the descriptive type of model does not necessarily describe what should be done to arrive at an optimum solution, rather it exemplifies how the design engineer performs the process of design. Consequently, the descriptive type of model, unlike the prescriptive

type, is entirely subjective.

The prescriptive model typically represents systematic and algorithmic approaches to design. Many of the regulatory bodies concerned with approving the design of marine and other large MTO products actually encourage design engineers to follow a prescriptive model. The prescriptive model which may simply consist of a number of steps starts with the identification of essential problems and finishes with the design being worked up in great detail. Unfortunately, this kind of representation does not usually permit the concept of concurrency to be modelled. It should be noted that those activities would take place in practice, especially in the design of MTO products [2.6].

The descriptive model involves the continuing development of a project from recognition of need through feasibility study, preliminary study, detailed design, qualification testing, production planing, production and acceptance testing to operations.

Applicability of both the prescriptive and descriptive types of model has been extensively studied with respect to MTO products [2.6]. A number of mismatches exist between prescriptive design theory and actual design practice. This is mainly due to the fact that heuristics play such a significant and influential role in MTO product design. The empirical knowledge actually allows the design engineer to treat the product to be designed as a complete system. Heuristics are often used to firm up on certain "global" aspects of the design of a MTO product [2.6]. For example, when a topside of an offshore production platform is designed, heuristics are usually used to locate compartments/activities/items of equipment in three-dimensional space at the initial stages of the preliminary design phase [2.6]. Therefore, MTO product design is initiated as a top down process which requires that the design engineer uses very crude representations of information during the early stages of development but gradually progresses to more meaningful and detailed information models. The design engineer is then able to provide a fairly comprehensive but preliminary definition of the design. As the conceptual design activity is completed detailed design starts.

It is clear that certain elements of the prescriptive methodology are not closely relevant to MTO product design [2.6]. Generally, the generation of a large number of possible candidate designs and subsequent selection of most promising alternatives do not often happen for most MTO products. The only occasions on which this is likely to happen

are either when the design engineer is generating alternative preliminary arrangements or selecting major items of equipments. It is therefore concluded that the prescriptive design methodology is not really applicatable to the development of most MTO products although it is, in some occasions, worthwhile to be utilised to ensure that the design engineer approaches all problems in a systematic and rational manner in order to scan all possible solutions without in any way predicating the choice of a particular solution. A more appropriate descriptive methodology relating the details of the design problem is required. The details of such a descriptive engineering design methodology are outlined as follows.

2.2.3 A Proposed Methodology for Marine and Other Large MTO Products

Figure 2.1, which is proposed on the basis of the design frameworks described in [2.6] and [2.7], depicts the typical steps in the design process of MTO products. This framework is considered to be generally applicable to most design efforts of MTO products but it should be recognised that individual projects may require variation of the process, including total elimination of some steps.

2.2.3.1 Prospect Evaluation

Specification

The scale and variety of the need are vast, but any listing would have to include following information [2.9]:

- Formal request.
- Informal request.
- Assignment from superiors.
- The need pursuant to new regulations.

Information

Based on the description of the need, design concepts can be identified to satisfy the need constraints. The best concept can then be selected.

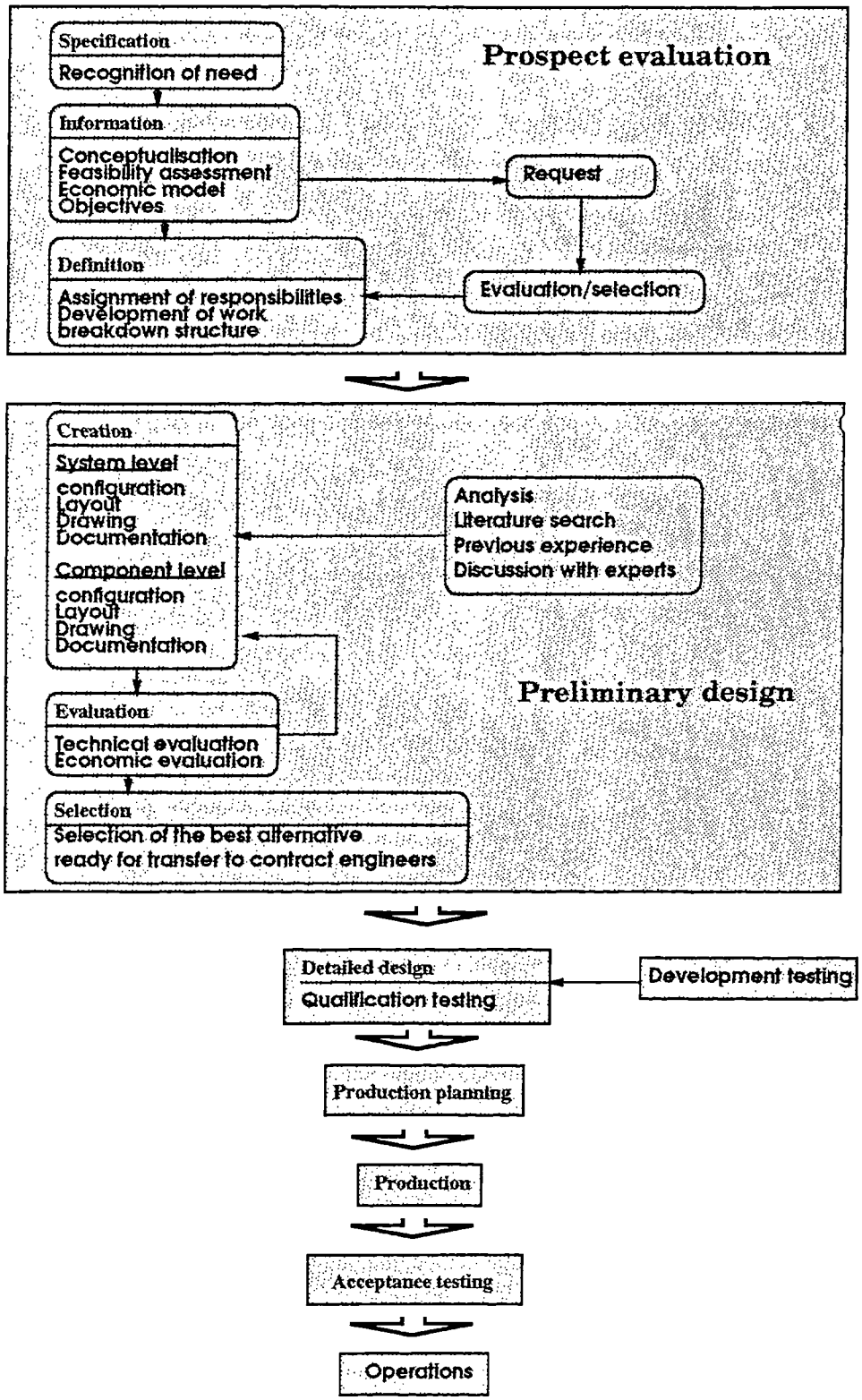


Figure 2.1 The steps in the design process of MTO products

The feasibility assessment of the selected concept is often accomplished as a part of the conceptualisation task. The aim of assessing the feasibility of the chosen concept is basically to ensure that the project proceeds to the design phase on the basis of a concept that is achievable both technically and economically. Feasibility assessment is very important for defining the concept to such a degree that the design can proceed with confidence that the end product will accomplish the intended purpose within the available resources. Cost estimating is involved in the feasibility study.

Establishing the requirements of a project is one of the most important and difficult elements in the design process. This task should be accomplished prior to initiating the design and after the concept has been defined. The requirements are so critical to the ultimate product capability and cost that they must be established as early as possible in the design process. Although the requirements are established to be permanent, nevertheless they should be continuously reviewed and revalidated during the design process to ensure that they continue to reflect the goals and objectives of the project.

Definition

After the concept has been approved, overall system configuration and component specifications need to be studied in order to establish requirements at the component, subsystem and system levels. This is repeated continuously over the design process as the system and its constituent elements continue to be defined, tested, evaluated, produced, and finally assembled to form a working system.

Once the project becomes viable, a systematic structure breakdown of the effort must be made. The breakdown structure is basically a family tree subdivision of the effort which is used to provide a means for management of the various work elements. It relates each task to the others and to the end product and provides a baseline against which the technical, schedule, cost and manpower reporting may be accounted. The degree to which a design process is subdivided for work assignment and management responsibility is a function of the complexity and duration of effort, the overall cost of the project, the organisational structure, etc [2.9].

2.2.3.2 Preliminary Design

Preliminary design is the phase of the design process that bridges the gap between the design concept and the detailed design phase of the effort. This phase of the effort is referred to as embodiment design in some textbooks [2.9].

Creation

During the preliminary design stage, the overall system configuration is defined and schematic layout and definition drawings are developed to provide early project configuration. Both the system level and component level may be involved in this creation stage.

Careful analysis should be carried out in the creation process. This may involve detailed literature search of design and analysis methods, previous experience of designs of similar products, and discussions with experts in particular areas. Testing may also be involved in the the preliminary phase. In general, it is costly for MTO products to run test programmes. Therefore, it is desirable to minimise testing during this design phase.

Evaluation

As the design concept continues to be refined and the layout of the design at both the component and subsystem levels is gradually constructed, both the technical and economical estimations will become more realistic. The technical evaluation is carried out to make sure that the designed parameters satisfy the requirements. The examples of such parameters are stability, weight distribution, flows, safety, reliability and availability. The economical evaluation should also be undertaken with regard to aspects such as costs of construction, equipment and operation and maintenance. It may be beneficial if the system test, checkout, operation and maintenance procedures are taken into account from the initial stages in the design.

Selection

As the design is further defined during the preliminary design phase and if more than one alternative is involved, an evaluation leading to selection of the "best" alternative is conducted.

2.2.3.3 Detailed Design

The intent of the detailed design phase of a project is to develop a comprehensive system description that completely describes the design. At this stage, all the various disciplinary organisations are actively involved, resolving the system design concept into component parts, evaluating components to validate previously established

requirements, specifying those design requirements left undefined, and assessing the effects of the component requirements and the overall system requirements.

During the detailed design phase of the project, the cost of the end items must continue to be authenticated. A qualification testing may then be carried out, if necessary, to validate the design in a sense that it proves that the product meets the specifications.

2.2.3.4 Production Planning, Production, Acceptance Testing and Operation

Production planning is initiated by reviewing the design drawings to identify machines and tooling required and to determine machinery operations to be used. After the production planning is finished, the production process begins. The design process is finalised with the completion of acceptance testing. Operations can then be started by the customer.

2.3 "Design for Safety" Methodology for MTO Products

2.3.1 Introduction

Although the concept of "design for safety" was introduced in the aerospace, nuclear and chemical industries many years ago, a series of standards, covering the general use of safety and reliability through other industries, were used from 1980 [2.17]. "Design for safety" of most MTO products is usually based on British standards and classification society requirements (or their equivalent), which incorporate the necessary rules and codes implemented over the years and updated, often under public pressure, following catastrophic accidents. Safety analysis is still mostly applied (if applied at all) at the final stages of the design mainly for verification purposes, although many of the decisions having the greatest impact on product safety may be taken at the earlier design stages [2.14].

The growing technical complexity of large MTO products and the public concern regarding their safety have aroused great interest in the development and application of safety assessment procedures. This may be demonstrated by the conclusions and recommendations of the public inquiries of the Piper Alpha accident and some serious marine accidents such as the capsize of the Herald of Free Enterprise.

2.3.2 Safety Case

2.3.2.1 Safety Case of Offshore Installations

On 6 July 1988, an explosion and subsequent fire on the Piper Alpha offshore installation led to the loss of 167 lives. As a result of this, a public inquiry was established to discover the circumstances of the accident and its causes. The produced report (Cullen report) suggests that a "safety case" is required for the design of offshore installations, and the "safety case" approach is currently in use in the offshore industry.

A safety case covers all aspects of the safety of the plant or process in question, and how the risks involved are to be minimised [2.12]. It should include sufficient particulars to demonstrate that [2.8]:

- hazards with the potential to cause major accidents have been identified, and
- risks have been evaluated and measures have been taken to reduce them to a As Low As Reasonably Practicable (ALARP) level.

A safety case should be prepared demonstrating safety by design, describing operational requirements, providing for continuing safety assurance by means of regular review, and setting out the arrangements for emergency response. It should also include identification of a representative sample of major accident scenarios and assessment of the consequences of each scenario together with an assessment in general terms of the likelihood of its happening. The report suggests that innovative safety analysis methods and cost-benefit analysis may be beneficially used for the prediction and control of safety.

The report recommends Quantitative Risk Analysis (QRA) to be used in the process of hazard identification and risk assessment in preparing a safety case [2.8]. QRA can help to provide a structured objective approach to the assessment of risks, provided that it relies on and is supplemented by good engineering judgement and the limitation of the data used is roughly understood. The significant pathways leading to serious system failure conditions can be systematically identified using QRA and hence all reasonably practicable steps can be taken to reduce them.

2.3.2.2 Safety Aspects of Ship Design and Technology

As a result of several serious marine disasters such as the capsize of the Herald of Free Enterprise on 6 March 1987, the Carver report was produced not only to see that the particular calamity is not repeated, but also to reduce the inherent hazards of "Ro-Ro" ferries [2.12].

The report points out that there is a general trend towards more scientific forms of safety regulations to deal with hazardous activities. Shipping industries should use the "safety case" approach that the offshore industries are adopting and which the nuclear, chemical and aerospace industries have already used. It recommands that formal safety assessment methods should be used to prepare the safety case for U.K. shipping.

2.3.3 "Design for Safety" Methodology

It is necessary for "design for safety" of large MTO products to be undertaken from the fairly early stages of the design process as suggested by the Carver report and the Cullen report [2.8][2.12]. There is a perceived need for a "design for safety" framework to be developed to allow various safety assessment tools to be applied individually and in combination so that as the design process advances and the available information increases in detail, safety assessment can move from a qualitative basis to a quantitative basis, and from an assessment function to a decision making function to a verification function, ensuring that a final design meets explicitly defined levels of safety [2.19].

For a MTO product design, the following phases are proposed for the process of "design for safety":

i. Problem definition.

ii. Risk identification.

iii. Risk estimation.

iv. Risk evaluation.

v. Design review.

"Design for safety" is an iterative process. For example, risk identification phase may make use of the information produced from design review, converging to safety design goals defined in the problem definition phase. The interactions of the above phases are

shown in Figure 2.2. The above five phases comprise the general parts of a "design for safety" framework for MTO products. Each phase is described as follows in more detail with respect to the proposed design process as shown in Figure 2.1.

2.3.3.1 Problem Definition

"Design for safety" begins with an identified need. Problem definition involves identifying the need regarding the safety of a product, and it should be conducted in conjunction with the classification of the project and the elaboration of the product specification in the project evaluation phase of the design process. Specification of the need is accomplished in the feasibility study process.

After the general need for safety is established, more specific requirements should be produced for practical realisation. Both the operational and design requirements regarding safety and reliability should be specified and they may have to be made at different levels (i.e., the system and subsystem levels) as required. The extent to which safety requirements are defined is also relevant to the level of innovation which has a significant impact on the course of safety assessments.

The following typical items may need to be specified in the problem definition phase.

- Sets of rules and regulations made by the national authorities and classification societies.
- Deterministic requirements for the life of the product, reliability, availability, etc..
- Criteria referring to probability of occurrence of serious system failure events and the possible consequences (i.e., Frequency-Consequence Curve).

2.3.3.2 Risk Identification

As the design process proceeds, the design moves from the prospect evaluation phase to the preliminary design phase. In this phase, as the configuration of the product at both the component and subsystem levels is defined, risk identification process is initiated. Risk identification is a process of identifying all potential hazardous conditions or events, and respective causes and possible consequences. Experience has shown that a large proportion of critical failures results from overlooking potential system failure

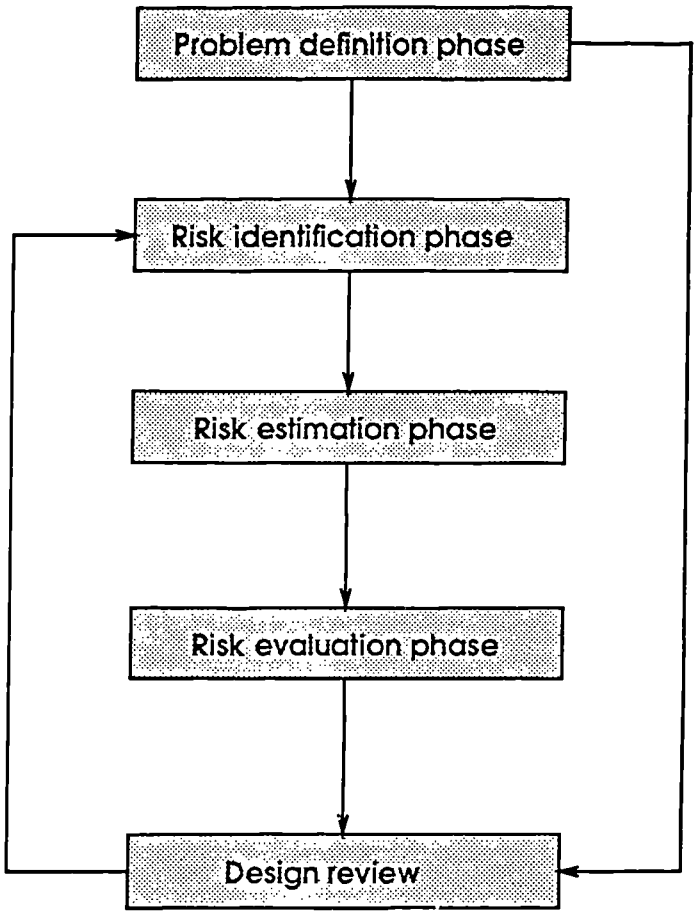


Figure 2.2 Interrelations of five phases in the "design for safety" framework

events. Actually, if complete systematic safety analysis had been carried out and proper measures had been taken from the early design stages, most disastrous failures of MTO products could have been prevented.

In the risk identification phase, the combined experience and insight of engineers are required to systematically identify all potential failure events at each required indenture level with a view to assessing their influences on system safety and performance. Various safety analysis methods may be used individually or in combination to identify the potential risks of a system. Such typical methods are:

- Preliminary Hazard Analysis (PHA).
- Fault Tree Analysis (FTA).
- Event Tree Analysis (ETA).
- Cause-Consequence Analysis (CCA).
- Failure Mode, Effects and Criticality Analysis (FMECA).
- HAZard and OPerability analysis (HAZOP).
- Modified Boolean Representation Method (MBRM).
- Simulation analysis.

The study of these methods will be undertaken in more detail in Chapters 3, 4, 5, and 6.

2.3.3.3 Risk Estimation

Risk estimation should be carried out in the preliminary design phase of the design procedure to process the information produced from the risk identification phase. In the risk estimation phase, the likelihood of occurrence of each identified system failure event and possible consequences can be assessed on either a qualitative or a quantitative basis.

In the early stage of the risk estimation process, the likelihood and possible consequences of each system failure event are usually estimated on a qualitative basis because the identified events may not be readily quantified. The methods used for conducting qualitative risk estimation include PHA, FMECA, MBRM, FTA, ETA and

CCA.

As the design proceeds more and more information regarding safety is collected. After the minimal cut sets leading to a top event (a system failure event) have been identified and the failure data of the basic events associated with the minimal cut sets has been obtained, quantitative risk estimation can be undertaken. The typical methods used in carrying out quantitative risk estimation include FTA, ETA, CCA, MBRM and simulation. Construction of the minimal cut sets leading to a top event is one of the most important steps in the risk estimation phase. Therefore, it will be studied in more detail in this work.

The probability of occurrence of each basic or primary event associated with the minimal cut sets of a top event may be obtained either from historical analysis, FMECA and simulation, or from the data collection programmes and engineering judgement. The level of possible potential consequences of a top event may be quantified in economic terms with regard to the loss of lives and property and the degradation of the environment caused by the occurrence of the top event.

The results produced from the risk estimation phase may be used through the risk evaluation phase and design review, and may also be used to assist designers in developing maintenance and operation policies.

2.3.3.4 Risk Evaluation

Risk evaluation is carried out at the evaluation stage of the preliminary design phase of the design process. It is subject to the requirements defined in the problem definition phase to maintain the functional performance of the product. Risk evaluation is a process of defining risks as a function of the estimated measures of the frequency or likelihood and possible consequences, on the basis of which decisions on the selection of design alternatives and actions on further risk reduction may be made.

Risk evaluation can be undertaken on a qualitative basis if only qualitative safety information is available. Qualitative risk evaluation of a system failure event can make use of the information produced in the risk estimation phase to construct a risk assessment matrix as will be shown in Chapter 3. The design engineer can then determine which parts or possible failure conditions have priority for design action.

If the probabilities of occurrence of the system failure events and the possible consequences can be quantitatively assessed, a frequency-consequence curve (Figure 2.3) can be produced to represent the risks. The acceptable and unacceptable regions are divided by a transition region commonly termed by various authorities as As Low As Reasonably Practicable (ALARP). If unacceptable risks are identified, design review actions may need to be taken or the design may have to be reconsidered, if necessary, to reduce either the frequencies of hazards or magnitudes of their respective consequences to an acceptable extent.

2.3.3.5 Design Review

Design review can be integrated into the evaluation and selection phases of the preliminary design process of a MTO product. Since the probability of occurrence of each serious system failure event is determined by its minimal cut sets which are associated with some basic individual failure events, effective reduction or elimination of an unacceptable failure event involves eliminating the cut sets with the highest probability of occurrence. Measures to be taken may include the provision of protection systems and alarm devices or use of more reliable components, for example. Reduction of human error should also be taken into account in the design review. The probability of human error may be reduced by the introduction of sensing and alarm devices if applicable or better training. Improved inspection and maintenance policies may also be useful for reducing the probabilities of occurrence of system failure events.

Design review should be incorporated with a cost-benefit analysis [2.8][2.12]. Cost-benefit analysis becomes increasingly attractive as more advanced technology is introduced and the benefits of techno-economic analysis are realised. Cost-benefit analysis basically involves comparing the cost of safety proposals with their benefits in economic terms, on the basis of which design decisions can be made. It can make use of the information produced from the risk estimation and risk evaluation phases and may be best undertaken using formal decision making tools such as Multiple Attribute Decision Making (MADM) and Multiple Objective Decision Making (MODM) approaches to study both design and maintenance aspects to achieve an optimal design alternative and the best maintenance and operation policies.

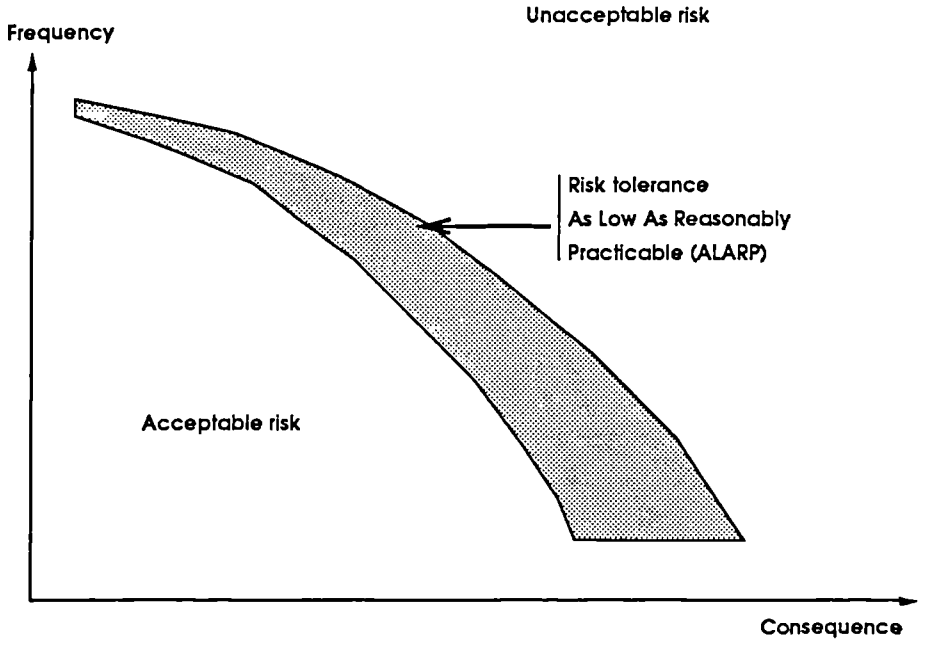


Figure 2.3 Frequency-Consequence Curve

2.4 Concluding Remarks

This chapter proposes a "design for safety" methodology for marine and other large MTO products. This methodology may be effectively used to incorporate safety into the design process from the initial stages so that unexpected cost and delays due to late modifications regarding safety can be reduced to a minimum. Such a methodology may allow consideration of safety as a design criterion for decision making purposes and also accelerate the verification process.

The proposed "design for safety" methodology could form the basis for further development of individual safety analysis methods and safety based decision making tools to face the challenge imposed by the increasing technical standards and the growing complexity of MTO products.

Further work required in the areas of "design for safety" of MTO products includes:

- Implement the proposed "design for safety" methodology.
- Investigate the existing safety analysis methods and their interrelations within the "design for safety" process.
- Synthesise some of the safety analysis methods to create more flexible and applicable mixed safety analysis tools.
- Develop novel safety analysis methods to make safety analysis more flexible and efficient.
- Develop techno-economic modelling techniques to integrate safety analysis and economic modelling in order to optimise design aspects and operation policies.

REFERENCES - CHAPTER 2

[2.1] Aldwinckle D. S., Pomeroy R. V., *A rational assessment of ship reliability and safety*", Transaction of RINA, 1983, 269-288.

[2.2] Bridges D. C., *The application of reliability to the design of ship's machinery,* Trans. I.Mar.E., Vol.86, 1974, 109-120.

[2.3] Brown D. B., *Systems analysis & design for safety,* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.

[2.4] *B. S. 5760: Part 1, 2, 3: Reliability of systems, requirements and components,* 1979.

[2.5] Cleland G., *Review of design methodologies,* EDCN/EXPS/DISC/1/1, Engineering Design Centre, University of Newcastle upon Tyne, October 1991, 28 pages.

[2.6] Cleland G., King B., J., *A perspective of the conceptual design process for a large, complex Made-To-Order engineering artifact,* Journal of Engineering Design, Vol.4, No.1, 1983, 55-67.

[2.7] Cross N., *Engineering design methods,* Wiley, 1989.

[2.8] Department of Energy, *The public inquiry into the Piper Alpha disaster,* (Cullen Report), HMSO, ISBN 0 10 113102, 1990.

[2.9] Ertas A., Jones J. G., *The engineering design process,* John Wiley & Sons Inc., 1993.

[2.10] Finkelstein L., Finkelstein A. C. W., *Review of design methodology,* IEE Proceedings, Vol.130, Pt.A, No.4, 1983, 213-221.

[2.11] Henley E. J., Kumamoto H., *Probabilistic risk accessment,* IEEE Press, New York, 1992.

[2.12] House of Lords, *Safety aspects of ship design and technology,* (Carver Report), Select Committee on Science and Technology, 2nd Report, HL Paper 30-I, February 1992.

[2.13] Jones J. V., *Engineering design: reliability, maintainability and testability,* TAB Books Inc., USA, 1988.

[2.14] Labrie C. R., *Design for safety: design methodology,* Research Report, EDCN/SAFE/RESC/12/1, Engineering Design Centre, University of Newcastle upon Tyne, June 1992, 29 pages.

[2.15] MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* Military Standard, Naval Ship Engineering Center, Washington D.C..

[2.16] Papalambros P. Y., Wilde D. J., *Principle of optimal design: modelling and computation,* Cambridge University Press, 1988.

[2.17] Ruxton T., Wang J., *Advances in marine safety technology applied to marine engineering systems,* Proceeding of First Joint Conference on Marine Safety and Environment, Delft, The Netherlands, June 1992, 421-432.

[2.18] Ruxton T., *Safety analysis required for safety assessment in the shipping industries,* Presented to NECJB, Institute of Marine Engineers and the Royal Institute of Naval Architects, December, 1992.

[2.19] Sen P., Labrie C. R., Wang J., Ruxton T., Chan J., *A general design for safety framework for large made-to-order engineering products,* Proceeding of First Newcastle International Conference on Quality and Its Applications, Newcastle, September 1993, 499-505.

[2.20] Wang J., *Fault diagnosis of marine automatic control systems and application of decision table and expert system to marine engineering,* MSc Dissertation, Department of Marine Technology, University of Newcastle upon Tyne, 1989, 189 pages.

[2.21] Wang J., *Design for safety: a general review in marine field,* Research Report, EDCN/SAFE/RESC/1/1, Engineering Design Centre, University of Newcastle upon Tyne, February 1991, 60 pages.

[2.22] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12.

[2.23] Wang J., Ruxton T., Thompson R. V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, Presented at the Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, December 1993, 1-10.

CHAPTER 3

Safety Analysis Methods Applied to the "Design for Safety" Process

SUMMARY

"Design for safety" is a process of identifying hazards, estimating them and finally evaluating them in terms of two basic parameters, namely the probability of occurrence of each hazard and possible consequences. These two parameters can be assessed using either a top-down or a bottom-up approach on either a qualitative or a quantitative basis, depending on the nature of the particular engineering system and the safety assessment techniques in hand.

This chapter describes the concepts of qualitative and quantitative safety analysis, and bottom-up and top-down safety modelling approaches. The typical safety analysis techniques are studied with respect to the proposed "design for safety" framework. An analysis of the input requirements and the outcomes of the safety analysis methods is carried out to identify their possible inter-relationships within the safety analysis process in order to make full use of the advantages of each method. The selection of these safety analysis methods is discussed in the context of MTO products. Problems concerned with failure and repair data collection programmes are studied and some typical failure and repair data sources are described.

3.1 Introduction

In performing the safety analysis of a MTO product, it is almost impossible to treat the system in its entirety. The logical approach may be to break down the system into functional entities comprising subsystems and components. Safety modelling of these functional entities can be carried out to fit such a logical structure, then the interrelationships can be examined and finally a system safety model can be formulated to calculate the safety parameters.

The formulation of the system safety model can be difficult for a large and sophisticated MTO product and thus requires approximations and judgement. It may be best done by someone who knows the system operation thoroughly. The safety analysis methods may be applied individually or in a combined way to carry out either a qualitative or a quantitative safety analysis.

It is very beneficial to effectively and efficiently use the safety analysis methods in the "design for safety" process. In the literature, these methods are only studied in a very general way. When and how these methods are specifically applied in the design process and how these methods interrelate are usually not specified. This chapter specifies how to deal with such problems. This requires an understanding of the concepts of qualitative and quantitative safety analysis and the concepts of top-down and bottom-up safety analysis techniques.

In this chapter, qualitative and quantitative safety analysis is described, top-down and bottom-up event-based safety analysis approaches are studied, and the typical safety analysis methods are outlined and discussed with respect to each phase of the "design for safety" process. Then, the interactions of the outlined safety analysis methods are studied in order to make full use of their advantages, and the selection of such methods is discussed with reference to the characteristics of MTO products.

Since the quality of safety data significantly affects the results of safety analysis, failure and repair data collection programmes are also studied and some typical data sources are recommended.

3.2 Qualitative and Quantitative Safety Analysis

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

3.2.1 Qualitative Safety Analysis

Qualitative safety analysis is used to locate possible hazards and to identify proper precautions (design changes, administrative procedures, etc.) that will reduce the frequencies or consequences of such hazards.

Qualitative safety analysis should become an integral part of the design process of a product. It may be performed with one or more of the following objectives:

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

The general steps in a qualitative system safety analysis are to:

i. Identify significant risks.

ii. Display the above information in a table, a chart, a fault tree or other format.

The consequences of a hazard can be classified as one of the four severity categories as shown in Table 3.1 [3.13]. They range from catastrophic to negligible. The probability of occurrence of a hazard can be described using the levels ranging from frequent to remote as shown in Table 3.2 [3.13].

Table 3.1 Hazard consequence classification

Categories	Description	Equipment	Personnel
i	Catastrophic	System loss	Death
ii	Critical	Major system damage	Severe injury or severe occupational illness.
iii	Marginal	Minor system damage	Minor injury or minor occupational illness
iv	Negligible	Less than minor system damage	Less than minor injury or minor occupational illness

Table 3.2 Hazard Probability

Level	Description	Frequency
1	Frequent	Likely to happen
2	Probable	Several time during lifetime.
3	Occasional	Likely to happen once
4	Remote	Unlikely but possible during lifetime

Engineering judgement and past experience are required to carry out a qualitative safety analysis. Measures can be taken to eliminate or control hazards based on the information produced from qualitative safety analysis. Table 3.3 forms the basis of design actions required to deal with identified hazards based on the combined consequence severity and probability of occurrence [3.13]. For example, a catastrophic hazard requires some corrective action regardless of the probability of occurrence while a marginal hazard with a remote probability of occurrence would normally not receive any corrective action since it would not be considered to be cost-effective.

Table 3.3 Risk assessment matrix

	Frequent	Probable	Occasional	Remote
Catastrophic	I-1	I-2	I-3	I-4
Critical	II-1	II-2	II-3	II-4
Marginal	III-1	III-2	III-3	III-4
Negligible	IV-1	IV-2	IV-3	IV-4

where: design action is required to eliminate or control hazards classified as I-1, I-2, I-3, II-1, II-2 and III-1;
hazard consequences must be controlled or hazard probabilities must be reduced for hazards classified as III-2, II-3 and I-4;
hazard control is desirable for hazards classified as III-3 and II-4 if cost-effective; and
no design action is normally required for hazards classified as III-4, IV-1, IV-2. IV-3 and IV-4.

3.2.2 Quantitative Safety Analysis

The purpose of a quantitative safety analysis is to help the designer to be aware of the characteristics of the product, particularly its capabilities with the environment and other technical design aspects, and to provide the designer with the quantified probability of occurrence of each critical failure condition and the associated consequences. Quantitative safety analysis utilises what is known and assumed about the failure characteristics of each individual component to build a mathematical model which is associated with some or all of the following information:

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

Typical parameters that need to be obtained in a quantitative safety analysis include availability, the probability of occurrence of each system failure event and possible consequences.

Availability

This parameter is very useful, especially when techno-economic modelling is used for design decision making. The availability of a system is given by:

$$Availability\ (A(\infty)) = \frac{Up\ time}{Up\ time + Down\ time}$$

Probability of occurrence of a system failure event

A system failure event results from simultaneous occurrence of the basic events associated with each of the minimal cut sets leading to this system failure. The probability of occurrence of a system failure event may be calculated on the basis of the identified cut sets and failure probability data of the associated basic events. The probability of occurrence of a basic event for a period of time t can be obtained from the following expression if the failure follows an exponential distribution:

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

where t is the period of time of interest, $P(t)$ represents the probability of occurrence of the basic event at t, and λ is the failure rate.

Consequences

As described in Chapter 2, the possible consequences of a system failure event can be quantified in terms of the possible loss of lives and property damage, and the degradation of the environment caused by the occurrence of the failure event. They are normally quantified by experts with respect to the particular operating situation.

Consistency checking is required to validate the results produced from quantitative analysis. The following studies are always useful for obtaining the reliable results [3.30].

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

3.3 Top-down and Bottom-up Safety Analysis Approaches

System "design for safety" is a complex subject. It is not so much a question of looking at an individual piece of equipment and determining how its safety can be improved; rather it is to look at interactions of the components in the system and determine how the overall safety can be improved. To achieve this, safety analysis methods may be applied to carry out safety analysis on the basis of hardware elements or hazardous events.

Efficient use of the safety analysis methods in the "design for safety" process involves the study of the characteristics of each safety analysis method and the "design for safety" process in terms of the way in which safety analysis is carried out. A "design for safety" process may be classified as either top-down or bottom-up by studying the way in which risks of a system are identified. The safety analysis methods can also be classified in such a way.

3.3.1 Top-down Approach

A top-down event-based "design for safety" process of a product starts with the study of previous accidents and incident reports of similar products. The top events required for further study are determined and the causes leading to them are then identified deductively until all the causes are identified at the required level of resolution. A Fault Tree Analysis (FTA) is a typical top-down safety analysis method which can be integrated into a top-down "design for safety" process.

In a top-down event-based "design for safety" process, both qualitative and quantitative analysis can be carried out to estimate and evaluate risks regarding the demand for safety. A design review can then be undertaken, by making use of the information produced, to close the loop of the "design for safety" process. The diagram of a top-down "design for safety" process is shown in Figure 3.1. The phases in this diagram are in harmony with the proposed "design for safety" methodology shown in Figure 2.2.

For MTO products with a comparatively low level of innovation, a top-down safety approach may prove convenient and time-saving because it only deals with failure paths leading to particularly serious system failure events by studying the relationships of the subsystems and components and the safety data from previous accidents and incident reports of similar products. Obviously, experience, good judgement and understanding

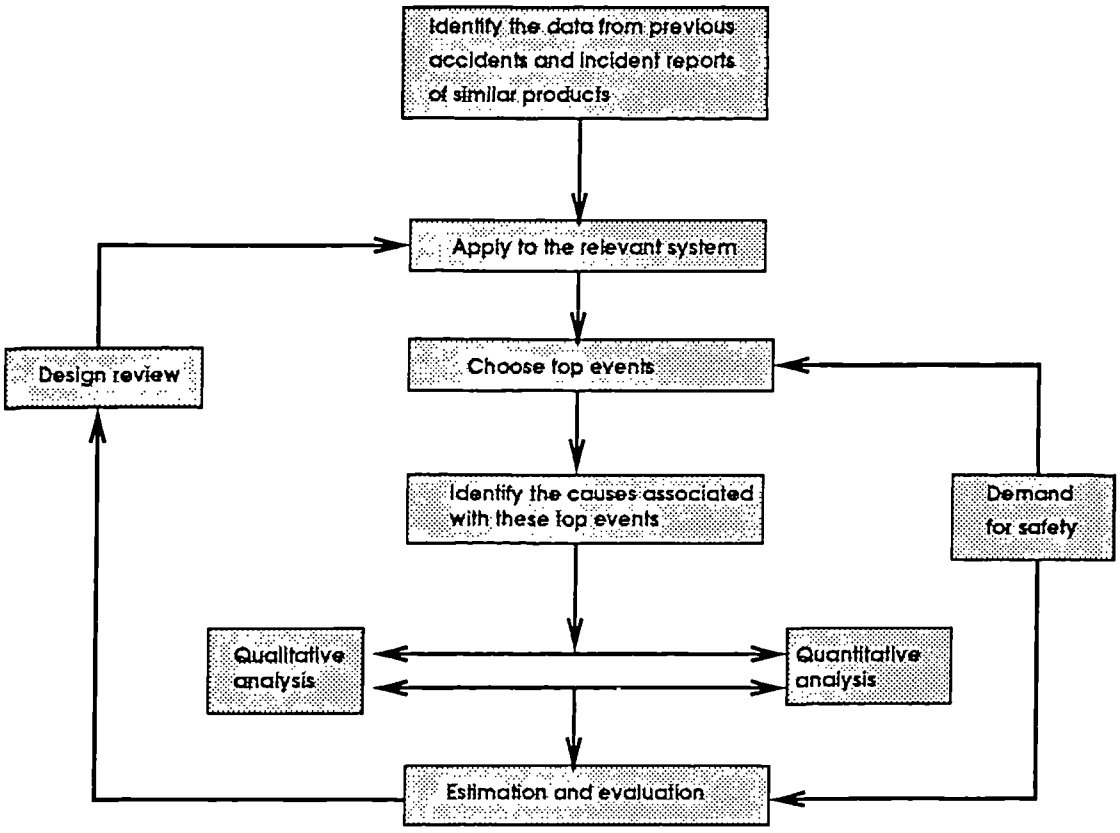


Figure 3.1 A top-down "design for safety" process

of the system are very important for an efficient use of this approach.

However, for the design of MTO products with a comparatively high level of innovation, there will often be a lack of knowledge or experience regarding the determined design solutions and their possible effects on product safety. In such a case, the top-down approach may have following problems:

- Failure data from similar products may not be available.
- Lack of certainty that all system failure events and respective failure causes have been identified.
- The deductive properties of a top-down approach may not address all the complex interactions present in a large MTO product in an analytically rigorous manner.

Therefore, a bottom-up event-based safety analysis approach may be required.

3.3.2 Bottom-up Approach

In a bottom-up "design for safety" process, a system to be analysed can be divided into subsystems which can be further broken down to the component level in order to identify all possible hazards. The hazard identification can be initially carried out at the component level, progressed up to the sub-system level and finally to the system level. All combinations of possible failure events at both the component and the subsystem levels may be studied to identify all the possible system failure events. The analysis at the sub-system level may make use of the information produced at the component level. Finally, risk evaluation and design review can be conducted.

A bottom-up "design for safety" framework incorporating three specific safety analysis methods, namely FMECA, the Modified Boolean Representation Method (MBRM) (it will be studied in more detail in Chapter 4) and the Monte Carlo simulation analysis is presented as shown in Figure 3.2. In this framework, FMECA is carried out to identify all possible failure events of a system at the component level in the risk identification phase, and the MBRM and the Monte Carlo simulation method are used to identify the minimal cut sets leading to each system failure event and to estimate the probability of occurrence of each such failure event. The information produced from the risk estimation phase can then be evaluated together with a design review.

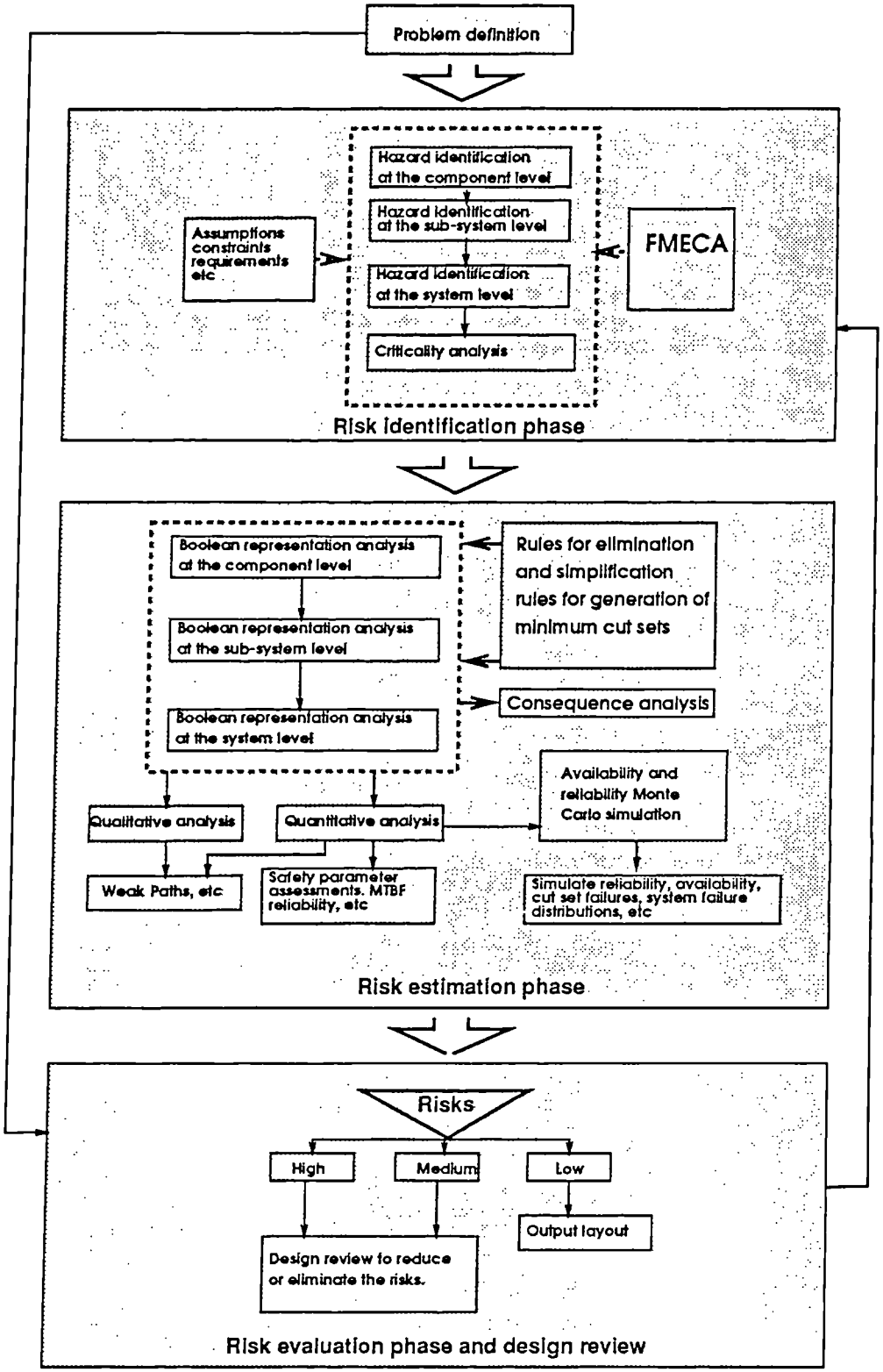


Figure 3.2 A bottom-up "design for safety" framework

The use of an inductive bottom-up safety analysis approach yields a higher level of confidence that all of the failure events of a system and their respective causes are identified. Therefore, compared to the top-down approach, the bottom-up approach has the following advantages:

- Omission of system failure events and their respective causes is less likely.
- It may be more convenient to be incorporated into a computer package.
- It may be more suitable to be applied to original MTO product design as discussed above.

It may however be more time-consuming although the provision of powerful computers may overcome such a shortcoming.

3.4 Safety Analysis Methods Applied to the "Design for Safety" Process

3.4.1 Preliminary Hazards Analysis (PHA)

A preliminary identification of the system elements or events that lead to hazards is the first step of a safety analysis. If it is extended in a more formal manner to include considerations of the event sequences which transfer a hazard into an accident, as well as corrective measures and consequences of the accident, the study is called a Preliminary Hazards Analysis (PHA).

PHA is a qualitative approach which involves a mixture of inductive and deductive logic. It is conducted on the basis of information such as casualty statistics and comprehensive knowledge of similar systems. A PHA may provide an essential foundation for further analysis of individual hazards, with particular reference to Fault Tree Analysis and Event Tree Analysis [3.33]. The detailed description of PHA is described in many references [3.9][3.13][3.15]. The typical steps of a PHA are described as follows:

i. Identification of hazardous events.

ii. Identification of hazardous event causes.

iii. Identification of hazardous event effects.

iv. Classification of risks.

v. Determination of preventive measures.

PHA may be very useful in the problem definition and risk identification phases of the "design for safety" process. It is strongly suggested that PHA be carried out in the initial stages of the MTO product design process.

3.4.2 **Fault Tree Analysis (FTA)**

Fault Tree Analysis (FTA) is probably the most widely applied technique for risk identification and risk evaluation. Such an analysis is a process of deductive reasoning which can be applied to the safety assessment of a system of any size. It is particularly suitable for the safety analysis of large MTO products for which the associated top events can be identified by experience, from previous accidents and incident reports of similar products, or by some other means.

A FTA is a systematic engineering technique that provides a diagrammatic representation of the relationships between specific events or component failures and an undesirable top event. It provides an engineering capacity to identify potential problem areas, to evaluate their overall system impact, and to numerically assess the level of safety inherent in the system design. In a fault tree analysis, an event with a catastrophic nature or an event that cannot be tolerated, such as total loss of a system, is usually selected as a top event for investigation. The selected top event is placed at the top of the logic diagram, and the failure events that lead to the top event are located immediately below in successive levels of indenture. The pathways through the fault tree diagram represent all the failure modes which give rise to the top event. These pathways are known as "cut sets" or "implicant sets". After some simplification rules have been applied, the irreducible pathways can be obtained and these irreducible pathways are referred to as "minimal cut sets" or "implicant sets".

Careful consideration must be given to the selection of the top event; it must be sufficiently defined to constrain the fault tree to the specific conditions to be investigated. Intimate knowledge of the system design is required to perform a fault tree analysis as the analyst must be familiar with the various modes of system operations and the types of component failures that can occur. Since a fault tree

construction is event-based, human error (caused by operators, design or maintenance), hardware or software failures, environmental conditions or operational conditions can be taken into account [3.33].

The steps in FTA are outlined as follows:

i. Identification of top events.

ii. Representation of each top event by means of a fault tree.

iii. Evaluation of the probability of occurrence of each top event.

iv. Determination of critical failure modes.

Detailed description of FTA and its applications can be found in various published documents such as [3.2][3.13][3.15].

The top events of a system to be investigated in FTA may also be identified through a PHA or may correspond to a branch of an event tree or a system Boolean representation table. The information produced from FMECA may be used in construction of fault trees.

FTA may be carried out in the risk identification and risk estimation phases of the "design for safety" process to identify the minimal cut sets associated with serious system top events and to assess the probability of occurrence of each top event in order to assist in design decision making.

3.4.3 Failure Mode, Effects and Criticality Analysis (FMECA)

Failure Mode, Effects and Criticality Analysis (FMECA) is probably the most widely applied hazard identification method. It can be carried out at any indenture level required to examine each failure mode of an item and its possible consequences. A FMECA may consist of the following steps [3.26]:

i. Define the constraints and assumptions of the analysis.

ii. Break down the system to its indenture levels such as the sub-system level and the component level.

iii. For each item at the indenture level analysed, identify all possible modes of failures and respective causes.

iv. For each identified failure mode, identify or provide the following information:

(i) All the distinctive operating conditions under which failure may occur.

(ii) The failure rate of the identified failure mode.

(iii) The effects (consequences) on the safety and operability of the higher indenture levels (including the level analysed).

(iv) The possible means by which failure may be identified.

(v) Design provisions and/or actions in operation to eliminate or control the possible resulting effects.

(vi) The severity class of the resulting identified effects where such a class may be defined by one of the following linguistic variables:

1.	Catastrophic:	Involving death and/or system loss.
2.	Critical:	Involving severe injury and/or major system damage.
3.	Marginal:	Involving minor injury and/or minor system damage.
4.	Negligible:	Involving no injury and negligible damage to the system.

(vii) Failure consequence probability defining the likelihood that the failure effects of the identified failure mode will occur, given that the failure mode has taken place.

v. Criticality analysis

Criticality analysis allows a qualitative or a quantitative ranking of the criticality of the failure modes of items as a function of the severity classification and a measure of the frequency of occurrence.

If the probability of occurrence of each failure mode of an item can be obtained from a reliable source, the criticality number of the item under a particular severity class may be quantitatively calculated as follows [3.26]:

$$C = \sum_{i=1}^{N} E_i \, L_i \, t$$

where E_i = failure consequence probability of failure mode i,
L_i = likelihood of occurrence of failure mode i,
N = number of the failure modes of the component, which fall under a particular serverity classification,
t = duration of applicable mission phase.

After all criticality numbers of the item under all severity classes have been obtained, a criticality matrix can be constructed which provides a means of identifying and comparing each failure mode to all others with respect to the same severity class. Such a matrix display shows the distributions of criticality of the failure modes of the item and provides a tool for assigning priority for corrective action. Criticality analysis can be performed at different indenture levels. Information produced at low indenture levels may be used for criticality analysis at a higher indenture level.

To maximise the usefulness of a FMECA as a decision making tool, it should be initiated at the earliest stage of design and updated and expanded to lower indenture levels as the design progresses.

A FMECA is an inductive process which involves the compilation of reliability data, where available, for individual items. Information produced from FMECA may be used to assist in construction of fault trees, and especially in construction of Boolean representation descriptions as will be described in Chapter 4.

FMECA can be integrated into the risk identification phase of the "design for safety" process. As described above, some corrective actions, or in other words design changes, can be undertaken on the basis of FMECA.

3.4.4 HAZard and OPerability studies (HAZOP)

A HAZard and OPerability (HAZOP) study is an inductive technique which is an extended FMECA and which can be applied by a multidisciplinary team using a checklist to stimulate systematic thinking for identifying potential hazards and operability problems, particularly in the process industries [3.15]. In recent years, HAZOP studies have become increasingly recognised as an essential part of the process plant design. The HAZOP methodology is probably the most effective of all hazard identification techniques used in the chemical process industries. Its distinctive features are:

i. A focus on state variables rather than mechanical components.

ii. An emphasis on an expert team approach.

iii. An explicit consideration of operator effects.

iv. A good foundation for subsequent quantitative risk analysis.

A HAZOP study investigates the proposed scheme systematically for every conceivable deviation, and looks backwards for possible causes and forward for the possible consequences. It is normally based on a word model and the flow sheet or diagram of the system to be examined. HAZOP study planning is determined by the level of detail, depending on the time and merits. A good knowledge of the system is essential. HAZOP studies involve normal plant operation, foreseeable changes in normal operation, startup and shutdown, suitability of plant materials and failures of equipment and instrumentation. A HAZOP study may involve the following eight basic steps [3.25]:

i. Define the scope of the study.

ii. Select the correct analysis team.

iii. Gather the information necessary to conduct a thorough and detailed study.

iv. Review the normal functioning of the process.

v. Subdivide the process into logical, manageable sub-units for efficient study and confirm that the scope of the study has been correctly set.

vi. Conduct a systematic review according to the established rules for the procedure being used and ensure that the study is within the special scope.

vii Document the review proceedings.

viii. Follow up to ensure that all recommendations from the study are adequately addressed.

The HAZOP methodology may stand a better chance of being a comprehensive detector of failure modes than other alternative methods used in risk identification of chemical process plants [3.5], and it is relatively easier to incorporate into a computer package than the other hazard identification techniques [3.36]. The form of HAZOP notes closely parallels the requirements of fault tree analysis as a HAZOP study yields a clear identification of top events and a detailed description of failure sequences and associated operating conditions. FMECA, cause-consequence analysis and Boolean representation analysis can also make use of the information produced from HAZOP studies. It is strongly suggested that HAZOP studies be conducted in the initial stages of the process plant design process.

HAZOP studies can be integrated into the risk identification and risk estimation phases of the "design for safety" process. The detailed description of this methodology can be found in [3.5][3.17][3.25][3.26][3.48].

3.4.5 Decision Table Method (Boolean Representation Method (BRM))

Decision table analysis was initially introduced as an automatic fault tree construction technique in the 1970s [3.3][3.10][3.12][3.15][3.19][3.28][3.32] because its logical approach reduced the possibility of omissions which could easily occur in fault tree construction. A decision table is a Boolean representation model [3.26].

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

After components and their interactions have been modelled, the Boolean representation modelling can be started initially at the component level, progressed up to the subsystem level if necessary, and finally to the system level in order to obtain the final system Boolean representation description. Given sufficient information about a system to be analysed, this approach can allow a rapid and systematic construction of a Boolean representation table of the system on the basis of the Boolean representation models of the components and their interactions.

The final system Boolean representation table contains all the possible system top events and the associated cut sets. Although the construction of such a table is not diagrammatic, as FTA can be, it can allow a less cumbersome representation of failure modes for components having multiple states, and it can also allow systems with feedback loops to be easily modelled [3.15][3.19][3.44]. This method is extremely useful for analysing systems with a comparatively high degree of innovation since their associated top events are usually difficult to obtain by experience, from previous accidents and incident reports of similar products, or by other means.

Decision table modelling is an inductive bottom-up method and can be integrated into the risk identification and risk estimation phases of the "design for safety" process to inductively identify system top events and associated causes. On the basis of the obtained system Boolean representation table, both qualitative and quantitative analysis can be carried out to estimate the probabilities of occurrence of each identified top event and associated cut sets. The information produced from FMECA may be directly used to assist in the construction of the system Boolean representation table [3.44].

This inductive bottom-up method may be very suitable to the safety analysis of most MTO products, and it will therefore be studied in more detail in Chapters 5 and 6.

3.4.6 Event Tree Analysis (ETA)

If a failure occurs it may propagate through the system and result in some possible consequences. Event Tree Analysis (ETA) is often used to deduce such consequences, step by step, that involve the complex relationships among the components or subsystems of the system given the occurrence of an initiating event. Event trees are diagrammatically constructed by using forward logic, that is, inductive bottom-up logic [3.13]. Quantitative analysis can be carried out to assess the probability of occurrence of each possible resulting consequence on the basis of the constructed event trees.

ETA provides a systematic and logical approach to identify the consequences and to assess the probability of occurrence of each possible resulting sequence caused by the initiating failure event [3.15][3.39]. Such an analysis can be integrated into the risk identification and risk estimation phases of the "design for safety" process.

3.4.7 Cause-Consequence Analysis (CCA)

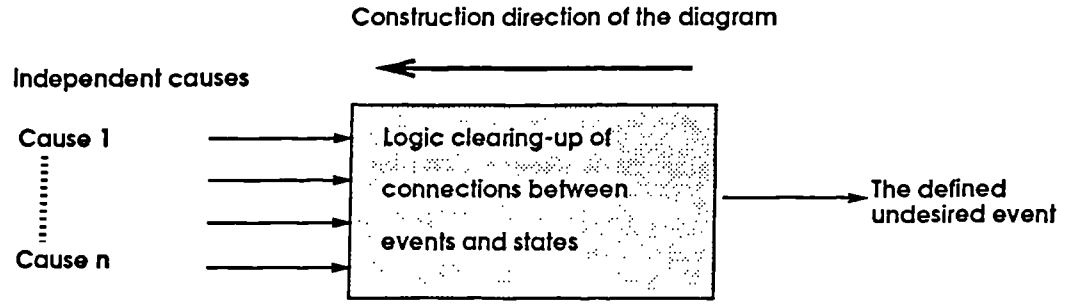
Cause-Consequence Analysis (CCA) is a marriage of fault tree analysis (to show causes) and event tree analysis (to show consequences). CCA is a diagrammatic approach. Construction of cause-consequence diagrams starts with a choice of a critical event. The "consequence tracing" part of a CCA involves taking the initial event and following the resulting chains of events through the system. The "cause identification" part of a CCA involves drawing the fault tree and identifying the minimal cut sets leading to the identified critical event. CCA is extremely flexible as it can work forward using event trees and backward using fault trees. The inputs and outputs of cause diagram and consequence diagram of CCA are shown in Figure 3.3.

The detailed description and applications of this approach are the same as discussed in FTA and ETA in this chapter.

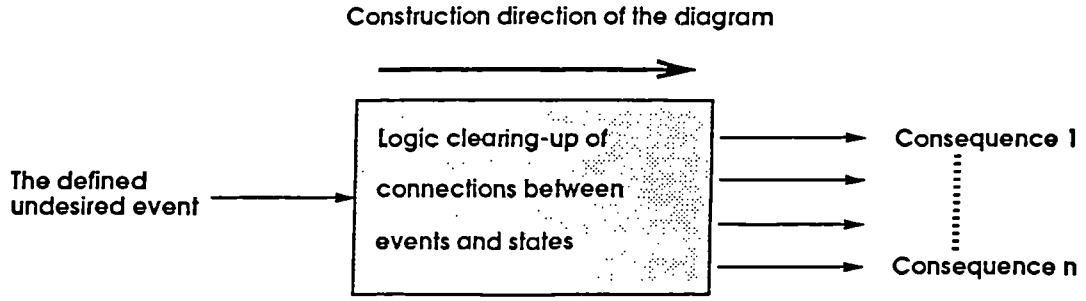
3.4.8 Digraph-based Analysis (DA)

Digraph-based Analysis (DA) is becoming increasingly attractive, especially in the process industries, because relatively little information is needed to set up digraphs and perform safety analysis [3.18]. In a digraph-based analysis, the nodes correspond to the state variables, alarm conditions, or failure origins, and the edges represent the causal influences between the nodes. The direction of deviation of the nodes can also be represented by signs on the branches on the Directed Signed DiGraph (DSDG) [3.18].

DA is a bottom-up event-based qualitative technique. From the constructed digraph, the causes of a state change and the manner of the associated propagation can be easily found out [3.38]. Digraph representation provides explicit causal relationships among variables and events of systems with feedback loops.



The input and output data of the cause diagram



The input and output data of the consequence diagram

Figure 3.3 The cause and consequence diagram of cause-consequence analysis

The digraph approach may be very efficient for identifying possible causes of process disturbances [3.18]. The rules generated from DA can be used as knowledge of an expert system for plant operations.

DA may be integrated into the risk identification phase of the "design for safety" process, especially in chemical process plant designs.

3.4.9 Simulation

Generally, simulation techniques can be classified as two categories, namely quantitative simulation and qualitative simulation. These two kinds of simulation techniques are briefly described as follows.

3.4.9.1 Quantitative Simulation

FTA, ETA, CCA and BRM discussed above are deterministic methods. In other words, given that the model is correct, for given reliability data there is only one answer. Such deterministic methods are usually limited to deal with simple AND/OR logic and constant failure rates and straightforward mean down times [3.36]. For dealing with failure events with different distributions and taking into account other factors such as maintenance and repairs, computer-based simulation, sometimes known as Monte Carlo simulation analysis, may provide a quick and cost-effective way to conduct a quantitative safety analysis using probability distributions.

There are a variety of algorithms for carrying out quantitative simulation analysis when simulation techniques are used together with other formal safety analysis methods such as FMECA, FTA, ETA, CCA and BRM. For example, on the basis of the cut sets associated with a top event of a system obtained using the fault tree technique, failures of each cut set can be determined by comparing each cut set with simulated basic event failures, and the probabilities of occurrence of the top event and associated cut sets can be assessed using the Monte Carlo simulation method. Such a simulation permits basic events associated with each cut set to be specified by a range of statistical distributions such as Normal, Weibull and Exponential.

Simulation analysis is increasingly being used in safety analysis of engineering products. This method may be used in the risk estimation phase of a "design for safety" process. It will be studied in more detail in Chapter 6.

3.4.9.2 Qualitative Simulation (Qualitative Reasoning)

Qualitative simulation (qualitative reasoning) analysis was initially developed in the field of Artificial Intelligence. As will be stated in more detail in Chapter 5, this method can be modified to be applied to failure propagation analysis and to modelling the behaviour of a system.

Qualitative reasoning analysis is an inductive process. It can be combined with FTA and BRM to form mixed approaches to efficiently and conveniently model a system for safety analysis. This method can be used in the risk identification and risk estimation phases of the "design for safety" process.

3.4.10 Subjective Reasoning Analysis (SRA)

As described in Chapter 1, the safety of an engineering system is affected by many factors such as design, installation and operations. Therefore, in some cases, it could be very difficult for the safety engineer to precisely obtain the parameters of basic failure events to carry out quantitative analysis using the probabilistic safety analysis methods outlined above (from 3.4.1 to 3.4.9) since a great deal of uncertainty is involved. However, Subjective Reasoning Analysis (SRA) may prove relatively easier to deal with such problems with uncertainty. SRA involves the use of fuzzy set modelling and subjective descriptors such as "*Very good*" and "*Very low*", which are commonly used by safety analysts. Such an analysis is extremely useful to model systems which are operated in a very changeable environment. SRA may be effectively used as an alternative approach in the risk identification and risk estimation phases of the "design for safety" process. This method will be studied in more detail in Chapter 7.

3.4.11 Human error

Human error was involved in the majority of well-known major incidents such as the Three Mile Island and Chernobyl disasters. Therefore, the contribution of human error to system failures should be taken into account in safety analysis. In assessing the safety of a MTO product it is necessary to ensure that facilities are provided to reduce the probability of human error and consequential effects.

Human error study is a complex subject which may involve the following factors:

i. Environmental factors — physical, organisational and personal.

ii. Internal error — training, experience, toleration by supervisor and lack of supervision.

iii. Technical error — lack of sufficient instruction, poor concentration, feasibility of the product design, and unforeseen causes.

iv. Unknown or undetermined causes.

Human error rates for various forms of activities may be needed to carry out quantitative safety analysis involving human error. Human error rates are often difficult to obtain from failure and repair data collection programmes. The difficulties come from the following causes [3.36]:

- Low probabilities of human error require a large amount of experience.
- Most of the data collection programmes concentrate on recording the events rather than analysing the causes.
- Many large organisations have not been prepared to commit the necessary resources to collect human error data.

If there is no human error data available from failure and repair data collection programmes, human error assessment models may be used to assess human error rates with respect to the factors such as the complexity of the task, the level of training and experience of personnel involved. There are currently several such models developed by separate groups of analysts working in this field [3.36]. The examples of such models are:

- HEART (Human Error Assessment and Reduction Technique) developed by J. C. Williams [3.36].
- THERP (Technique for Human Error Rate Prediction) developed by A. D. Swain and H. E. Guttmann [3.36].
- TESEO (Empirical Technique To Estimate Operator Errors) developed by G. C. Bellow and V. Colombari [3.36].

When several models are available for quantifying a human error event, the need arises to compare them and to decide which is the most suitable for the task in hand. The factors for comparison may include accuracy, consistency, usefulness and resources [3.36].

In some cases, there may not be sufficient resources for using human error assessment models, and simple human error rates in some particular situations may need to be assigned. Such simple human error rates may be obtained from various publications such as [3.35][3.36][3.49].

Human error should be considered in the "design for safety" process and should be reduced to a minimum extent, especially in those cases where the consequences of human error are critical. Generally, the probability of human error may be reduced by following measures:

- The introduction of safety warning devices such as sensors and alarms for the timely detection of the condition and the generation of an adequate warning signal so that personnel can evaluate the area and take corrective action.
- Improving training, supervision and communication.
- Increasing the level of automation.

3.4.12 Discussion

The following are some general observations on the range of safety analysis tools that are available:

i. The use of the methods outlined above can offer considerable benefits to MTO product design. The safety of a MTO product can be demonstrated on either a qualitative or quantitative basis using these techniques, and safety aspects may then be improved to suit the requirements of both owners and regulatory authorities.

ii. The above outlined safety analysis methods are the typical ones which can be applied to the "design for safety" process of MTO products. Besides these methods, there are some other safety analysis methods which may also be used in some particular situations. These include:

   - Markov techniques [3.6][3.27].
   - Network modelling techniques [3.6][3.27].
   - Critical item analysis [3.11][3.41].
   - Limit state reliability analysis [3.2][3.20][3.33][3.42].

iii. Each of the safety analysis methods outlined above may be used in different ways or in different formats by safety analysts. For example, a FMECA of a

system may be carried out using the United States Military Standard [3.26] in an organisation, and it may be carried out using the guide published by the Institute of Electrical and Electronics Engineers [3.16] in another organisation.

iv. The safety analysis methods outlined above are being extensively developed in various possible application areas. For example, the research on applications of FTA is being undertaken in the areas such as evaluation of fault trees using the gate-by-gate method [3.9], and evaluation of fault trees based on fuzzy logic [3.34].

v. Various computer codes for the safety analysis methods outlined above are available [3.14][3.26].

vi. The safety analysis methods outlined above are increasingly applied in the "design for safety' process of MTO products as more and more computer-based safety analysis tools are made available and as the importance of the safety analysis for MTO products is realised.

vii. Further developments of the safety analysis methods outlined above are still required to make safety analysis more flexible, effective and accurate to satisfy the requirements of designing safer and more reliable MTO products.

viii. It has also been realised that some of these safety analysis methods may be more beneficially used in a combined manner for effective and efficient safety analysis [3.46].

3.5 Failure Data Collection Programmes

It is essential to obtain reliable statistical failure and repair data of components in order to carry out quantitative safety analysis using the described probabilistic safety assessment techniques. Generally, such failure and repair data of components can be obtained from the following sources [3.42][3.27]:

i. Field experience.

ii. Life testing under controlled conditions in laboratory.

iii. Field experience and laboratory testing of similar components.

In addition, repair data may also be compiled from the agreed judgemental estimates of experts [3.27].

The collection of failure and repair data based on field experience and accelerated life tests of MTO products is precluded as the former may not be possible due to the characteristics of MTO products and the latter is a very expensive and labour demanding operation. Hence, extensive use is made of failure and repair data collected from laboratory tests and field reports on similar components (generic data collection programmes).

It should be noted that for some components there is fairly close agreement between different data banks and in other cases there is a wide range of failure rates [3.36]. The latter may be due to a number of reasons as, for example:

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

Great care should be taken to use failure and repair data obtained from data banks to reflect the environment to which the product is designed. When no data for a component failure mode can be obtained, it may be possible to express the failure in terms of fundamental and quantifiable parameters and to analyse it using limit state reliability analysis [3.42], although even here there is uncertainty about the relevant distributions.

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

The following sources may be useful for obtaining failure and repair data to carry out quantitative safety analysis.

i. *FARADIP.THREE [3.36].* This database is a summary of all the other databases and shows, for each component, the range of failure values. The failure data of various components such as alarms, mechanical items and instruments is included in this database.

ii. *US Military Handbook 217.* This data source is produced by the Rome Air Development Centre under contract to the US Department of Defence and is an electronic failure data bank.

iii. *Nonelectronic Parts Reliability Data - NPRD3(1985).* This document is produced by the Rome Air Development Center. It contains field data information of electromechanical, mechanical, hydraulic and pneumatic parts.

iv. *Handbook of Reliability Data for Electronic Components Used in Telecommunications Systems HRD4 (1986).* This document is produced, from field data, by British Telecom's Materials and Components Centre.

v. *Electronic Reliability Data - INSPEC/NCSR (1981).* This book, published jointly by the Institute of Electrical Engineers and the National Centre of Systems Reliability (Warrington) in 1981, consists of simple multiplicative models for semiconductor and passive electronic components with tables from which to establish the multipliers according to the environment, temperature and other parameters.

vi. *OREDA- Offshore Reliability Data (1984).* It is a collection of offshore failure rate and failure mode data with an emphasis on safety-related equipment. It covers a great range of components and equipment.

vii. *Green and Bourne - Reliability Technology, Wiley, 1972.* This book contains failure rate data obtained mostly from US and UK atomic energy sources.

viii. *UK Atomic Energy SRD Data Bank.* It contains the generic reliability data of various components and is maintained by the SRD (Systems Reliability Department) at the UKAEA (UK Atomic Energy Authority at Culcheth), Warrington, Cheshire.

x. *Lloyds Data Bank [3.23][3.24].* It mainly covers the failure data in the shipping industries.

ix. *Others.* The reliability data of the various electronic and nonelectronic components may also be obtained from various published papers and books such as [3.35][3.36].

3.6 Selection of Safety Analysis Methods

As described in Chapter 2, "design for safety" is an iterative process involving five phases, namely problem definition, risk identification, risk estimation, risk evaluation and design review, converging to safety design objectives defined in the problem definition phase. Each phase in the "design for safety" process may involve the use of the safety analysis methods outlined in this chapter.

It has been realised that use of the safety analysis methods in an intergrated manner may make safety analysis comparatively efficient and convenient since safety information and the advantages of each method may be more efficiently explored by doing so [3.46]. In such an integration, one method may be used to process the information produced using another method. The example of such an integration is that a system top event is identified using PHA, the associated minimal cut sets are identified using FTA, and the probabilities of occurrence of the system top event and the associated cut sets are assessed using simulation analysis.

To make full use of the safety analysis methods, an analysis of their input requirements and outcomes is required.

The possible inter-relationships of various safety analysis methods are identified as shown in Figure 3.4. This network of safety analysis methods and data flows constitutes a general framework within which the safety of a product may be assessed as the design evolves.

The outlined safety analysis methods, classified as either top-down or bottom-up event-based as described before, may be applied to study the system states, operational conditions, environmental conditions and other design considerations which contribute to the likelihood of occurrence of the hazardous conditions associated with a MTO product and define the magnitude of possible resulting consequences. The selection of

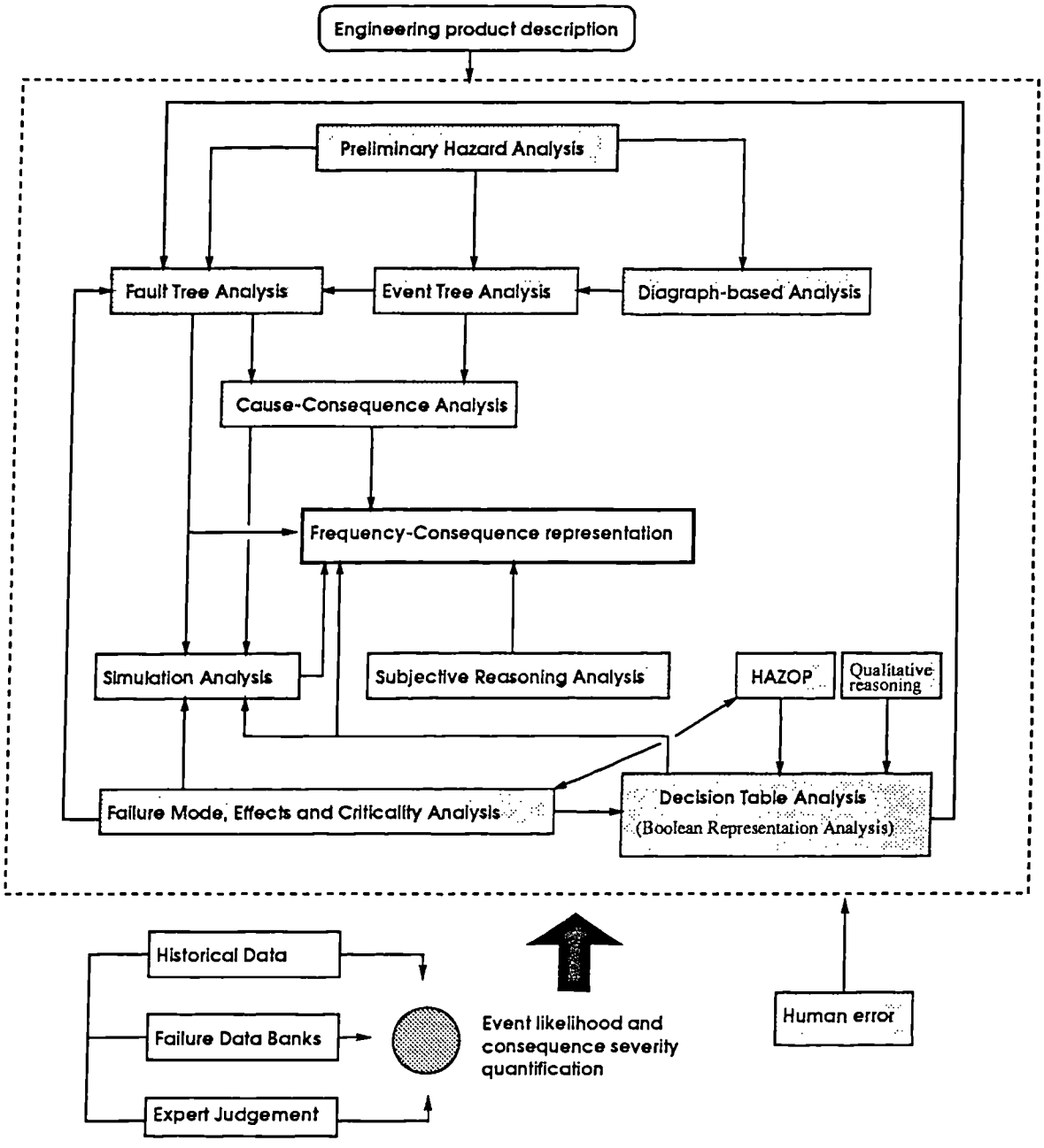


Figure 3.4 Information flow diagram of safety analysis methods

the outlined safety analysis methods, or the decision as to which methods are more appropriate for the safety analysis of a particular product, is dependent on the following considerations:

i. The level (system, subsystem or component level) of the product breakdown at which the risk identification is carried out.

ii. The degree of complexity of the inter-relationships of the items at the investigated indenture level of the product breakdown.

iii. The degree of innovation associated with the product design (the availability of product failure data for safety analysis).

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

Top-down and bottom-up methods may also be used in an integrated manner. For example, a top-down fault tree analysis method may be combined with a bottom-up modified Boolean representation method to form a mixed approach in which fault tree analysis is carried out to focus on the specific areas of interest and the Boolean representation analysis is carried out to study the details of the particular identified areas [3.46].

3.7 Concluding Remarks

This chapter studies the safety analysis methods with respect to the ways they are used in the "design for safety" process of MTO products. The typical safety analysis methods are outlined and the range of them is discussed within the context of their inter-relationships. Failure and repair data collection programmes are studied and some typical data sources are described.

The safety analysis methods outlined in this chapter may be applied individually or in combination in the "design for safety" process.

REFERENCES - CHAPTER 3

[3.1] Aldwinckle D. S., Pomeroy R. V., *A rational assessment of ship reliability and safety*", Transaction of RINA, 1983, 269-288.

[3.2] Ang A. H. S., Tang W. H., *Probability concepts in engineering planning and design,* John Wiley & Sons, England, 1984

[3.3] Apostolakis G. E., Salem S. L., Wu J. S., *CAT: a computer code for automated construction of fault trees,* EPRI Report, March 1978.

[3.4] Bazovesky I., *Reliability theory and practice,* Prentice Hall, Englewood Cliffs, N.J., 1961.

[3.5] Bendixen L. M., O'Neil J. K., Little A. D., *Chemical plant risk assessment using HAZOP and fault tree methods,* Plant/Operations Progress, Vol.3, No.3, July 1984, 179-184.

[3.6] Billinton R., Allan R. N., *Reliability evaluation of engineering systems,* 2nd ed., Plenum Press and Pitman Publishing Limited, 1992.

[3.7] Brown D. B., *Systems analysis & design for safety,* Prentice-Hall, Inc., Englewood Cliffs, New Jersey, *1976.*

[3.8] *BS 5760: Part 1, 2, 3: Reliability of systems, requirements and components,* 1979.

[3.9] Deolp L. C., Lee G. K., Ormsby R. W., *Quantitative fault tree analysis: gate-by-gate method,* Plant/Operations Progress, Vol.3, No.4, October 1984, 227-238.

[3.10] Dixon P., *Decision tables and their applications,* Computer and Automation, Vol.13, No.4, 1964, 376-386.

[3.11] Duregger R. A., Sample J. R., *System safety analysis techniques as applied to shipboard systems,* Presented at the SNAME Spring Meeting, Williamsburg, Virginia, May, 1972, 6/1-6/15.

[3.12] Fussel J. B., *Synthetic tree model - formal methodology for fault tree construction,* ANCR-1098, Spring Field, VA 11151, March 1973.

[3.13] Halebsky M., *System safety engineering as applied to ship design,* Marine Technology, Vol.26, No.3, July 1989, 245-251.

[3.14] Heino P., Poucet A., Suokas J., *Computer tools for hazard identification, modelling and analysis,* Journal of Hazardous Materials, No.29, 1992, 445-463.

[3.15] Henley E. J., Kumamoto H., *Probabilistic risk assessment,* IEEE Press, New York, 1992.

[3.16] IEEE Std 352-1975, *IEEE guide for general principles of reliability analysis of nuclear power generating station protection systems,* (An American National Standard), IEEE Press, ANSI N41-4-1976, 1975.

[3.17] Kletz T., A., *HAZOP and HAZAN: identifying and assessing process industry hazards,* 3rd ed., AIChE, 1992.

[3.18] Kramer M. A., Palowitch B. L., *A rule-based approach to fault diagnosis using the signed directed graph,* AIChE Journal, July, 1987, Vol.33, No.7, 1067-1077.

[3.19] Kumamoto H., Henley E. J., *Safety and reliability synthesis of systems with control loops,* AIChE Journal, Vol 25, No. 1, January 1979, 108-113.

[3.20] Labrie C. R., *Design for safety: design methodology,* Research Report, EDCN/SAFE/RESC/12/1, Engineering Design Centre, University of Newcastle upon Tyne, June 1992, 29 pages.

[3.21] Lawley H. G., *Operability studies and hazard analysis,* Chemical Engineering Progress, Vol.70, No.4, April 1974, 45-56.

[3.22] Lees F P, *A review of instrument failure data,* IChemE. Symposium Series No. 47, 73-91.

[3.23] LR Reliability Data, *Pump system reliability data,* Lloyds Register of Shipping, 1982.

[3.24] LR Report, *Pump system reliability data,* Lloyds Register of Shipping, 1982.

[3.25] McKelvey T. C., *How to improve the effectiveness of hazard and operability analysis,* IEEE Transaction on Reliability, Vol.37, No.1, June 1988.

[3.26] MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* Military Standard, Naval Ship Engineering Center, Washington D.C..

[3.27] Misra K. B., *Reliability analysis and prediction,* Elsevier Science Publishers B.V., 1992.

[3.28] Powers G. J., Tompkins F. C., *Fault tree analysis for chemical processes,* AIChE Journal, Vol.20, No.2, March 1974, 376-386.

[3.29] Ruxton T., *Information engineering for ship operation,* Proceeding of Maritime Communications and Control Conference, IMarE, London, November 1990.

[3.30] Ruxton T., Wang J., *Advances in marine safety technology applied to marine engineering systems,* Proceeding of First Joint Conference on Marine Safety and Environment, Delft, The Netherlands, June 1992, 421-432.

[3.31] Ruxton T., *Safety analysis required for safety assessment in the shipping industries,* Presented to NECJB, Institute of Marine Engineers and the Royal

Institute of Naval Architects, December, 1992.

[3.32] Salem S. L., *A new methodology for the computer-aided construction of fault tree,* Ann Nucl Energy, Vol.4 1977, 417-433.

[3.33] Sen P., Labrie C. R., Wang J., Ruxton T., Chan J., *A general design for safety framework for large made-to-order engineering products,* Proceeding of First Newcastle International Conference on Quality and Its Applications, Newcastle, September 1993, 499-505.

[3.34] Singer, D., *Fault tree analysis based on fuzzy logic,* Computers Chem. Engng., Vol.14, No.3, 1990, 259-266.

[3.35] Smith D. J., *Reliability and maintainability and perspective,* 2nd ed., Macmillan Publishers Ltd, 1985.

[3.36] Smith D. J., *Reliability, maintainability and risk,* 4th ed., Butterworths-Heinemann Ltd, 1992.

[3.37] Timoner J., *On the modelling of the operator's tasks in automated process plants,* North-Holland Publishing Company, 1980.

[3.38] Umeda T., Kuryama T. E., O'Shima E., Matsuyama H., *A graphical approach to cause and effect analysis of chemical processing systems,* Chem. Eng. Sci., Vol.35, 1980, 2379-2386.

[3.39] Villemeur A., *Reliability, availability, maintainability and safety assessment,* John Wiley & Sons, England, 1992.

[3.40] Wang J., *Fault diagnosis of marine automatic control systems and application of decision table and expert system to marine engineering,* M.Sc Dissertation, Department of Marine Technology, University of Newcastle upon Tyne, September 1989, 186 pages

[3.41] Wang J., *Design for safety: a general review in marine field,* EDCN/SAFE/RESC/1/1, Engineering Design Centre, University of Newcastle upon Tyne, February 1991, 60 pages.

[3.42] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), Vol.105, 1993, 21-34.

[3.43] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12

[3.44] Wang J., Ruxton T., Labrie C. R., *Design for safety of marine engineering systems with multiple failure state variables*", Accepted March 1994 for Publication by Reliability Engineering and System Safety (Research Report EDCN/SAFE/RESC/10/1, EDC, October 1991).

[3.45] Wang J., Sen P., Thompson R. V., *A mixed modelling approach for safety analysis,* SRA - Europe; 4th Conference on European Technology and Experience in Safety Analysis and Risk Management; 18 - 20 Oct 1993, Rome, Italy, 1-7.

[3.46] Wang J., Ruxton T,, Thompson R.V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, The Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, December 1993, 1-10.

[3.47] Weatgerukk T., Cameron I. T., *A prototype expert system for hazard and operability studies,* Chem. Engng, Vol.13, No.11/12, 1989, 1229-1234.

[3.48] Wells G. L., *Safety in process plant design,* John Wiley & Sons, England, 1980.

[3.49] Williams J C., *Human reliability data - the state of the art and the possibilities,* Reliability'89, 1989, 3B/5/1-3B/5/16.

[3.50] Yang Y. S., *Marine hazard assessment,* Ph.D Thesis, Department of Marine Technology, University of Newcastle upon Tyne, September 1985.

[3.51] Yannoutsos P., *Implementation of reliability engineering in the marine field - physics of exhaust valves failure due to high temperature corrosion,* Ph.D Thesis, Department of Marine Technology, University of Newcastle upon Tyne, November 1989.

CHAPTER 4

Modified Boolean Representation Method (MBRM)

SUMMARY

Since possible system failure events of most large MTO products may not be obtained by experience or from previous accidents and incident reports of similar products, and since the "design for safety" of large MTO products requires that all failure causes associated with such possible system failure events be identified, the top-down approach is not always satisfactorily applied in the risk identification and risk estimation phases and a more objective and flexible bottom-up approach may be more effective.

This chapter proposes an inductive bottom-up risk identification and estimation methodology combining FMECA and the Modified Boolean Representation Method (MBRM). This methodology can be used to identify all possible system failure events and respective causes particularly in those cases where multiple state variables and feedback loops are involved, and to assess the probabilities of occurrence of the identified system failure events and the associated cut sets. The MBRM is developed and presented together with its use in modelling cause-effect relationships. The overall model and the algorithms are described and tested in association with the associated computer software. The possible applications of this methodology in association with other system modelling methods are discussed, An illustrative example is presented to demonstrate the proposed methodology.

4.1 Introduction

As described in Chapter 2, the "design for safety" of a MTO product is a process of identifying the possible failure events (top events) and associated consequences, assessing them, and finally evaluating them. In such a process, risk identification and risk assessment are very difficult and important steps which always merit a great deal of attention by safety engineers and researchers.

As described in Chapter 3, risk identification consists of identifying, given the system description and functional requirements, potential hazardous conditions or events, for which all the possible respective causes and corresponding consequences must be identified by studying the causal relationships between the basic human, hardware and environmental events. The risk identification phase in the "design for safety" process is, without question, the most critical. Risk identification requires the combined expertise and insight of engineers and scientists to cover all aspects of the system process and operation to systematically decompose the system and analyse the interactions of primary and intermediate events on system safety and performance.

On the basis of the information produced from the risk identification phase, risk estimation can be carried out. Risk estimation is a process of estimating the likelihood of occurrence of the identified failure events and the severity of respective potential consequences. Information produced from the risk estimation phase may help designers to minimise the possibilities or possible consequences of critical failures and to provide a safe and reliable product design. Mission time, the interrelations of the components, failure rate and repair rate of each component are usually used in the risk estimation analysis of a system.

Assumptions are always necessary for the convenient application of identifying and estimating risks. The following typical assumptions are often used to estimate the probability of occurrence of each identified system failure event.

i. Failures of a component or a subsystem don't affect other components or subsystems at the same analysis level.

ii. A continuous variable can be expressed by two or more discrete states such as high, normal and low, each of which corresponds to a certain range of values.

iii. Failure events can be represented by probability distributions.

iv. There is no preventive maintenance carried out during missions and failed components are repaired same-as-new.

Various safety analysis methods can be applied to identify and estimate risks. FTA and FMECA are usually used to carry out such an analysis. As discussed in Chapter 3, for a system with a comparatively low level of innovation, the undesired system states may be obtained by experience or from previous accidents and incident reports of similar systems, and the respective causes may be identified deductively using FTA which may make use of the information produced from FMECA. However, FTA, as a top-down deductive method, suffers from the disadvantages described in section 3.3.1 as well as the following ones:

i The representation of variables with multiple states can prove to be comparatively complex. For example, the representation of a temperature variable T with five possible states (i.e, 1. high, 2. too high, 3. normal, 4. low, 5. too low) may require five gates in FTA, but such a variable may be represented simply by T_i (i = 1, 2, $\cdots$, 5) using the Boolean representation method as will be described later, where T_i represents the occurrence of state i of T.

ii. FTA may not completely benefit from the information produced using FMECA to obtain the minimal cut sets associated with the system top events and neither may it directly make use of the information when a complex engineering system is analysed.

Furthermore, when there is a lack of experience of similar system design solutions and when the complexity of the system and constituent elements increases, a top-down approach like FTA may prove unsuitable and a bottom-up approach may be more appropriate.

FMECA is a bottom-up approach and is usually carried out on the basis of the evaluation of hardware elements. However, FMECA does not close the loop between risk identification and estimation. In FMECA, how combinations of occurrence of failure modes affect system performance and safety is not studied. Some combinations of occurrence of failure modes result in definite occurrence of system failures. Such combinations of failure modes are required to be studied. Therefore, an inductive

approach is required to efficiently process the information produced from FMECA and to study combinations of failure modes to close the loop. The Modified Boolean Representation Method (MBRM) is such an approach which can be used to automate the construction of the system Boolean representation table which contains all undesired system events and associated causes. Due to its inductive nature, the modified Boolean representation method can fully benefit from the information produced from FMECA. Additional benefits of the modified Boolean representation method over FTA are that systems with feedback loops can be easily modelled and variables with multiple states can be easily dealt with.

4.2 A Proposed Risk Identification and Risk Estimation Framework Incorporating the MBRM and FMECA

A methodology for the risk identification and risk estimation of engineering systems is proposed as shown in Figure 4.1. This methodology combines FMECA and the MBRM to systematically identify and assess all system failure events and their respective causes.

Having completed the risk identification phase using FMECA at the component level, the Boolean representation descriptions of the components of the subsystems of a system can be constructed. The failure modes identified in the FMECA of a component can be used as the input attributes of the Boolean representation table. To reduce the degree of complexity of the Boolean representation modelling, only the failure modes with severity classes 1, 2 and 3 are used to construct the component Boolean representation table. Experience and a good understanding of the system is very important for the efficient construction of the component Boolean representation table. The component Boolean representation table describes, in the form of a table, the conditions which must exist for the occurrence of the identified component output states. The last column of the Boolean representation table describes the states of the output of the component being modelled while other columns prescribe the states of the input attributes. Each row represents a possible condition for an occurrence of the component's output state.

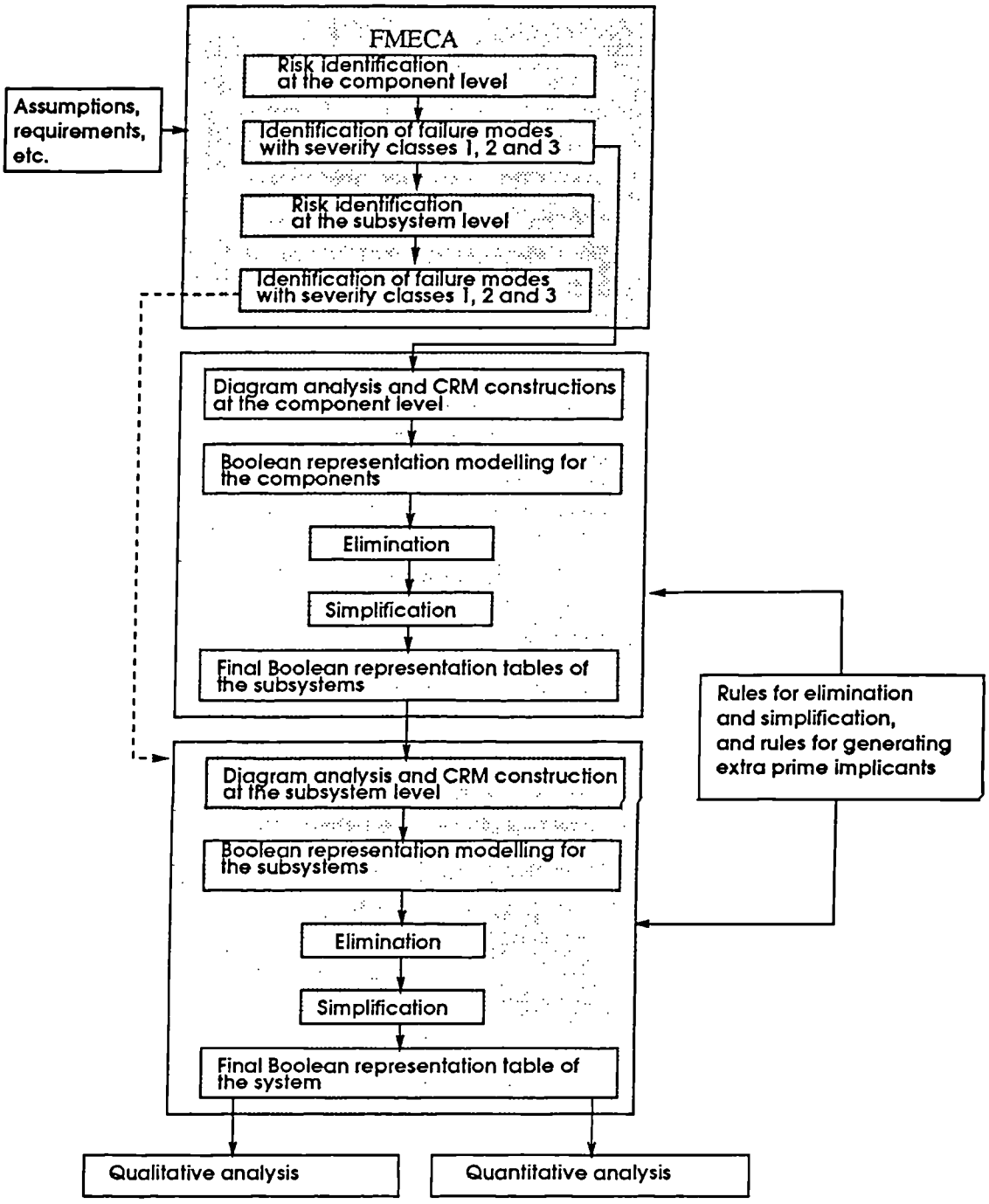


Figure 4.1 An inductive bottom-up risk identification and risk estimation framework incorporating the MBRM and FMECA

Constructed from the results of the FMECA, a component Boolean representation table normally has some degree of redundancy. The rules of simplification can be applied to absorb and merge redundant rows and redundant attributes to generate the irreducible Boolean representation table of the component. After all the Boolean representation tables of the components of a subsystem have been constructed, the construction of the subsystem Boolean representation table can be started using a process of aggregation. Intermediate variables need to be eliminated by substituting them with primary variables regarding the interactions of the components. A Component Relationship Matrix (CRM) described in the next section can be constructed from the system process diagram to describe the component relationships for the purpose of eliminating intermediate variables. After the elimination, the rules of simplification described in the next section should be applied again to produce the irreducible Boolean representation table of the subsystem.

After all the Boolean representation tables of the subsystems have been constructed, the Boolean representation modelling can be progressed up to the system level, and the same procedures repeated to ultimately obtain the irreducible Boolean representation table for the system. The rules of deduction of extra prime implicants as will be described in section 4.3.4 can then be applied to the irreducible system Boolean representation table to obtain the final system Boolean representation table. The final system Boolean representation table contains all the prime implicants associated with the system output states. A prime implicant can be considered to be the equivalent of a cut set in fault tree analysis but for systems with multiple state variables.

If the risk identification phase is completed using FMECA at the subsystem level, the Boolean representation analysis can be carried out directly at that level. Both qualitative and quantitative analysis can be carried out on the basis of the obtained final system Boolean representation table.

In the following sections, FMECA, the components relational model, the rules and procedures for obtaining the final Boolean representation table for a system, and the algorithms for qualitative and quantitative analysis are described. For the simplification of the description, Boolean representation modelling at the component level is progressed directly up to the system level.

4.3 Modified Boolean Representation Method (MBRM)

A component can be modelled by a Boolean representation table which is an extended version of a truth table and which describes how each combination of input events specifies the output event or the state of the output. As described in the last section, Boolean representation modelling can make direct use of the information produced from FMECA to possibly define the input attributes and output states. The Boolean representation table of a component can be constructed by studying all possible combinations of the input variable states. After all the Boolean representation tables of the components have been constructed, Boolean representation modelling can be progressed up to a higher level (i.e., the sub-system or system level) by studying the component relationships.

4.3.1 System Modelling

Variables used in Boolean representation modelling can be classified in the following two categories:

i. Intermediate variable.

ii. Primary variable.

The output from a component within the system is called an intermediate variable. Any variable which is an input from the system environment or an internal mode of a component is called a primary variable. An internal mode of a component represents its functioning. The examples of internal modes are "*Working*" and "*Failed*". Each primary variable or intermediate variable may have several states. The investigated system states are top events.

An engineering system can be described in terms of components and their interactions. Furthermore, a component can be described in the form of a Boolean representation table involving primary and intermediate variables. The component relationships within the system can be described in the form of a Component Relationship Matrix (*CRM*) as follows:

$$CRM = \begin{bmatrix} M_{11} & M_{12} & M_{13} & \cdot & M_{1n} \\ M_{21} & M_{22} & M_{23} & \cdot & M_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ M_{n1} & M_{n2} & M_{n3} & \cdot & M_{nn} \end{bmatrix}$$

In a *CRM*, if the element M_{ij} is equal to 0, it means that the output of component i is not an input to component j; if M_{ij} is equal to 1, it means that the output of component i is the input to component j; and if M_{ii} is equal to 1, it means that there is a self-feedback for component i.

Given the process diagram of a system, the components can first be labelled by integer numbers, and the *CRM* can then be constructed. Given the diagram of a process system shown in Figure 4.2, the *CRM* is constructed as follows:

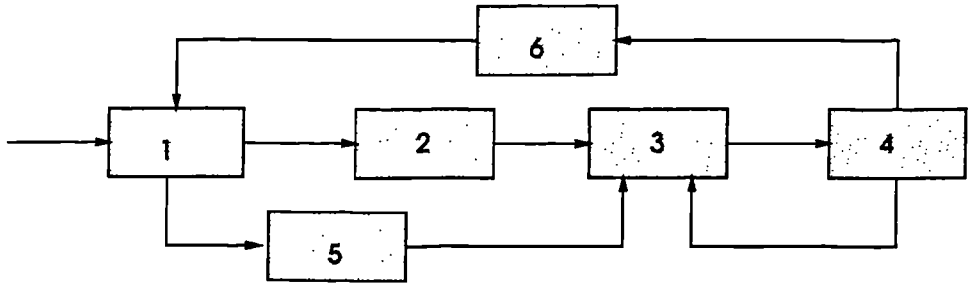


Figure 4.2 A process system diagram

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

When the software as will be described in this chapter is used to process and manipulate the Boolean representation tables of the components to obtain the irreducible table of the system, it is is required to construct *CRM* as the input data to describe the relationships of the components of the system. The construction of the Boolean representation table starts with the component Boolean representation model for which the output states are top events.

When a component has more than one output variable, Boolean representation modelling should be conducted for each of the output variables, and one or more "dummy" components should be provided in the system process diagram for the *CRM* construction [4.6][4.18]. More than one Boolean representation description may be required to model a component.

4.3.2 Rules for Boolean Representation Manipulation

Based on the binary logic relationships,

the rules for manipulation of Boolean representation tables involving variables with multiple states are defined as follows:

i. Definition

$$A_i \cap 1 = A_i \tag{4.1}$$

$$A_i \cap 0 = 0 \tag{4.2}$$

$$A_i \cup 1 = 1 \tag{4.3}$$

$$A_i \cup 0 = A_i \tag{4.4}$$

$$\sum_{i=1}^{n} A_i = 1 \tag{4.5}$$

$$A_i \cap A_j \ (i \neq j) = 0 \tag{4.6}$$

ii. Identities

$$A_i \cap A_i = A_i \tag{4.7}$$

iii. Commutative law

$$A_i \cap B_i = B_i \cap A_i \tag{4.8}$$

iv. Associative laws

$$A_i \cap (B_j \cap C_k) = (A_i \cap B_j) \cap C_k \tag{4.9}$$

$$A_i \cup (B_j \cap C_k) = (A_i \cup B_j) \cap (A_i \cup C_k) \tag{4.10}$$

v. Absorption laws

$$A_i \cup (A_i \cap B_j) = A_i \quad A_i \cap (A_i \cap B_j) = A_i \cap B_j \tag{4.11}$$

$$A_i \cup * = * \tag{4.12}$$

where A_i represents state i of variable A, A_j represents state j of variable A, B_j represents state j of variable B, and * stands for "Don't care" which means a variable could be in any state.

The rules for Boolean representation simplification are absorption and merging. Two examples of their applications are shown in Tables 4.1 and 4.2.

Table 4.1 Absorption

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

Table 4.2 Merging

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

where the number of the states of variable B is equal to 3, and F, W and N stands for *"Failed"*, *"Working"* and *"Normal"*, respectively.

4.3.3 Elimination of Intermediate Variables

The input entries of a final system Boolean representation table should be primary variables. Therefore, intermediate variables should be eliminated by substitution with primary variables. During the elimination process, some intermediate variables may be used to replace other intermediate variables. Gradually, all intermediate variables are eliminated and a Boolean representation table in which all the entries are primary variables can be obtained. At this stage, a simplification of the Boolean representation table can be carried out. If the number of the entries of a Boolean representation table

is large the simplification process may prove time-consuming. Therefore, it is suggested that the simplification rules be applied after each intermediate variable is eliminated. An example of elimination of intermediate variables is presented as shown in Tables 4.3 and 4.4.

$$\begin{aligned} \text{If} \quad & Y = A_iB_iE_i + A_iB_j \\ \text{and} \quad & E_i = C_iD_i + C_jD_j \\ \text{Then} \quad & Y = A_iB_i\,(C_iD_i + C_jD_j) + A_iB_j \\ & = A_iB_iC_iD_i + A_iB_iC_jD_j + A_iB_j \end{aligned}$$

where A, B, C and D are primary variables, and E is an intermediate variable.

Table 4.3 The tables concerned with variables Y and E

A	B	E	Y		C	D	E
F	W	N	High	and	N	N	N
F	N	*	High		F	W	N

Eliminating intermediate variable E, then

Table 4.4 The Boolean representation table after elimination

A	B	C	D	Y
F	W	N	N	High
F	W	F	W	High
F	N	*	*	High

An input variable should only occupy one column in a Boolean representation table. However, it may happen that an input variable may occupy more than one column during the elimination of intermediate variables. This is called duplication of variables. Duplication of variables has been found to arise only in the construction of Boolean representation tables of systems in which one or more of the components has multiple outputs. Duplication of variables can be eliminated by applying the following rule in association with rules (4.6) and (4.7):

$$A_i \cap (*) = A_i \tag{4.13}$$

During the elimination of intermediate variables, if the combination of a variable in a row is 0, that row is deleted. In the example shown in Table 4.5, the combination of variable C in row 2 is 0. Therefore, row 2 is eliminated.

Table 4.5 An example of elimination of duplicated input variables

Row	A	B	C	C	D	C_{out}		A	B	C	D	C_{out}
1	N	F	*	*	N	F		N	F	*	N	F
2	N	N	F	N	F	F	->					
3	N	F	*	F	F	F		N	F	F	F	F
4	N	N	F	F	W	F		N	N	F	W	F

The difference between the Boolean representation descriptions of systems with and without feedback loops is that the former has the output variable in the input attributes of the Boolean representation table, and the latter does not. For a system with feedback loops, the output variable in the input attributes of the Boolean representation table can be eliminated by applying the rules (4.6), (4.7) and (4.13). An example is shown in Table 4.6 where row 2 is eliminated.

Table 4.6 Elimination of the output variable appearing in the input attributes

Row	*A*	*B*	C_{out}	C_{out}		*A*	*B*	C_{out}
1	N	F	F	F		N	F	F
2	F	N	N	F	->			
3	F	F	*	F		F	N	F

4.3.4 Deduction of Prime Implicants

A Boolean representation table can be simplified to an irreducible form using the described rules. However, the irreducible table is not guaranteed to contain all of the prime implicants since variables with multiple states may be involved. An example is given as in Table 4.7:

Table 4.7 An irreducible Boolean representation table

Row	A	B	C_{out}
1	N	F	High
2	F	*	High
3	W	*	High

where the number of states of variable A is equal to 3.

Obviously, Table 4.7 is an irreducible table. However, there is one more prime implicant [A = *][B = F], which is not contained in Table 4.7. As will be described later, such an extra prime implicant can be produced from the existing irreducible table.

Quine's algorithm theory can be used to produce the extra prime implicants from the obtained irreducible table [4.6][4.18]. Such a method is called consensus operation since it creates new terms out of the terms already in the table by mixing and matching their input events. The theory for obtaining the extra prime implicants from the obtained irreducible table is described as follows.

If there is an event variable A and a set of n prime implicants σ_1, σ_2, $\cdots$, σ_n associated with all the possible states (A_1, A_2, $\cdots$, and A_n) of variable A in the irreducible Boolean representation table, $\prod_{j=1}^{n}\sigma_j$ is also a prime implicant provided that it exists. This can be proved as follows:

Suppose Y represents the total prime implicants associated with all the possible states of variable A. Then

$$Y = \sum_{i=1}^{n} A_i \sigma_i \tag{4.14}$$

where n is the number of the states of variable A.

From the equations (4.1), (4.4) and (4.7), the following equation can be obtained.

$$A_i\sigma_i = A_i\sigma_i \cap (1 \cup A_i \prod_{j=1}^{n}\sigma_j) = A_i\sigma_i \cup A_i \prod_{j=1}^{n}\sigma_j \tag{4.15}$$

Therefore

$$Y = \sum_{i=1}^{n}(A_i\sigma_i \cup A_i \prod_{j=1}^{n}\sigma_j) = \sum_{i=1}^{n} A_i\sigma_i \cup \sum_{i=1}^{n} A_i \prod_{j=1}^{n}\sigma_j \tag{4.16}$$

From rule 4.7, $\sum_{i=1}^{n} A_i \prod_{j=1}^{n} \sigma_j = \prod_{j=1}^{n} \sigma_j \sum_{i=1}^{n} A_i$ is obtained.

Since

$$\sum_{i=1}^{n} A_i = 1 \tag{4.17}$$

Then

$$Y = \sum_{i=1}^{n} A_i \sigma_i \cup \prod_{j=1}^{n} \sigma_j \tag{4.18}$$

Therefore $\prod_{j=1}^{n} \sigma_j$ is also a prime implicant.

After the extra prime implicants have been created out of the obtained irreducible Boolean representation table, they should be added to the obtained irreducible Boolean representation table, and the rules for simplification should be applied again to obtain the final Boolean representation table. An example is shown as follows.

Suppose an irreducible system Boolean representation table is obtained as shown in Table 4.8.

Table 4.8 An irreducible system Boolean representation table

Row	*A*	*B*	*E*	*F*	C_{output}
1	N	F	F	F	High
2	*	N	F	F	High

where the number of the states of variable *B* is equal to 2.

Deducing the extra prime implicant, Table 4.9 is obtained.

Table 4.9 Deduction of the extra prime implicant.

Row	*A*	*B*	*E*	*F*	C_{output}
1	N	F	F	F	High
2	*	N	F	F	High
3	N	*	F	F	High

where row 3 is the new prime implicant

The final system Boolean representation table can be obtained by applying the rules for simplification.

Table 4.10 The final system Boolean representation table

Row	*A*	*B*	*E*	*F*	Y_{output}
1	N	*	F	F	High
2	*	N	F	F	High

It should be pointed out that it is meaningless to study extra prime implicants in fault tree analysis because only one state for a variable appears in the minimal cut sets. For a system in which multiple state variables contribute to system failures, the failure cause expressions are prime implicants rather than minimal cut sets in the fault tree analysis. If the state of each variable in a system is 1, the final Boolean representation table would be exactly the same as obtained in the fault tree analysis.

4.3.5 System Safety Analysis

Both qualitative and quantitative safety analysis can be carried out on the basis of the final system Boolean representation table.

Qualitative analysis

In the obtained Boolean representation table, a prime implicant consisting of n primary events is called an n-event prime implicant. One-event prime implicants are significant contributors to the associated top event unless their probabilities of occurrence are very low. If there are no one-event prime implicants, two or three-event prime implicants leading to the top event should be given more attention rather than other higher-order prime implicants. Common cause failures should also be studied if there are some common causes in higher-order prime implicants.

Quantitative analysis

Boolean representation analysis deals with variables with multiple states. The traditional quantitative safety analysis theory which usually deals with variables with single failure state cannot be directly applied to the final system Boolean representation table.

Therefore, a modified quantitative safety analysis method is required to assess the probability of occurrence of each system top event. Such a method is developed as follows:

The simultaneous occurrence of the basic events associated with any of the prime implicants C_1, C_2, C_3, $\cdots$, and C_N will result in the occurrence of the top event T_c. Thus, the probability of occurrence of the top event T_c can be calculated as follows:

$$\begin{aligned} P(T_c) &= P(C_1 \cup C_2 \cup \cdots \cup C_N) \\ &= (P(C_1) + P(C_2) + \cdots P(C_N)) - (P(C_1 \cap C_2) + P(C_1 \cap C_3) \\ &\quad + \cdots P(C_i \cap C_j)_{[i \neq j]} \ldots) \cdots + (-1)^{N-1} P(C_1 \cap C_2 \cdots \cap C_N) \\ &= \sum_{i=1}^{N} P(C_i) - \sum_{i=1 i \neq j}^{N} P(C_i \cap C_j) + \cdots + (-1)^{N-1} P(C_1 \cap C_2 \cdots \\ &\quad \cap C_N) \end{aligned} \tag{4.19}$$

where N is the number of the prime implicants associated with the top event T_c.

The rules (4.5) and (4.7) can be applied to simplify the intersections of the prime implicants in the above formula. If any of the terms (say $C_1 \cap C_2 = I_k$) in the expression (4.19) is expressed in terms of the associated basic events E_{k1}, E_{k2}, $\cdots$, and E_{km}, then

$$P(I_k) = P(E_{k1} \cap E_{k2} \cap \cdots \cap E_{km}) \tag{4.20}$$

where m is the number of the basic events associated with I_k.

Usually, the basic events E_{k1}, E_{k2}, E_{k3}, $\cdots$, and E_{km} are assumed to be independent, that is, the occurrence of a given basic event is in no way affected by the occurrence of any other basic events. Thus,

$$P(I_k) = P(E_{k1})\, P(E_{k2}) \cdots P(E_{km}) \tag{4.21}$$

If each basic event E_{ki} ($i = 1, 2, \cdots, m$) is assumed to follow an exponential distribution, then the probability of its occurrence at time t can be calculated by:

$$P(E_{ki}) = 1 - e^{-\lambda_{E_{ki}} t} \tag{4.22}$$

where $\lambda_{E_{ki}}$ is the failure rate of the basic event E_{ki}.

After $P(E_{k1}), P(E_{k2}), \cdots$, and $P(E_{km})$ have been obtained, $P(I_k)$ can be calculated. The probability of occurrence of the top event $P(T_c)$ can then be obtained using formula (4.19).

4.4 Software

A computer model has been developed with respect to the described MBRM. The programme is written in *MODSIM II*™ which is an object-oriented simulation language and which can also be used as a general purpose programming language. A brief description of *MODSIM II*™ can be seen from Appendix 2. The selection of this language is justified by the possible future implementation of event-based simulation to predict and assess system performance.

The software has been designed to satisfy the functional requirements of simplification, elimination, safety parameter calculation and an efficient man/machine interface.

Simplification

The following functions are involved in the simplification module:

i. Absorption

ii. Merging

The characteristics of the simplification module are:

i. The number of the states of each input variable is currently limited to 5 although it can easily be expanded.

ii. There is no limitation on the number of input variables.

iii. The result obtained can easily be monitored through a simple interactive interface.

Elimination

The elimination is based on the rules developed in sections 4.3.2 and 4.3.3.

Deduction of extra prime implicants

Deduction of extra prime implicants is based on the rules described in section 4.3.4. After extra prime implicants have been deduced, the rules for simplification are applied again to obtain the final system Boolean representation table.

Inputs

The input data includes:

i. Names of component variables.

ii. Boolean representation descriptions of components.

iii. The number of the states of each variable.

iv. Failure rates of the failure modes associated with each component.

v. *CRM*.

Quantitative analysis

This software is limited to assess the probability of occurrence of a system top event for which the associated basic events follow exponential distributions.

Consistency checks

The consistency checks are designed to make sure that the input data is correct.

4.5 An Example

An hydraulic hoist transmission system of a marine crane is shown functionally in Figure 4.3. This system is used to control the crane motions such as hoisting up and hoisting down loads as required by the operator [4.9][4.15]. It consists of five subsystems, namely an hydraulic oil tank, an auxiliary system, a control system, a protection system and an hydraulic servo transmission system. Each subsystem is associated with several failure modes. The occurrence of each failure mode associated with each subsystem may result in certain possible consequences, with the severity class depending on the nature of the failure mode and the interactions of the subsystems.

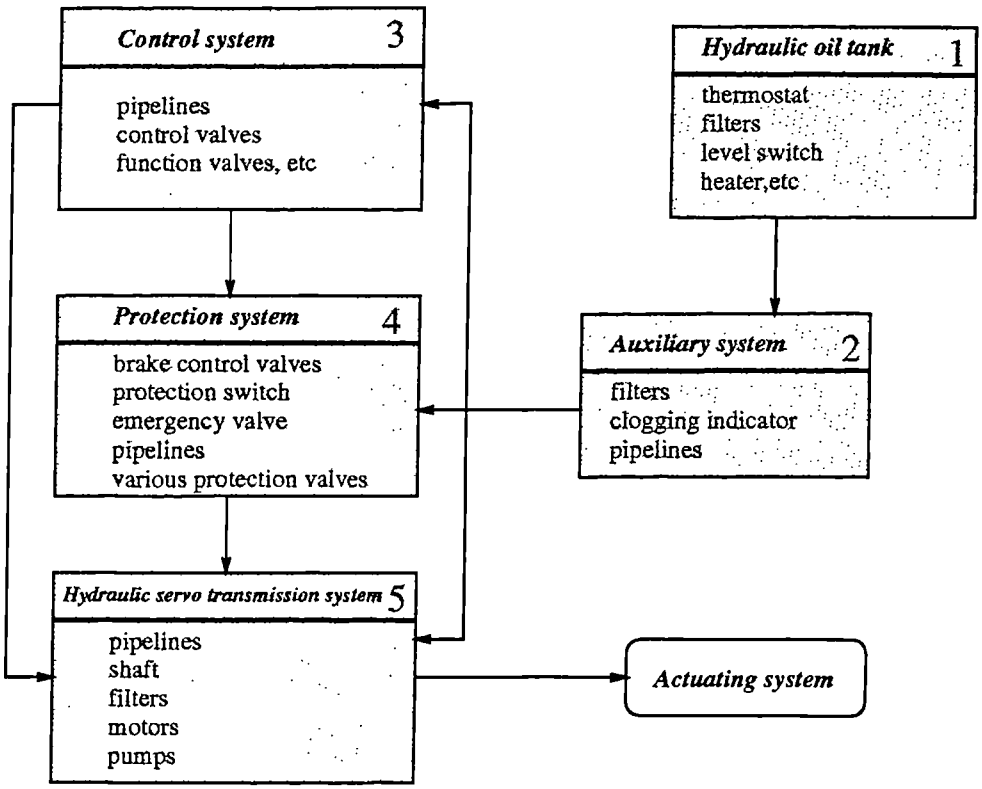


Figure 4.3 The diagram of an hydraulic hoist transmission system of a marine crane

4.5.1 **Risk Identification Using FMECA**

The following assumptions are set for the convenience of analysis:

i. The system will not be operated at any time above the rated maximum pressures and capacities.

ii. Structural failure of any subsystem causing loss of hydraulic oil will be considered as a possible failure mode of that subsystem.

iii. All piping connections are properly made and will not leak.

iv. All parts of the hydraulic systems will be properly purged of air at commissioning.

v. The electrical circuitry will be adequately and properly protected against the ingress of water or other harmful fluids.

vi. All maintenance activities are expertly and properly carried out and no faults which affect operation and safety are introduced.

vii. Failure rates of the failure modes of the subsystems are assumed to be constant.

viii. When a failure mode is defined as a major leak, this means that the leak of all fluid would result from a disconnected pipe or a burst casing.

ix. Pipes and hoses are not considered as components. A burst in any pipe or hose is considered as a major leak in the next downstream component.

The results of the FMECA for the subsystems of this marine crane hoist transmission system are shown in Tables 4.11, 4.12, 4.13, 4.14 and 4.15. The failure rate of each failure mode in Tables 4.11, 4.12, 4.13, 4.14 and 4.15 is obtained from [4.9].

Table 4.11 FMECA of the hydraulic tank

Name		Hydraulic oil tank			
Function		Supplying the oil for hydraulic control system, servo transmission system and protection system			
Failure rate		51 (failures per million hours)			
Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
1	0.443	oil temperature too high or too low	reduce efficiency.	self-annunciating	4
2	0.103	level gauge failure	could result in insufficient oil supply.	self-annunciating & by maintenance	3
3	0.059	major leak	no flow for the system supply.	self-annunciating	3
4	0.395	minor leak	none.	self-annunciating	4

Table 4.12 FMECA of the auxiliary system

Name		Auxiliary system			
Function		Filtering, cooling and supplying the hydraulic oil			
Failure rate		106 (failures per million hours)			
Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
1	0.284	failure allowing contaminant into system	pump servo may stick.	by maintenance	3
2	0.011	filter blocked	loss of servo pressure.	by maintenance	3
3	0.085	blocking indicator fails to operate	loss of servo pressure.	self-annunciating	3
4	0.566	minor leak	none.	self-annunciating & by maintenance	4
5	0.011	major leak	loss of servo pressure and motion.	self-annunciating	3
6	0.043	no output from control pump	no flow for system.	self-annunciating & by maintenance	2

Table 4.13 FMECA of the hydraulic servo transmission system

Name		Hydraulic servo transmission system			
Function		Producing hydraulic power for hoisting			
Failure rate		265 (failures per million hours)			
Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
1	0.094	major leak	loss of hoisting pressure; in lowering motion, load could fall.	self-annunciating	1
2	0.522	minor leak	none	self-annunciating & by maintenance	4
3	0.013	shaft failure	loss of hoisting motion; no output.	self-annunciating & by maintenance	1
4	0.311	no output from the package motor	loss of hoisting pressure; no output.	self-annunciating & by maintenance	1
5	0.026	hydraulic short circuit	loss of hoisting pressure; in lowering motion, load could fall.	self-annunciating & by maintenance	1
6	0.026	motor seizure	load holds.	self-annunciating & by maintenance	3
7	0.008	pipe burst	major leak will happen; hoisting pressure will lose; in lowering motion, load could fall.	self-annunciating	1

Table 4.14 FMECA of the control system

Name		Control system			
Function		Controlling the servo hydraulic transmission system			
Failure rate		36 (failures per million hours)			
Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
1	0.015	major leak	loss of hoisting pressure; in lowering motion, load could fall.	self-annunciating	2
2	0.310	minor leak	none.	self-annunciating	4

Table 4.14 FMECA of the control system (Continued)

Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
3	0.365	no output when required	loss of hoisting pressure; in lowering motion, load could fall.	by maintenance	3
4	0.155	control output for "lower" motion can not be closed when required	when de-energised by slack rope/lowering limit hoist, possibility of fall or damage of snagged load.	by maintenance	1
5	0.155	control output for "hoist up" motion can not be closed when required	jib and boom could be damaged.	by maintenance	1

Table 4.15 FMECA of the protection system

Name		Protection system			
Function		Protecting the various consequences caused by hazards			
Failure rate		92 (failures per million hours)			
Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
1	0.132	failure of switch when energised	lost hoist motion.	self-annunciating & by maintenance	3
2	0.066	failure of return for hoisting up when de-energised	possibility of damage of jib.	by maintenance	1
3	0.530	minor leak	possibility of fall of snagged load.	self-annunciating	4
4	0.046	major leak	when brakes are applied, pump goes to zero stroke; "emergency release" and "wave following" disable.	self-annunciating	1

Table 4.15 FMECA of the protection system (Continued)

Failure mode number	Failure mode rate	Failure mode	Effects on system	Detecting method	Sev.
5	0.066	failure of emergency stop	load could be hoisted up or lowered down not as required even in emergency situation.	by maintenance	1
6	0.066	failure of hoisting up limit	when de-energised, pump remains at stroke and motor runs. otherwise no effect.	by maintenance	1
7	0.066	failure of hoisting down limit/slack rope prevention.	when de-energised by limit hoist, pump is not returned to zero stroke.	by maintenance	1
8	0.028	low boost pressure switch fails to open	hoisting pump is allowed to continue running at low pressures with a risk of cavitation damage.	by maintenance	1

* Sev. : Severity Class

For the convenience of constructing the Boolean representation tables of the subsystems, the following notation is given to the failure modes with severity classes 1, 2 and 3, and the output states of the subsystems.

Hydraulic oil tank

HM_1: major leak in the hydraulic oil tank

HM_2: level gauge failure

H_o: the output variable of oil supply tank

H_1: no oil supply from the oil tank

H_2: supplying oil from the oil tank

Auxiliary system

AM_1: failure allowing contaminant into system

AM_2: filter blocked

AM_3: blocking indicator fails to operate

AM_4: major leak

AM_5: no output from the control pump

A_o: the output variable of the auxiliary system

A_1: no output (including supplying uncontaminated oil)

A_2: supplying contaminated hydraulic oil

Control system

CM_1: major leakage

CM_2: no output when required

CM_3: control output can not be closed for "lowering motion"

CM_4: control output for "hoisting up" motion can not be closed when required

C_o: the output variable of the control system

C_1: no output from the control system when required

C_2: control signal for "hoisting up" can not be closed when required

C_3: control signal for "lowering motion" can not be closed when required

Hydraulic servo transmission system

SM_1: major leak

SM_2: shaft failure

SM_3: no output from the package motor

SM_4: hydraulic short circuit

SM_5: motor seizure

SM_6: pipe burst

S: the output variable of the hydraulic servo transmission system

S_1: hoisting up continuously not as required

S_2 lowering continuously not as required

S_3: no output from the package motor of the hydraulic servo transmission system

Protection system

PM_1: failure of switch when energised

PM_2: failure to return for hoisting up when de-energised

PM_3: major leak

PM_4: failure of emergency stop

PM_5: failure of hoist up limit

PM_6: failure of hoist lower limit/slack rope prevention

PM_7: low boost pressure switch fails to open

P_o: the output variable of the protection system

P_1: no protection for emergency stop

P_2: no protection for "hoist up" limit

P_3: no protection for "hoist lower" limit/slack rope

P_4: no low boost pressure protection

4.5.2 Construction of the Boolean Representation Tables and Assessment of the Probabilities of Occurrence of the System Failure Events

The information produced from the FMECA of a subsystem can be utilised to construct the Boolean representation table by studying each possible combination of input attributes which are the possible failure modes with severity classes 1, 2 and 3. The Boolean representation tables of the five subsystems are constructed as shown in Tables 4.16, 4.17, 4.18, 4.19 and 4.20, respectively. In the constructed Boolean representation tables, N stands for "*Failure not happening*" of a variable state and F stands for "*Failure happening*".

Table 4.16 Hydraulic oil tank

HM_1	HM_2	H_o
F	F	H_1
N	*	H_2
*	N	H_2

Table 4.17 Auxiliary system

AM_1	AM_2	AM_3	AM_4	AM_5	H_o	A_o
*	F	F	*	*	*	A_1
*	*	*	F	*	H_1	A_1

Table 4.17 Auxiliary system (Continued)

AM_1	AM_2	AM_3	AM_4	AM_5	H_o	A_o
*	*	*	*	F	H_1	A_2
F	N	*	N	N	H_2	A_2
F	*	N	N	N	H_2	A_2

Table 4.18 Control system

CM_1	CM_2	CM_3	CM_4	A_o	C_o
*	F	*	*	*	C_1
*	*	*	*	A_1	C_1
F	*	*	*	A_2	C_1
*	*	F	*	*	C_2
*	*	*	F	*	C_3

Table 4.19 Protection system

A_o	C_o	PM_1	PM_2	PM_3	PM_4	PM_5	PM_6	PM_7	P_o
*	*	*	*	*	F	*	*	*	P_1
A_1	*	*	*	F	*	*	*	*	P_1
*	C_2	*	*	*	*	*	*	*	P_2
A_1	*	*	F	*	*	F	*	*	P_2
A_1	C_3	*	*	*	*	*	*	*	P_3
A_2	*	F	*	*	*	*	F	*	P_3
A_1	*	*	*	*	*	*	*	F	P_4

Table 4.20 Hydraulic servo transmission system

A_o	C_o	P_o	SM_1	SM_2	SM_3	SM_4	SM_5	SM_6	S_o
*	C_2	P_2	*	F	*	*	*	*	S_1
*	C_1	P_2	*	*	*	*	*	*	S_1
A_2	*	P_2	*	*	*	*	F	*	S_1
*	C_3	P_3	*	*	*	*	*	*	S_2
*	C_1	P_3	*	*	*	*	*	*	S_2
A_1	*	P_3	*	*	*	*	*	*	S_2
*	*	P_3	F	*	*	*	*	*	S_2
*	*	P_3	*	*	*	*	F	*	S_2
*	*	P_3	*	F	*	*	*	*	S_2

Table 4.20 Hydraulic servo transmission system (Continued)

A_o	C_o	P_o	SM_1	SM_2	SM_3	SM_4	SM_5	SM_6	S_o
*	*	P_3	*	*	F	*	*	*	S_2
*	*	P_3	*	*	*	F	*	*	S_2
*	*	P_3	*	*	*	*	*	F	S_2
*	*	P_1	*	F	*	*	*	*	S_2
*	*	P_1	*	*	*	F	*	*	S_2
*	*	P_1	*	*	*	*	*	F	S_2
A_1	*	*	F	*	*	*	*	*	S_3
A_1	*	*	*	*	F	*	*	*	S_3
A_1	*	*	*	*	*	F	*	*	S_3
A_1	*	*	*	*	*	*	*	F	S_3
A_2	*	*	*	*	*	*	F	*	S_3
A_2	*	P_4	*	*	*	*	*	*	S_3

The failure events of the hydraulic hoist transmission system are the same as those of the hydraulic servo transmission system. Therefore, the construction of the system Boolean representation table starts from the hydraulic servo transmission system. The CRM is constructed as follows to describe the subsystems relationships.

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

After the *CRM*, the subsystem Boolean representation tables and the failure data of the variables have been prepared in the input file, the developed software can be used to produce the final Boolean representation table of the hydraulic hoist transmission system shown in Table 4.21 and to calculate the probability of occurrence of each system top event.

Table 4.21 The final system Boolean representation table

HM	*AM*	*CM*	*PM*	*SM*	
1 2	1 2 3 4 5	1 2 3 4	1 2 3 4 5 6 7	1 2 3 4 5 6	S
* *	* * * * *	* * F *	* * * * * * *	* F * * * *	S_1
* *	* F F * *	* * * *	* F * * F * *	* * * * * *	S_1
F F	* * * F *	* * * *	* F * * F * *	* * * * * *	S_1
* *	* F F * *	* * F *	* * * * * * *	F * * * * *	S_1
F F	* * * F *	* * F *	* * * * * * *	F * * * * *	S_1

Table 4.21 The final system Boolean representation table (Continued)

HM	*AM*	*CM*	*PM*	*SM*	
1 2	1 2 3 4 5	1 2 3 4	1 2 3 4 5 6 7	1 2 3 4 5 6	S
F F	* * * * F	* * F *	* * * * * * *	* * * * F *	S_1
N *	F N * N N	* * F *	* * * * * * *	* * * * F *	S_1
* N	F N * N N	* * F *	* * * * * * *	* * * * F *	S_1
N *	F * N N N	* * F *	* * * * * * *	* * * * F *	S_1
* N	F * N N N	* * F *	* * * * * * *	* * * * F *	S_1
* *	* F F * *	* * * F	* * * * * * *	* * * * * *	S_2
F F	* * * F *	* * * F	* * * * * * *	* * * * * *	S_2
F F	* * * * F	* * * F	F * * * * F *	* * * * * *	S_2
N *	F N * N N	* * * F	F * * * * F *	* * * * * *	S_2
* N	F N * N N	* * * F	F * * * * F *	* * * * * *	S_2
N *	F * N N N	* * * F	F * * * * F *	* * * * * *	S_2
* N	F * N N N	* * * F	F * * * * F *	* * * * * *	S_2
* *	* * * * *	* F *	F F * * * * *	* F * * * *	S_2
F F	* * * * F	F * *	F F * * * * *	* F * * * *	S_2
* N	F N * N N	F * *	F F * * * * *	* F * * * *	S_2
N *	F * N N N	F * *	F F * * * * *	* F * * * *	S_2
* N	F * N N N	F * *	F F * * * * *	* F * * * *	S_2
* *	* * * * *	* * * *	F * * * * * *	F * * * * *	S_2
F F	* * * * F	* * * *	F * * * * * *	F * * * * *	S_2
* N	F N * N N	* * * *	F * * * * * *	F * * * * *	S_2
N *	F * N N N	* * * *	F * * * * * *	F * * * * *	S_2
* N	F * N N N	* * * *	F * * * * * *	F * * * * *	S_2
* *	* * * * *	* * * *	F * * * * * *	* F * * * *	S_2
F F	* * * * F	* * * *	F * * * * * *	* F * * * *	S_2
* N	F N * N N	* * * *	F * * * * * *	* F * * * *	S_2
N *	F * N N N	* * * *	F * * * * * *	* F * * * *	S_2
* N	F * N N N	* * * *	F * * * * * *	* F * * * *	S_2
* *	* * * * *	* * * *	F * * * * * *	* * F * * *	S_2
F F	* * * * F	* * * *	F * * * * * *	* * F * * *	S_2
* N	F N * N N	* * * *	F * * * * * *	* * F * * *	S_2
N *	F * N N N	* * * *	F * * * * * *	* * F * * *	S_2
* N	F * N N N	* * * *	F * * * * * *	* * F * * *	S_2
* *	* * * * *	* * * *	F * * * * * *	* * * F * *	S_2
F F	* * * * F	* * * *	F * * * * * *	* * * F * *	S_2

Table 4.21 The final system Boolean representation table (Continued)

HM	*AM*	*CM*	*PM*	*SM*	
1 2	1 2 3 4 5	1 2 3 4	1 2 3 4 5 6 7	1 2 3 4 5 6	S
* N	F N * N N	* * * *	F * * * * * *	* * * F * *	S_2
N *	F * N N N	* * * *	F * * * * * *	* * * F * *	S_2
* N	F * N N N	* * * *	F * * * * * *	* * * F * *	S_2
* *	* * * * *	* * * *	F * * * * * *	* * * * F *	S_2
F F	* * * * F	* * * *	F * * * * * *	* * * * F *	S_2
* N	F N * N N	* * * *	F * * * * * *	* * * * F *	S_2
N *	F * N N N	* * * *	F * * * * * *	* * * * F *	S_2
* N	F * N N N	* * * *	F * * * * * *	* * * * F *	S_2
* *	* * * * *	* * * *	F * * * * * *	* * * * * F	S_2
F F	* * * * F	* * * *	F * * * * * *	* * * * * F	S_2
* N	F N * N N	* * * *	F * * * * * *	* * * * * F	S_2
N *	F * N N N	* * * *	F * * * * * *	* * * * * F	S_2
* N	F * N N N	* * * *	F * * * * * *	* * * * * F	S_2
* *	* * * * *	* * * F	* * * * * * *	F * * * * *	S_2
* *	* F F * *	* * F *	* * * * * * *	F * * * * *	S_2
F F	* * * F *	* * F *	* * * * * * *	F * * * * *	S_2
* *	* F F * *	* * F *	* * * * * * *	* * F * * *	S_2
F F	* * * F *	* * F *	* * * * * * *	* * F * * *	S_2
* *	* F F * *	* * F *	* * * * * * *	* * * * * F	S_2
F F	* * * F *	* * F *	* * * * * * *	* * * * * F	S_2
* *	* F F * *	* * * *	* * * * * * *	F * * * * *	S_3
F F	* * * F *	* * * *	* * * * * * *	F * * * * *	S_3
* *	* F F * *	* * * *	* * * * * * *	* * F * * *	S_3
F F	* * * F *	* * * *	* * * * * * *	* * F * * *	S_3
* *	* F F * *	* * * *	* * * * * * *	* * * * * F	S_3
F F	* * * F *	* * * *	* * * * * * *	* * * * * F	S_3
* *	* F F * *	* * * *	* * * * * * *	* * * F * *	S_3
F F	* * * F *	* * * *	* * * * * * *	* * * F * *	S_3
F F	* * * * F	* * * *	* * * * * * *	* * * * F *	S_3
N *	F N * N N	* * * *	* * * * * * *	* * * * F *	S_3
* N	F N * N N	* * * *	* * * * * * *	* * * * F *	S_3
N *	F * N N N	* * * *	* * * * * * *	* * * * F *	S_3
* N	F * N N N	* * * *	* * * * * * *	* * * * F *	S_3
F F	* * * * *	* * * *	* * * * * * F	* * * * * *	S_3

The failure probabilities for S_1, S_2 and S_3 at time t = 10000 hours are equal to 0.101, 0.015 and 0.039, respectively.

The possible consequences resulting from the occurrence of S_1, S_2 and S_3 can be described as follows:

S_1: Possibility of damage to the boom, ranging from minor distortion to total collapse (buckling). Possible rupture of the hoisting rope resulting in a dropped load. A dropped load may result in a total destruction of the lifted load, damage to the surrounding structure and other goods within the operating radius and possible death or severe injury to personnel.

S_2: A dropped load resulting in the probable consequences described in S_1.

S_3: A dropped load resulting in the probable consequences described in S_1.

The safety information produced above can be used by the designer to determine where design actions are required to eliminate or control serious system failure events, and can also be utilised to prepare maintenance policies as will be described in Chapter 8.

4.6 Discussion and Application

Compared to the fault tree method, the MBRM has the following advantages:

i. It can deal with engineering systems with multiple state variables and feedback loops.

ii. Top events of a large engineering system with a relatively higher level of innovation can be identified.

iii. Omissions of failure causes are less likely than in fault tree analysis.

iv. The information produced from FMECA can be used directly for Boolean representation modelling.

In addition, the MBRM can be used together with other formal safety analysis techniques such as fault tree analysis, qualitative reasoning analysis and the Monte Carlo simulation. The use of the MBRM is greatly extended by such combinations. These combinations are briefly discussed as follows:

i. The inductive MBRM can be combined with the inductive qualitative reasoning approach to form a mixed modelling methodology in which qualitative reasoning is applied at the component level and the MBRM is used at the system level [4.19]. This will be studied in more detail in the next chapter.

ii. The MBRM can be used together with the fault tree analysis as discussed in Chapter 3. This would involve partial "top down" fault tree analysis to focus upon areas of interest and partial "bottom up" Boolean representation analysis to explore the areas at a greater level of detail [4.21].

iii. The MBRM can also be used together with the Monte Carlo simulation techniques. The probabilities of occurrence of each top event and each associated cut set can be simulated on the basis of the obtained Boolean representation table [4.16]. This will be attempted in Chapter 6.

4.7 Concluding Remarks

A generalised modified Boolean representation modelling methodology is developed in this chapter. In the methodology, the information produced from a FMECA is directly and efficiently used to construct the Boolean representation tables of components of a system. After all the Boolean representation tables of the components have been constructed and the CRM has been produced, the rules for simplification, elimination of intermediate variables and deduction of extra prime implicants are applied to obtain the final system Boolean representation table. Both qualitative and quantitative analysis can then be carried out to assess the probabilities of occurrence of the system top events and the associated prime implicants.

The modified Boolean representation method can be combined with other formal safety analysis techniques. This will be demonstrated in Chapters 5 and 6.

REFERENCES - CHAPTER 4

[4.1] Apostolakis G. E., Salem S. L., Wu J. S., *CAT: A computer code for automated construction of fault trees,* EPRI Report, March 1978.

[4.2] Cross N., *Engineering design methods,* Wiley, 1989.

[4.3] Dixon P., *Decision table and their applications,* Computer and Automation, Vol.13, No.4, 1964, 376-386.

[4.4] Fussel J. B., *A formal methodology for fault tree construction,* Nucl Sci Eng, Vol.2, 1973, 421-432.

[4.5] Fussel J. B., *Synthetic tree model - formal methodology for fault tree construction,* ANCR-1098, Spring Field, VA 11151, March 1973.

[4.6] Henley E. J., Kumamoto H., *Probabilistic risk assessment,* IEEE Press, New York, 1992.

[4.7] Kumamoto H., Henley E. J., *Safety and reliability synthesis of systems with control loops,* AIChE Journal, Vol 25, No. 1, January 1979, 108-113.

[4.8] MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* Military Standard, Naval Ship Engineering Center, Washington D.C..

[4.9] NEL, *FMECA of NEI pedestal crane,* Report No. NECL/01, May 1987.

[4.10] Pollack S. L., *Decision tables: theory and practice,* Wiley-Interscience, New York, 1971.

[4.11] Powers G. J., Tompkins F. C., *Fault tree analysis for chemical processes,* AIChE Journal, Vol.20, No.2, March 1974, 376-386.

[4.12] Salem S. L., *A new methodology for the computer-aided construction of fault tree,* Ann Nucl Energy, Vol.4 1977, 417-433.

[4.13] Salem S. L., *Decision table development and application to the construction of fault trees,* Nuclear Technology, Vol.42, 1979, 51-64.

[4.14] Sen P., Labrie C. R., Wang J., Ruxton T., Chen J., *A general design for safety framework for large Made-To-Order engineering products,* Proceeding of First Newcastle International Conference on Quality and Its Applications, Newcastle, 1-3 September, 1993, 499-505.

[4.15] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12.

[4.16] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), .Vol.105, 1993, 21-34.

[4.17] Wang J., *System modelling for safety and reliability analysis,* EDCN/SAFE/RESC/5/1, June 1991, 13 pages.

[4.18] Wang J., Ruxton T., Labrie C. R., *Design for safety of marine engineering systems with multiple failure state variables",* Accepted March 1994 for Publication by Reliability Engineering and System Safety (Research Report EDCN/SAFE/RESC/10/1, EDC, October 1991).

[4.19] Wang J., Sen P., Thompson R. V., *A mixed modelling approach for safety analysis,* SRA - Europe; 4th Conference on European Technology and Experience in Safety Analysis and Risk Management; 18 - 20 Oct 1993, Rome, Italy, 7 p.

[4.20] Wang J., Ruxton T., Thompson R. V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, Presented at the Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, 29 November-3 December, 1993, 1-10.

[4.21] Waters A., Ponton J. W., *Qualitative simulation and fault propagation in process plants,* Chem. Eng. Res. Des., Vol. 67, July 1989.

CHAPTER 5

Qualitative Reasoning Applied to Safety Modelling

SUMMARY

This chapter reviews some typical qualitative reasoning methods originally developed in the field of Artificial Intelligence (A.I.), and discusses their applicability and limitation with respect to safety modelling. Based on De Kleer's method, a modified qualitative reasoning method is proposed to describe the behaviour of a system.

The proposed qualitative reasoning method can be applied to failure propagation analysis. A "Level Structured Digraph", which may be effectively used in the prediction of failure propagation, is proposed together with a failure propagation analysis model incorporating the qualitative reasoning method.

The proposed qualitative reasoning method is then combined with the MBRM to form a flexible mixed safety modelling methodology. In the mixed modelling methodology, the qualitative reasoning method is used to obtain the precise input-output relations of each component at the component level and the MBRM is then employed to process the information obtained to produce a description of the total system behaviour. The overall model and associated algorithms are described and tested together with the corresponding computer software. An illustrative example is used to demonstrate the proposed mixed modelling methodology.

5.1 Introduction

Qualitative reasoning about the behaviour of a system is dealt with in Artificial Intelligence (A.I.) literature [5.3][5.6][5.8]. In general, the qualitative modelling of the behaviour of a system starts with the description of the structure and produces interpretations which describe the behaviour. Qualitative reasoning concerns reasoning about the behaviour of a system in nonquantitative terms using words and concepts rather than numbers. This is in harmony with the fact that human beings can reason very successfully about physical systems where the knowledge they have is not quantitative but qualitative [5.18]. Qualitative reasoning may be extremely helpful when the values of system parameters are not completely known [5.18].

Very often in design, a quantitative representation of the behaviour of a system may not be possible because, for example, some parameters in the describing differential equations may not be completely and exactly identified. On the other hand, the description of an engineering design, particularly in the early stages, is often more qualitative than quantitative and there is often a partial or total absence of numerical information for quantitative safety analysis. Therefore, a system may have to be described qualitatively.

The possible behaviour of a system can be predicted from its respective constraint equations using qualitative reasoning. A set of constraint equations (qualitative equations and filtering equations) describing the relevant structural relationships in the system may be derived by examination of the physical structure. The possible behaviour of the system may then be produced by generating a set of possible interpretations from the derived constraint equations and initial conditions [5.18].

Qualitative reasoning of the behaviour of a system is an inductive process in which the behaviour of each component, including the tendency of states and state transitions in detail, can be explored and the behaviour of the system can then be predicted with respect to the relationships between the components. The information explored at the component level may be used to conduct the analysis at the system level. The qualitative reasoning technique may be effectively applied to failure propagation analysis [5.18][5.20].

As described in Chapter 4, the MBRM is also an inductive approach and is capable of dealing with variables with multiple states. There are many similarities between the

qualitative reasoning method and the MBRM. In the later sections, the two approaches are compared and integrated to form a flexible mixed safety modelling methodology in which the MBRM is used to process the information produced using the qualitative reasoning method at the component level in order to produce a description of total system behaviour. The methodology may even be used to model a system for which complete input-output relations of the components are difficult to obtain using the MBRM.

5.2 Literature Survey of Qualitative Reasoning

Qualitative reasoning of the behaviour of a system is intended to yield a corresponding abstraction of its behaviour. Qualitative constraints used in a qualitative reasoning analysis are similar to the corresponding quantitative differential equations. A diagram of the abstract levels of modelling physical systems is shown in Figure 5.1.

The three principal qualitative reasoning methods developed in the A.I. field can be summarised as those developed by Forbus, Kuipers and De Kleer.

5.2.1 Forbus' Approach

Forbus' qualitative process theory provides a representational framework for a certain class of deductions about the physical world [5.6]. His qualitative process theory asserts that processes are the mechanisms that directly cause changes. Reasoning about processes, their effects and limits forms an important part of the commonsense physical reasoning.

Forbus uses the idea of a process as something that acts through time to change the parameters of objects in a situation. Simple examples of processes include flows of heat or fluid; boiling; motion and compression.

Forbus' qualitative theory is process-based. A process description may include individuals, preconditions, quantity conditions and influences [5.6]. Forbus' qualitative theory gives a general framework for process system modelling.

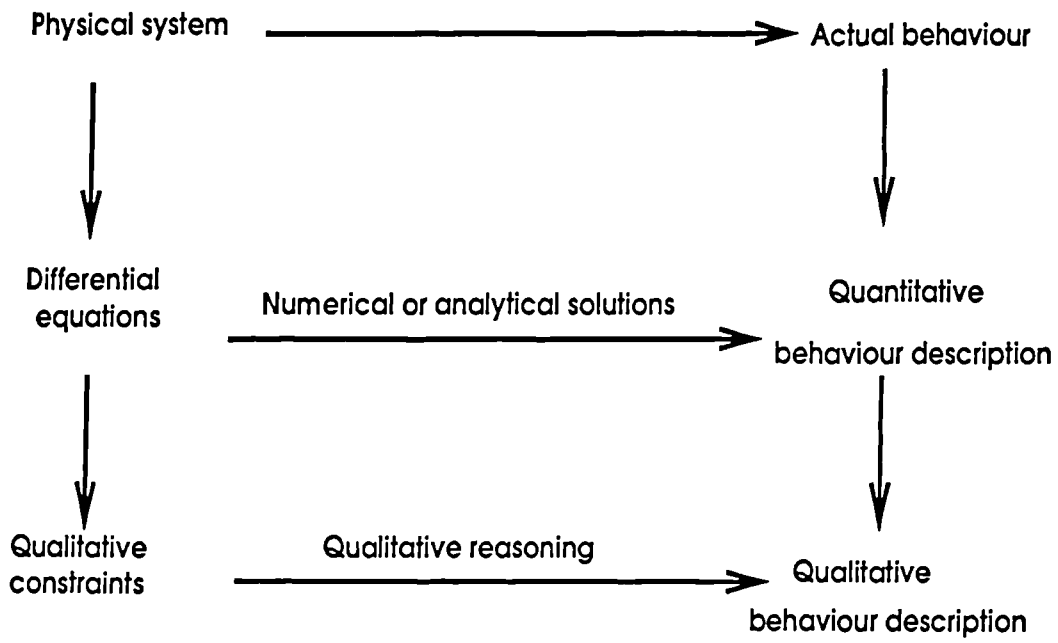


Figure 5.1 The abstract levels of modelling physical systems

5.2.2 Kuipers' Approach

Kuipers' qualitative reasoning is regarded as constructing qualitative constraint functions, solving these functions and interpreting the results in qualitative terms. Each physical parameter in Kuipers' qualitative reasoning model is a continuously differentiable real-valued function of time, and its value at any given point in time is specified qualitatively in terms of the relationship with a totally ordered set of landmark values which may be either numerical (e.g. zero) or symbolic where a landmark value is a chosen value within which a process variable changes. Kuipers' approach allows new landmarks to be discovered during the qualitative reasoning process. As the qualitative reasoning proceeds, Kuipers' dynamic approach can discover and add new landmark values to the sequences.

Inputs to a Kuipers' qualitative reasoning analysis may include following information of a component or a system.

i. A set of symbols representing the functions in the component or system.

ii. A set of qualitative constraints applied to the function symbols.

iii. An ordered set of landmark values for each function.

iv. Upper and lower range limits for each function.

v. Initial time point.

After the input data is prepared, Kuipers' qualitative reasoning algorithm *QSIM* can be used to qualitatively reason about the system behaviour [5.8]. After an initial state is placed on *ACTIVE* whose successors need to be determined, *QSIM* repeatedly takes an *ACTIVE* state and generates all possible success states, filtering out states that violate some consistency criteria [5.8]. Because the next state may not uniquely be determined, *QSIM* builds a tree of states representing the possible behaviours of the mechanism. Kuipers' qualitative reasoning repeats the reasoning process until *ACTIVE* becomes empty or the resource limit is exceeded [5.8].

Kuipers' method is function-based.

5.2.3 De Kleer's Approach

In De Kleer's approach, the behaviour of a physical system can be described by the values of the variables such as forces, velocities, positions, pressures and temperatures at each time interval. The essence of his qualitative reasoning physics is regarded as modelling a physical situation, solving the qualitative equations, and then interpreting the results in qualitative terms. Every physical situation is some type of physical system or machine made up of individual components, each component contributing to the behaviour of the overall system with respect to the relationships with other components.

De Kleer's qualitative reasoning produces a description of the behaviour of a system in terms of the allowable states and the values of the system's variables, and the direction in which these variables are changing [5.3]. Quasi-static approximation is used to ignore behaviour of short enough duration. The quantity space of a qualitative variable consists of only three values: +, - and 0. ∂x is used as abbreviation for dx/dt. The behaviour of a component is divided into different regions within each of which different qualitative equations are involved [5.3].

In De Kleer's approach, a state diagram shows the state transition of the behaviour of a system. Constructing the state diagram is analogous to solving a set of simultaneous differential equations characterising the behaviour of a physical system. The structure of a state transition diagram can be used to answer questions about whether something could happen.

A programme called *ENVISION* has been developed by De Kleer. *ENVISION* takes a description of the physical structure of a system and a library of component models, constructs the model for the overall system, solves the model and produces explanations. *ENVISION* can be used to construct all possible behaviour and all cause and effect relations.

De Kleer's method is device-based.

5.2.4 Applications of Qualitative Reasoning

Qualitative reasoning methods have the ability to predict the qualitative behaviour of a system from the qualitative models based on incomplete knowledge of the process parameters and functionalities [5.1]. The possible applications of qualitative reasoning methods have been extensively discussed in the literature, especially in the areas of

expert system construction and chemical plant design. For instance, Oyeleye and Kramer have used a qualitative reasoning method to predict the steady-state measurement patterns generated as a result of process malfunctions [5.13]. The possible applications of qualitative reasoning methods have also been studied in the areas of safety analysis. Waters and Ponton have discussed the possible applications of qualitative reasoning in a mixed top-down and the bottom-up safety analysis framework in which partial top-down fault tree analysis is used to focus upon areas of interest and partial bottom-up qualitative reasoning is used to explore the areas at a level of detail [5.20]. The mixed approach may be useful for a user to choose the balance between the two techniques in order to exploit the advantages of each [5.20].

In addition, qualitative reasoning methods can also be used for performance monitoring and fault diagnosis. A method, which uses the knowledge derived from a qualitative model of the monitored system to predict the system's temporal behaviour for fault diagnosis, has been developed to assess any departure from the expected behaviour [5.11].

5.2.5 Applicability and Limitation of Qualitative Reasoning

Qualitative reasoning theory can be used to draw several types of basic qualitative deductions, including describing what is happening in a physical situation, reasoning about the combined effects of several processes and predicting when processes will start and stop. The resons why qualitative reasoning theory seems to be useful are [5.10]:

i. Sometimes a system may not be suitably described using a quantitative model.

ii. It can guide quantitative modelling.

iii. It can be used for human reasoning.

iv. It can make computers "clever", that is, it can give expert systems some commonsense knowledge.

The complexity of qualitative reasoning, to a certain extent, depends on the number of dimensions. Consequently, the difference between low dimensionality problems considered in the A.I. literature and high dimensionality problems that arise in real industrial processes must be considered. However, some of the representational

techniques used in qualitative reasoning may effectively be applied to system safety modelling.

A qualitative reasoning is a bottom-up process and uses a clearer notation of system states than top-down approaches [5.20]. It may be effectively applied to the prediction of failure propagation since its principle is quite similar to the one used in the traditional failure propagation analysis [5.17].

The possible applications of qualitative reasoning in safety analysis have been extensively discussed [5.3][5.6][5.8], but not many practical applications are available in the literature. The reason probably lies in efficiency. The complexity of high dimensionality problems limits the applicability even further.

Consequently, direct applications of the qualitative reasoning technique are likely to be of limited value as a practical safety modelling tool. However, this method can be modified and used together with other formal safety modelling methods to effectively exploit its advantages.

5.3 Proposed Qualitative Reasoning Framework for Safety Modelling

It can be noted from the above study that De Kleer's method is a device-based and quasi-steady-state approach and Kuipers' method is a dynamic function-based approach. In De Kleer's method, the behaviour of a system is determined from that of each of the constituent components rather than from more "structural" knowledge of the system. However, Kuipers' method requires every variable to be represented as a continuous function of time. Kuipers' method is probably more formalised than De Kleer's but is more complex and less well suited to quasi-steady state problems. Since a device-based and quasi-steady state approach is often used to give reasonable answers for less work in system safety modelling [5.18], De Kleer's method is chosen for further exploration.

De Kleer's method is still too complex and it is difficult to directly apply the method to system safety modelling. Therefore, a simple and effective qualitative modelling approach is required.

Based on De Kleer's method, a qualitative reasoning framework is proposed as shown in Figure 5.2. In the proposed framework, the qualitative equations and filtering equations for the components of a system are first derived, and the qualitative reasoning

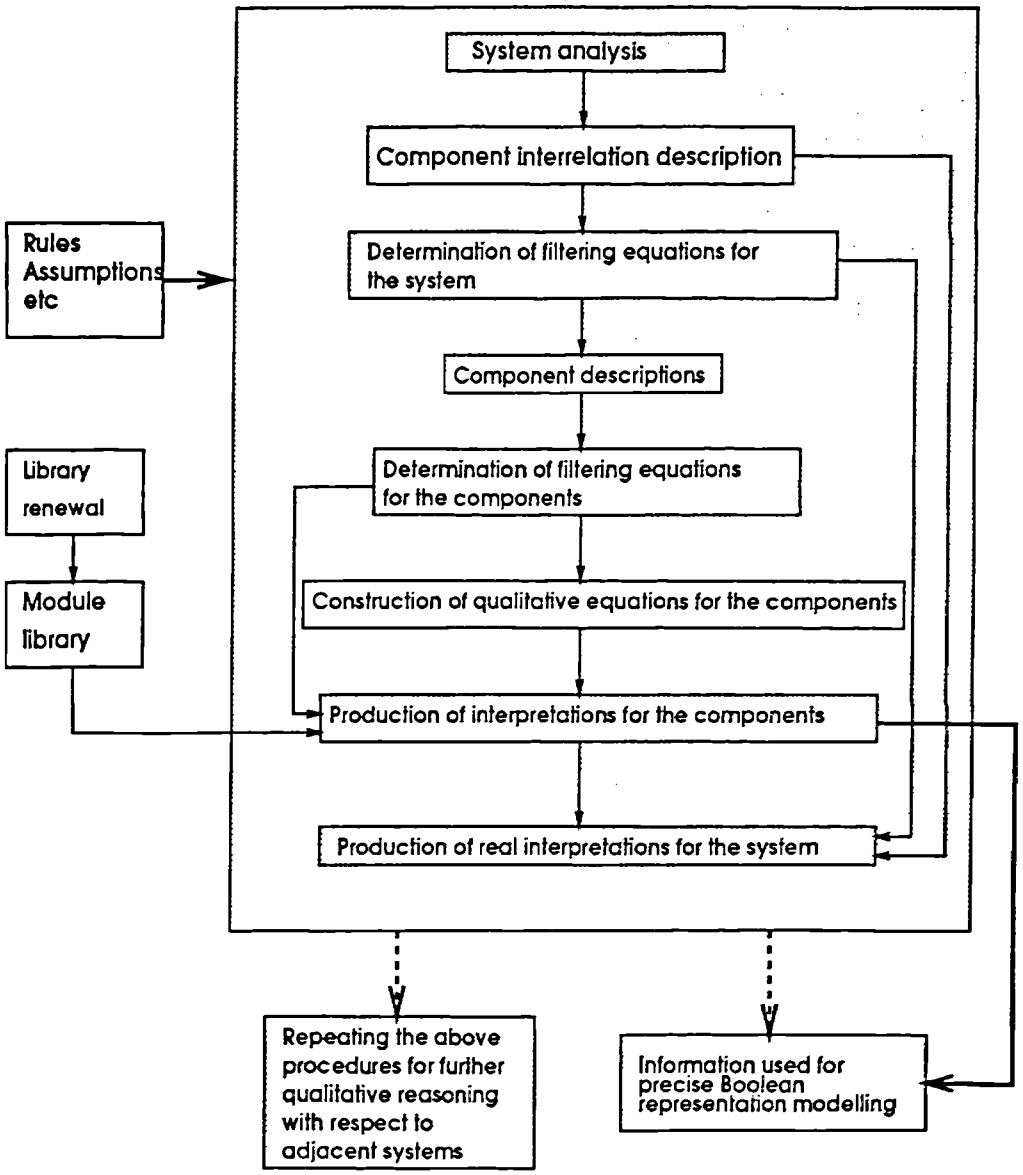


Figure 5.2 A proposed qualitative reasoning framework

for the behaviour of the components is then undertaken. The information developed at the component level can be used for the analysis at the system level.

Each component of a system can be viewed as a simple information processor. The overall behaviour of a system can be produced by studying causal interactions between the components. A component model characterises the possible behaviour a component can generate. A component model can be described by a set of qualitative equations and respective filtering equations. Qualitative equations can be obtained from either commonsense knowledge or differential equations. In general, the rules for transferring a quantitative differential equation to a qualitative one are described as follows:

i. $[E_1 \cdot E_2] \Rightarrow [E_1][E_2]$

ii. $[0][E] \Rightarrow [0]$

iii. $[+][E] \Rightarrow [E]$

iv. $[-][E] \Rightarrow -[E]$

where $[E]$ represents the qualitative value of the variable E.

For example, the flow rate through an orifice is given by [5.3]:

$$Q = CA\sqrt{2P/\rho} \qquad P > 0$$

where Q is the flow rate through the orifice, C is the discharge coefficient of the orifice, A is the cross-section area, P is the pressure across the valve, and ρ is the the mass density of the fluid. The above model can be transformed as follows:

$$[Q] = [C][A][\sqrt{2P/\rho}] = [+][+][\sqrt{2P/\rho}] = [P]$$

The qualitative equation $\partial Q = \partial P$ is then obtained.

Care should be taken to introduce qualitative equations. It has not been determined yet as to how many qualitative equations are actually necessary for effective reasoning about the behaviour of a system [5.18][5.20]. There is a motivation for having all the equations independent (i.e. no redundant equations involved).

The interpretations of a component can be produced by solving the qualitative equations. The interpretations produced can be used to assist in the construction of fault trees or Boolean representation modelling for safety analysis [5.18].

The proposed qualitative reasoning model of a component is described as follows:

Component:

Initial conditions:

Normal: Qualitative equations:

Filtering equations:

Failed: Qualitative equations:

Filtering equations:

The qualitative equations of a component are constructed under two distinct conditions which are Normal and Failed. The quantity space for each variable in qualitative equations consists of three values: +, - and 0. The symbol + represents the case when the quantity is positive, the symbol 0 represents the case when the quantity is zero, and the symbol - represents the case when the quantity is negative.

The algebra of the qualitative reasoning is described as follows:

<1> for the qualitative equation $\partial X = \partial Y + \partial Z$

∂X	∂Y	∂Z
+	+	+
+	+	0
+	0	+
0	0	0
-	-	-
-	-	0
-	0	-
#	+	-
#	-	+

where # stands for "undetermined".

<2> for the qualitative equation $\partial X = \partial Y \cdot \partial Z$

∂X	∂Y	∂Z
+	+	+
-	+	-
0	+	0
0	0	+
0	0	-
0	0	0
-	-	+
-	-	-
0	-	0

It is noted that the states of ∂X in <1> can not be determined when ∂Y and ∂Z have different signs. This ambiguity problem can only be solved by adding the proper filtering equations.

Filtering equations can be determined by comparing the relative importance of two variables affecting the component behaviour. For example, if ∂Y is a more important factor than ∂Z, then [-] = [-] + [+] and [+] = [+] + [-] can be obtained as the filtering equations.

By studying the behaviour of the components and their relationships, the system behaviour can be qualitatively predicted. Obtaining the total set of interpretations for a complex system may be time-consuming [5.18][5.20].

5.4 The Applications of the Qualitative Reasoning Method to Failure Propagation Analysis

5.4.1 A "Level Structured Digraph" for Failure Propagation Analysis

The aim of a failure propagation analysis is to determine all the failure propagation paths and the associated consequences. Failure propagation analysis is very important for improving the safety of a product by safer operation. For example, during operation of a MTO product, if a sensor shows some parameter beyond the range or an alarm is activated, the operator can use the knowledge produced from the failure propagation

analysis to identify the possible consequences and can then decide what actions need to be taken to avoid potential accident situations.

A failure always propagates from one level to another in a system. Therefore, a "Level Structured Digraph" for failure propagation analysis is proposed as shown in Figure 5.3 and described as follows.

Failure propagation analysis can be carried out at different levels within a system. Each level in the failure propagation model may contain a structured representation of the system under particular operational considerations. Each structure may contain a set of components. The failure propagation analysis can operate on an individual structure of the hierarchical failure propagation model and track along all feasible paths and the associated consequences. The information produced at a lower level may be used as input data for the analysis at the next level. The failure analysis is initially started from the failure point indicated by an alarm or a sensor.

If high resolution is not required, failure propagation analysis may be confined to the lower levels of the hierarchal structure to prevent slow analysis caused by the inclusion of an excess of detail.

In the framework shown in Figure 5.3, special details have not been specified such as how to model the system for failure propagation analysis with respect to the different analysis methods and system structures and also how to select the number of levels and the resolution at each level. This framework is considered to be general enough to accommodate many failure analysis methods and various systems. In the next section, the proposed qualitative reasoning method is embedded into this framework to conduct failure propagation analysis.

5.4.2 Failure Propagation Analysis Model Incorporating the Qualitative Reasoning Method

A failure propagation analysis model incorporating the qualitative reasoning method is proposed as shown in Figure 5.4. The qualitative reasoning framework (Figure 5.2) can be applied to construct such a failure propagation model. Given initial conditions, the state transitions of the variables in the system can be analysed. How failures propagate in the system may also be investigated.

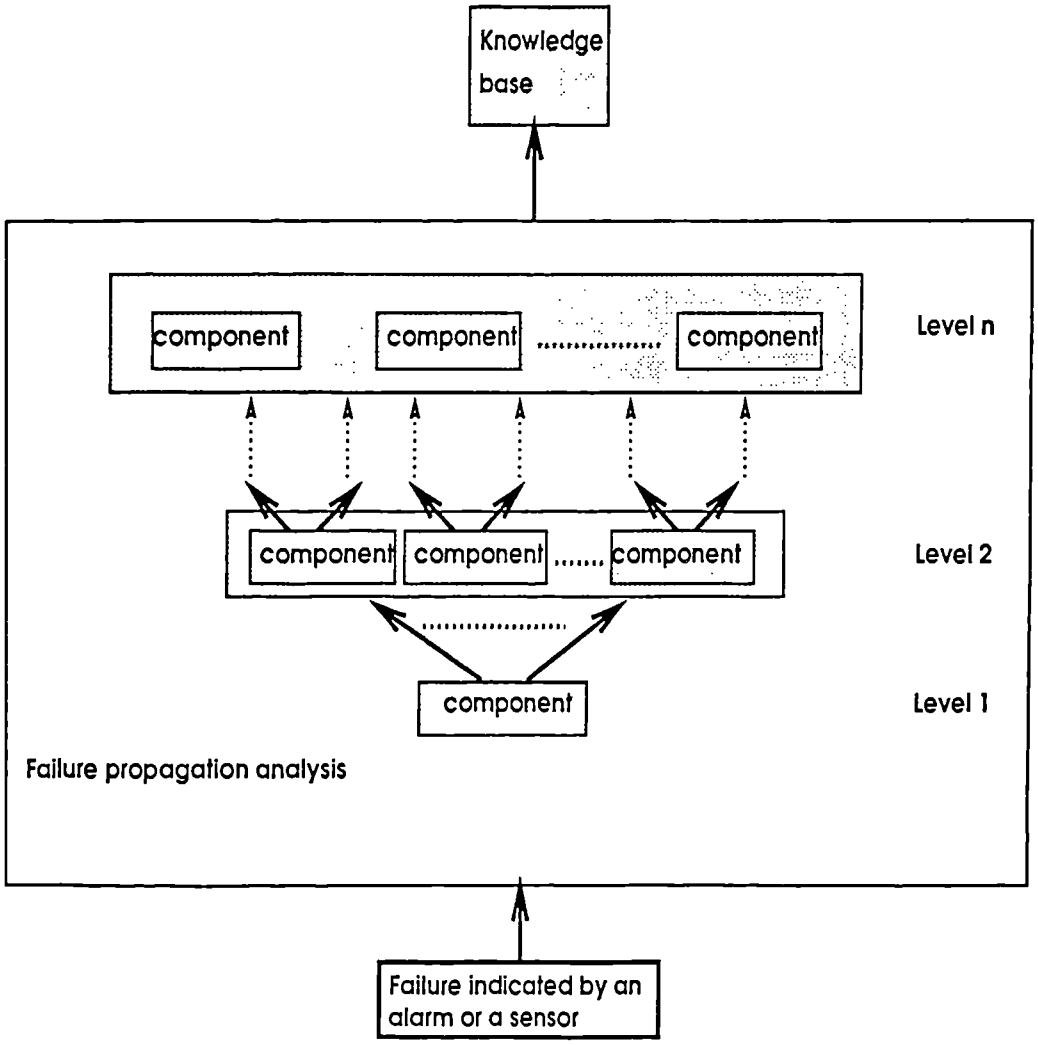


Figure 5.3 A "Level Structured Digraph" for failure propagation analysis

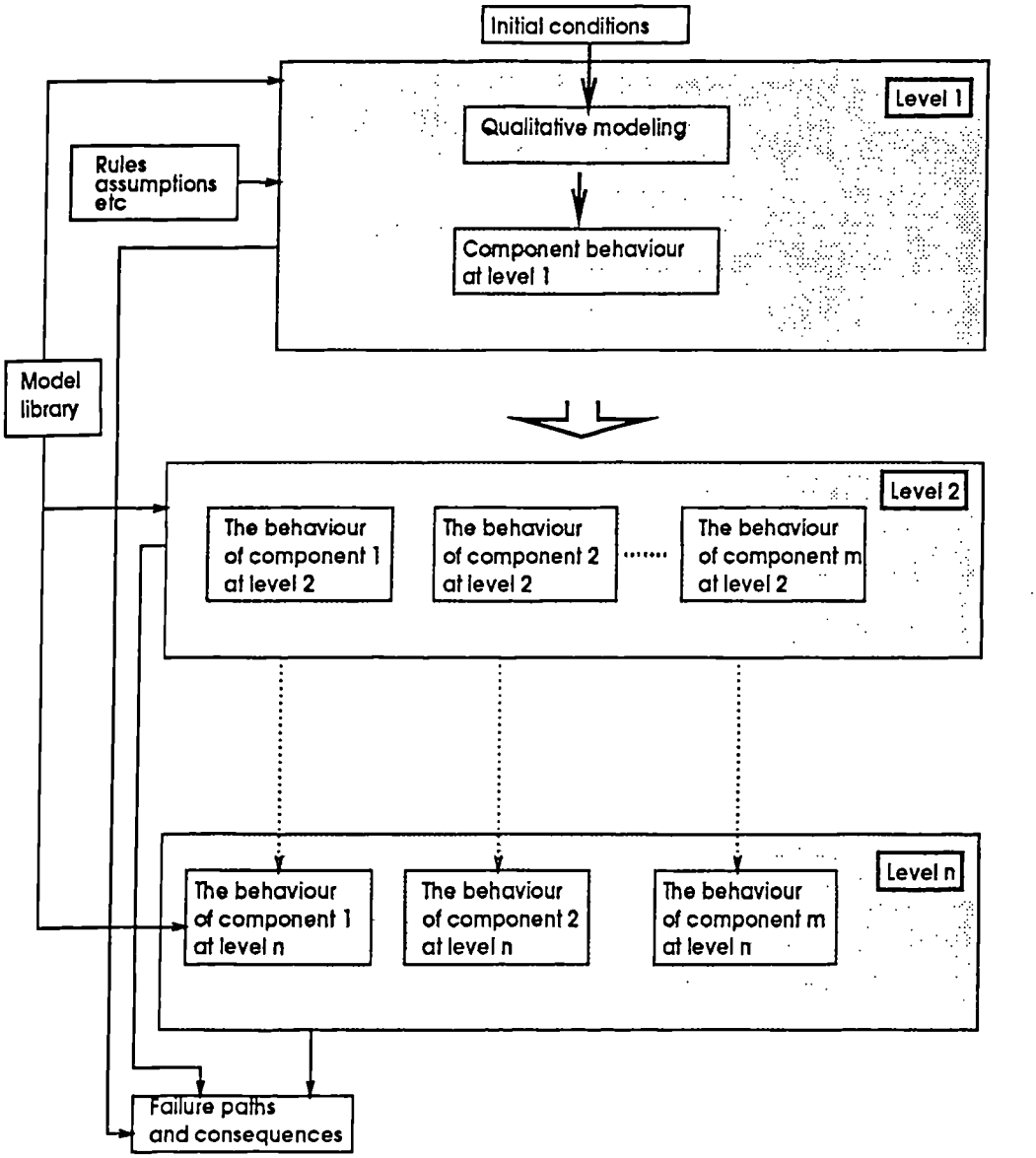


Figure 5.4 A failure propagation model incorporating qualitative reasoning

Assumptions and simplifications are necessary for the convenience of modelling complex MTO products for failure propagation analysis. The aim of making assumptions and simplifications is to allow the failure propagation analysis to be carried out effectively and economically. The following typical assumptions and simplifications may usefully be made for building a failure propagation analysis model.

i. Components or subsystems at the same analysis level are considered to be independent.

ii. Alarms and sensors are considered to be fault free.

iii. At each point in time, only one alarm is activated or only one sensor shows some parameter beyond the acceptable range.

iv. All failures are persistent.

5.4.3 An Example

Figure 5.5 shows a heat exchanger of a diesel engine cooling water system. Suppose the temperature of output sea water is a constant and not considered in the modelling. If alarm 1 is activated, the initial conditions can be obtained which are $\partial T_i = +$ (increasing), $\partial S_v = 0$ (unchanging) and $\partial T_t = 0$ (unchanging). The heat exchanger can be modelled as follows:

Component	**Heat exchanger**	
Initial conditions:	$\partial T_t = +$ $\partial S_v = 0$ $\partial T_t = 0$	
Normal	Qualitative equations:	$\partial T_i - \partial S_v + \partial T_t = \partial T_o$
	Filtering equations:	none
Failed	Qualitative equations:	$\partial T_o = +$
	Filtering equations:	none

where T_o is the outlet temperature, T_i is the inlet temperature, S_v is the flow rate of sea water to the heat exchanger and T_t is the temperature of sea water to the heat exchanger.

If the heat exchanger is in "*Normal*" condition, we can deduce from the above model that, under the given initial conditions, ∂T_o is +. The diagram of the variable changes is shown in the Figure 5.6. Internal system status can clearly be seen. T_o can be taken as an input for the analysis at the next level.

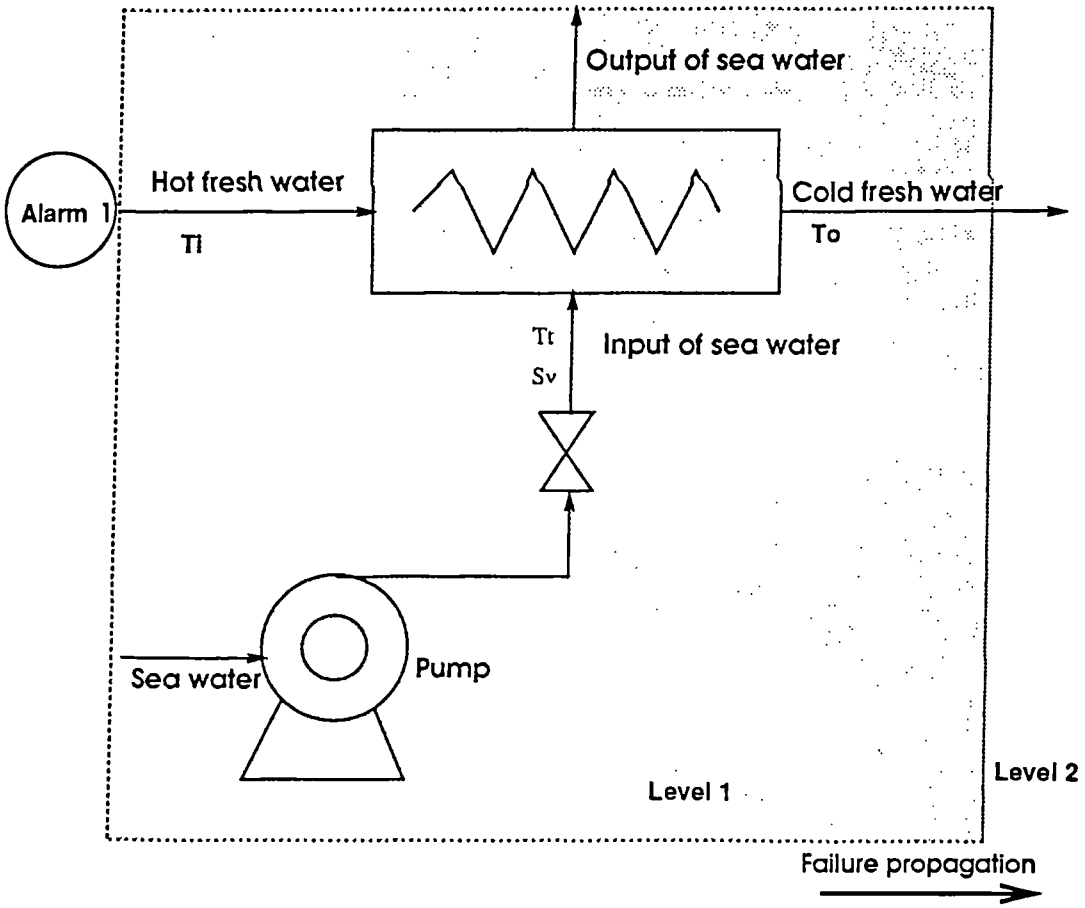


Figure 5.5 An example of failure propagation analysis

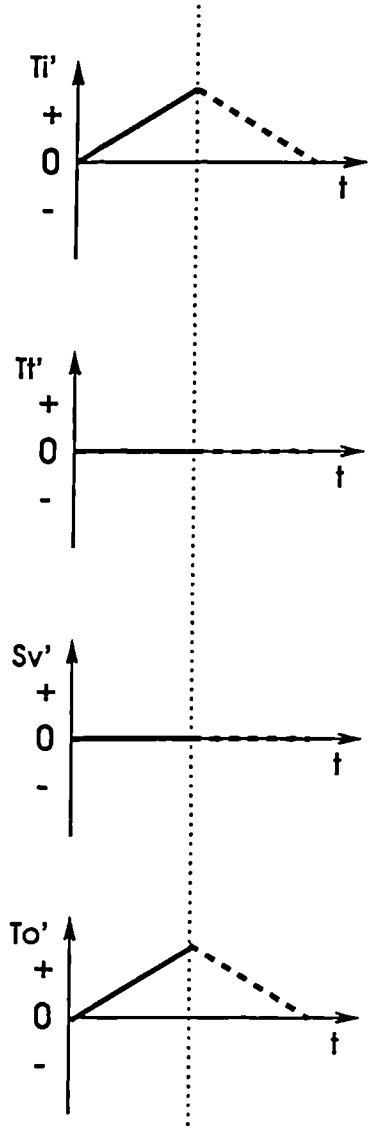


Figure 5.6 The diagram of the variable changes

5.5 Comparison and Integration of the Qualitative Reasoning Method and MBRM

5.5.1 A Mixed Modelling Approach for Safety Analysis

As described in Chapter 4, the usual way to model a component using the MBRM is to study the logical combinations of the input attributes leading to the possible output states. However, it may be difficult at times to choose input-output relations to produce a precise Boolean representation model. It is at this point that the information produced from qualitative reasoning may be used to assist in the construction of the precise Boolean representation models for components.

Two methods are compared as follows:

i. Both methods work in an inductive way.

ii. In both methods, a variable is described in terms of several discrete states.

iii. Both methods have strong inferencing power.

iv. An interpretation in qualitative reasoning is, by nature, similar to a prime implicant in the modified Boolean representation.

v. Both methods are device-based.

It is noticeable that there are a lot of similarities between the qualitative reasoning method and the MBRM. A mixed modelling philosophy is therefore proposed in which the qualitative reasoning method is used to obtain the precise input-output relations of each component at the component level and the MBRM is used to process the information obtained, to produce all the prime implicants associated with all possible top events.

The proposed mixed modelling methodology can make use of the advantages of both the qualitative reasoning method and the MBRM. It may be used as an automatic modelling tool for safety modelling. Given the components and their relationships in a system, the final system Boolean representation description can conveniently be produced.

5.5.2 Software

A software written in *MODSIM II*^{TM} has been developed to obtain the interpretations for components. Only three states (i.e. +, 0 and -) of each component can be dealt with. Interpretations of each component are obtained by processing the corresponding qualitative equations and filtering equations. The software described in chapter 4 has been combined with this one to form a qualitative reasoning software which can be used to study the obtained interpretations of components and their relationships to obtain the system failure events and respective prime implicants. The flowchart for the software is shown in Figure 5.7.

In this chapter, component models are constructed by users rather than obtained from the model library. It would be worthwhile for ease of analysis to build a model library which can contain the qualitative models of components so that given a component's description a qualitative model can be directly obtained by referring to the model library.

5.5.3 An Example

A cooling water system for a marine diesel engine is functionally shown in Figure 5.8. This system is used to supply cooling water for a marine diesel engine system.

The following assumptions are made for the convenience of analysis.

- Each component in the system normally works under an equilibrium state, i.e., if all inputs ∂(*input* 1), ∂(*input* 2), ---, ∂(*input n*) are 0, then ∂(*output*) is 0.
- Each component in the system can only work under either Normal (N) or Failed (F) *condition.*

H, S, C, M, F and V represent the internal modes of Heat Exchanger, Sensor, Controller, Set Point Monitor, Water Filter and Valve, respectively (as shown in Figure 5.8). The notation of other variables for this cooling water system is described as follows:

T_c: Temperature of sea water to the control valve

S_m: Input to the control valve

S_c: Output of the controller

S_s: Output of the temperature sensor

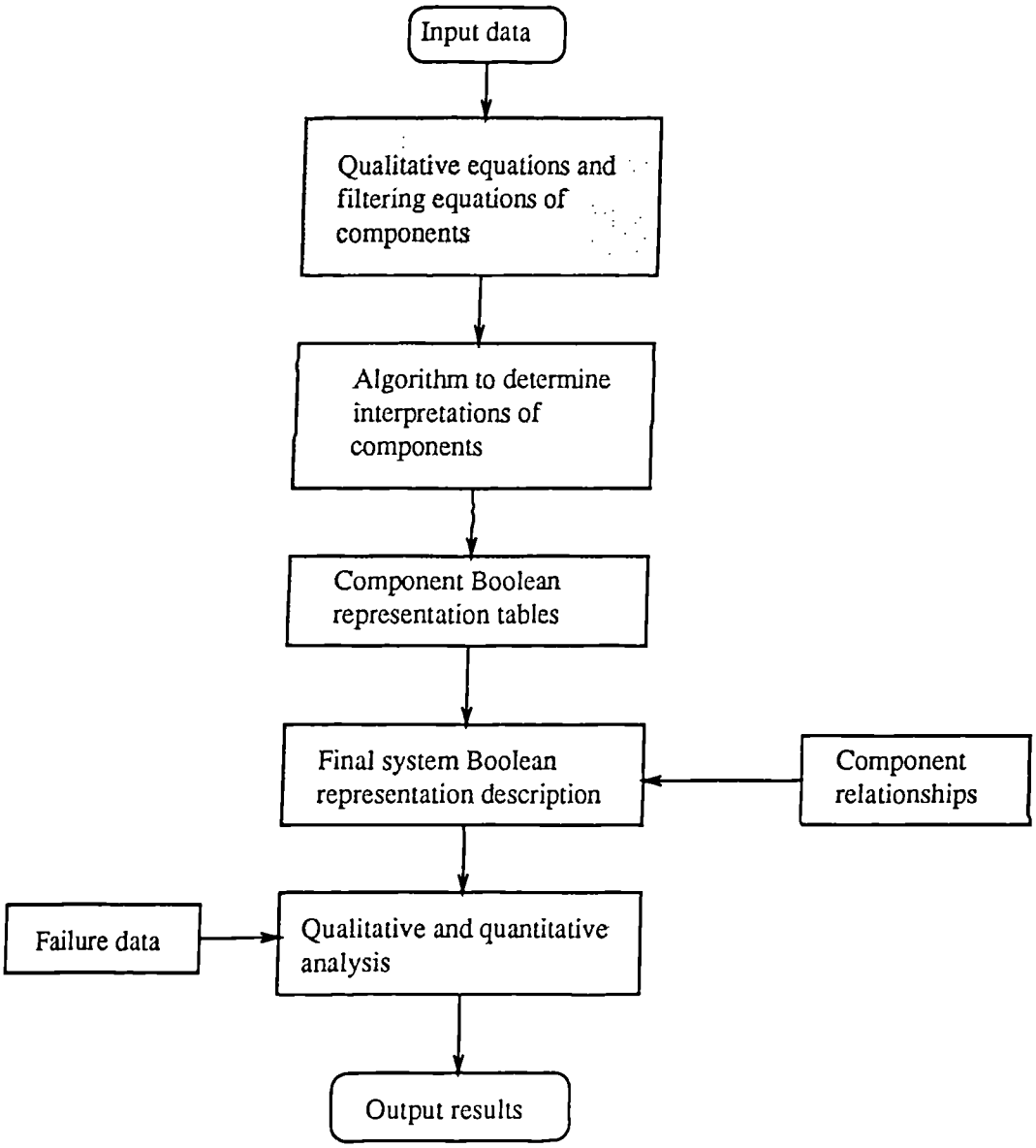


Figure 5.7 The function of the qualitative reasoning software

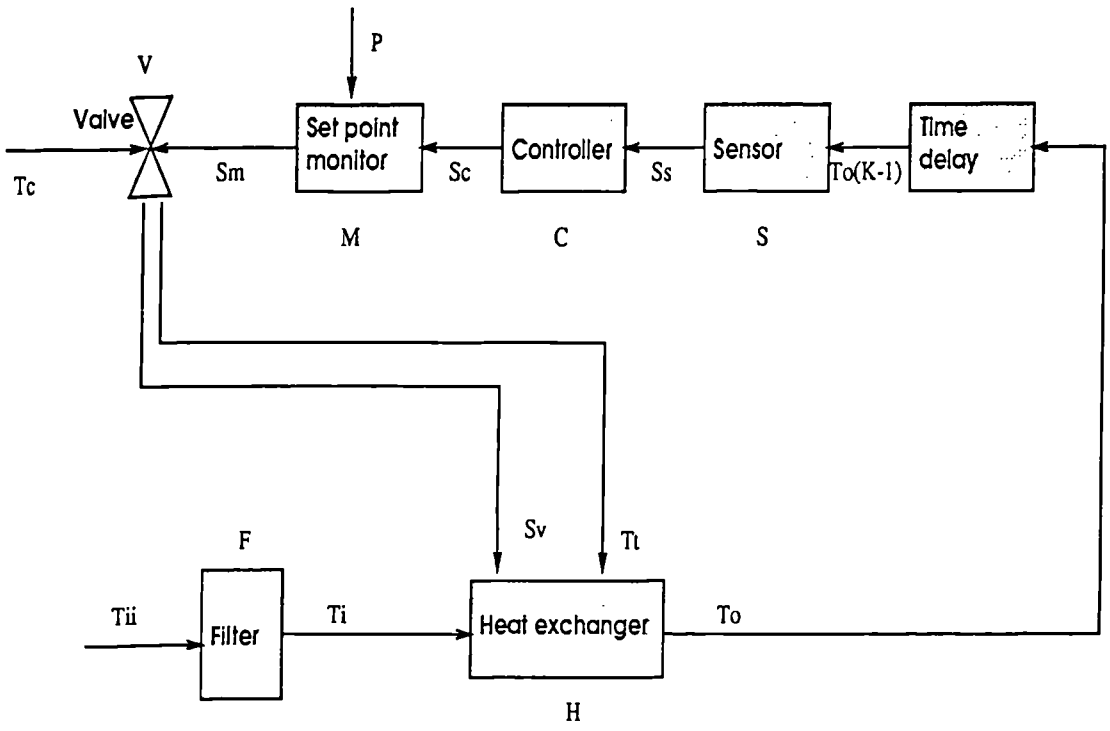


Figure 5.8 A cooling water system for a marine diesel engine

T_o: Temperature of fresh water from the heat exchanger

S_v: Flow rate of sea water to the heat exchanger

T_t: Temperature of sea water to the heat exchanger

T_{ii}: Temperature of fresh water to the filter

T_i: Temperature of fresh water to the heat exchanger

P: Input to the set point monitor

$T_o(k-1)$: Temperature of fresh water from the heat exchanger because of time lag

k: Time interval number

S_m, S_c, S_s, T_i, S_v and T_t are intermediate variables and the others are primary variables.

The components of the cooling system are modelled as follows using the described qualitative reasoning method.

Filter (L)

L = Normal (N):	Qualitative equations:	$\partial T_i = \partial T_{ii}$
	Filtering equations:	none
L = Failed (F):	Qualitative equations:	$\partial T_i = +$
	Filtering equations:	none

Heat exchanger (H)

H = Normal (N):	Qualitative equations:	$\partial T_0 = \partial T_i - \partial S_v + \partial T_t$
	Filtering equations:	$\partial T_i[\pm] - \partial T_t[\pm] = 0$; $\partial S_v[\pm] - \partial T_t[\pm] = [\pm]$; $\partial T_i[\pm] - \partial S_v[\pm] = 0$
H = Failed (F):	Qualitative equations:	$\partial T_i = -$
	Filtering equations:	none

Sensor (S)

S = Normal (N):	Qualitative equations:	$\partial S_s = \partial T_o(k-1)$
	Filtering equations:	none
S = Failed (F):	Qualitative equations:	$\partial S_s = 0$

Filtering equations: none

Controller (C)

C = Normal (N): Qualitative equations: $\partial S_c = \partial S_s$
(for proportional controller)
Filtering equations: none
C = Failed (F): Qualitative equations: $\partial S_c = 0$
Filtering equations: none

Set point monitor (M)

M = Normal (N): Qualitative equations: $\partial S_m = \partial S_c + \partial P$
Filtering equations: $\partial S_m[\pm] = -\partial S_c[\pm] + \partial P[\pm]$
M = Failed (F): Qualitative equations: $\partial S_m = 0$
Filtering equations: none

Valve (V)

V = Normal (N): Qualitative equations: $\partial S_v = \partial S_m$
$\partial T_i = \partial T_c$
Filtering equations: none
V = Failed (F): Qualitative equations: $\partial S_v = -$
$\partial T_i = -$
Filtering equations: none

The Boolean representation tables of the components of the cooling water system can automatically be generated from the obtained qualitative models using the developed software, and are shown in Tables 5.1, 5.2, 5.3, 5.4, 5.5 and 5.6.

Table 5.1 The Boolean representation table of the water filter

L	∂T_{ii}	∂T_i
F	*	+
N	+	+
N	0	0
N	-	-

Table 5.2 The Boolean representation table of the heat exchanger

H	∂T_i	∂S_v	∂T_c	∂T_0
F	*	*	*	+
N	0	0	-	-
N	-	0	-	-
N	+	0	-	0
N	0	-	-	+
N	-	-	-	-
N	+	-	-	+
N	0	+	-	-
N	-	+	-	-
N	+	+	-	-
N	0	0	0	0
N	-	0	0	-
N	+	0	0	+
N	0	-	0	+
N	-	-	0	0
N	+	-	0	+
N	0	+	0	-
N	-	+	0	-
N	+	+	0	0
N	0	0	+	+
N	-	0	+	0
N	+	0	+	+
N	0	-	+	+
N	-	-	+	+
N	+	-	+	+
N	0	+	+	-
N	-	+	+	-
N	+	+	+	+

Table 5.3 The Boolean representation table of the sensor

S	$\partial T_o(k-1)$	∂S_s
F	*	0
N	+	+
N	0	0
N	-	-

Table 5.4 The Boolean representation table of the controller

C	∂S_s	∂S_c
F	*	0
N	+	+
N	0	0
N	-	-

Table 5.5 The Boolean representation table of the set point monitor

M	∂S_c	∂P	∂S_m
F	*	*	0
N	0	0	0
N	0	-	-
N	0	+	+
N	-	-	-
N	-	0	-
N	-	+	+
N	+	0	+
N	+	-	-
N	+	+	+

Table 5.6 The Boolean representation table of the valve

V	∂S_m	∂S_v
F	*	-
N	+	+
N	0	0
N	-	-

V	∂T_c	∂T_t
F	*	-
N	+	+
N	0	0
N	-	-

where * stands for "Don't care".

The final Boolean representation table can then be produced as shown in Table 5.7 using the software developed.

Table 5.7 The final system Boolean representation table

No.	H	L	∂T_{ii}	V	M	C	S	$\partial T_O(k-1)$	P	∂T_c	∂T_o
1	N	N	+	N	N	N	N	+	0	0	0
2	N	N	-	N	N	N	N	-	0	0	0
3	N	F	*	N	N	N	N	+	0	0	0
4	N	N	-	N	N	*	*	*	-	0	0
5	N	N	-	N	*	*	*	0	0	+	0
6	N	N	-	N	*	*	F	*	0	+	0
7	N	N	0	N	*	*	F	*	0	0	0
8	N	N	0	N	*	*	*	0	0	0	0
9	N	N	-	N	*	F	*	*	0	+	0
10	N	N	0	N	*	F	*	*	0	0	0
11	N	N	+	N	*	*	F	*	0	-	0
12	N	N	+	N	*	F	*	*	0	-	0
13	N	N	+	N	*	*	*	0	0	-	0
14	N	N	-	N	F	*	*	*	*	+	0
15	N	F	*	N	*	*	F	*	0	-	0
16	N	F	*	N	*	F	*	*	0	-	0
17	N	N	0	N	F	*	*	*	*	0	0
18	N	N	+	N	F	*	*	*	*	-	0
19	N	F	*	N	*	*	*	0	0	-	0
20	N	F	*	N	F	*	*	*	*	-	0
1	N	N	+	N	N	N	N	+	0	-	-
2	N	N	-	N	N	N	N	*	-	-	-
3	N	N	-	N	N	*	N	*	+	+	-
4	N	N	+	N	N	N	*	-	+	-	-
5	N	F	*	N	N	N	N	+	0	-	-
6	N	N	-	N	N	N	F	*	*	-	-
7	N	N	0	N	N	N	N	+	0	*	-
8	N	N	-	N	N	N	N	-	*	-	-
9	N	N	-	N	N	N	N	+	0	*	-
10	N	N	*	N	N	N	F	*	+	-	-
11	N	N	0	N	*	*	N	0	0	-	-
12	N	F	*	N	N	*	*	0	+	-	-
13	N	N	0	N	*	N	N	*	+	-	-
14	N	N	-	N	N	*	*	+	+	*	-
15	N	N	-	*	N	*	*	0	0	-	-

Table 5.7 The final system Boolean representation table (Continued)

No.	H	L	∂T_{ii}	V	M	C	S	$\partial T_O(k-1)$	P	∂T_c	∂T_o
16	N	N	-	N	N	*	N	0	+	*	-
17	N	N	0	N	N	*	*	*	+	+	-
18	N	N	0	N	N	*	*	*	+	0	-
19	N	N	0	N	N	*	F	*	+	*	-
20	N	N	0	N	*	*	F	*	0	-	-
21	N	N	-	N	N	*	F	*	+	*	-
22	N	F	*	N	N	*	F	*	+	-	-
23	N	N	-	*	N	*	F	*	0	-	-
24	N	N	0	N	*	F	*	*	0	-	-
25	N	N	-	*	N	F	*	*	0	-	-
26	N	N	0	N	N	F	*	*	+	*	-
27	N	F	*	N	N	F	*	*	+	-	-
28	N	N	-	N	N	F	*	*	+	*	-
29	N	N	-	F	N	*	F	*	0	*	-
30	N	N	-	F	F	*	*	*	*	-	-
31	N	N	-	F	N	*	*	0	0	*	-
32	N	N	0	N	F	*	*	*	*	-	-
33	N	N	-	F	N	F	*	*	0	*	-
1	N	*	-	N	N	N	N	-	0	+	+
2	N	N	+	N	N	N	*	+	+	+	+
3	N	N	+	N	N	N	*	0	+	+	+
4	N	N	+	N	N	*	N	+	-	-	+
5	N	*	-	N	N	N	N	*	-	+	+
6	N	N	+	N	N	N	*	0	-	0	+
7	N	N	+	N	N	*	*	+	0	+	+
8	N	N	-	N	N	*	F	*	-	+	+
9	N	N	+	N	N	N	*	+	-	0	+
10	N	N	0	F	N	N	N	0	0	*	+
11	N	N	+	N	N	F	*	*	-	-	+
12	N	*	0	N	N	N	N	0	0	+	+
13	*	N	+	N	N	N	F	*	+	+	+
14	*	N	+	N	N	N	N	-	0	*	+
15	N	F	*	N	N	N	N	-	0	*	+
16	N	*	0	F	N	N	F	*	0	0	+
17	N	F	*	N	N	N	*	-	-	+	+

Table 5.7 The final system Boolean representation table (Continued)

No.	H	L	∂T_{ii}	V	M	C	S	$\partial T_O(k-1)$	P	∂T_c	∂T_o
18	N	*	0	N	N	*	N	-	-	-	+
19	N	F	*	N	N	*	*	+	0	+	+
20	*	N	+	N	N	N	F	*	-	-	+
21	N	*	0	N	N	*	N	+	-	-	+
22	*	N	0	N	N	N	N	-	0	*	+
23	N	*	0	N	N	N	N	*	-	0	+
24	*	N	+	N	N	N	F	*	-	0	+
25	N	N	+	F	N	*	*	0	0	*	+
26	N	N	+	F	N	*	F	*	0	*	+
27	*	*	*	N	N	N	N	+	-	+	+
28	N	N	+	N	N	*	F	*	0	+	+
29	*	N	+	N	N	*	N	0	0	0	+
30	N	*	0	N	N	N	F	*	0	+	+
31	*	N	+	N	N	*	N	0	0	+	+
32	*	N	-	N	N	F	*	*	-	+	+
33	N	N	+	N	N	*	F	*	0	0	+
34	N	F	*	N	N	*	*	0	0	+	+
35	*	F	*	N	N	N	N	-	0	*	+
36	*	*	0	N	N	N	N	-	0	*	+
37	*	N	0	N	N	F	*	*	-	0	+
38	*	N	0	N	N	N	F	*	-	*	+
39	*	N	0	F	N	F	*	*	0	0	+
40	N	*	0	N	N	F	*	*	-	-	+
41	N	*	0	F	N	*	F	*	0	*	+
42	*	F	*	N	N	*	*	*	+	+	+
43	N	*	0	F	N	*	*	0	0	*	+
44	N	F	*	N	N	*	F	*	0	+	+
45	*	N	+	F	N	F	*	*	0	*	+
46	*	N	+	N	N	F	*	*	0	+	+
47	*	N	0	N	N	F	*	*	0	+	+
48	*	F	*	N	N	N	F	*	-	*	+
49	*	F	*	N	*	N	N	*	-	0	+
50	N	F	*	N	*	*	*	0	0	0	+
51	*	N	+	N	N	F	*	*	0	0	+
52	*	F	*	N	N	F	*	*	-	-	+
53	*	F	*	N	N	*	N	*	-	-	+

Table 5.7 The final system Boolean representation table (Continued)

No.	H	L	∂T_{ii}	V	M	C	S	$\partial T_O(k-1)$	P	∂T_c	∂T_o
54	N	F	*	F	*	*	F	*	0	-	+
55	N	F	*	F	*	*	*	0	0	-	+
56	N	F	*	N	*	*	F	*	0	0	+
57	N	F	*	F	*	*	F	*	0	*	+
58	*	*	0	F	N	F	*	*	0	*	+
59	*	F	*	N	N	F	*	*	0	+	+
60	N	F	*	F	*	*	*	0	0	*	+
61	N	N	0	N	F	*	*	*	*	+	+
62	*	F	*	N	*	F	*	*	0	0	+
63	*	F	*	F	*	F	*	*	0	-	+
64	N	F	*	F	F	*	*	*	*	+	+
65	*	F	*	F	*	F	*	*	0	*	+
66	*	N	0	F	F	*	*	*	*	*	+
67	*	F	*	F	F	*	*	*	*	-	+
68	*	F	*	F	F	*	*	*	*	*	+
69	*	F	*	N	F	*	*	*	*	0	+
70	F	*	*	*	*	*	*	*	*	*	+

The last column of the above Boolean representation table describes the states of the output of the system and other columns prescribe the states of the input attributes. Each row represents a possible condition for an occurrence of the system's output state. Both qualitative and quantitative safety analysis can be carried out to assess the probability of occurrence of each system failure event on the basis of the above Boolean representation table. The possible consequences of each system failure event can also be assessed with respect to the particular environment in which the marine cooling system is working. The improvement of design aspects and maintenance policies may then be made.

5.6 Concluding Remarks and Further Trends

This chapter has reviewed the development on qualitative reasoning from the A.I in the domain of safety analysis. De Kleer's method is found to be most suitable to be applied to safety modelling. Based on De Kleer's method, a modified qualitative reasoning

method is proposed. The proposed qualitative reasoning framework can be applied to failure propagation analysis with respect to a failure signal indicated by an alarm or a sensor.

It is concluded that although the direct application of the qualitative reasoning method to safety modelling is unlikely to be widely used as a practical modelling tool on its own it is worthwhile to intergrate it with other formal safety modelling methods to explore the advantages of each. A mixed modelling approach is therefore proposed in which qualitative reasoning is used at the component level and the Boolean representation modelling at the system level. This mixed modelling approach allows a bottom-up approach to be taken even in those cases where it is difficult to obtain complete input-output relations for all the components of the system, as the qualitative descriptions of components can form the basis for generating the rest of the required input-output relations. This mixed modelling approach can also be used in a "design for safety" knowledge based system as shown in Figure 5.9 in which qualitative reasoning, Boolean representation analysis, component modules and a failure database may be involved in building the knowledge base.

Further study in the areas of qualitative reasoning may address the following areas:

- Implementation of the proposed qualitative reasoning method for system performance description.
- Integration of further aspects of the qualitative reasoning method with other formal safety analysis methods.
- Construction of a model library.
- Building a "design for safety" knowledge-based system incorporating the qualitative reasoning method.

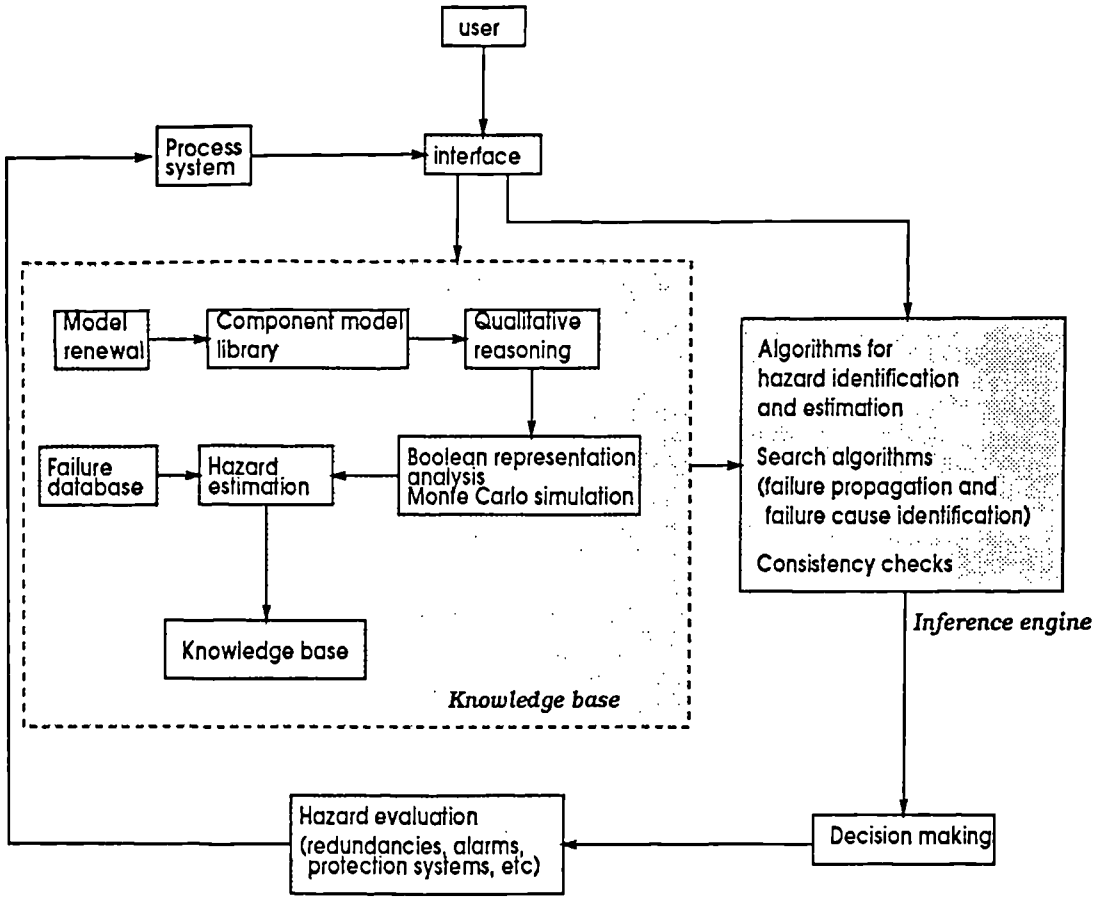


Figure 5.9 A "design for safety" knowledge-based system incorporating the qualitative reasoning approach

REFERENCES - CHAPTER 5

[5.1] Dalle Molle D. T., Edgar T. F., *Qualitative simulation for process modelling and control,* American Control Conference Proceeding, IEEE, 1989, 1360-1367.

[5.2] Dalle Molle D. T., Edgar T. F., Kuipers B., *Modelling chemical processes with unknown parameters,* Proceeding of the ISA/89, Int. Conf. & Exhibition, ISA, 1988, 59-66.

[5.3] De Kleer J., Brown J. S., *A qualitative physics based on confluences,* Artificial Intelligence, Vol.24, 1984, 7-83.

[5.4] Dvorak D. L., Dalle Molle D. T., Kuipers B., Edgar T. F., *Qualitative simulation for expert systems,* 11th Triennia World Congress of the Int Federation of Automatic Control, IFAC 1991, Tallinn USSR, 204-209.

[5.5] Fishwick P. A., *A study of terminology and issues in qualitative simulation,* Simulation, January 1989, 5-9.

[5.6] Forbus K. D., *Qualitative process theory,* Artificial Intelligence, Vol.24, 1984, 85-168.

[5.7] Gassimo M., Stefanini A., Tomada L., *ODS: A diagnostic system based on qualitative modelling techniques,* CH2712-8/89, IEEE, 1989, 141-149.

[5.8] Kuipers B., *Qualitative simulation,* Artificial Intelligence, Vol.29, 1986, 289-338.

[5.9] Kuipers B., *Qualitative simulation as causal explanation,* IEEE Transactions on Systems, Man, and Cybernetics, Vol.17, No.3, May/June 1987, 432-444.

[5.10] Janowski R., *An introduction to QSIM and qualitative simulation,* Artificial Intelligence in Engineering, Vol.2, No.2, 1987, 65-71.

[5.11] McDowell J. K., Davis J. F., *Managing qualitative simulation in knowledge-based chemical diagnosis,* AIChE Journal, Vol.37, No.4, April 1991, 569-580.

[5.12] Narayanan N. H., Viswanadham N., *A methodology for knowledge acquisition and reasoning in failure analysis of systems,* IEEE Transactions on Systems, Man, and Cybernetics, Vol.17. No.2, March/April 1987, 274-288.

[5.13] Oyeleye O. O., Kramer M. A., *Qualitative simulation of chemical process systems: steady-state analysis,* Vol.34, No.9, AIChE Journal, September 1988, 1441-1453.

[5.14] Wang J., *Qualitative reasoning and its applications to safety analysis,* EDCN/SAFE/RESC/15/1, Research Report, Engineering Design Centre, University of Newcastle upon Tyne, December 1992, 21 p.

[5.15] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12.

[5.16] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), Vol.105, 1993, 21-34.

[5.17] Wang J., Ruxton T,, Thompson R.V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, The Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, December 1993, 1-10.

[5.18] Wang J., Sen P., Thompson R. V., *A mixed modelling approach for safety analysis,* SRA - Europe; 4th Conference on European Technology and Experience in Safety Analysis and Risk Management; 18 - 20 Oct 1993, Rome, Italy, 7 p.

[5.19] Wang J., Ruxton T., Labrie C., *Design for safety of marine engineering systems with multiple failure state variables,* Accepted March 1994 for Publication by Reliability Engineering and System Safety (Research Report EDCN/SAFE/RESC/10/1, EDC, October 1991).

[5.20] Waters A., Ponton J. W., *Qualitative simulation and fault propagation in process plants,* Chem Eng Res Des, Vol.67, July 1989, 407-422.

[5.21] Yu C., Lee C., *Fault diagnosis based on qualitative/quantitative process knowledge,* AIChE Journal, Vol.37, No.4, April 1991, 617-628

CHAPTER 6

Simulation Models Applied to the Assessment of Safety

SUMMARY

As described in Chapter 3, the Cullen and Carver reports recommend that more formal safety analysis be used to help preventing major accidents in large MTO products [6.4]. One such technique is computer simulation. As a consequence, attention is being increasingly directed towards the development of simulation methods and their applications.

In this chapter, various simulation techniques are studied. The techniques and steps used in the verification and validation processes are described in some detail. Various related issues such as the requirements and assumptions for simulation modelling are also addressed. After a brief review of the work on simulation modelling developed for safety analysis, two simulation models are developed to simulate system availability and component/subsystem failures, and the probability of occurrence of each system top event.

The two simulation models developed in this chapter make use of the information produced using FMECA and the MBRM. An illustrative example is presented to demonstrate the use of the proposed computer simulation models and the interactions between simulation modelling and other formal safety analysis methods.

6.1 Introduction

As MTO products become more and more complex, simulation technology becomes increasingly useful in the prediction of their safety. Simulation techniques can be effectively used together with other safety modelling methods to improve the prediction of the safety of MTO products both at the design stage and in operation [6.28].

Computer simulation or (more accurately) the study of the response of system models using computers is becoming a flexible standard tool for the practising engineer, although it is recognised that a major difficulty in the application of computer simulation to safety prediction is in the development of system models [6.28].

In Chapter 4, the MBRM was used to calculate the safety parameters for MTO products. In such a deterministic analysis, the probability of occurrence of a top event is calculated given the failure rate of each basic event. However, as discussed in section 3.4.9.1, simulation may prove to be a more flexible and suitable method to calculate safety parameters of a complex system, especially when different distribution types of component failures and repairs are involved, and also when covert and revealed failures [6.27][6.28] as well as maintenance activities are taken into account.

Good safety simulation modelling depends on the selection of suitable simulation techniques and simulation languages, and the effective application of verification of validation programmes. Therefore, various aspects of a simulation process needs to be studied in detail.

Safety simulation analysis can be used to assess system availability, component/subsystem failures and system top events. Component/subsystem failures can be predicted by studying the information produced from FMECA and system top events can be studied on the basis of the minimal cut sets or prime implicants produced using FTA or the MBRM. In this chapter, two simulation models are developed as follows:

i. The computing of system availability and the prediction of component/subsystem failures on the basis of information developed from FMECA.

ii. The computing of the probabilities of occurrence of system top events on the basis of the final system Boolean representation table obtained using the

MBRM.

The information produced from the simulation analysis for system availability, failures of each component/subsystem and the probability of occurrence of each system failure event may be used for design and maintenance decision making.

6.2 System Modelling

6.2.1 Classification of Simulation Techniques

Depending on the nature of the problem being modelled, a simulation model may be classified as one of the following three types [6.28]:

i. Continuous.

ii. Discrete.

iii. Combined discrete-continuous.

A continuous model is one whose states vary continuously with time, so that the effects of the events and the intervals between event times are infinitesimal. In such a simulation model, a system is usually described by a set of differential equations, and the operation paths (functions that satisfy the equations) are usually determined solely by the initial and boundary conditions. This type of simulation is widely used in mechanics, electrical engineering and economics [6.16].

A discrete event model mimics a system or process whose behaviour of interest changes values or states at discrete moments in time. Discrete stochastic models come in a variety of shapes and sizes, but may be divided into two broad categories — discrete-time event and continuous time-discrete event simulation [6.16]. In a discrete-time event simulation, a system is studied only at selected moments in time. Any changes of states are noticed only at observation points. It is obvious that a continuous event simulation can be approximated to any degree of accuracy by choosing a sufficiently small fixed time increment. However, in a continuous time-discrete event simulation, the time parameter is continuous and the observation period is a real interval, usually taken to start at zero for convenience. The characteristic feature of a continuous time-discrete event simulation is that its performance is completely determined by the sequence of event times $t_1, t_2, \cdots, t_j, \cdots$ and by the discrete

changes in the system states which take place at those moments. Obviously, it is not necessary for a continuous time-discrete event simulation to make small, fixed increments in the model's time variable and to change the system states as required at each increment in time. The continuous time-discrete event simulation model can advance its internal time directly from one discrete occurrence to the next.

A system behaviour may depend on both discretely and continuously changing state variables, in which case continuous system simulation and discrete event simulation techniques may be combined. Such a simulation is defined as a combined discrete-continuous simulation. Three types of interactions, which may occur between discretely changing and continuously changing state variables, are described as follows:

i. A discrete event may cause a discrete change in the value of a continuous state variable.

ii. A discrete event may cause the relationship governing a continuous state variable to change at a particular time.

iii. A continuous state variable achieving a threshold value may cause a discrete event to occur or to be scheduled.

Modelling of a discrete behaviour differs significantly from that of a continuous system. Discrete event modelling is based on logical expressions defining the conditions required for events to occur while modelling of a continuous system usually involves the solution of algebraic and differential equations of the behaviour being investigated [6.28]. From the above descriptions about the types of simulation models, it can be concluded that a continuous time-discrete event simulation may be more suitable to be applied to safety analysis than others since safety analysis of a system is usually concerned with discrete state changes.

A Monte Carlo simulation can be used as a continuous time-discrete event simulation involving the use of random variables. Monte Carlo simulations have been used extensively for fault tree and block diagram analyses [6.9]. A Monte Carlo simulation consists of building, usually with a computer program, a probabilistic model of the system under investigation [6.9]. The model is repeatedly run and on the assumption that each simulation run is independent the performance of the synthesised system is recorded. The probability of occurrence of a system failure can then be determined. For example, if 25 of 100 trials for the synthesised system lasted longer than 10000 hr and

75 failed prior to that time, it could be concluded that the probability of occurrence of the system failure at 10000 hr is approximately equal to 0.75. In general, a Monte Carlo simulation is easy to carry out and can be conveniently applied to systems which are too complex or too large to solve by other deterministic methods. Techniques for constructing continuous discrete event simulation models using Monte Carlo techniques will be discussed in detail in this chapter.

6.2.2 **Random Variables**

A simulation of a system or process involving random variables requires a method of generating or obtaining random numbers [6.14]. Examples of random variables which can be modelled by distribution sampling within a simulation model are component repair and failure times, the number of individuals within a given compartment at a given time and the mass of a lifted load.

Given the probability distribution type and the distribution parameters describing the statistical character of a variable, random numbers can be generated to sample instances of the variable from the defined distribution. Depending on the nature of the modelled variable, the sampled probability distribution may be either continuous or discrete. The distribution types can be found in various sources [6.9][6.11][6.14][6.20][6.21]. The typical ones are briefly listed as follows:

Continuous distributions

- Uniform
- Exponential
- Gamma
- Weibull
- Normal
- Lognormal
- Beta
- Triangular

Discrete distributions

- Bernoulli
- Discrete Uniform
- Binomial
- Geometric
- Negative Binomial
- Poisson

Most events can be approximately modelled using the above distributions. For example, compiled statistics of operational data may show that the repair time of a certain type of a component follows a normal distribution with a given mean and a standard deviation and the failure time of a component follows an exponential distribution.

A random variable R with a uniform distribution over the interval [0, 1] is a foundation on which all other distributions can be successfully modelled. Its distribution function is:

$$F_R(x) = P(R < x) = \begin{cases} 0 & x \leq 0 \\ x & 0 < x \leq 1 \\ 1 & x > 1 \end{cases}$$

and the density function is:

$$f_R(x) = \begin{cases} 1 & x \text{ in } [0, 1] \\ 0 & \text{not in } [0, 1] \end{cases}$$

On the basis of a uniform distribution, the following two basic methods of generating a series of random numbers in computer simulation are used:

i. Generation of random numbers.

ii. Generation of pseudo-random numbers.

Real random numbers have proved to be not suitable for computer simulation. Therefore, they are not discussed further.

Pseudo-random numbers, which are transformed to account for the shape and attributes of the desired distribution, are not really random but can be used instead of real random numbers in solving certain problems [6.6][6.11]. The output of a pseudo-random

number generator is always the same for the same input data. Pseudo-random number generators are widely used in computer simulation. The advantages of pseudo-random numbers are described as follows [6.21]:

- *Flexibility:* For a new stochastic (statistical) process only input data needs to be changed, and the random number generator itself doesn't. Once the generator is certified, it can be used with different input data to produce independent random numbers.
- *Ease of computing:* A small number of program statements are sufficient to compute a new pseudo-random number, without additional memory requirements.

Most general purpose programming languages provide procedures for sampling from a uniform distribution to produce pseudo-random numbers, and special purpose simulation languages normally provide procedures for sampling pseudo-random numbers from a wide range of discrete and continuous distribution types (so-called random number generators).

6.2.3 Verification and Validation

Simulation of the safety of a system is conducted on the basis of the system models which describe the system behaviour. When simulation models are constructed, verification and validation programmes are always necessary, yet sometimes they are neglected [6.11].

A verification programme is used to determine whether a simulation model performs as intended. It usually implies debugging the computer program, which can be quite an arduous task for a large-scale simulation model. A validation programme is used to determine whether a simulation model (as opposed to the computer program) is an accurate representation of the real-world system being studied [6.14].

Verification programmes are especially difficult for computer models in which random variables are involved. It must confirm that the logic of the conceptualised model has been correctly implemented in the computer model and this is achieved by the continuous process of testing the coded algorithms and tracing the flow of information within the computer model. Verification programmes can be simplified not only by effectively structured programming practice but also by the use of effective debugging

utilities and the use of strongly typed programming languages in which each of expressions, assignments and parameters is type checked at compilation time for consistency.

The following techniques may be useful in a verification process:

- Write and debug the computer program in modules.
- Have more than one person read the computer program.
- List the states of the simulated system, including the contents of the events, the state variables, etc.
- Run the program under simplifying assumptions for which the true characteristics of the model can be easily observed.
- Display the simulation output on a graphics screen as the simulation actually progresses.

The validation process is as important as the verification process for a system simulation. A validation programme should be of continuous concern throughout the development of a simulation model. All levels of the system should be tested for reasonableness. Omissions of real system elements in the model because of irrelevance or insignificance should also be validated [6.11]. The following three steps may be useful in a validation process:

i. *Develop a rational model.*

   In order to develop such a model, simulation modellers should make use of all available information, including:

   - conversation with expert,
   - existing theory,
   - observation of the system, and
   - common knowledge.

ii. *Check all assumptions and simplifications:*

Since a simulation model of a complex real-world system is always only an approximation, regardless of how much effort is put into developing the model, assumptions and simplifications are always needed. Assumptions and simplifications should be tested during the initial stages of the model development process. When pseudo-random number generators are developed and used to model random variables, statistical tests should be conducted to prove that the randomness and the uniformity of the generated sequences of random numbers are satisfactory. When theoretical distributions are assigned to random variables, goodness-of-fit statistical tests with collected data may need to be conducted to validate such assumptions. Sensitivity analysis should also be carried out to make sure that assumptions and simplifications are properly made.

iii. *Study of simulation output data.*

Simulation output data should be studied to determine if they are reasonable. If a system similar to the one being studied exists, the results of the simulation model of the existing system should be compared with those produced from the simulation model being developed.

Mistakes in a simulation model can be either in programming or in system modelling. The validation process is much easier if the programmer and designer for system modelling are the same person.

6.2.4 Simulation Languages

With respect to the characteristics of system safety simulation, the typical requirements for simulation languages are described as follows:

- Random number generator.
- Features for keeping track of simulation time.
- Dynamic data structures such as queues and stacks.
- Presentation graphics utilities.
- General requirements such as readability, initialisation and error checking.

There are high level languages such as FORTRAN, COBOL, BASIC, PASCAL and C, which can be used to code just about everything. All of them are general-purpose languages but none are particularly suitable for safety simulation.

Safety analysts are mainly users and not computer specialists. Therefore, specialised simulation languages are required in which the developed program contains statements similar to the theoretical concepts of a simulation model. Some advantages of programming a simulation model using a simulation language rather than a general high level language are as follows:

- Simulation languages provide a natural framework in which the model and the program are integrated together, and the verification and validation phases are also merged.
- They provide better error detection because many potential types of error can be checked and identified during compilation.
- They provide most features needed for simulation, resulting in a decrease in programming time which can often be significant.
- Simulation models are easier to change when written using a simulation language.

Generally, two basic approaches, event-scheduling and process-interaction approaches, are used in continuous time-discrete event simulation [6.1]. In the event-scheduling approach, a system is modelled by identifying the characteristic events and then determining a detailed description of changes of state. There is no simulation time recorded during simulation execution. However, in the process-interaction approach, a system is modelled by processes (a time-ordered sequence of events) which delineate everything, as it moves through the corresponding process. In the process-interaction approach, a system may contain many processes interacting with each other at a given time. There is a passage of simulated time for the process-interaction approach. In the simulation models developed in this chapter, the event-scheduling approach is used.

Choosing a general purpose language or a simulation language may depend on the following criteria [6.14]:

- Availability of the language.

- Cost of installing and maintaining the language.
- Number of simulation studies likely to be carried out.
- Types of systems that will be simulated.
- Ease of learning the language.
- Computer storage requirements of the language.
- Computer time efficiency of the language.
- Flexibility and power of the language.

The computer simulation models described in this chapter are written in *MODSIM II*™. The characteristics of this simulation language have been briefly discussed in section 4.4.

6.2.5 Steps in a Continuous Time-discrete Simulation Study

A simulation study is not strictly a sequential process. The proposed steps, that may constitute a typical well-formulated continuous time-discrete event simulation study, and the relationships between them are shown in Figure 6.1. It should be noted that not all simulation studies will necessarily contain all these listed steps and some simulation studies may contain steps that are not depicted in Figure 6.1. The proposed steps are briefly discussed as follows:

i. *Problem formulation:* Every study must begin with a clear statement of the objectives.

ii. *Data collection and system modelling:* Data should be collected on the system of interest and used to estimate input parameters.

iii. *Model validation:* Validation should be carried out through the entire simulation study.

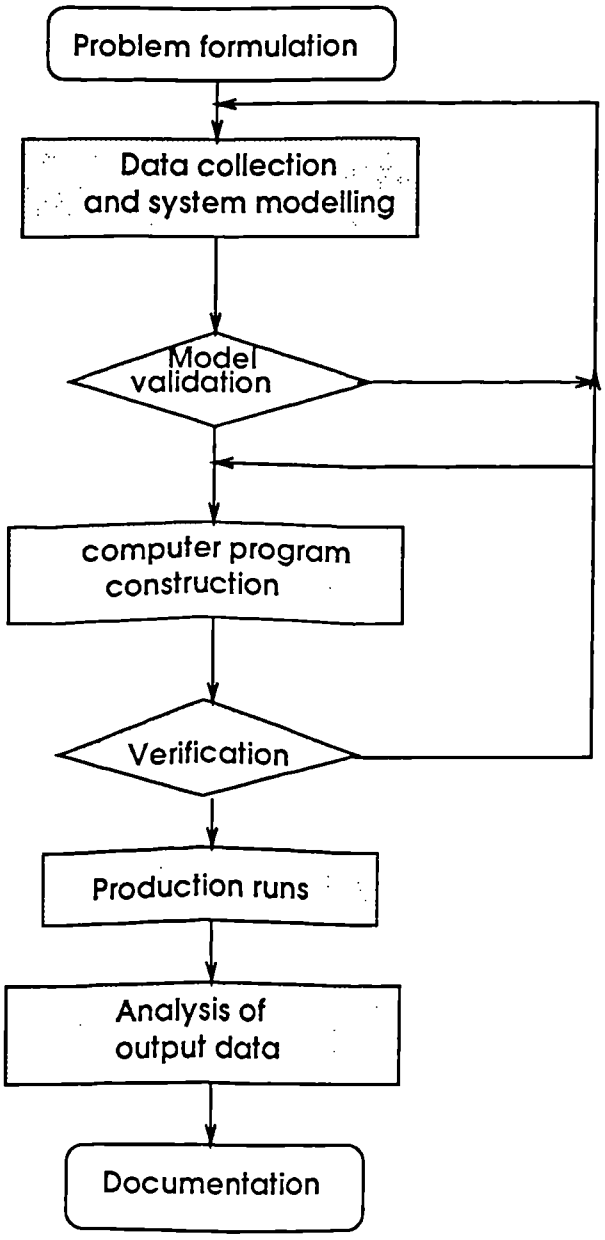


Figure 6.1 Steps in a time-discrete event simulation study

iv *Computer program construction:* The simulation modeller must decide whether to code a model in a general-purpose language or in a specially designed simulation language.

v. *Verification:* Sensitivity study and program verification may be involved.

vi. *Production runs:* Production runs are made to provide the results of the system analysis.

vii. *Analysis of output data:* Output data should be analysed to avoid making serious mistakes leading to fallacious conclusions and ultimately poor decisions.

viii. *Documentation:* It is important to document the assumptions which went into the model as well as the computer program itself.

6.3 Brief Review of Simulation Methods Applied to Safety Analysis

Many simulation models have been developed for safety, reliability and availability analyses, but few have been reported in the literature [6.13]. The characteristics of some typical examples are briefly described as follows:

i. Taha et al [6.24] developed a simulation language (SIMNET) that permits a general safety model to accommodate any system which is described in terms of minimal cut sets. In this simulation model, the algorithms based on minimal cut sets are used to assess system failure events.

ii. Clark et al [6.2] proposed a new simulation technique which combines discrete simulation with fault tree analysis.

iii. Gonzales-Vega et al [6.8] developed a simulation model to analyse logistics policies for complex systems. This model takes into account system configuration, repair facilities, inventory policies and delays for transportation and inspection.

iv. Fritz [6.7] reported a large simulation model which may be used to study system availability and maintenance manpower requirements.

v. Pizzano [6.18] developed a Monte Carlo simulation model in FORTRAN to determine system failures by processing complex logic statements. Any model changes require substantial modification of the FORTRAN code.

vi. Pritsker et al [6.19] developed several simulation models in which design changes require substantial revision of the program code.

vii. Landers et al [6.13] described a simulation model for use in the engineering design process, focusing on mission reliability analysis in which the reliability of a system is simulated on the basis of a given reliability block diagram.

viii. Deans et al [6.3] developed a reliability simulator to predict system performance for the establishment of operational and maintenance policies.

The above simulation models can be grouped as follows:

- Examples [i, ii, iii, iv] illustrate the degree of complexity.
- Examples [v, vi] demonstrate the inflexibility of system-specific models and the limitation of programming languages.
- Examples [vii, viii] illustrate the degree of incomplete description of an engineering system and the degree of independence from other formal safety analysis methods such as FMECA.

Although some existing simulation packages such as MIRIAM, RAMP and @RISK [6.22] can in theory be integrated with the developed methodologies developed in this thesis, it is in practice very difficult to do so since the methodologies developed in this thesis are implemented using MODSIM. Therefore, two simulation models are proposed in this chapter to make the simulation process more straightforward and clearer.

6.4 Proposed System Simulation Models

Simulation can be used together with other formal safety analysis methods. In this chapter, the proposed component/subsystem failure simulation model can make use of the information produced from FMECA, and the proposed simulation model for the prediction of the probability of occurrence of a system failure event is constructed on the basis of the minimal prime implicants obtained using the MBRM.

6.4.1 Assumptions and Simplifications

Assumptions and simplifications are necessary for modelling systems. The following assumptions and simplifications are often used in the construction of simulation models:

- Failed components are repaired same-as-new and the rest of the components are not affected by such repairs.
- All components are same-as-new after a full maintenance activity.
- The failure time and repair time of each component follow some types of distributions.
- Each component may have multiple failure states.
- A system is capable of being maintained.

6.4.2 The Proposed System Availability and Component/subsystem Failure Simulation Model

In the proposed simulation model for the prediction of system availability and failure of each component/subsystem of a system, it is assumed that only failure modes with severity classes 1 and 2, or those described as catastrophic and critical, may cause the system to stop. The failure data for each failure mode of each component/subsystem can be obtained from a FMECA.

Redundancy is considered in this simulation model. Given the Reliability Block Diagram (RBD) of a system being investigated, the components/subsystems can first be labelled by integer numbers. Then, a Redundancy Relationship Matrix (RRM) which describes the state of redundancy of each component/subsystem can be constructed. A RRM is constructed in the following form:

$$RRM = \begin{bmatrix} R_{11} & R_{12} & R_{13} & \cdot & R_{1n} \\ R_{21} & R_{22} & R_{23} & \cdot & R_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ R_{n1} & R_{n2} & R_{n3} & \cdot & R_{nn} \end{bmatrix}$$

If component i is parallel to component k in the system reliability block diagram, R_{ik} and R_{ki} are equal to 1, otherwise equal to 0. The RRM for the reliability block diagram

shown in Figure 6.2 is constructed as follows:

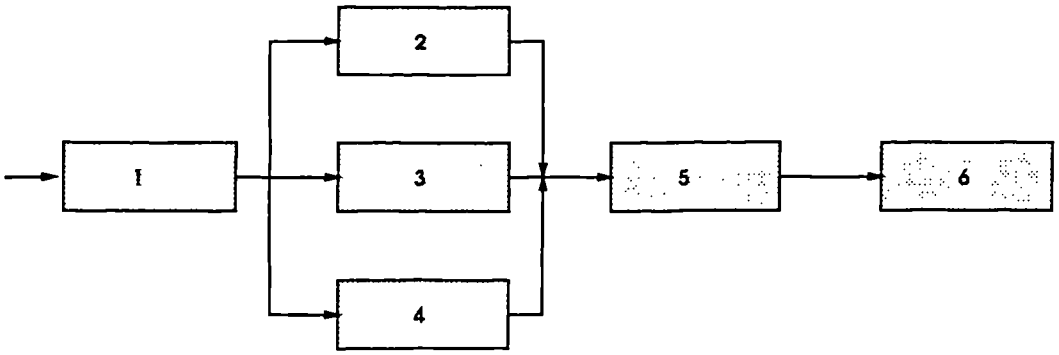


Figure 6.2 A system reliability block diagram

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

RRM provides a way of representing structural redundancy information. After the RRM has been constructed the failure data produced from the FMECA can be utilised to simulate the system availability and to predict failure of each component/subsystem. The diagram of this availability and component/subsystem failure simulation model is shown in Figure 6.3.

Typical model inputs are:

- Failure and repair distributions and associated parameters of components/subsystems.
- Mean Time Between Maintenance (MTBM).
- Redundancy Relationship Matrix (RRM).
- The number of simulation trials required.

Typical model outputs are:

- Number of failures of each component/subsystem.

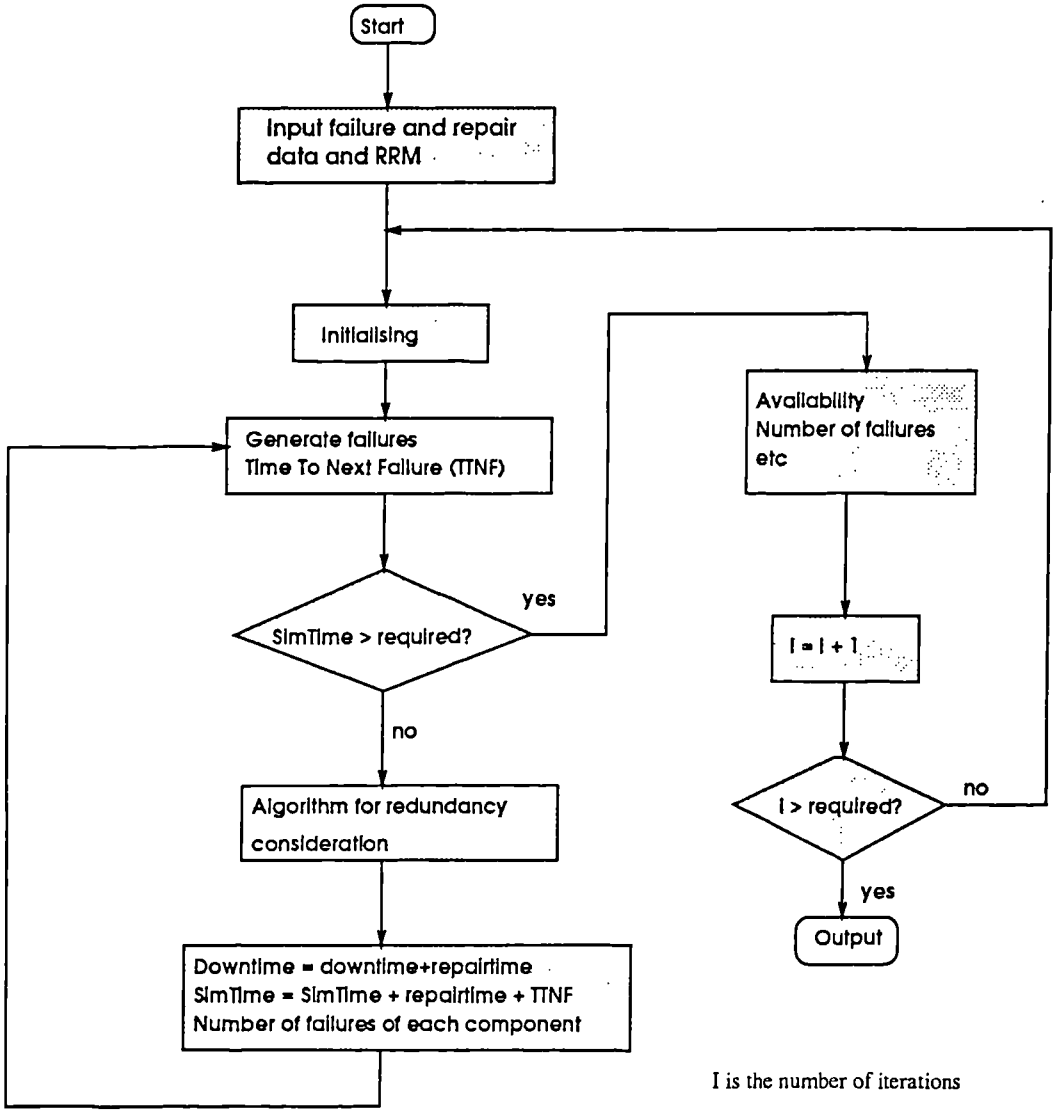


Figure 6.3 The diagram of a proposed system availability and component/subsystem failure simulation model

- System breakdown distribution with MTBM.
- System availability.

6.4.3 The Proposed Simulation Model for the Prediction of the Probability of Occurrence of a System Failure Event

A simulation model is developed as shown in Figure 6.4 to estimate the probability of occurrence of a system top event on the basis of the associated minimum prime implicants. The minimum prime implicants can be obtained using the MBRM [6.27][6.28].

After the final Boolean representation table of a system has been generated using the MBRM, the following steps are necessary for simulating the probability of occurrence of a system top event:

i. Generate failure and repair distributions of the basic events associated with the system top event.

ii. Accumulate component failures in a fixed maintenance process.

iii. Use the algorithms described below to determine the system top event occurrence and prime implicant (cut set) failures.

iv. Repeat above steps.

v. Output results.

A Minimal Cut Set Matrix (MCSM) is a $M \times N$ matrix in which M is the number of lines and N is the number of input columns (attributes) of the minimal cut sets or prime implicants associated with a system top event. If a basic event in column j is associated with a prime implicant in line i, $MCSM_{ij}$ is equal to 1, otherwise $MCSM_{ij}$ is equal to 0. Current Failure State Vector (CFSV) is a $1 \times N$ matrix. If component k fails, $CFSV_k$ is equal to 1, otherwise $CFSV_k$ is equal to 0. Cut set failures and system failures can be determined by comparing CFSV with the row vectors in MCSM. A system top event occurs when the CFSV is not less than a row vector in MCSM, that is, $CFSV_k \geq MCSM_{ik}$ for $k = 1$ to N for any row i ($i = 1, 2, \cdots, M$). The above algorithms for determining the system top event occurrence and cut set failures are shown in Figure 6.5.

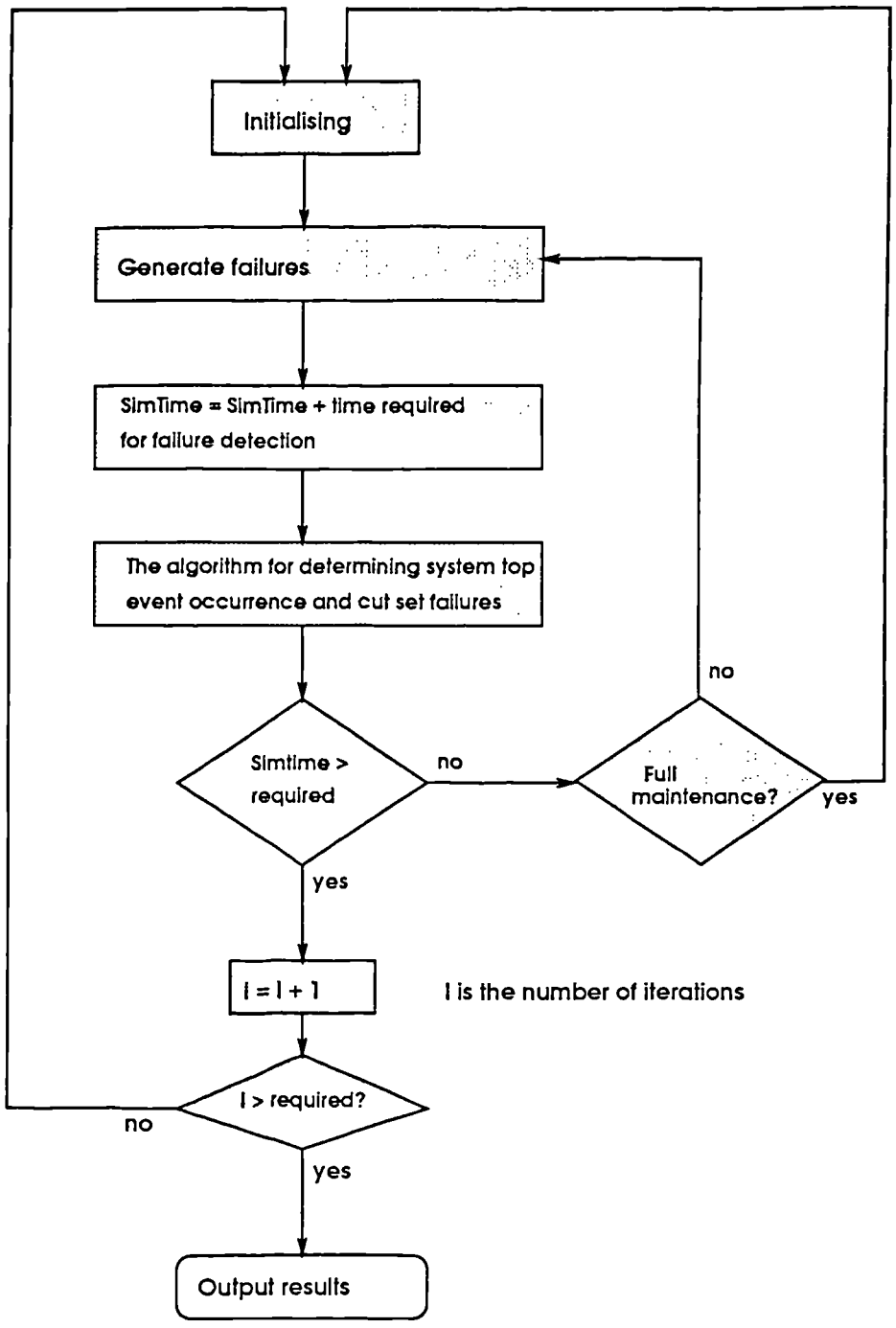


Figure 6.4 The diagram of a simulation model for the prediction of the probability of occurrence of a system top event

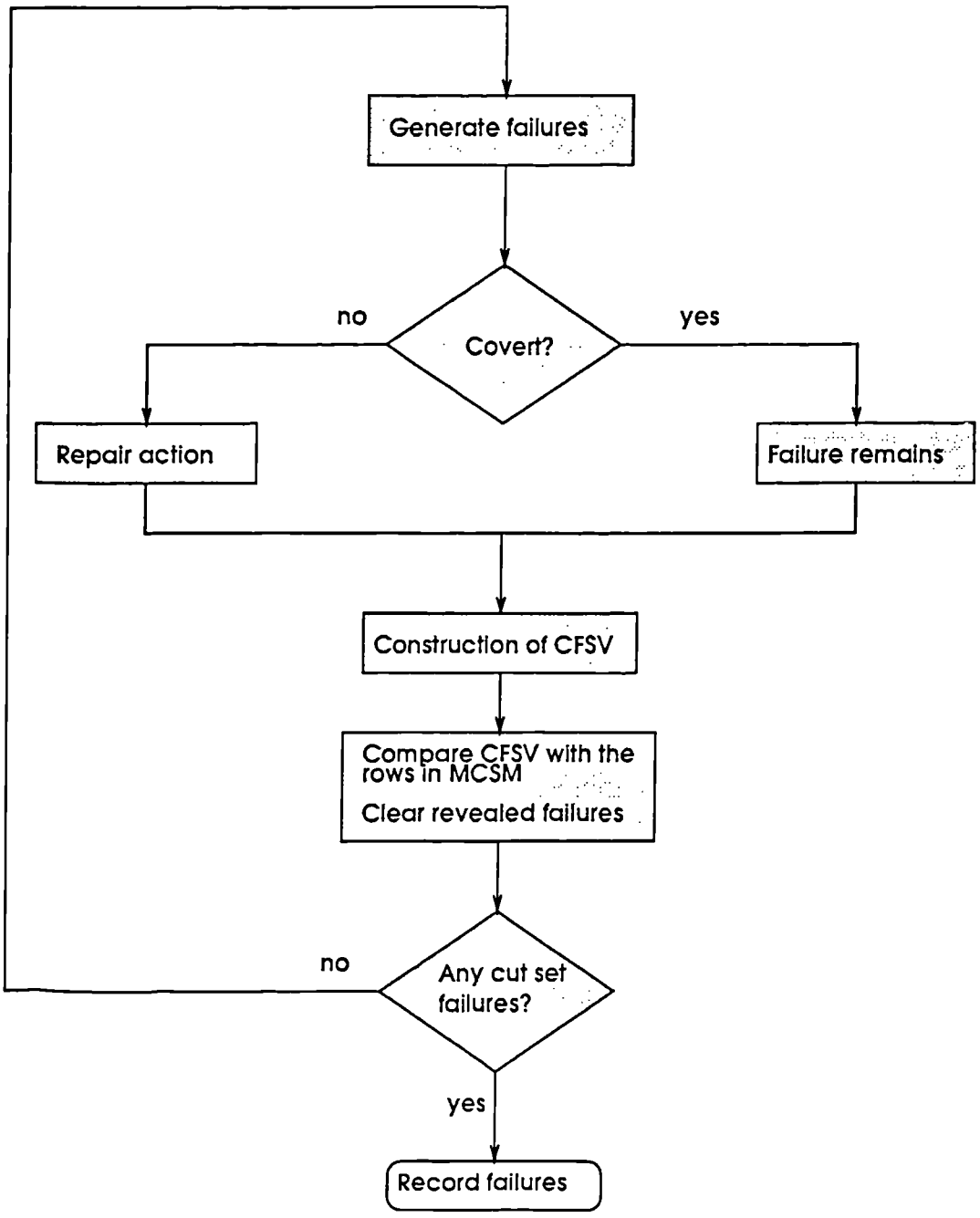


Figure 6.5 The algorithm for determining a system top event occurrence and prime implicant (cut set) failures

In this simulation model, each basic event failure associated with a system top event is assumed to be either revealed or covert [6.28]. Revealed failures are those which can be detected and repaired immediately after they occur. Covert failures are those which cannot be detected until next full maintenance activity takes place. To detect cover failures, it is necessary to carry out periodic maintenances and testing of the system prone to such failures. The ability to detect and remedy covert failures of a system may be vital to the safety of that system.

Typical model inputs are:

- MCSM.
- MTBM.
- Failure and repair distributions and associated parameters of components/subsystems.
- The number of simulation trials.

Typical model outputs are:

- The probability of occurrence of the system top event.
- The probability of occurrence of each associated prime implicant (cut set).

6.4.4 Software

Software has been developed in *MODSIM*^{II} simulation language to simulate system availability, component/subsystem failures and the probabilities of occurrence of a system top event and associated prime implicants (cut sets). The program package which has been developed to obtain the final system Boolean representation table (described in Chapters 4 and 5) has been integrated into this software.

The software has been designed to satisfy the functional requirements of simulation of system availability and component/subsystem failures, and simulation of the probabilities of occurrence of a system top event and associated prime implicants (cut sets). The function of the software is shown in Figure 6.6.

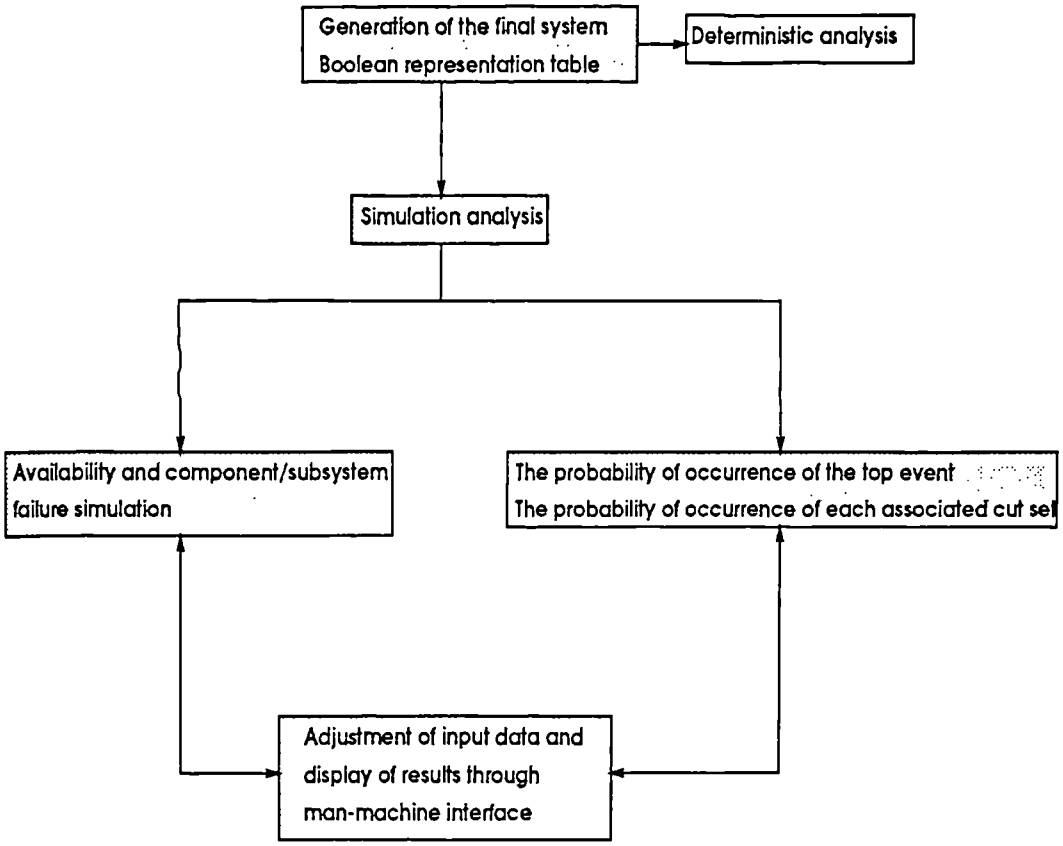


Figure 6.6 The function of the developed simulation models

6.4.5 Discussion

In this chapter, two Monte Carlo simulation models are proposed in a generic sense. Compared with previous work in the literature [6.7][6.8][6.13][6.18][6.19][6.24], the proposed simulation models have the following advantages:

- The models are developed in an Objected-Oriented Programming (OOP) environment. This makes further modification of the software much easier.
- Design change does not require substantial revision of the whole model.
- The models are easily used.

As discussed early in this chapter, the outcomes produced from these two simulation models can be used by designers and operators to assist in the construction of effective maintenance schedules and to optimise design aspects.

6.5 An Illustrative Example

The diagram of a hydraulic hoist transmission system of a marine crane can be found in Figure 4.3 in Chapter 4. The diagram of a hydraulic servo transmission system of the hydraulic hoist transmission system is shown in Figure 6.7.

6.5.1 System Availability and Component/Subsystem Failure Simulation

The system availability and component/subsystem failure simulation can be carried out at either the component level or the subsystem level as required.

Component level

The Reliability Block Diagram (RBD) of the hydraulic servo transmission system is shown in Figure 6.8. The failure modes with severity classes 1 and 2 of the components of the hydraulic servo transmission system, which can be obtained from the FMECA [6.17], are shown in Table 6.1.

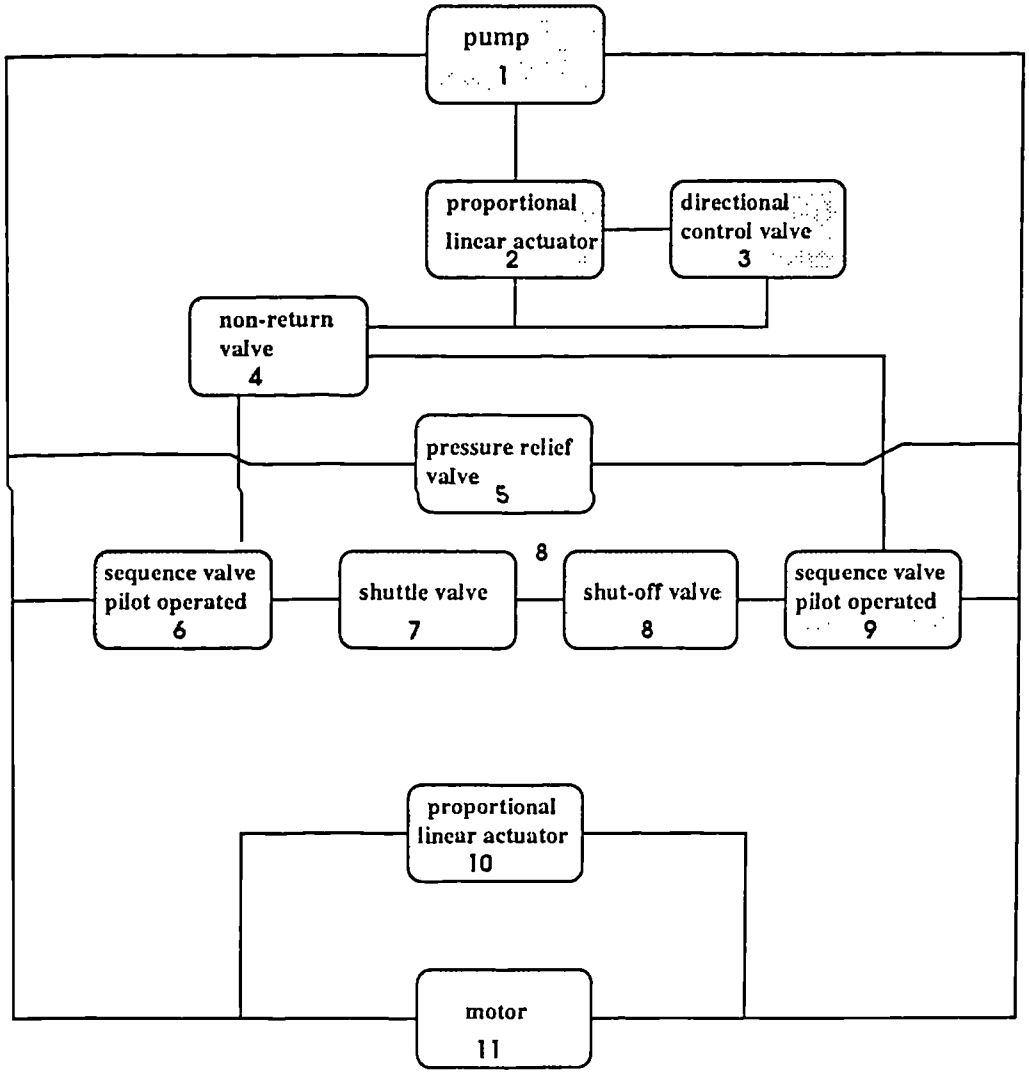


Figure 6.7 The diagram of a hydraulic servo transmission system

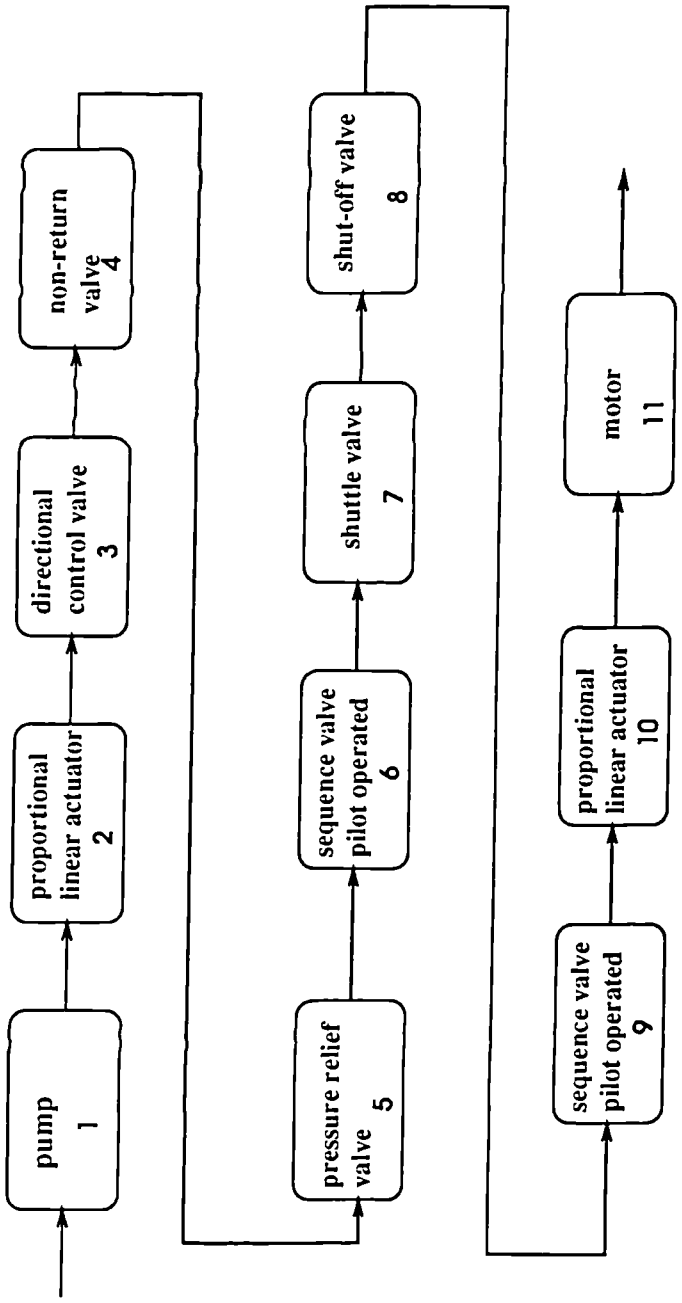


Figure 6.8 The reliability block diagram of the hydraulic servo transmission system

Table 6.1 The failure modes with severity classes 1 and 2

Component	FM No.	Failure modes	Failure rate (per million)	FM rate	Sev.	Det.
1	1	failure to prevent debris to enter circuit	70.00	0.25	2	C
	2	port plate separation causing major leak		0.1	1	C
	3	shaft fails		0.05	1	R
	4	major leak		0.05	1	R
2	1	fails to open	7.00	0.07	1	C
	2	fails to close		0.16	1	C
	3	major leak		0.08	1	R
3	1	fails to switch in accordance with high pressure port	6.00	0.2	1	C
	2	major leak		0.08	1	R
4	1	fails to close	7.00	0.15	1	C
	2	major leak		0.08	1	R
5	1	fails to open	7.00	0.08	1	C
	2	major leak		0.08	1	R
6	1	major leak	7.00	0.08	1	R
7	1	fails to close	7.00	0.15	1	C
	2	major leak		0.08	1	R
8	1	fails to close	7.00	0.16	1	C
9	1	major leak	10.00	0.04	1	R
10	1	fails to open	3.00	0.05	2	C
	2	fails to close		0.24	1	C
	3	major leak		0.07	1	R
11	1	failure to cause debris to enter circuit	70.00	0.25	2	C
	2	port plate separation causing short circuit		0.1	1	C
	3	shaft fails		0.05	1	R
	4	major leak		0.05	1	R

R - Revealed C - Covert Sev. - Severe class Det. - Fault detectability
FM - Failure Mode

If each component repair activity is assumed to follow a normal distribution with the expected value μ = 35 hr and the standard deviation σ = 10 hr, the availability of the hydraulic servo transmission system and the number of failures of each component for a time period of 10000 hr with MTBM = 10000 hours are simulated as shown in

Tables 6.2 and 6.3, respectively.

Table 6.2 Availability

Failure hours	Availability
75	99.25%

Table 6.3 The number of failures of each component

The number of	failures of component	1	0.71980
The number of	failures of component	2	0.04980
The number of	failures of component	3	0.03760
The number of	failures of component	4	0.03840
The number of	failures of component	5	0.02340
The number of	failures of component	6	0.01200
The number of	failures of component	7	0.03880
The number of	failures of component	8	0.02480
The number of	failures of component	9	0.05420
The number of	failures of component	10	0.02600
The number of	failures of component	11	0.72680

Subsystem level

The Reliability Block Diagram (RBD) of the hydraulic hoist transmission system is shown in Figure 6.9. The FMECA can be progressed up to the subsystem level based on the information produced at the component level [6.31]. The failure modes with severity classes 1 and 2 for the sub-systems of the hydraulic hoist transmission system (Figure 4.3) can be obtained from section 4.5.1 and are shown in Table 6.4.

If each subsystem repair activity is assumed to follow a normal distribution with the expected value μ = 45 hr and the standard deviation σ = 10 hr, the availability of the hydraulic hoist transmission system and the number of failures of each subsystem for a time period of 10000 hr with MTBM = 10000 hr are obtained as shown in Tables 6.5 and 6.6, respectively.

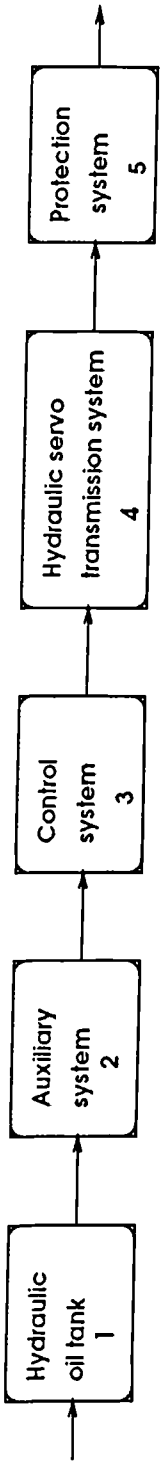


Figure 6.9 The reliability block diagram of a hydraulic hoisting transmission system

Table 6.4 **The failure modes with severity class 1 and 2**

Sub-systems	FM No.	Failure mode	Failure rate (per million)	FM rate	Sev.	Det.
Control system	1	major leak	35.9	0.015	2	R
	2	control output for "lower" motion cannot be closed when required		0.155	1	C
	3	control output for "hoist up" motion cannot be closed when required		0.155	1	C
Protection system	1	fails to return for hoisting up when de-energised	92.3	0.066	1	R
	2	major leak		0.046	1	R
	3	failure of emergency stop		0.066	1	C
	4	failure of "hoisting down" limit		0.066	1	C&R
	5	failure of slack rope prevention		0.066	1	C&R
	6	low boost pressure switch fails to open		0.028	1	C&R
Hydraulic servo system	1	major leak	265	0.094	1	R
	2	shaft fails		0.013	1	C&R
	3	no output from the package motor		0.311	1	C&R
	4	hydraulic short circuit		0.026	1	C&R
	5	pipe burst		0.008	1	R
Hydraulic oil tank	1	no output	70.0	0.043	1	C&R
Auxiliary	—	—	—	—	—	—

R - Revealed C - Covert Sev. - Severe class Det. - Fault detectability
FM - Failure Mode

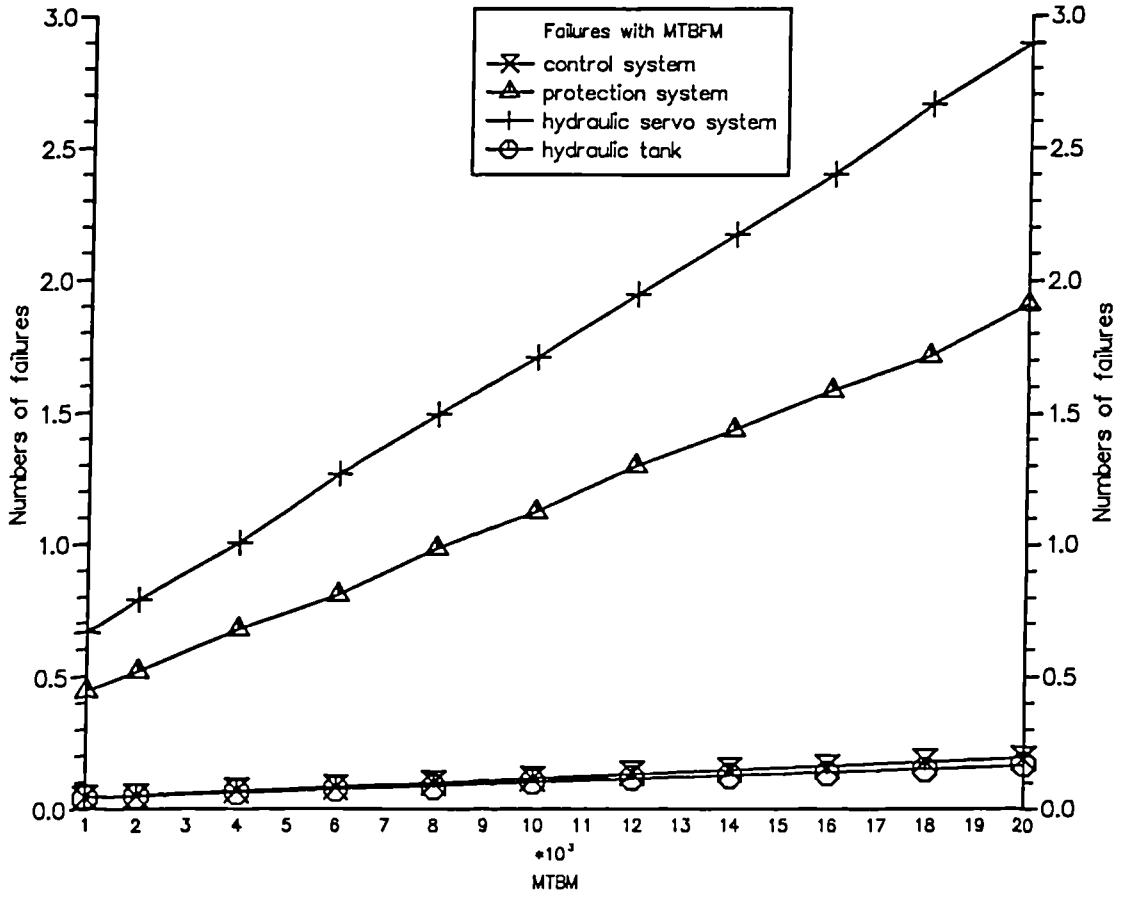


Figure 6.10 Subsystem failure distributions with MTBM

Table 6.5 Availability

Failure hours	Availability
129	99.12%

Table 6.6 The number of failures of each subsystem

Subsystems	Number of failures
Control system	0.11340
Protection system	1.12440
Hydraulic servo system	1.70920
Hydraulic oil tank	0.10240

The failure distributions of the subsystems with MTBM are also produced using this simulation model and shown in Table 6.7 and Figure 6.10, respectively.

Table 6.7 The failure distribution of each subsystem with MTBM

MTBM (hr)	Subsystems	Number of failures	MTBM (hr)	Subsystems	Number of failures
1000	control	$f1 = 0.0428$	2000	control	$f1 = 0.0504$
	protection	$f2 = 0.4474$		protection	$f2 = 0.5188$
	servo	$f3 = 0.6656$		servo	$f3 = 0.7922$
	tank	$f4 = 0.0398$		tank	$f4 = 0.05$
4000	control	$f1 = 0.07$	6000	control	$f1 = 0.0824$
	protection	$f2 = 0.6758$		protection	$f2 = 0.8078$
	servo	$f3 = 1.0054$		servo	$f3 = 1.2692$
	tank	$f4 = 0.0644$		tank	$f4 = 0.0774$
8000	control	$f1 = 0.099$	10000	control	$f1 = 0.1134$
	protection	$f2 = 0.9858$		protection	$f2 = 1.1244$
	servo	$f3 = 1.4958$		servo	$f3 = 1.7092$
	tank	$f4 = 0.0846$		tank	$f4 = 0.1024$

Table 6.7 The failure distribution of each subsystem with MTBM (Continued)

MTBM (hr)	Subsystems	Number of failures	MTBM (hr)	Subsystems	Number of failures
12000	control	$f1 = 0.1364$	14000	control	$f1 = 0.148$
	protection	$f2 = 1.3004$		protection	$f2 = 1.4398$
	servo	$f3 = 1.9486$		servo	$f3 = 2.1734$
	tank	$f4 = 0.1188$		tank	$f4 = 0.1278$
16000	control	$f1 = 0.161$	18000	control	$f1 = 0.182$
	protection	$f2 = 1.5866$		protection	$f2 = 1.7176$
	servo	$f3 = 2.4022$		servo	$f3 = 2.6664$
	tank	$f4 = 0.1356$		tank	$f4 = 0.1492$
20000	control	$f1 = 0.1916$	30000	control	$f1 = 0.261$
	protection	$f2 = 1.9128$		protection	$f2 = 2.6186$
	servo	$f3 = 2.8956$		servo	$f3 = 4.05$
	tank	$f4 = 0.1684$		tank	$f4 = 0.2312$

6.5.2 Simulation of the Probabilities of Occurrence of System Top Events

The probabilities of occurrence of the top events S_1, S_2 and S_3 (described in Chapter 4) of the hydraulic hoist transmission system for a time period of 10000 hr with MTBM = 10000 hr are simulated as shown in Table 6.8.

The probabilities of occurrence of the top events S_1, S_2 and S_3 of the hydraulic hoist transmission system for various MTBM values are also studied. The results are shown in Table 6.9 and Figure 6.11, respectively.

Table 6.8 Probabilities of occurrence of S_1, S_2 and S_3

Top events	Probability of occurrence (%)
S_1	0.0803
S_2	0.0140
S_3	0.0366

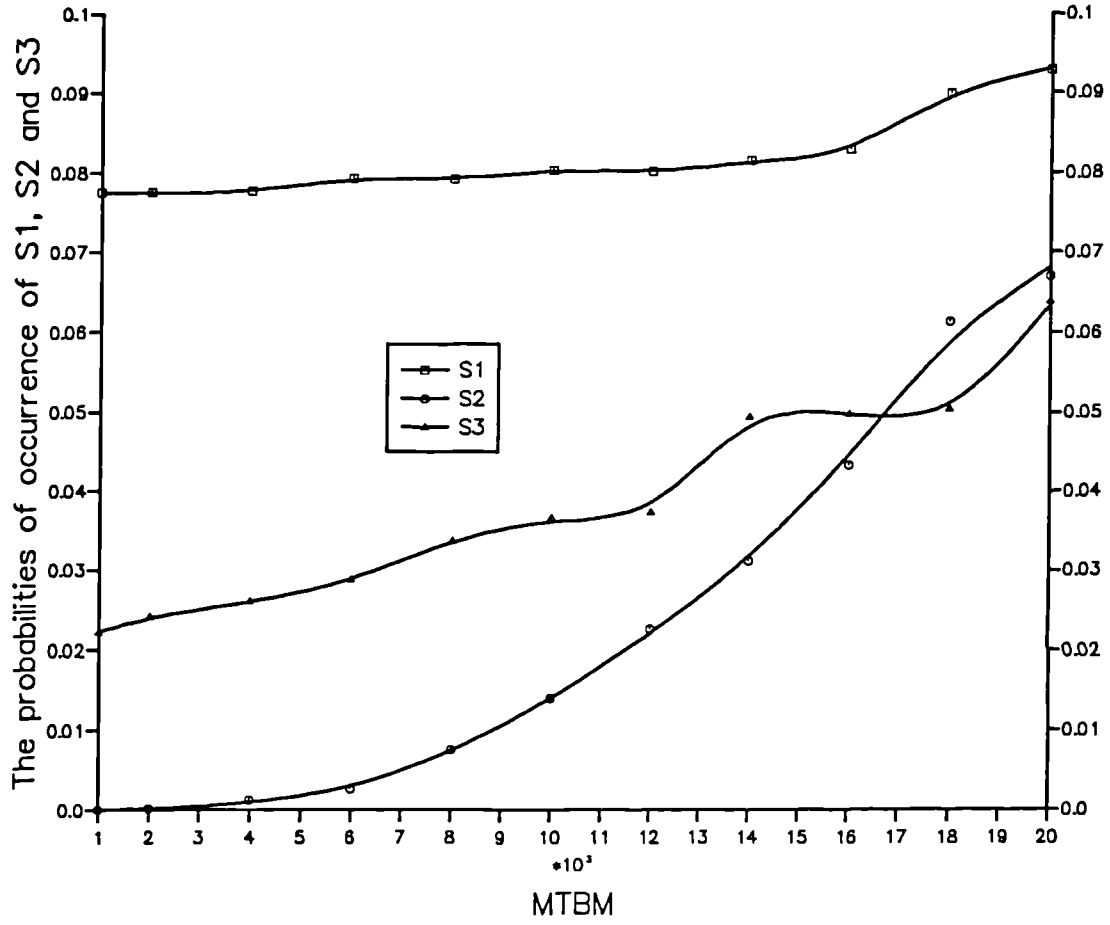


Figure 6.11 The probabilities of occurrence of the top events

Table 6.9 The probabilities of occurrence of the top events S_1, S_2 and S_3

MTBM (hr)	Probability of occurrence of S_1(%)	Probability of occurrence of S_2(%)	Probability of occurrence of S_3(%)
1000	0.0775	0.0001	0.0222
2000	0.0775	0.0002	0.0250
4000	0.0776	0.0012	0.0275
6000	0.0792	0.0026	0.0288
8000	0.0792	0.0075	0.0336
10000	0.0803	0.0140	0.0366
12000	0.0810	0.0227	0.0374
14000	0.0815	0.0312	0.0494
16000	0.0830	0.0433	0.0498
18000	0.0899	0.0514	0.0504
20000	0.0929	0.0670	0.0638

From Figure 6.11, it can be noted that in some sections the probability distributions of occurrence of top event S_1 and S_3 increase very slowly as MTBM increases. It implies that in these sections the probability distributions of occurrence of top event S_1 and S_3 are not significantly affected by MTBM. This is because in these sections the probabilities of occurrence of the basic events associated with the minimal cut sets leading to top event S_3 are not significantly affected by MTBM. For example, this phenomenon produces waviness in the curve of top event S_3.

The information produced above can be used in the "design for safety" process. As will be demonstrated in Chapter 8, the information obtained above can be utilised in techno-economic modelling and decision making.

6.6 Concluding Remarks

There is no doubt that computer simulation techniques can play a very important role in the development of safety prediction and management methods. A major problem is in the development of the appropriate modelling methods which are necessary to obtain simple and flexible models, to which simulation techniques could be easily and effectively applied. If such a problem is satisfactorily solved, simulation analysis would enable the safety of complex engineering systems to be predicted effectively and

efficiently.

This chapter has attempted to demonstrate how the prediction of the safety of engineering systems can be made on the basis of the results obtained using various formal safety analysis methods such as FMECA and the MBRM. Many problems remain to be solved in the application and integration of simulation techniques with established formal safety prediction methodologies. To contribute to the solution of these problems further work will be required in the following areas:

- Construction of a methodology for the systematic development of computer simulation models.
- Design of an integrated environment where simulation models may interact and share system information with other formal safety assessment procedures.
- Construction of explicit safety criteria with respect to life, the environment and material losses, and methodical techno-economic analysis approaches for satisfying those criteria.

REFERENCES - CHAPTER 6

[6.1] CACI Products Company, *MODSIM II™: The Language for Object-Oriented Programming (OOP) and SIMGRAPHICS II™, Reference Manual,* La Jolla, USA, May 1991.

[6.2] Clark B., Lewis K. J., Aldwinckle D. S., *Simulation in marine design and operation,* RINA Transactions, London, 1985, 145-160.

[6.3] Deans N., Miller A. J., *System reliability simulation,* IEE Conference on Simulators, Brighton, 1983.

[6.4] *Department of Energy, The public inquiry into the Piper Alpha disaster,* (Cullen Report), HMSO, ISBN 0 10 113102, 1990.

[6.5] Dragoljub S., *Basic technical systems simulation,* Butterworths & Co. Ltd, 1978.

[6.6] Fishman G, *Principles of discrete event simulation,* John Wiley & Sons, NY, USA, 1978.

[6.7] Fritz S. J., *T-46A availability model,* HQ AFOTEC/LG4A, Kirtland AFB, New Mexico, USA, Jan. 1988.

[6.8] Gonzales-Vega O., Foster J. W., Hogg G. L., *A simulation programme to model effects of logistics on R & M of complex systems,* Proc. Ann. Reliability and Maintainability Symp., Los Angeles, CA, USA, 1988.

[6.9] Henley E. J., Kumamoto H., *Probabilistic risk assessment,* IEEE Press, New York, 1992.

[6.10] Kolmberg K., Folkeson A., *Operational reliability and systematic maintenance,* Elsevier Science Publishers Ltd, England, 1991.

[6.11] Hoover S., Perry R., *Simulation, a problem-solving approach,* Addison-Wesley Publishing Company, USA, 1989.

[6.12] Labrie C., *Design for safety: design methodology,* Engineering Design Centre, University of Newcastle upon Tyne, EDCN/SAFE/RESC/12/1, May 1992, 28 pages.

[6.13] Landers T. L., Taha H. A., King C. L., *A reliability simulation approach for use in the design process,* IEEE Transactions on Reliability, Vol.40, No.2, NJ, USA, June 1991.

[6.14] Law A.M., Kelton W.D., *Simulation modelling and analysis,* McGraw-Hill Book Company, 1982.

[6.15] MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* Military Standard, Naval Ship Engineering Center, Washington D.C..

[6.16] Mitrani I., *Simulation techniques for discrete event systems,* Cambridge University Press, U.K., 1982.

[6.17] NEL, *FMECA of NEI pedestal crane,* Report No. NECL/01, Glasgow, UK, May 1987.

[6.18] Pizzano F., *Reliability and maintenance simulation of the Hubble space telescope,* Proc. Ann. Reliability Maintainability Symp., Las Vegas, USA, 1986.

[6.19] Pritsker A. A. B., Sigal C. E., *Management decision making: a network simulation approach,* Prentice-Hall, 1983.

[6.20] Rubinstein R., *Simulation and the Monte Carlo method,* John Wiley & Sons, NY, USA, 1981.

[6.21] Savic D., *Basic technical systems simulation,* Butterworths Basic series, 1989.

[6.22] Smith D. J., *Reliability, maintainability and risk,* 4th ed., Butterworths-Heinemann Ltd, 1992.

[6.23] Tang A., Ang W., *Probability concepts in engineering planning and design,* John Wiley & Sons, NY, USA, 1984.

[6.24] Taha H. A., Nuno P., *A SIMNET simulation model for estimating system reliability,* Proc. 11th Ann. Conf. Computers & Industrial Engineering, 1989.

[6.25] Teleb B., Miller A. J., Deans N. D., *Design of a hardware reliability simulator for complex systems,* IEE Conference on Simulators, Coventry, UK, 1986.

[6.26] Vinogradov O., *Introduction to mechanical reliability: a designer's approach,* Hemisphere Publishing Corporation, USA, 1991.

[6.27] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Design Conference, Chicago, March 1993, 1-12.

[6.28] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Third International Conference on Maritime Communications and Control, Marine Management (Holding) Ltd, London, 7-8 July 1993, 1/2-10/2.

[6.29] Wang J., Yang. J. B., Sen P., *Techno-economic modelling for design and maintenance optimisation based on safety analysis,* Submitted March 1994 to Quality and Reliability Engineering International, (Research Report, EDCN/SAFE/RESC/19/1, Engineering Design Centre, February 1994).

[6.30] Wu T. K., Kim S. S., *Modelling system simulation-based mechanical system's reliability study,* Institute of Marine Engineers, Transactions (C), Vol.105, Marine Management (Holdings) LTD, 1993, 21-34.

[6.31] Yannoutsos P., *Implementation of reliability engineering in the marine field - physics of exhaust valves failure due to high temperature corrosion,* Ph.D Thesis, Department of Marine Technology, University of Newcastle upon Tyne, November 1989.

CHAPTER 7

Safety Analysis and Synthesis Using Fuzzy Sets and Evidential Reasoning

SUMMARY

As described in Chapter 3, great uncertainty is involved in safety analysis of large MTO products. Problems of uncertainty can be treated using two principal types of method involving probability and possibility. The safety analysis methods described in Chapters 4 and 6 can be be classified as the probabilistic type since in such methods probability distributions are used to describe basic failure events. The probabilistic type of method has been extensively used in various industrial projects. However, in some cases, this type of method may prove not suitable since it could be very difficult to precisely determine the parameters of probability distributions of failure events. However, the other type of the method, the one involving possibility, may prove to be comparatively more suitable. Possibility safety analysis often involves the use of fuzzy set modelling and subjective reasoning.

This chapter presents a new methodology for safety analysis and synthesis of a complex engineering system with a structure that is capable of being decomposed into a hierarchy of levels. In this methodology, fuzzy set theory is used to describe each failure event and an evidential reasoning approach is then employed to synthesise the information produced to assess the safety of the whole system. Three basic paramenters

— failure likelihood, consequence severity and failure consequence probability are used to analyse a failure event. These three parameters are described by linguistic variables which are characterised by membership functions to a set of defined categories. The fuzzy safety score of the failure event is initially defined by the parameters and characterised by a membership function to the defined categories. As safety can also be clearly described by linguistic variables referred to as the safety expressions, the obtained fuzzy safety score can be mapped back to the safety expressions which are characterised by membership functions over the same categories. This mapping results in the identification of the safety of each failure event in terms of the degree to which the fuzzy safety score belongs to each of the safety expressions. Such degrees represent the uncertainty in safety evaluations and can be synthesised using an evidential reasoning approach so that the safety of the whole system can be evaluated in terms of these safety expressions. Finally, an example is presented to demonstrate the proposed safety analysis and synthesis methodology.

7.1 Introduction

As described in Chapter 3, the safety of a large engineering system is affected by many factors regarding its design, manufacturing, installation, commissioning, operation and maintenance. Consequently, it may be extremely difficult, if not impossible, to construct an accurate and complete mathematical model for the system in order to assess the safety because of inadequate knowledge about the basic failure events. This leads inevitably to problems of uncertainty in representation.

Problems of uncertainty in safety analysis can be treated using two principal types of method involving probability and possibility, respectively. Probability theory deals with uncertainty which is essentially random in nature but of an ordered kind. Possibility theory studies problems which are not really probabilistic but cause uncertainty due to imprecision associated with the complexity of a system as well as vagueness of human judgement. Possibility theory often uses fuzzy sets and approximate reasoning.

Traditionally, safety analysis is carried out on a probabilistic basis. As described in Chapters 4 and 6, probability distributions are used to describe basic failure events and to deal with uncertainty in order to evaluate potential hazards and assess system safety. In many cases, however, it may be difficult or even impossible to precisely determine the parameters of a probability distribution for a given event due to lack of evidence or

due to the inability of the safety engineer to make firm assessments. Therefore, one may have to describe a given event in terms of vague and imprecise descriptors like "*Likely*" or "*Impossible*", terms that are commonly used by safety analysts, Such judgements are obviously fuzzy and hence fuzzy set modelling may be more appropriate to analyse the safety of systems with incomplete information of the kind described above.

It is not surprising, therefore, that the possible applications of subjective reasoning and fuzzy set theory in safety analysis have been widely discussed. A few of these may be briefly outlined as follows:

i. *Bayesian modelling with imprecise prior probabilities [7.5].* An extension of the standard Bayesian approach based on the theory of imprecise probabilities and intervals of measures is developed to reflect expert opinions using prior distributions. The opinions of several experts can be combined using the approach developed.

ii. *Modelling of risk using approximate reasoning and fuzzy sets [7.9].* Linguistic variables are used to assess the risk of an event.

iii. *Identification of hazardous events using fuzzy set theory [7.10][7.11].* A survey of the possible applications of fuzzy logic is carried out with respect to the analysis of hazardous events.

iv. *Application of fuzzy sets and possibility theory for risk analysis and decision making [7.1].* Subjective linguistic assignments are modelled for risk analysis using fuzzy set theory.

v. *Use of fuzzy set theory for uncertainty analysis [7.4].* The potential applicability of fuzzy set theory to uncertainty analysis of accident progression event trees with imprecise and uncertain branch probabilities and/or with a number of phenomenological uncertainty issues is examined as a possible alternative procedure to that used in the current probabilistic risk assessments.

Example (i) suffers from the numerical stability problems involved in Bayesian modelling, as indicated in [6]. Examples (ii), (iii) and (iv) mainly focus on safety assessment of a single failure event, and are not concerned either with safety synthesis of many events at a single level or with safety synthesis at different levels (component

level, subsystem level and system level). Example (v) causes the loss of safety information due to the use of min-max operations in the process of safety synthesis. Such information loss could be rather serious in safety analysis of large and complex engineering systems.

The safety of a system is determined by the constituent subsystems and the safety of each subsystem is, in turn, determined by the associated components and their possible failure modes. Figure 7.1 shows a diagram of a framework for safety analysis of an engineering system. Safety analysis of an engineering system using subjective reasoning and fuzzy set modelling should be carried out by taking into account such an evaluation hierarchy. However, the existing work briefly described above mainly focuses on safety assessment of a single failure event, and is not concerned neither with safety synthesis of many events at a single level nor safety synthesis at different levels (the component level, the subsystem level and the system level).

In a hierarchical structure, it is usually the case that safety analysis at a high level makes use of the information produced at lower levels. There is therefore a need to develop a framework for hierarchical system safety analysis. Such a framework could be established by developing an approach using fuzzy set modelling and approximate reasoning in an integrated manner, and it is largely the aim of this chapter to present such an approach.

In Figure 7.1, a failure mode at the bottom level can be initially analysed and described using fuzzy sets. The fuzzy safety score of the failure mode can thus be obtained. On the other hand, a set of linguistic variables may be used to express various safety levels. Such linguistic variables may be referred to as safety expressions, which can also be described using fuzzy sets. The obtained fuzzy safety description of the failure mode could then be mapped back to the defined safety expressions using the so-called Best-Fit method [7.14]. In the mapping, each of the safety expressions may be confirmed to some extent, depending upon the obtained fuzzy safety description of the failure mode as well as the defined fuzzy descriptions of the safety expressions. The degree of confirmation to a safety expression representing a safety level could then be viewed as a degree of confidence with which the safety associated with a failure mode is evaluated to the given safety level. Such uncertainty can conveniently be handled using an evidential reasoning approach, which has been developed on the basis of the Dempster-Shafer theory to deal with hierarchical evaluation problems with uncertainty [7.18][7.19][7.20][7.22].

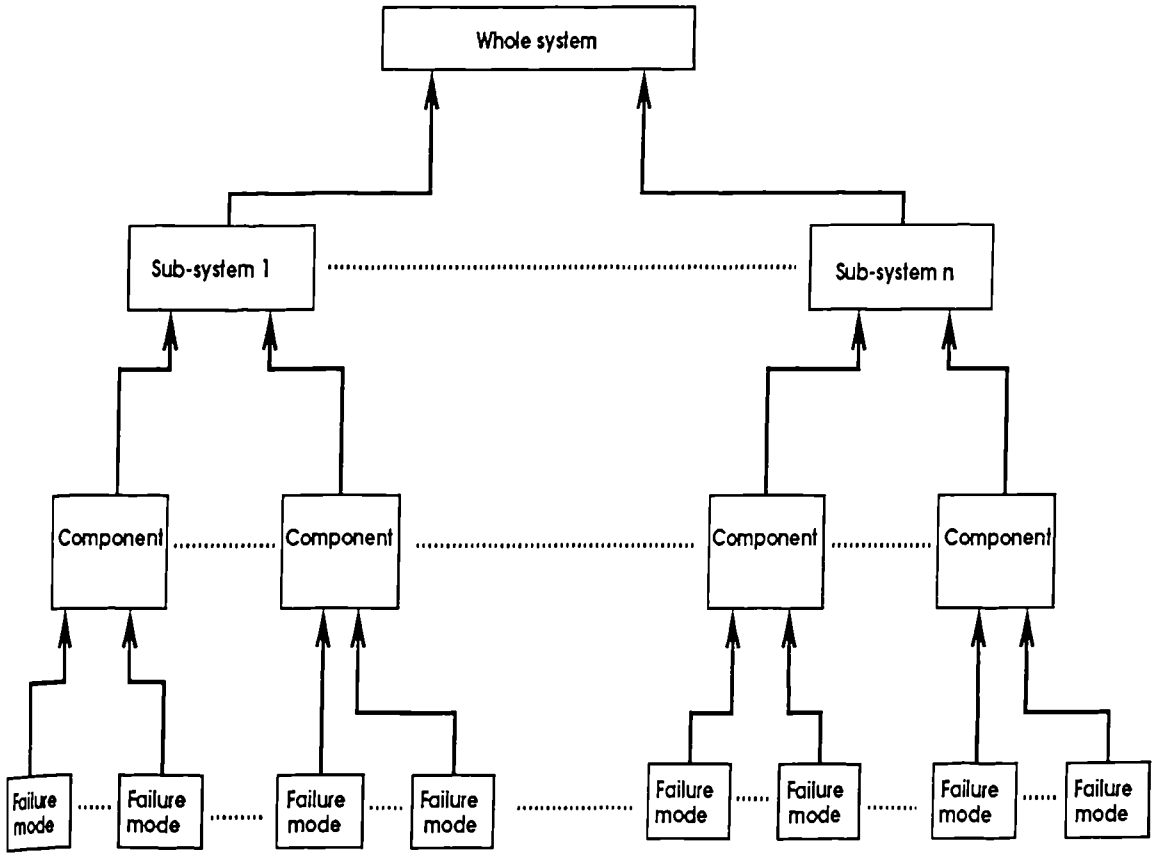


Figure 7.1 The diagram of a safety analysis for an engineering system

In this way, the safety associated with all failure modes can be evaluated with respect to the safety levels defined. Then, these uncertain evaluations of the failure modes associated with a component can be combined to produce an evaluation of the safety of the component using the evidential reasoning algorithm. Similarly, the uncertain evaluations for the components of a subsystem can be synthesised to evaluate subsystem safety. The safety of the whole system can finally be assessed by synthesising the safety information of the subsystems.

In this chapter, the proposed methodology combines safety modelling of failure modes at the bottom level using fuzzy set theory and safety assessment of the whole system using the evidential reasoning approach.

7.2 System Modelling for Safety Analysis and Synthesis

Section 7.1 has examined how an engineering system may be composed of several sub-systems which can be further broken down to the component level. In probabilistic safety analysis, the safety of a system is assessed by analysing each of its constituent components. For example, such an analysis could be carried out by identifying the following information for each component using FMECA [7.16].

i. Failure likelihood of occurrence of each identified failure mode.

ii. Possible consequences described by *catastrophic*, *critical*, *marginal*, or *negligible*.

iii. Failure consequence probability defining the likelihood that the failure consequences of the identified failure mode will occur, given that the failure mode has taken place.

As described in Chapter 3, given the above information, all criticality numbers of a component under all severity classes can be obtained and a criticality matrix can be constructed to show the distributions of criticality of component failure modes and to provide a tool for assigning priorities for corrective action.

From the above, it can be seen that there are three basic parameters (failure likelihood, consequence severity and failure consequence probability) which are used in assessing the safety associated with each failure mode of a component. The safety level associated with a particular failure mode is determined by these three parameters and the product of these three parameter values is called "safety score" [7.7][7.5] if

consequence severity can be described numerically. Safety scores are often used in the judgement of safety where a high safety score represents poor safety and a low safety score represents good safety. The safety score of a component is the sum of the safety scores of its failure modes and the safety score of a system can be synthesised by similarly processing the information produced for each of its components.

In the probabilistic method discussed above, it is implicitly assumed that the consequence severity of a failure mode is described by linguistic variables, and the failure likelihood and the failure consequence probability are assumed to take numerical values. However, the failure likelihood and the failure consequence probability are affected by so many factors in real life that, in some cases, it may be difficult to define them precisely in numerical terms as the probabilities may often be made on the basis of subjective judgements. Such subjective judgements are especially meaningful when one deals with non-numerical data. In fact, it has sometimes been argued that although human beings find quantitative prediction of safety difficult they may be comparatively efficient at qualitative assessments using linguistic variables [7.14]. To describe the likelihood of occurrence of a failure mode, for example, one may often use linguistic variables such as *"Highly frequent"*, *"Frequent"*, *"Reasonably frequent"*, *"Average"*, *"Reasonably low"*, *"Low"* and *"Very low"*. To describe a failure consequence probability, linguistic variables such as *"Definite"*, *"Highly likely"*, *"Reasonably likely"*, *"Likely"*, *"Reasonably unlikely"*, *"Unlikely"* and *"Highly unlikely"* may be used.

It may also be noted that in the above discussion it is assumed that the consequence severity, the failure likelihood or the failure consequence probability of a failure mode only belongs to one of the linguistic descriptions used to describe the respective extent. For instance, the consequence severity of a failure mode only belongs to one of the four severity classes — *"Catastrophic"*, *"Critical"*, *"Marginal"* and *"Negligible"*. However, such a description may at times be inadequate. For example, the consequence severity of a failure mode may be something between *"Catastrophic"* and *"Critical"* or even between *"Catastrophic"* and *"Negligible"*.

Fuzzy set theory is well suited to model such subjective linguistic variables. In fuzzy set theory, linguistic variables used in describing failure likelihood, consequence severity and failure consequence probability can be characterised by their membership functions to a set of categories which describe the degrees of failure likelihood, severity class and failure consequence probability and which are usually graduated from low to high. For instance, if $U = \{1, 2, 3, \cdots n\text{-}1, n\}$ represents a set of categories, the

linguistic variables "*Catastrophic*", "*Very low*" and "*Highly likely*" may be modelled by:

"*Catastrophic*" = {1/0, $\cdots$, n-3/0, n-2/0, n-1/0.75, n/1.0}

"*Very low*" = {1/1.0, 2/0.75, 3/0, 4/0, $\cdots$, n/0}

"*Highly likely*" = {1/0, $\cdots$, n-4/0, n-3/0, n-2/0.75, n-1/1.0, n/0.25}

where the integers in the numerators of each term within the brackets represent the categories and the real numbers in the denominators stand for the membership degrees.

The membership values for the components in U belonging to each of the linguistic variables "*Catastrophic*", "*Very low*" and "*Highly likely*" can thus be denoted as follows:

$\mu_{Catastrophic} = (0, \cdots, 0, 0.75, 1.0)$

$\mu_{Very\ low} = (1.0, 0.75, 0, \cdots, 0)$

$\mu_{Highly\ likely} = (0, \cdots, 0, 0.75, 1.0, 0.25)$

The fuzzy safety score of a failure mode of a component can be estimated by the product of the fuzzy descriptions of the corresponding failure likelihood, consequence severity and failure consequence probability. If L, C and E represent the fuzzy sets of the failure likelihood, consequence severity and failure consequence probability of a failure mode, the fuzzy safety score S can be defined as follows using fuzzy set manipulation [7.14]:

$$S = C \circ E \times L$$

$$\mu_S = \mu_{C \circ E \times L} = (\mu_S^1, \cdots, \mu_S^j, \cdots)$$

where symbol "o" represents composition operation and "×" Cartesian product operation in fuzzy set theory as will be stated later.

μ_S is the description function of safety score S in terms of membership degrees μ_S^j (j = 1, 2, $\cdots$, n) representing the extent to which S belongs to element j in U. Each element in μ_S can be obtained using the max-min method as will be shown in the next section. It should be pointed out that the fuzzy safety score of a failure mode obtained using this method is the maximal possible one because of characteristics of Cartesian and composition rules.

In the above, S represents a fuzzy description for the safety score of a failure mode while the relevant fuzziness is described by μ_S. To express the safety of the failure mode in a clear way, linguistic variables such as *"Poor"*, *"Average"*, *"Good"* and *"Excellent"* may be used. For instance, it may be quite clear to state that the safety of a failure mode is to a large extent *"Good"*. Such linguistic variables may be referred to as safety expressions. The safety expressions may also be characterised by membership degrees to each element in U so that the fuzzy safety score of the failure mode could be identified in terms of these expressions. For instance, *"Poor"* could be defined as follows:

$$\text{"Poor"} = \{1/0, \cdots, n\text{-}2/0, n\text{-}1/0.75, n/1.0\}$$

Such a definition needs to be consistent with the ones for other linguistic variables. Thus, if a failure mode occurs *"Highly frequently"* and if it may cause *"Definite"* failure effect classified to be *"Catastrophic"*, then the safety of the failure mode should be *"Poor"*.

When fuzzy descriptions of the failure modes of each component have been evaluated in terms of the safety expressions, it is desirable, as shown in Figure 7.1, to synthesise them to assess the safety for each component, then for each subsystem if necessary, and finally for the system being investigated. A novel synthesis approach is therefore required for such a hierarchical evaluation propagation without any loss of useful information generated for each failure mode of each component. The evidential reasoning approach is one such method which is capable of combining uncertain evaluations at a single level and implementing hierarchical propagation of such evaluations between different levels.

Following a brief introduction of fuzzy operations, the rest of this chapter will present how to describe, evaluate and identify the safety associated with a failure mode of a component. Then, the evidential reasoning approach will be employed to synthesise assessments of safety for each component and the system.

7.3 Safety Analysis Using Fuzzy Sets

7.3.1 Fuzzy Operations

Let U be a set and A and B subsets of U where $U = \{u_1, u_2, \cdots, u_n\}$. Suppose the membership values for the elements in U belonging to the subsets A and B are denoted

by $\mu_A = (\mu_A^1, \mu_A^2, \cdots, \mu_A^n)$ and $\mu_B = (\mu_B^1, \mu_B^2, \cdots, \mu_B^n)$, respectively. Then, some typical fuzzy operations such as union, intersection, complement, Cartesian product and composition of fuzzy sets are described as follows:

i. Complement. Complement of A is defined by:

$$\mu_{\bar{A}} = (\mu_{\bar{A}}^j)_{1\times n}$$

where $\mu_{\bar{A}}^j = 1 - \mu_A^j$, j = 1, 2, $\cdots$, n.

ii. Intersection. Intersection of A and B is defined by:

$$\mu_{A\cap B} = (\mu_{A\cap B}^j)_{1\times n}$$

where $\mu_{A\cap B}^j = \min(\mu_A^j, \mu_B^j)$, j = 1, 2, $\cdots$, n.

iii. Union. Union of A and B is defined by:

$$\mu_{A\cup B} = (\mu_{A\cup B}^j)_{1\times n}$$

where $\mu_{A\cup B}^j = \max(\mu_A^j, \mu_B^j)$, j = 1, 2, $\cdots$, n.

iv. Cartesian product. Cartesian product of A and B is defined by:

$$\mu_{A\times B} = (\mu_{A\times B}^{ij})_{n\times n}$$

where $\mu_{A\times B}^{ij} = \min(\mu_A^i, \mu_B^j)$. For example, if μ_A = (1, 0.5, 0.1, 0, 0, 0, 0) and μ_B = (0, 0, 0, 0, 0.1, 0.5, 1), then

$$\mu_{A\times B} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0.1 & 0.5 & 1 \\ 0 & 0 & 0 & 0 & 0.1 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 & 0.1 & 0.1 & 0.1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

v. Composition. Given the membership functions for set C and for the Cartesian product of sets A and B, the composition of them is denoted by:

$$\mu_{C\circ A\times B} = (\mu_{C\circ A\times B}^j)_{1\times n}$$

where $\mu_{C\circ A\times B}^j = \max(\min(\mu_C^1, \mu_{A\times B}^{1j}), \cdots, \min(\mu_C^n, \mu_{A\times B}^{nj}))$, j = 1, 2, $\cdots$, n. Suppose μ_C = (1, 0.5, 0.1, 0, 0, 0, 0). $\mu_{C\circ A\times B}^j$ can be calculated as follows using the max-min method.

$$\mu_{C \circ A \times B} = (0, 0, 0, 0, 0.1, 0.5, 1)$$

where, for example, $\mu^6_{C \circ A \times B}$ = max(min(1, 0.5), min(0.5, 0.5), min(0.1, 0.1), min(0, 0), min(0, 0), min(0, 0), min(0, 0)) = 0.5.

7.3.2 Fuzzy Safety Description

As discussed early in this chapter, linguistic variables can be used to describe failure likelihood, consequence severity and failure consequence probability. A linguistic variable may then be characterised by a membership function to a set of categories with regard to the particular condition. It is often recommended that the number of categories be restricted to no more than seven in order to remain within the practical bounds of human discrimination [7.5]. The use of categorical judgements has been quite successful in many practical situations [7.3][7.14]. It is usually convenient for engineers to use categories to articulate safety information. The typical linguistic variables for failure likelihood, consequence severity and failure consequence probability of a failure event may be defined and characterised as shown in Tables 7.1, 7.2 and 7.3. From Tables 7.1, 7.2 and 7.3, it can be noted that the membership values for each linguistic variable are asymmetric. This is because the conditions for the definition of the safety expressions, as will be described in section 7.3.3, need to be satisfied. It is obviously possible to have some flexibility in the definition of membership functions to suit different situations.

Table 7.1 **Failure likelihood**

μ_L	Categories						
Linguistic variables:	1	2	3	4	5	6	7
Highly frequent:	0	0	0	0	0	0.75	1
Frequent:	0	0	0	0	0.75	1	0.25
Reasonably frequent:	0	0	0	0.75	1	0.25	0
Average:	0	0	0.5	1	0.5	0	0
Reasonably low:	0	0.25	1	0.75	0	0	0
Low:	0.25	1	0.75	0	0	0	0
Very low:	1	0.75	0	0	0	0	0

Table 7.2 **Consequence severity**

μ_C	Categories						
Linguistic variables:	1	2	3	4	5	6	7
Catastrophic:	0	0	0	0	0	0.75	1
Critical:	0	0	0	0.75	1	0.25	0
Marginal:	0	0.25	1	0.75	0	0	0
Negligible:	1	0.75	0	0	0	0	0

Table 7.3 **Failure consequence probability**

μ_E	Categories						
Linguistic variables:	1	2	3	4	5	6	7
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
Likely:	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
Highly unlikely:	1	0.75	0	0	0	0	0

From above fuzzy descriptions of failure likelihood, consequence severity and failure consequence probability, it may be observed that the linguistic variables are not exclusive, so that the sum of the membership degrees for the linguistic variables belonging to a category may be greater than 1. For example, the sum of the elements in column 1 of Table 7.1 is 1.25. This is because there are intersections among the defined linguistic variables describing failure likelihood, consequence severity and failure consequence probability. Inclusive expressions may make it more convenient for the safety analyst to judge a failure mode.

Given a failure mode i, the failure likelihood, consequence severity and failure consequence probability, denoted by L_i, C_i and E_i, respectively, may be characterised by their membership functions with respect to the seven categories. Such membership functions need to be assigned by safety analysts with reference to the above three tables.

The safety score S_i of the ith failure mode of a component can be expressed by $S_i = C_i \circ E_i \times L_i$. The membership function of S_i is thus described by $\mu_{S_i} = \mu_{C_i \circ E_i \times L_i}$

7.3.3 **Fuzzy Safety Evaluation**

The safety score S_i characterised by μ_{S_i} provides a fuzzy description of the safety of the ith failure mode of a component. However, the safety may be expressed more clearly in terms of linguistic variables. For instance, it is commonly understood that the safety of a failure mode of a component can be expressed by degrees to which it belongs to such linguistic variables as "*Poor*", "*Average*", "*Good*", and "*Excellent*". Each of these linguistic variables may be referred to as a safety expression. To evaluate S_i in terms of these linguistic variables, it is necessary to characterise them using membership values with respect to the seven categories defined. These safety expressions need to be defined to be exclusive for each category. The reasons for doing so are stated as follows:

i. Exclusive expressions can more clearly represent safety than inclusive ones although it may be slightly more difficult for the safety analyst to make direct judgement using the former.

ii. It makes it easier for the obtained fuzzy safety score to be mapped back to one (or all) of the defined exclusive safety expressions.

iii. It facilitates the implementation of the evidential reasoning approach to synthesise the safety of a large complex system.

The extent to which each safety expression belongs to each of the seven categories is defined by a membership value. The sum of membership values for each expression with respect to the seven categories is assigned to be the same. The purpose of doing so is to make a rational projection of the obtained fuzzy safety score description back to the defined safety expressions. In addition, following conditions also need to be satisfied to confine the safety expression space within the certain extent:

i. $S_{Poor} = C_{Catastrophic} \circ E_{Definite} \times L_{Highly\ frequent}$

ii. $S_{Average} = C_{Critical} \circ E_{Reasonably\ likely} \times L_{Reasonably\ frequent}$

iii. $S_{Good} = C_{Marginal} \circ E_{Reasonably\ unlikely} \times L_{Reasonably\ low}$

iv. $S_{Excellent} = C_{Negligible} \circ E_{Highly\ unlikely} \times L_{Very\ low}$

The above equations are commonly understood in the design process. For example, if the likelihood of occurrence of a failure mode is *highly frequent* and its occurrence will *definitely* result in *catastrophic* consequences, the safety of the failure mode should be considered to be *poor*. The aim of having the above equations is to confine the safety expressions to a certain extent. Considering the above requirements, the four safety expressions are defined, on the basis of Tables 7.1, 7.2 and 7.3, as shown in Table 7.4.

Table 7.4 **Safety expressions**

μ_{S_i}	Categories						
Linguistic variables:	1	2	3	4	5	6	7
1. Poor:	0	0	0	0	0	0.75	1
2. Average:	0	0	0	0.5	1	0.25	0
3. Good:	0	0.25	1	0.5	0	0	0
4. Excellent:	1	0.75	0	0	0	0	0

The four defined safety expressions in Table 7.4 have the following characteristics:

i. "*Poor*" is described only by the membership values with regard to categories 6 and 7.

ii. "*Excellent*" is described only by the membership values with regard to categories 1 and 2.

iii. The membership functions of "*Good*" and "*Average*" are not symmetric with respect to categories 3 and 5, respectively, and actually they lay slightly more weight on category 4.

7.3.4 Safety Identification

Using the Best-Fit method [7.14], the obtained fuzzy safety score description S_i of failure mode i of a component can be mapped back to one (or all) of the defined safety expressions (i.e., "*Excellent*", "*Good*", "*Average*" and "*Poor*"). 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 instance, the distance between the obtained fuzzy safety score description S_i and the expression "*Poor*" is defined as follows:

$$d_{i1}(S_i, Poor) = (\sum_{j=1}^{7} (\mu_{S_i}^j - \mu_{Poor}^j)^2)^{\frac{1}{2}}$$

Similarly, we can define:

$$d_{i2}(S_i, Average) = (\sum_{j=1}^{7} (\mu_{S_i}^j - \mu_{Average}^j)^2)^{\frac{1}{2}}$$

$$d_{i3}(S_i, Good) = (\sum_{j=1}^{7} (\mu_{S_i}^j - \mu_{Good}^j)^2)^{\frac{1}{2}}$$

$$d_{i4}(S_i, Excellent) = (\sum_{j=1}^{7} (\mu_{S_i}^j - \mu_{Excellent}^j)^2)^{\frac{1}{2}}$$

It should be pointed out that each d_{ij} (j = 1, 2, 3, 4) is an unscaled distance. The closer S_i is to the jth expression, the smaller d_{ij} is. More specially, d_{ij} is equal to zero if S_i is just the same as the jth expression in terms of the membership functions. In such a case, S_i should not be evaluated to other expressions at all due to the exclusiveness of these expressions. To embody such features, new indices need to be defined based on d_{ij} (j = 1, 2, 3, 4).

Suppose d_{iJ} ($1 \le J \le 4$) is the smallest among the obtained distances for S_i and let α_{i1}, α_{i2}, α_{i3} and α_{i4} represent the reciprocals of the relative distances between the identified fuzzy safety description S_i and each of the defined safety expressions with reference to d_{iJ}. Then, α_{ij} (j = 1, 2, 3, 4) can be defined as follows:

$$\alpha_{ij} = \frac{1}{d_{ij}/d_{iJ}} \qquad j=1, 2, 3, 4$$

If d_{iJ} = 0 it follows that α_{iJ} is equal to 1 and the others are equal to 0. Then, α_{ij} (j = 1, 2, 3, 4) can be normalised by:

$$\beta_{ij} = \frac{\alpha_{ij}}{\sum_{m=1}^{4} \alpha_{im}} \qquad j=1, 2, 3, 4.$$

Each β_{ij} (j = 1, 2, 3, 4) represents the extent to which S_i belongs to the jth defined safety expression. It can be noted that if S_i completely belongs to the jth expression then β_{ij} is equal to 1 and the others are equal to 0. The sum of values of these indices for S_i is equal to 1, that is, $\sum_{j=1}^{n} \beta_{ij} = 1$. Thus β_{ij} could be viewed as a degree of confidence that S_i belongs to the jth safety expression.

The following example shows the developed method for the obtained safety score description to be mapped back to the defined safety expressions. Suppose μ_{S_i} = (0, 0, 0, 0, 0.1, 0.5, 1). Then, d_{ij} and α_{ij}, (j = 1, 2, 3, 4) can be calculated by:

$$d_{i1} = \sqrt{0^2 + 0^2 + 0^2 + 0^2 + 0.1^2 + 0.25^2 + 0^2} = 0.269,$$

$d_{i2} = 1.457$, $d_{i3} = 1.604$, $d_{i4} = 1.680$ and

$\alpha_{i1} = 1.000$, $\alpha_{i2} = 0.185$, $\alpha_{i3} = 0.168$, $\alpha_{i4} = 0.160$

β_{i1}, β_{i2}, β_{i3} and β_{i4} can then be calculated by:

$\beta_{i1} = 0.661$, $\beta_{i2} = 0.122$, $\beta_{i3} = 0.111$, $\beta_{i4} = 0.106$

Thus, S_i is identified to belong to "*Poor*" with a confidence level of 66.1 percent, to "*Average*" with 12.2 percent, to "*Good*" with 11.1 percent and to "*Excellent*" with 10.6 percent. Such an evaluation may be summerised by the following expectation:

$$S(s_i) = \{(0.661, \text{"}Poor\text{"}), (0.122, \text{"}Average\text{"}), (0.111, \text{"}Good\text{"}), (0.106, \text{"}Excellent\text{"})\}$$

7.4 Synthesis of Safety Evaluation by Hierarchical Evidential Reasoning

7.4.1 Evidential Reasoning Scheme

As discussed above, the safety of a component is determined by the associated failure modes. If a component only has one failure mode whose safety is absolutely evaluated as "*Good*", then the safety of the component will be "*Good*". Generally, a component may have several failure modes. If the safety levels associated with the failure modes are all absolutely evaluated as "*Good*", then the safety of the component should also be "*Good*". However, such certain and consistent evaluations can hardly be expected in real life safety analysis. Problems may then arise as to how uncertain and inconsistent evaluations of safety analysis of all the failure modes of a component may be synthesised in a rational way so as to attain an (often uncertain) evaluation of the safety of the component. The problems may be generalised as one of determining how the safety of a system with a hierarchy as shown in Figure 7.1 could be evaluated. As argued before, a hierarchical evaluation process may be expected to provide a reasonable way of dealing with such problems [7.18][7.19][7.20][7.22].

This evaluation process is based on the Dempster-Shafer (simply D-S) theory which is well suited for handling incomplete assessment of uncertainty. The D-S theory can model the narrowing of the hypothesis set with the accumulation of evidence. In other words, it will become more likely that a given hypothesis is true if more pieces of evidence support that hypothesis. In Figure 7.1, whether the safety of a component is "*Excellent*", "*Good*", "*Average*" or "*Poor*" would be regarded as a hypothesis. The obtained safety evaluation of a failure mode may be viewed as a single piece of evidence. If the safety associated with a failure mode is to a certain extent evaluated as "*Good*", then the safety of the associated component would be to some degree "*Good*". The hierarchical evaluation process provides a systematic way of synthesising such uncertain safety evaluations of multiple failure modes to produce an evaluation for a component.

To apply the D-S theory, the mutual exclusiveness and exhaustiveness of all hypotheses have to be satisfied. It is therefore necessary that all the linguistic variables for expression of system safety be defined as distinct grades. In other words, if one of the variables is absolutely confirmed, all the others must not be confirmed at all; if more than one variable is confirmed simultaneously, the total degree of confidence must be one or smaller than one. The linguistic variables defined in section 7.3.3 satisfy the requirements of exclusiveness and exhaustiveness. This enables us to employ the evidential reasoning algorithm developed to synthesise the uncertain safety evaluations generated for failure modes using fuzzy sets.

7.4.2 Algorithm

Suppose H represents a set of linguistic variables for safety expressions and H_j the jth linguistic variable such as "*Good*". Then, H is defined by:

$$H = \{H_1, \cdots, H_j, \cdots, H_N\}$$

where N is the number of the linguistic variables defined. In section 7.3.3, for example, H is defined by:

$$H = \{Poor, \quad Average, \quad Good, \quad Excellent\}$$

Suppose there are L_k failure modes associated with the kth component. Let e_{ki} denote failure mode i associated with component k, denoted by c_k. The set of the failure

modes for the component can then be defined by:

$$E_k = \{e_{k1}, \cdots, e_{ki}, \cdots, e_{kL_k}\}$$

Let λ_{ki} be the normalised relative weight of failure mode i in evaluation of the safety of component k where $0 \le \lambda_{ki} \le 1$. The way of assigning λ_{ki} can be found in [7.18][7.20] and will be outlined in the next section. Suppose $m_{ki}^j = m(H_j/e_{ki})$ $(m_{ki}^j \le 1)$ is a real number, referred to as a basic probability assignment, which represents a degree to which the obtained safety evaluation of the ith failure mode supports a hypothesis that the safety of the kth component is confirmed to H_j. Then, m_{ki}^j may be obtained as follows:

$$m_{ki}^j = \lambda_{ki}\beta_{ij}$$

where β_{ij} is given with respect to the kth component, as discussed in section 7.3.4.

As $0 \le \lambda_{ki} \le 1$ and $\sum_{j=1}^{N}\beta_{ij} = 1$, then $\sum_{j=1}^{N} m_{ki}^j \le 1$. Suppose $m_{ki}^H = m(H/e_{ki})$ is the basic probability assignment to H, which is the remaining belief unassigned after commitment of belief to all H_j $(j=1, \cdots, N)$, that is, $m_{ki}^H = 1 - \sum_{j=1}^{N} m_{ki}^j$. A basic probability assignment matrix $M(c_k/E_k)$ for evaluation of the safety of the component c_k through the associated failure modes E_k may then be formulated by:

$$M(c_k/E_k) = \begin{bmatrix} m_{k1}^1 & \cdots & m_{k1}^j & \cdots & m_{k1}^N & m_{k1}^H \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ m_{ki}^1 & \cdots & m_{ki}^j & \cdots & m_{ki}^N & m_{ki}^H \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ m_{kL_k}^1 & \cdots & m_{kL_k}^j & \cdots & m_{kL_k}^N & m_{kL_k}^H \end{bmatrix} \begin{matrix} \{e_{k1}\} \\ \cdots \\ \{e_{ki}\} \\ \cdots \\ \{e_{kL_k}\} \end{matrix}$$

Suppose m_{ck}^j is a degree of confidence to which the safety of the kth component is evaluated to H_j. Then, m_{ck}^j can be obtained by synthesising the basic probability assignments as listed in $M(c_k/E_k)$ using the evidential reasoning algorithm as described below.

Suppose Ψ is a subset of H. Define a subset $e_{I_k(i)}$ of E_k and a combined probability assignment $m_{I_k(i)}^{\Psi}$ as follows:

$$e_{I_k(i)} = \{e_{k1} \cdots e_{ki}\},\ 1 \le i \le L_k; \qquad m^{\Psi}_{I_k(i)} = m(\Psi/e_{I_k(i)})$$

where $m(\Psi/e_{I_k(i)})$ is a combined probability assignment to Ψ confirmed by $e_{I_k(i)}$. Then, the algorithm can be stated as follows:

$$\{H_j\}:\ m^j_{I_k(i+1)} = K_{I_k(i+1)}(m^j_{I_k(i)}m^j_{k,i+1} + m^j_{I_k(i)}m^H_{k,i+1} + m^H_{I_k(i)}m^j_{k,i+1}),\ j=1, \cdots, N$$

$$\{H\}:\ m^H_{I_k(i+1)} = K_{I_k(i+1)}m^H_{I_k(i)}m^H_{k,i+1}$$

$$K_{I_k(i+1)} = \left[1 - \sum_{\tau=1}^{N}\sum_{\substack{j=1 \\ j\neq\tau}}^{N} m^{\tau}_{I_k(i)}m^j_{k,i+1}\right]^{-1}$$

$$i=1, \cdots, L_k-1$$

7.4.3 Hierarchical Propagation

It can be proven from the algorithm that $m^{\Psi}_{I_k(L_k)}$ is the overall probability assignment to $\Psi\ (\subseteq H)$ confirmed by E_k and $m^{\Psi}_{I_k(L_k)} = 0$ for any $\Psi \subseteq H$ other than $\Psi = H_j\ (j=1, \cdots, N)$ and H [7.18], or

$$m^j_{ck} = m(H_j/E_k) = m^{j}{}_{I_k(L_k)},\quad j = 1, \cdots, N, \text{ and } m^H_{ck} = m(H/E_k) = m^H_{I_k(L_k)}$$

$$m(\Psi/E_k) = m^{\Psi}_{I_k(L_k)} = 0 \text{ for } any\ \Psi \subseteq H\ but\ \Psi \neq H_j\ (j=1, \cdots, N) \text{ and } H$$

Consequently, the safety of the kth component can be evaluated in terms of the safety expressions defined in H by the following expectation:

$$S(c_k) = \{(m^j_{ck},\ H_j),\ j=1, \cdots, N\}$$

that is, the kth component is evaluated to H_j with a degree of confidence of m^j_{ck}, $j=1, \cdots, N$. Such an evaluation is generated by synthesising the given safety evaluations of the relevant failure modes.

In a similar way, the safety evaluation of each component could be obtained. A further problem is then to produce an evaluation on the safety of a subsystem which is composed of several components. Suppose there are L_l components associated with the lth subsystem. The set of the components in subsystem l is defined by:

$$F_l = \{c_{l1}, \cdots, c_{lk}, \cdots, c_{lL_l}\}$$

At this stage, the safety evaluations of components have been generated. So, the fact that the safety of the kth component is confirmed to H_j to an extent of m_{ck}^j $(j=1, \cdots, N)$ could be viewed as a piece of evidence while the safety of the lth subsystem may be assumed to be evaluated to any of H_j $(j=1, \cdots, N)$. Suppose m_{sl}^j is a degree of confidence that the safety of the lth subsystem is confirmed to H_j. The problem then becomes how to obtain m_{sl}^j from m_{ck}^j $(j=1, \cdots, N;\ k=1, \cdots, L_l)$. This problem can be solved in the same way as described in the last subsection if c_{lk} is treated as e_{ka}, m_{ck}^j as β_{ij} and m_{sl}^j as m_{ek}^j.

The safety of the lth subsystem can then be evaluated by:

$$S(s_l) = \{(m_{sl}^j,\ H_j),\ j=1, \cdots, N\}$$

Let m^j be a degree of confidence to which the safety of the whole system is confirmed to H_j. Then, m^j can be obtained from m_{sl}^j $(j = 1, 2, \cdots, N;\ l = 1, 2, \cdots, S_l$ where S_l is the number of the subsystems) using the evidential reasoning algorithm. The safety of the whole system can thus be evaluated by:

$$S(s) = \{(m^j,\ H_j),\ j=1, \cdots, N\}$$

7.5 An Example

The hydraulic hoist transmission system of a marine crane is functionally shown in Figure 4.3 in Chapter 4. Each constituent subsystem is associated with several failure modes. The precise values of the three variables (the failure likelihood, consequence severity and failure consequence probability) used to describe the safety associated with a failure mode of a subsystem may be difficult to estimate as the marine crane is working in a changing environment. However, it could be comparatively easier to use fuzzy subjective judgements to describe these three variables in order to evaluate the

safety of this crane hydraulic hoist transmission system.

7.5.1 Failure Mode Modelling

1. Hydraulic oil tank

Four failure modes of this subsystem are identified. These are:

i. Level gauge failure

ii. Oil temperature too high or too low

iii. Major leak

iv. Minor leak

The safety associated with each of these failure modes is analysed using the methodology described above.. The detailed analysis for the first failure mode is presented. The analyses for other failure modes are conducted in a similar manner.

i. Level gauge failure

For this failure mode, the failure likelihood is considered to be approximately "*Reasonably low*" and may vary about "*Reasonably low*". With reference to Table 7.1, the failure likelihood L_{11} is modelled as follows:

$$L_{11} = \{1/0.1, 2/0.3, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0\}$$

The consequence severity is considered to be approximately "*Marginal*" and may vary about "*Marginal*". With reference to Table 7.2, the failure likelihood C_{11} is modelled as follows:

$$C_{11} = \{1/0, 2/0.25, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0\}$$

The failure consequence probability is considered to be approximately "*Unlikely*" and may vary about "*Unlikely*". With reference to Table 7.3, the failure likelihood E_{11} is modelled as follows:

$$E_{11} = \{1/0.25, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0\}$$

The fuzzy safety score S_{11} of this failure mode is calculated as follows:

$$S_{11} = C_{11} \circ E_{11} \times L_{11} = \{1/0.1,\ 2/0.3,\ 3/0.8,\ 4/0.8,\ 5/0.1,\ 6/0,\ 7/0\}$$

The obtained fuzzy safety score of the failure mode can be mapped back to the defined safety expressions ("*Poor*", "*Average*", "*Good*" and "*Excellent*"). The safety associated with this failure mode is identified as follows:

$$S(s_{11}) = \{(0.127399,\ \text{"}Poor\text{"}),\ (0.167771,\ \text{"}Average\text{"}),\ (0.560565,\ \text{"}Good\text{"}),\ (0.144265,\ \text{"}Excellent\text{"})\}$$

It can be noted that the three parameters, namely the failure likelihood, the consequence severity and the failure consequence probability of this failure mode, are estimated approximately as "*Reasonably low*", "*Marginal*" and "*Unlikely*", respectively. Therefore, the evaluation of this failure mode should be identified to belong to "*Good*" and "*Excellent*" to a large extent. This is confirmed by the above results.

λ_{kj} is a normalised relative weight for the jth failure mode of the kth subsystem, which can be calculated on the basis of the designer's judgements on the relative weights of the failure modes associated with the kth subsystem. λ_{kj} can be assigned using the method described in [7.18][7.20]. It is assumed that if all the failure modes of the hydraulic tank are absolutely evaluated as "*Excellent*" the hydraulic oil tank is judged as "*Excellent*" with a confidence degree of over 99.5 percent. The following formulae can be used to assign the value of λ_{kj} as shown in [7.18][7.20]:

$$\lambda_{kj} = \alpha_k \frac{\zeta_k^j}{\zeta_K^I}, \qquad \prod_{j=1}^{4} (1 - \alpha_k \frac{\zeta_k^j}{\zeta_k^I}) \le \delta$$

where $\delta = 1 - 0.995 = 0.005$

ζ_k^j = the relative weight of the j failure mode of the hydraulic oil tank ($k = 1$),

ζ_k^I = the largest value among the weights of the failure modes of the hydraulic oil tank ($k = 1$),

α_k = a priority coefficient representing the importance of the role the most importance factor plays in evaluation of the safety of the hydraulic oil tank ($k = 1$).

$\lambda_{11} = 0.46.$

ii. Oil temperature too high or too low

$L_{12} = \{1/0, 2/0, 3/0.3, 4/1.0, 5/0.8, 6/0.1, 7/0\}$

$C_{12} = \{1/1.0, 2/0.75, 3/0.1, 4/0, 5/0, 6/0, 7/0\}$

$E_{12} = \{1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0\}$

$S_{12} = C_{12} \circ E_{12} \times L_{12} = \{1/0, 2/0, 3/0.25, 4/0.25, 5/0.25, 6/0.1, 7/0\}$

$S(s_{12})$ = {(0.203344, "*Poor*"), (0.306207, "*Average*"), (0.295963, "*Good*"), (0.194486, "*Excellent*")}

$\lambda_{12} = 0.92$

iii. Major leak

$L_{13} = \{1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0\}$

$C_{13} = \{1/0, 2/0.25, 3/1.0, 4/0.75, 5/0.1, 6/0, 7/0\}$

$E_{13} = \{1/0, 2/0.1, 3/0.9, 4/1.0, 5/0.9, 6/0.1, 7/0\}$

$S_{13} = C_{13} \circ E_{13} \times L_{13} = \{1/0.3, 2/0.9, 3/0.8, 4/0.1, 5/0, 6/0, 7/0\}$

$S(s_{13})$ = {(0.172777, "*Poor*"), (0.183395, "*Average*"), (0.361116, "*Good*"), (0.282711, "*Excellent*")}

$\lambda_{13} = 0.92$

iv. Minor leak

$L_{14} = \{1/0.3, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$

$C_{14} = \{1/1.0, 2/0.75, 3/0, 4/0, 5/0, 6/0, 7/0\}$

$E_{14} = \{1/1.0, 2/0.75, 3/0, 4/0, 5/0, 6/0, 7/0\}$

$S_{14} = C_{14} \circ E_{14} \times P_{14} = \{1/0.3, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0\}$

$S(s_{14})$ = {(0.179706, "*Poor*"), (0.187129, "*Average*"), (0.328012, "*Good*"), (0.305152, "*Excellent*")}

$\lambda_{14} = 0.23$

$\lambda_1 = 0.24$

2. Auxiliary system

Six failure modes of this subsystem are identified and evaluated as follows:

i. Failure allowing contaminant into system

L_{21} = {1/0, 2/0, 3/0.2, 4/0.8, 5/1.0, 6/0.25, 7/0}

C_{21} = {1/0.1, 2/0.4, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

E_{21} = {1/0.4, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S_{21} = C_{21} \circ E_{21} \times P_{21}$ = {1/0, 2/0, 3/0.2, 4/0.8, 5/0.8, 6/0.25, 7/0}

$S(s_{21})$ = {(0.140185, "*Poor*"), (0.545059, "*Average*"), (0.183801, "*Good*"), (0.130956, "*Excellent*")}

$\lambda_{21} = 0.5$

ii. Filter blocked

L_{22} = {1/0.25, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

C_{22} = {1/0.1, 2/0.4, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

E_{22} = {1/0.4, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S_{22} = C_{22} \circ E_{22} \times P_{22}$ = {1/0.25, 2/0.8, 3/0.75, 4/0, 5/0, 0, 7/0}

$S(s_{22})$ = {(0.176247, "*Poor*"), (0.184596, "*Average*"), (0.360054, "*Good*"), (0.279103, "*Excellent*")}

$\lambda_{22} = 0.25$

iii. Blocking indicator fails to operate

L_{23} = {1/0, 2/0.3, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

C_{23} = {1/0, 2/0.25, 3/1.0, 4/0.75, 5/0.1, 6/0, 7/0}

E_{23} = {1/0.25, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

$S_{23} = C_{23}$ o $E_{23} \times P_{23}$ = {1/0, 2/0.3, 3/0.75, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{23})$ = {(0.126268, "*Poor*"), (0.167319, "*Average*"), (0.568525, "*Good*"), (0.137888, "*Excellent*")}

$\lambda_{23} = 0.25$

iv. Minor leak

L_{24} = {1/0, 2/0.2, 3/0.6, 4/1.0, 5/0.5, 6/0, 7/0}

C_{24} = {1/1.0, 2/0.75, 3/0.1, 4/0, 5/0, 6/0, 7/0}

E_{24} = {1/0.25, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

$S_{24} = C_{24}$ o $E_{24} \times P_{24}$ = {1/0, 2/0.2, 3/0.6, 4/0.75, 5/0.5, 6/0, 7/0}

$S(s_{24})$ = {(0.157031, "*Poor*"), (0.297143, "*Average*"), (0.352437, "*Good*"), (0.166276, "*Excellent*")}

$\lambda_{24} = 0.25$

v. Major leak

L_{25} = {1/0.25, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{25} = {1/0.1, 2/0.3, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

E_{25} = {1/0, 2/0.25, 3/1.0, 4/0.75, 5/0.1, 6/0, 7/0}

$S_{25} = C_{25}$ o $E_{25} \times P_{25}$ = {1/0.25, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{25})$ = {(0.176890, "*Poor*"), (0.187174, "*Average*"), (0.352436, "*Good*"), (0.283500, "*Excellent*")}

$\lambda_{25} = 0.8$

vi. No output from control pump

L_{26} = {1/0.2, 2/1.0, 3/0.9, 4/0.2, 5/0, 6/0, 7/0}

C_{26} = {1/0.1, 2/0.4, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

E_{26} = {1/0, 2/0.1, 3/0.6, 4/1.0, 5/0.6, 6/0.1, 7/0}

$S_{26} = C_{26} \circ E_{26} \times P_{26}$ = {1/0.2, 2/0.8, 3/0.8, 4/0.2, 5/0, 6/0, 7/0}

$S(s_{26})$ = {(0.164996, "*Poor*"), (0.179384, "*Average*"), (0.410346, "*Good*"), (0.245275, "*Excellent*")}

$\lambda_{26} = 0.8$

$\lambda_2 = 0.24$

3. Control system

Five failure modes of this subsystem are identified and evaluated as follows:

i. Major leak

L_{31} = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{31} = {1/0, 2/0, 3/0.1, 4/0.8, 5/1.0, 6/0.4, 7/0.1}

E_{31} = {1/0, 2/0, 3/0.2, 4/0.8, 5/1.0, 6/0.3, 7/0}

$S_{31} = C_{31} \circ E_{31} \times P_{31}$ = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{31})$ = {(0.175962, "*Poor*"), (0.186099, "*Average*"), (0.346332, "*Good*"), (0.291607, "*Excellent*")}

$\lambda_{31} = 0.8$

ii. Minor leak

L_{32} = {1/0, 2/0, 3/0, 4/0.75, 5/1, 6/0.25, 7/0}

C_{32} = {1/1.0, 2/0.75, 3/0, 4/0, 5/0, 6/0, 7/0}

E_{32} = {1/0.25, 2/1.0, 3/0.75, 4/0.1, 5/0, 6/0, 7/0}

$S_{32} = C_{32} \circ E_{32} \times P_{32}$ = {1/0, 2/0, 3/0, 4/0.1, 5/0.8, 6/0.8, 7/0.3}

$S(s_{32})$ = {(0.272065, "*Poor*"), (0.377796, "*Average*"), (0.180610, "*Good*"), (0.169529, "*Excellent*")}

$\lambda_{32} = 0.2$

iii. No output when required

L_{33} = {1/0, 2/0, 3/0.1, 4/0.8, 5/1.0, 6/0.3, 7/0}

C_{33} = {1/0.1, 2/0.3, 3/1.0, 4/0.75, 5/0, 6/0, 7/0}

E_{33} = {1/0, 2/0, 3/0.6, 4/1.0, 5/0.6, 6/0, 7/0}

$S_{33} = C_{33} \circ E_{33} \times P_{33}$ = {1/0, 2/0, 3/0.1, 4/0.75, 5/0.75, 6/0.3, 7/0}

$S(s_{33})$ = {(0.137888, "*Poor*"), (0.568525, "*Average*"), (0.167319, "*Good*"), (0.126268, "*Excellent*")}

$\lambda_{33} = 0.4$

iv. Control output for lowering motion cannot be closed when required

L_{34} = {1/0, 2/.25, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{34} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{34} = {1/0, 2/0.1, 3/0.7, 4/1.0, 5/0.7, 6/0.1, 7/0}

$S_{34} = C_{34} \circ E_{34} \times P_{34}$ = {1/0, 2/0.1, 3/0.1, 4/0.1, 5/0.1, 6/0.1, 7/0}

$S(s_{34})$ = {(0.227082, "*Poor*"), (0.272918, "*Average*"), (0.272918, "*Good*"), (0.227082, "*Excellent*")}

$\lambda_{34} = 0.8$

v. Control output for hoisting up motion can not be closed when required

L_{35} = {1/0, 2/0.1, 3/0.7, 4/1.0, 5/0.7, 6/0.1, 7/0}

C_{35} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{35} = {1/0, 2/0.1, 3/0.7, 4/1.0, 5/0.7, 6/0.1, 7/0}

$S_{35} = C_{35} \circ E_{35} \times P_{35}$ = {1/0, 2/0.1, 3/0.1, 4/0.1, 5/0.1, 6/0.1, 7/0}

$S(s_{35})$ = {(0.227082, "*Poor*"), (0.272918, "*Average*"), (0.272918, "*Good*"), (0.227082, "*Excellent*")}

$\lambda_{35} = 0.8$

$\lambda_3 = 0.48$

4. Protection system

Eight failure modes of this subsystem are identified and evaluated as follows:

i. Failure of switch when energised

L_{41} = {1/0, 2/0.3, 3/0.6, 4/1.0, 5/0.6, 6/0.1, 7/0}

C_{41} = {1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0}

E_{41} = {1/0, 2/0, 3/0.1, 4/0.8, 5/1.0, 6/0.4, 7/0.1}

$S_{41} = C_{41} \circ E_{41} \times P_{41}$ = {1/0, 2/0.3, 3/0.6, 4/0.75, 5/0.6, 6/0.1, 7/0}

$S(s_{41})$ = {(0.160484, "*Poor*"), (0.321832, "*Average*"), (0.347827, "*Good*"), (0.169858, "*Excellent*")}

$\lambda_{41} = 0.32$

ii. Failure of return for hoisting up when de-energised

L_{42} = {1/0.3, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

C_{42} = {1/0, 2/0, 3/0, 4/0, 5/0.2, 6/0.9, 7/1.0}

E_{42} = {1/0, 2/0.1, 3/0.8, 4/1.0, 5/0.8, 6/0.1, 7/0}

$S_{42} = C_{42} \circ E_{42} \times P_{42}$ = {1/0.2, 2/0.2, 3/0.2, 4/0, 5/0, 6/0, 7/0}

$S(s_{42})$ = {(0.211166, "*Poor*"), (0.228852, "*Average*"), (0.283647, "*Good*"), (0.276335, "*Excellent*")}

$\lambda_{42} = 0.32$

iii. Minor leak

L_{43} = {1/0, 2/0, 3/0.1, 4/0.75, 5/1, 6/0.4, 7/0.1}

C_{43} = {1/1.0, 2/0.75, 3/0.1, 4/0, 5/0, 6/0, 7/0}

E_{43} = {1/0.25, 2/1, 3/0.75, 4/0, 5/0, 6/0, 7/0}

$S_{43} = C_{43} \circ E_{43} \times P_{43}$ = {1/0, 2/0, 3/0.1, 4/0.75, 5/0.75, 6/0.4, 7/0.1}

$S(s_{43})$ = {(0.154418, "*Poor*"), (0.542517, "*Average*"), (0.171944, "*Good*"), (0.131120, "*Excellent*")}

$\lambda_{43} = 0.16$

iv. Major leak

L_{44} = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{44} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{44} = {1/0, 2/0, 3/0.1, 4/0.2, 5/0.75, 6/1.0, 7/0.3}

$S_{44} = C_{44} \circ E_{44} \times P_{44}$ = {1/0.3, 2/0.8, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{44})$ = {(0.169529, "*Poor*"), (0.180610, "*Average*"), (0.377796, "*Good*"), (0.272065, "*Excellent*")}

$\lambda_{44} = 0.64$

v. Failure of emergency stop

L_{45} = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{45} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{45} = {1/0, 2/0, 3/0.1, 4/0.75, 5/1.0, 6/0.3, 7/0}

$S_{45} = C_{45} \circ E_{45} \times P_{45}$ = {1/0.3, 2/0.3, 3/0.3, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{45})$ = {(0.169529, "*Poor*"), (0.180610, "*Average*"), (0.377796, "*Good*"), (0.272065, "*Excellent*")}

$\lambda_{45} = 0.16$

vi. Failure of hoisting up limit

L_{46} = {1/0.3, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

C_{46} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{46} = {1/0, 2/0, 3/0.6, 4/1.0, 5/0.6, 6/0, 7/0}

$S_{46} = C_{46} \circ E_{46} \times P_{46}$ = {1/0.1, 2/0.1, 3/0.1, 4/0, 5/0, 6/0, 7/0}

$S(s_{46})$ = {(0.225805, "*Poor*"), (0.245933, "*Average*"), (0.272623, "*Good*"), (0.255638, "*Excellent*")}

$\lambda_{46} = 0.64$

vii. Failure of hoisting down limit

L_{47} = {1/0.3, 2/1.0, 3/0.75, 4/0, 5/0, 6/0, 7/0}

C_{47} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{47} = {1/0.1, 2/0.3, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

$S_{47} = C_{47} \circ E_{47} \times P_{47}$ = {1/0.1, 2/0.1, 3/0.1, 4/0, 5/0, 6/0, 7/0}

$S(s_{47})$ = {(0.225805, "*Poor*"), (0.245933, "*Average*"), (0.272623, "*Good*"), (0.255638, "*Excellent*")}

$\lambda_{47} = 0.64$

viii. Low boost pressure switch fails to open

L_{48} = {1/1.0, 2/0.9, 3/0.2, 4/0, 5/0, 6/0, 7/0}

C_{48} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{48} = {1/0, 2/0.1, 3/0.75, 4/1.0, 5/0.75, 6/0.1, 7/0}

$S_{48} = C_{48} \circ E_{48} \times P_{48}$ = {1/0.1, 2/0.1, 3/0.1, 4/0, 5/0, 6/0, 7/0}

$S(s_{48})$ = {(0.225805, "*Poor*"), (0.245933, "*Average*"), (0.272623, "*Good*"), (0.255638, "*Excellent*")}

$\lambda_{48} = 0.64$

$\lambda_4 = 0.48$

5. Hydraulic servo transmission system

Seven failure modes of this subsystem are identified and evaluated as follows:

i. Major leak

L_{51} = {1/0.1, 2/0.3, 3/1.0, 4/0.8, 5/0.1, 6/0, 7/0}

C_{51} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{51} = {1/0, 2/0, 3/0.1, 4/0.7, 5/1.0, 6/0.3, 7/0}

$S_{51} = C_{51} \circ E_{51} \times P_{51}$ = {1/0.1, 2/0.3, 3/0.3, 4/0.3, 5/0.1, 6/0, 7/0}

$S(s_{51})$ = {(0.186270, "*Poor*"), (0.241453, "*Average*"), (0.341080, "*Good*"), (0.231196, "*Excellent*")}

$\lambda_{51} = 0.88$

ii. Minor leak

L_{52} = {1/0, 2/0, 3/0.1, 4/0.08, 5/1.0, 6/0.3, 7/0}

C_{52} = {1/1.0, 2/0.75, 3/0.2, 4/0, 5/0, 6/0, 7/0}

E_{52} = {1/0.25, 2/1.0, 3/0.75, 4/0.1, 5/0, 6/0, 7/0}

$S_{52} = C_{52} \circ E_{52} \times P_{52}$ = {1/0, 2/0, 3/0.1, 4/0.75, 5/0.75, 6/0.3, 7/0}

$S(s_{52})$ = {(0.137888, "*Poor*"), (0.568525, "*Average*"), (0.167319, "*Good*"), (0.126268, "*Excellent*")}

$\lambda_{52} = 0.21$

iii. Shaft failure

L_{53} = {1/0.25, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{53} = {1/0, 2/0, 3/0, 4/0.1, 5/0.3, 6/0.8, 7/1.0}

E_{53} = {1/0, 2/0, 3/0, 4/0.1, 5/0.8, 6/1.0, 7/0.3}

$S_{53} = C_{53} \circ E_{53} \times P_{53}$ = {1/0.25, 2/0.8, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{53})$ = {(0.169884, "*Poor*"), (0.181104, "*Average*"), (0.385875, "*Good*"), (0.263138, "*Excellent*")}

$\lambda_{53} = 0.44$

iv. No output from the package motor

L_{54} = {1/0, 2/0, 3/0, 4/0.1, 5/0.9, 6/1.0, 7/0.3}

C_{54} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.8, 7/1.0}

E_{54} = {1/0, 2/0, 3/0.6, 4/1.0, 5/0.6, 6/0, 7/0}

$S_{54} = C_{54} \circ E_{54} \times P_{54}$ = {1/0, 2/0, 3/0, 4/0.1, 5/0.1, 6/0.1, 7/0.1}

$S(s_{54})$ = {(0.249886, "*Poor*"), (0.279311, "*Average*"), (0.249886, "*Good*"), (0.220917, "*Excellent*")}

λ_{54} = 0.44

v. Hydraulic short circuit

L_{55} = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{55} = {1/0, 2/0, 3/0, 4/0.1, 5/0.3, 6/0.8, 7/1.0}

E_{55} = {1/0, 2/0, 3/0, 4/0.1, 5/0.5, 6/0.8, 7/1.0}

$S_{55} = C_{55} \circ E_{55} \times P_{55}$ = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{55})$ = {(0.175962, "*Poor*"), (0.186099, "*Average*"), (0.346332, "*Good*"), (0.291607, "*Excellent*")}

λ_{55} = 0.44

vi. Motor seizure

L_{56} = {1/0.3, 2/1.0, 3/0.8, 4/0.1, 5/0, 6/0, 7/0}

C_{56} = {1/0, 2/0.25, 3/1.0, 4/0.75, 5/0, 6/0, 7/0}

E_{56} = {1/0.3, 2/0.7, 3/1.0, 4/0.7, 5/0.3, 6/0.1, 7/0}

$S_{56} = C_{56} \circ E_{56} \times P_{56}$ = {1/0.3, 2/0.75, 3/0.75, 4/0.1, 5/0, 6/0, 7/0}

$S(s_{56})$ = {(0.169055, "*Poor*"), (0.180786, "*Average*"), (0.376335, "*Good*"), (0.273824, "*Excellent*")}

λ_{56} = 0.44

vii. Pipe burst

L_{57} = {1/1.0, 2/0.75, 3/0.1, 4/0, 5/0, 6/0, 7/0}

C_{57} = {1/0, 2/0, 3/0, 4/0, 5/0.1, 6/0.75, 7/1.0}

E_{57} = {1/0, 2/0, 3/0, 4/0.1, 5/0.8, 6/1.0, 7/0.25}

$S_{57} = C_{57}$ o $E_{57} \times P_{57}$ = {1/0.75, 2/0.75, 3/0.1, 4/0, 5/0, 6/0, 7/0}

$S(s_{57})$ = {(0.106954, "*Poor*"), (0.112284, "*Average*"), (0.128371, "*Good*"), (0.652392, "*Excellent*")}

λ_{57} = 0.21

λ_5 = 0.98

7.5.2 Safety Synthesis

Using the hierarchical evidential reasoning approach described in section 7.4, the syntheses of safety evaluations at the subsystem level and system level can be carried out. Uncertain evaluations of the subsystems are obtained as follows:

1. Hydraulic oil tank

$S_{(1)}$ = {(0.134298, "*Poor*"), (0.201362, "*Average*"), (0.451697, "*Good*"), (0.200029, "*Excellent*")}

2. Auxiliary system

$S_{(2)}$ = {(0.116894, "*Poor*"), (0.200282, "*Average*"), (0.437804, "*Good*"), (0.202550, "*Excellent*")}

3. Control system

$S_{(3)}$ = {(0.162497, "*Poor*"), (0.299497, "*Average*"), (0.299230, "*Good*"), (0.211705, "*Excellent*")}

4. Protection system

$S_{(4)}$ = {(0.166221, "*Poor*"), (0.224034, "*Average*"), (0.325006, "*Good*"), (0.237506, "*Excellent*")}

5. Hydraulic servo transmission system

$S_{(5)}$ = {(0.141912, "*Poor*"), (0.207604, "*Average*"), (0.362763, "*Good*"), (0.246110, "*Excellent*")}

Uncertain evaluation of the whole system is obtained as follows:

S = {(0.115566, "*Poor*"), (0.203768, "*Average*"), (0.425980, "*Good*"), (0.223201, "*Excellent*")}

From the above results, it is obvious that four subsystems (the hydraulic oil tank, auxiliary system, protection system and hydraulic servo transmission system) have to a large extent been assessed as "*Good*". For example, the hydraulic oil tank has been assessed as "*Good*" with a belief of 45.1697 percent; as "*Excellent*" with 20.0029 percent; as "*Average*" with 20.1362 percent; and as "*Poor*" with 13.4298 percent. The control system has been evaluated to a slightly larger extent as "*Average*" and "*Good*". Since the safety of the hydraulic transmission system is determined by the safety of each of the constituent subsystems, the system safety should be evaluated as "*Good*" to a large extent. This is in harmony with the result obtained above as the safety of this hydraulic transmission system has been assessed as "*Good*" and "*Excellent*" to the extents of 42.5980 percent and 22.3201 percent, respectively.

The above information provides an analysis of the safety of the crane hydraulic transmission system and an idea of the potential problem areas. From this information, the design engineer can have an insight into system safety and may then decide if design actions need to be taken to improve matters.

7.6 Concluding Remarks

A new methodology is proposed in this chapter for safety analysis and synthesis based on fuzzy set theory and an evidential reasoning approach. In this methodology, the safety of a failure event is analysed using fuzzy set modelling. This provides the safety analyst with flexibility in articulating judgements about such parameters as failure likelihood, consequences severity and failure consequence probability which are often used in safety analysis. The examination of the safety of a complex system with a hierarchical evaluation structure is carried out using an evidential reasoning approach, based on the information produced. Such a reasoning framework provides the safety

analyst with a rational tool to make full use of the information generated at the lowest level in design to evaluate the safety of the whole system.

The proposed methodology can be used as an alternative approach for safety analysts to carry out analysis particularly in those situations where distributions of variables for use in probabilistic risk studies are difficult or impossible to obtain. Furthermore, since human reasoning is intrinsically fuzzy, it is believed that the proposed approach will be potentially useful in safety analysis and synthesis in many industrial environments.

REFERENCES - CHAPTER 7

[7.1] Andersson, L., *The theory of possibility and fuzzy sets: new ideas for risk analysis and decision making,* Swedish Council for Building Research, 1988.

[7.2] Apostolakis, G. E., Guedes Soares, C., Kondo, S. & Mancini, G., *Are reliability and risk assessment ready for fuzzy methods?,* Reliability Engineering and System Safety, Vol. 42, 1993, p65.

[7.3] Baldwin, J. F. & Pilsworth, B. W., *A model of fuzzy reasoning through multi-valued logic and set theory,* Int. J. Man-Machine Studies, Vol.11, 1979, 351-380.

[7.4] Chun, M. H. & Ahn, K. I., *Assessment of the potential applicability of fuzzy set theory to accident progression event trees with phenomenological uncertainties,* Reliability Engineering and System Safety, Vol. 37, 1992, 237-252.

[7.5] Coolen, F. P. A. & Newby, M. J., *Bayesian reliability analysis with imprecise prior probabilities,* Reliability Engineering and System Safety, Vol. 43, 1994, 75-85.

[7.6] Dubois, D. & Prade, H., *On the relevance on non-standard theories of uncertainty in modeling and pooling expert opinions, Reliability Engineering and System Safety,* Vol. 36, 1992, 95-107.

[7.7] Fine, W. T., *Mathematical evaluations for controlling hazards,* Academic press, Macon, GA, 1973.

[7.8] Kaufmann, A., *Introduction to the theory of fuzzy subsets,* Volume 1, Academic Press, 1975.

[7.9] Karwowski, W. & Mital, A., *Potential applications of fuzzy sets in industrial safety engineering,* Fuzzy sets and systems 19 (1986), 105-120.

[7.10] Keller, A. Z. & Kara-Zaitri, *Application of fuzzy logic to reliability assessment,* Reliability'87, Warrington, 14-16 April 1987, 3A/3/1-11.

[7.11] Keller, A. Z. & Kara-Zaitri, *Further application of fuzzy logic to reliability assessment and safety analysis,* Micro Reliab. Vol.29, No.3, 1989, 399-404.

[7.12] NEL, *FMECA of NEI pedestal crane,* Report No. NECL/01, May 1987.

[7.13] MIL-STD-1629A, *Procedures for Performing a Failure Mode, Effects and Criticality Analysis,* Military Standard, Naval Ship Engineering Center, Washington D.C..

[7.14] Schmucker, K. J., *Fuzzy sets, natural language computations, and risk analysis,* Computer Science Press, 1984.

[7.15] Singer, D., *Fault tree analysis based on fuzzy logic,* Computers Chem. Engng., Vol.14, No.3, 1990, 259-266.

[7.16] Wang, J., Ruxton, T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Design Conference, March 7-11, Chicago, IL, USA, 1-12.

[7.17] Wang J., Yang J. B., Sen P., *Safety analysis and synthesis using fuzzy set modelling and evidential reasoning,* Accepted July 1994 for Publication by Reliability Engineering and System Safety (Research Report EDCN/SAFE/RESC/17/1, EDC, Univerity of Newcastle upon Tyne, December 1993).

[7.18] Yang, J. B., Singh, M. G., *An evidential reasoning approach for multiple attribute decision making with uncertainty,* IEEE Transactions on Systems, Man, and Cybernetics, Vol.23, No.6, 1993.

[7.19] Yang J. B., & Sen P., *A hierarchical evaluation process for multiple attribute design selection with uncertainty,* in Industrial and Engineering Applications of Artificial Intelligence and Expert systems (IEA/AIE-93), P.W.H. Chung, G. Lovegrove and M. Ali Ed., Godon and Breach Science Publisher, Switzerland, 1993, 484-483.

[7.20] Yang J. B., & Sen P., *A general multi-level evaluation process for hybrid MADM with uncertainty,* IEEE Transactions on Systems, Man, and Cybernetics, SMC 093-03-0352, 1993 (to appear soon).

[7.21] Zadeh L. A., *Fuzzy sets and their applications to cognitive and decision processes,* Academic Press, 1975.

[7.22] Zhang Z. J., Yang J. B., & Xu D. L., *A hierarchical analysis model for multiobjective decision making,* in Analysis, Design and Evaluation of Man-Machine Systems 1989, Selected Papers from the 4th IFAC/IFIP/IFORS/IEA Conference (Xi'an, China, September 1989), Pergamon, Oxford, U.K., 1990, 13-18.

CHAPTER 8

Techno-economic Modelling for Design and Maintenance Optimisation Based on Safety Analysis

SUMMARY

"Design for safety" necessarily involves decisions about design features and/or operating practices that can be included in a practical design. A techno-economic analysis may be beneficially carried out to achieve this. A techno-economic analysis may be considered as one in which both safety and cost objectives are simultaneously analysed to aid design decisions.

In Chapters 4, 5 and 6, several safety methodologies have been developed to identify the top events and associated prime implicants (cut sets) of a MTO product, to assess their probabilities of occurrence, and to predict component/subsystem failures. Such information can be utilised to construct a techno-economic model for design and maintenance optimisation.

This chapter proposes a techno-economic modelling methodology which brings together safety and cost objectives into the decision making process for the improvement of design aspects and maintenance policies. Multiple Objective Decision Making (MODM) techniques are then employed to process the formulated techno-economic model. The produced results can assist designers in developing good compromise designs and maintenance policies that take into account system top event-caused consequences, maintenance cost, repair cost and design review cost. A technical example of a

hydraulic hoist transmission system of a marine pedestal crane is presented to demonstrate the interaction between economic modelling and safety analysis and to indicate the potential use of this techno-economic modelling methodology in the decision making process involving design and maintenance.

8.1 Introduction

As described in Chapter 2, the report on the inquiry into the Piper Alpha accident has identified the need for the consideration of "design for safety" issues from the early design stages to minimise the inherent hazards of a MTO product [8.3], and a "safety case" approach is suggested to include the identification of a representative sample of accident scenarios and the assessment of the consequences of each scenario together with an assessment, in general terms, of the likelihood of occurrence using Qualitative Risk Analysis (QRA). Techno-economic analysis is proposed here to evaluate reasonably practicable steps to control risks and to incorporate safety aspects into the design process from as early a stage as is possible. Then safety can be considered as a criterion and "design for safety" can move from an assessment function to a decision making function and finally to a verification function.

There are several general steps that appear in a decision making process. These may be presented in terms of the following three steps [8.2]:

i. Recognition and formulation of the problem.

ii. Search for feasible alternatives.

iii. Analysis and selection.

The recognition and formulation of the problem may be the key step in decision making. The search for feasible alternatives involves developing potential solutions to the problem. The aim of this step is to develop a list of potential alternatives, and then to screen these alternatives to select a small group of feasible alternatives. As will be described in this chapter, formal Multiple Objective Decision Making (MODM) tools for design synthesis may be used to process the constructed techno-economic model to produce feasible alternatives. Finally, an assessment of the feasible alternatives is carried out and the preferred alternative is then selected.

In Chapters 4, 5 and 6, several QRA methodologies involving FMECA, the MBRM, the qualitative reasoning approach and the Monte Carlo simulation method have been developed to identify the top events and associated prime implicants (cut sets) of a MTO product, to assess their probabilities of occurrence, and to predict component/subsystem failures. Such safety information has not been fully utilised to aid design decisions. However, such information may be effectively utilised to construct a techno-economic model in order to optimise both design aspects and maintenance policies of an engineering system within both economic and technical constraints.

Techno-economic modelling of the safety of large MTO products has been extensively discussed in literature[8.1][8.4][8.8][8.9], but relatively few practical applications are reported. This could be largely because of the uncertain value placed on human life and difficulties in quantifying risks [8.6]. However, it has been noted that if the uncertainty regarding the risks of a MTO product is not unacceptably high, a techno-economic analysis may be beneficially carried out to process the safety information produced and to make design decisions. Techno-economic analysis has been used by the Health and Safety Executive (HSE) to determine whether risks are acceptable [8.6]. However, risk reduction ceases to be "reasonable" when cost becomes "grossly disproportionate" [8.6]. It has been recognised that it is necessary to quantify not only risks but also the cost of proposed measures and the benefit in terms of the reduced risks. It has also been noted that techno-economic analysis may beneficially be carried out not only in comparative terms but also using formal decision making tools to achieve the effective and efficient risk reduction.

Safety and cost are obviously two conflicting objectives, with higher safety leading to higher cost. It is generally impossible to have a design which could maximise safety (i.e. minimise risks) and minimise the life cycle cost simultaneously. A compromise is therefore required. The decision as to which objective is to be stressed will be dependent on the particular situation in hand. The appropriate level of safety then becomes dependent on the relative importance of cost and safety objectives. If the non-dominated design options for such a situation have to be obtained, it becomes feasible to use a formal MODM tool to arrive at efficient or optimal decisions, although other approaches could also be used.

In this chapter, a techno-economic modelling methodology is proposed to interrelate economic modelling with safety analysis using the methodologies developed in Chapters 4, 5 and 6 to formulate a techno-economic model in which both safety and

cost objectives are involved. This model takes into account both design aspects and maintenance activities. MODM techniques are then employed to process the model to generate the best compromise maintenance policies and design review actions.

8.2 Safety Modelling

8.2.1 Safety Analysis

The top events and associated prime implicants (cut sets) of a MTO product can be identified, in the form of a Boolean representation table, using the inductive bottom-up methodology incorporating the MBRM and FMECA, as described in Chapter 4. Such an inductive methodology may give a higher level of confidence that all system top events and respective prime implicants are identified, especially for MTO products with a comparatively high level of innovation.

The probabilities of occurrence of the identified system top events and associated prime implicants can be quantitatively estimated, on the basis of the obtained final system Boolean representation table, using the simulation model developed in section 6.4.3. The typical model outputs are:

— probability distribution of occurrence of each system top event with MTBM, and

— probability distribution of occurrence of each prime implicant (cut set) with MTBM.

Component/subsystem failures can also be simulated on the basis of the constructed component/subsystem failure simulation model. As described in section 6.4.2, component/subsystem failure distributions of the system with MTBM can be produced by applying the Monte Carlo techniques to such a model.

After the top events of the system have been identified, consequence analysis can be carried out to study the possible effects caused by the occurrence of each identified system top event. As described in Chapter 3, the possible consequences caused by the occurrence of a system top event can be quantified in terms of the possible loss of lives and property, and the degradation of the environment.

The safety information produced can be used to construct a techno-economic model designed to improve the safety of the system and to reduce the life cycle cost. In the remainder of this chapter, a techno-economic modelling methodology is proposed in which both the probabilities of occurrence of the system top events and the costs of system failures, maintenance, repairs and design review over the product life time can be simultaneously taken into consideration.

8.2.2 Safety Modelling

The occurrence of a system top event could result in serious consequences. The safety of a large engineering system can be improved by reducing the probabilities of occurrence of the system top events.

The occurrence of a system top event is completely dependent on the occurrence of the associated minimal prime implicants (cut sets). Therefore, reduction of the probability of occurrence of a system top event is a matter of reducing or eliminating the probabilities of occurrence of the associated prime implicants. The usual way of reducing the probabilities of occurrence of the system top events is to reduce or eliminate the probabilities of occurrence of some significant prime implicants with relatively higher probabilities of occurrence since it is impractical and impossible to reduce or eliminate all the associated prime implicants.

Suppose there are n system top events and $P_i(MTBM)$ represents the probability of occurrence of top event T_i. Suppose c prime implicants are taken into account for reduction or elimination regarding all the system top events. Let $P_{Dj}(MTBM)$ represent the original probability of occurrence of the jth prime implicant before a design review action is taken and ΔP_{Dj} represent the probability reduction of occurrence of this prime implicant as a results of a design review action. $P_i(MTBM)$ and $P_{Dj}(MTBM)$ can be obtained using simulation as described in the last section. It should be noted that such probabilities are functions of MTBM. As MTBM increases, the probabilities become larger. Such probability functions are also discrete and nonlinear because they can only be obtained at discrete MTBM values.

The safety of a system can be improved by minimising risks. If the reduction or elimination of one prime implicant does not significantly affects others, the risk function can be expressed as the sum of the probabilities of occurrence of the system top events and c prime implicants considered for reduction or elimination while each

system top event is weighted on the basis of the severity of the possible consequences. Suppose *Risk* represents such a function. The safety model can be constructed as follows:

$$\text{min: } Risk = \sum_{i=1}^{n} K_i \times P_i(MTBM) + \sum_{j=1}^{c} K_{Dj} \times (P_{Dj}(MTBM) - \Delta P_{Dj})$$

$$\text{subject to: } MTBM_{max} \geq MTBM \geq MTBM_{min}$$

$$0 \leq \Delta P_{Dj} \leq P_{Dj}(MTBM) \; (j = 1, 2, \cdots, c)$$

where: K_i = the weighting factor for top event T_i.

$MTBM_{max}$ = the largest MTBM value used in the simulation analysis for the prediction of the probabilities of occurrence of the system top events and associated prime implicants.

$MTBM_{min}$ = the smallest MTBM value used in simulation analysis for the prediction of the probabilities of occurrence of the system top events and the associated prime implicants.

$K_{Dj} = K_i$ if the jth prime implicant is associated with top event T_i.

The first term of the *Risk* function deals with maintenance policies. This term represents the sum of the probabilities of occurrence of system top events before design actions are taken. The second term takes into account both maintenance policies and design review actions. This term represents the remainder of the probabilities of occurrence of c prime implicants after design actions have been taken. The occurrence of the prime implicants considered for reduction or elimination contributes to the occurrence of system top events. Obviously, the smaller the sum of the two terms is, the higher the safety level of the system. It can be noted that some prime implicants may be double accounted in the *Risk* function. The purpose of modelling safety in such a way is to make sure that *Risk* is a monotonicly increasing function of MTBM. Risk assessment is not affected by double accounting of some prime implicants. This implies that the model is sound. The above safety model implies that maintenance policies and design review actions should be implemented to minimise the risks associated with the system.

8.3. Economic Modelling

Cost is always an important issue in the design process of a large engineering product. The life cycle cost of a large engineering product may be modelled by taking into account the top event-caused consequences, repair cost, maintenance cost and design review cost. The following simplifying assumptions are made to implement economic modelling.

i. The basic diagram of the system to be analysed is not changed.

ii. Manpower and spare parts are sufficient for repair and maintenance activities.

iii. Cost incurred is expressed as the present value.

The life cycle cost model is proposed as follows.

8.3.1 Top Event-caused Cost Modelling

A system may have several serious top events, each of which could result in a system breakdown and possibly cause serious consequences such as injury or loss of lives, damage or loss of property and the degradation of the environment. Top event-caused cost includes the following three parts:

i. C_{TC}: cost directly resulting from the occurrence of the system top events.

ii. C_{TL}: lost income due to the loss of the production capacity.

iii. C_{TR}: repair cost caused by the occurrence of the system top events.

Top event-caused cost $COST_T$ is given by:

$$COST_T = C_{TC} + C_{TL} + C_{TR}$$

$$C_{TC} = \sum_{i=1}^{n} C_{Ti} \times P_i(MTBM)$$

$$C_{TL} = \sum_{i=1}^{n} C_{Li} \times P_i(MTBM)$$

$$C_{TR} = \sum_{i=1}^{n} C_{Ri} \times P_i(MTBM)$$

where: C_{Ti} = cost directly caused by the occurrence of top event T_i.

C_{Li} = lost income caused by the occurrence of top event T_i.

C_{Ri} = repair cost caused by the occurrence of top event T_i.

8.3.2 Maintenance Cost Modelling

Maintenance cost includes the following three parts:

i. C_{ML}: cost of labour.

ii. C_{MP}: cost of parts.

iii. C_{MM}: lost income during the periods of maintenance activities.

Maintenance cost $COST_M$ is given by:

$$COST_M = C_{ML} + C_{MP} + C_{MM}$$

$$C_{ML} = \sum_{i=1}^{\frac{T_{PT}}{MTBM}} C_{MLi}$$

$$C_{MP} = \sum_{i=1}^{\frac{T_{PT}}{MTBM}} C_{MPi}$$

$$C_{MM} = \sum_{i=1}^{\frac{T_{PT}}{MTBM}} C_{MMi}$$

where: C_{MLi} = cost of the labour required for the ith maintenance.

C_{MPi} = cost of the parts required for the ith maintenance.

C_{MMi} = lost income during the period of the ith maintenance.

T_{PT} = the project life time.

$\frac{T_{PT}}{MTBM}$ = the number of major maintenance activities to be conducted over T_{PT}.

If $C_{MLi} = C_{ML}$, $C_{MPi} = C_{MP}$ and $C_{MMi} = C_{MM}$ for $i = 1, 2, \cdots, \frac{T_{PT}}{MTBM}$, $COST_M$ can be

expressed as follows:

$$C_M = (C_{ML} + C_{MP} + C_{MM}) \times \frac{T_{PT}}{MTBM}$$

8.3.3 Repair Cost Modelling

If a key component/subsystem in a system fails, the system should be shut down and the failed component/subsystem should be replaced or repaired immediately. Repair cost includes the following three parts:

i. C_{RL}: cost of labour.

ii. C_{RP}: cost of parts.

iii. C_{RR}: lost income caused by the loss of the production capacity due to failures of the components/subsystems.

Repair cost $COST_R$ is given by:

$$COST_R = C_{RL} + C_{RP} + C_{RR}$$

$$C_{RL} = \sum_{i=1}^{m} C_{RLi} \times f_i(MTBM)$$

$$C_{RP} = \sum_{i=1}^{m} C_{RPi} \times f_i(MTBM)$$

$$C_{RR} = \sum_{i=1}^{m} C_{RRi} \times f_i(MTBM)$$

where: C_{RLi} = cost of the labour for repairing the ith subsystem.

C_{RPi} = cost of the parts for repairing the ith subsystem.

C_{RRi} = lost income caused by the loss of the production capacity due to failures of the ith subsystem.

$f_i(MTBM)$ = the number of failures of the ith component/subsystem, which is a function of MTBM and can be obtained from the component/subsystem failure simulation analysis as described in section 6.4.2.

m = the number of the components/subsystems.

8.3.4 Design Review Cost Modelling

Since the basic design diagram of the system to be analysed is not changed, a design review may only involve the use of more reliable components or provision of protection systems, sensors and redundancies, or combinations of such measures, to reduce or eliminate the most significant prime implicants associated with the identified system top events. Obviously, as more investment is directed at the system for safety improvement, a higher safety level of the system can be achieved. A higher safety level of the system results in the lower probabilities of occurrence of the system top events, which lead to a less expenditure in the operation and maintenance processes.

In the design review cost modelling, the following assumptions are made for the convenience of analysis.

i. The investment to be assigned to the system safety improvement first goes to the reduction or elimination of the prime implicants (associated with the identified system top events) with relatively higher probabilities of occurrence.

ii. After a design review action is taken on a prime implicant, other prime implicants are not significantly affected.

iii. The probability reduction in the occurrence of a prime implicant is normally proportional to the amount of money assigned to this prime implicant.

Suppose M_j (j = 1, 2, $\cdots$, or c) represents the cost required to eliminate the jth prime implicant in the design review process. The relationship between the amount of money assigned to this prime implicant (ΔM_j) and its probability reduction in occurrence (ΔP_{Dj}) can be described as follows:

$$\Delta P_{Dj} = \frac{\Delta M_j}{M_j} P_{Dj}(MTBM)$$

The cost incurred in the reduction or elimination of c prime implicants in the design review process is given by:

$$COST_R = \sum_{j=1}^{c} \Delta M_j$$

The elimination or reduction of the jth prime implicant can result in a probability reduction of occurrence of top event T_i if top event T_i is associated with the jth prime implicants. The possible benefit resulting from the elimination or reduction of c prime implicants is given by:

$$Benifit = \sum_{j=1}^{c} \Delta P_{Dj} \times C_{Dj}$$

where $C_{Dj} = C_{Ti} + C_{Li} + C_{Ri}$ if top event T_i is associated with the jth prime implicant.

The total design review cost $COST_D$ is given by:

$$COST_D = COST_R - Benefit$$

$$= \sum_{j=1}^{c} \Delta M_j - \sum_{j=1}^{c} \Delta P_{Dj} \times C_{Dj}$$

$$= \sum_{j=1}^{c} \left(\frac{M_j}{P_{Dj}(MTBM)} - C_{Dj}\right) \Delta P_{Dj}$$

8.3.5 Operational Cost Modelling

Average daily operational cost $COST_O$ is given by:

$$COST_O = \frac{C_O}{365}$$

where C_O is the annual operational cost of the system.

The models concerned with top event-caused consequences, maintenance cost, repair cost and design review cost should be modified by taking into account the operational cost. The modified models are shown as follows:

$$COST_T^* = COST_T - COST_{OT}$$

$$COST_M^* = COST_M - COST_{OM}$$

$$COST_R^* = COST_R - COST_{OR}$$

$$COST_D^* = COST_D + COST_{OD}$$

$$COST_{OT} = \sum_{i=1}^{n} COST_O \times P_i(MTBM) \times BT_{Ti}$$

$$= COST_O \sum_{i=1}^{n} P_i(MTBM) \times BT_{Ti}$$

$$COST_{OM} = COST_O \times BT_M \times \frac{T_{PT}}{MTBM}$$

$$COST_{OR} = \sum_{i=1}^{m} COST_O \times f_i(MTBM) \times BT_{Ri}$$

$$= COST_O \sum_{i=1}^{m} f_i(MTBM) \times BT_{Ri}$$

$$COST_{OD} = COST_O \sum_{j=1}^{c} \Delta P_{Dj}(MTBM) \times BT_{Dj}$$

where: $COST_T^*$ = top event-caused cost after the modification.

$COST_M^*$ = maintenance cost after the modification.

$COST_R^*$ = repair cost after the modification.

$COST_D^*$ = design review cost after the modification.

BT_{Ti} = the product breakdown time caused by the occurrence of the ith top event.

BT_{Mi} = the expected time required for the ith maintenance.

BT_{Ri} = the time required for repairing the ith subsystem.

$BT_{Dj} = BT_{Ti}$ if top event T_i is associated with the jth prime implicant.

8.3.6 Economic Modelling

An economic model is proposed to combine top event-caused cost, maintenance cost, repair cost and design review cost. Let *Cost* represent the life cycle cost function. Such a model is given by:

$$\text{min: } Cost = COST_T^* + COST_M^* + COST_R^* + COST_D^*$$

$$\text{subject to: } MTBM_{max} \geq MTBM \geq MTBM_{min}$$

$$0 \leq \Delta P_{Dj} \leq P_{Dj}(MTBM) \; (j = 1, 2, \cdots, c)$$

The first three terms of the cost model deal with the maintenance policies and the last term takes into account both the maintenance policies and design review cost. This model implies that maintenance policies and design review actions should be implemented to minimise the life cycle cost.

8.4 A Bi-criteria Model for Techno-economic Analysis

8.4.1 Techno-economic Modelling

A techno-economic model is proposed to combine the safety model with the economic model. Let X = MTBM, $y_j = \Delta P_{Dj}$ and $Y = [y_1, y_2, \cdots, y_c]^T$. Since $COST_T^*$, $COST_M^*$ and $COST_R^*$ are functions of X, and $COST_D^*$ is a function of X and Y, such a techno-economic model can be represented as follows:

$$\text{min: } Cost = COST_T^*(X) + COST_M^*(X) + COST_R^*(X) + COST_D^*(X, Y)$$

$$\text{min: } Risk = [\sum_{i=1}^{n} K_i \times P_i(X) + \sum_{j=1}^{c} K_{Dj} \times (P_{Dj}(X) - y_j)]$$

$$\text{subject to: } X_{max} \geq X \geq X_{min}$$

$$0 \leq y_i \leq P_{Dj}(X) \; (j = 1, 2, \cdots, c)$$

X and Y are design variables which need to be determined to attain the cost and risk objectives as closely as possible.

After the system process diagram has been constructed and safety analysis has been carried out using the safety analysis methodologies developed in Chapter 4, 5 and 6, the above techno-economic model can be formulated.

As described previously, *Cost* and *Risk* are two competing objectives, with a lower risk level (i.e. a higher safety level) leading to higher cost. The purpose of design synthesis is therefore to evolve compromise design solutions by balancing and effectively utilising resources so that these two objectives can be simultaneously achieved.

8.4.2 Problem Transformation and Optimisation

The probability distributions $P_i(X)$ and $P_{Dj}(X)$ ($i = 1, 2, \cdots, n$; $j = 1, 2, \cdots, c$) and the failure distributions $f_i(X)$ ($i = 1, 2, \cdots, m$) are generally not known explicitly. At a specific X, however, the values of these distributions can be obtained from the simulation analysis. If such a simulation analysis is conducted at a sufficient number of discrete values of X, the values of these distributions at any X with $X_{min} \le X \le X_{max}$ may then be predicted using the linear interpolation, resulting in piecewise linear distribution functions. Representation of piecewise linear functions is described in some detail in Appendix 3.

The piecewise linear probability function $P_i(X)$ of top event T_i can be represented as follows [8.23]:

$$P_i(X) = \sum_{j=1}^{N-1} \alpha_{Pi,j} |X - X^j| + \beta_{Pi} X + \gamma_{Pi} \qquad i=1, 2, \cdots, n$$

where: N = the number of the sections of $P_i(X)$.

X^j is a sampled value of X ($j = 0, 1, \cdots, N$).

$$\alpha_{Pi,j} = \frac{1}{2}(t_{Pi,j+1} - t_{Pi,j})$$

$$\beta_{Pi} = \frac{1}{2}(t_{Pi,1} + t_{Pi,N})$$

$$\gamma_{Pi} = \frac{1}{2}(s_{Pi,1} + s_{Pi,N})$$

$t_{Pi,j}$ is the slope of the jth section and $s_{Pi,j}$ is the y-intercept for the jth section of the probability function $P_i(X)$, starting from X^{j-1} and being terminated at X^j, that is

$$t_{Pi,j} = \frac{P_i(X^j) - P_i(X^{j-1})}{X^j - X^{j-1}}$$

$$s_{Pi,1} = P_i(X^0) - t_{Pi,1} X^0$$

$$s_{Pi,N} = P_i(X^N) - t_{Pi,N} X^N$$

If the following auxiliary variables a_j^+ and a_j^- are introduced,

$$a_j^+ = \frac{1}{2}\left\{|X - X^j| + (X - X^j)\right\}$$

$$a_j^- = \frac{1}{2}\left\{|X - X^j| - (X - X^j)\right\}$$

then the probability function $P_i(X)$ can be represented by [8.23]:

$$P_i(X) = \sum_{j=1}^{N-1} \alpha_{Pi,j}(a_j^+ + a_j^-) + \beta_{Pi}X + \gamma_{Pi}, \qquad i=1, 2, \cdots, n \tag{8.1}$$

under the restrictions

$$a_j^+ - a_j^- = X - X^j;$$
$$a_j^+ \times a_j^- = 0; \quad a_j^+, a_j^- \geq 0, \qquad j=1, \cdots, N-1;$$

Similarly, the subsystem failure functions $f_i(X)$ can be represented as follows:

$$f_i(X) = \sum_{j=1}^{N-1} \alpha_{fi,j}(a_j^+ + a_j^-) + \beta_{fi}X + \gamma_{fi}, \qquad i=1, 2, \cdots, m \tag{8.2}$$

where: $\alpha_{fi,j} = \frac{1}{2}(t_{fi,j+1} - t_{fi,j})$

$$\beta_{fi} = \frac{1}{2}(t_{fi,1} + t_{fi,N})$$

$$\gamma_{fi} = \frac{1}{2}(s_{fi,1} + s_{fi,N})$$

$$t_{fi,j} = \frac{f_i(X^j) - f_i(X^{j-1})}{X^j - X^{j-1}}$$

$$s_{fi,1} = f_i(X^0) - t_{fi,1}X^0$$

$$s_{fi,N} = f_i(X^N) - t_{fi,N}X^N$$

$P_{Di}(X)$ can also be represented as follows:

$$P_{Di}(X) = \sum_{j=1}^{N-1} \alpha_{PDi,j}(a_j^+ + a_j^-) + \beta_{PDi}X + \gamma_{PDi}, \qquad i=1, 2, \cdots, c \tag{8.3}$$

where: $\alpha_{PDi,j} = \frac{1}{2}(t_{PDi,j+1} - t_{PDi,j})$

$$\beta_{PDi} = \frac{1}{2}(t_{PDi,1} + t_{PDi,N})$$

$$\gamma_{PDi} = \frac{1}{2}(s_{PDi,1} + s_{PDi,N})$$

$$t_{PDi,j} = \frac{P_{Di}(X^j) - P_{Di}(X^{j-1})}{X^j - X^{j-1}}$$

$$s_{PDi,1} = P_{Di}(X^0) - t_{PDi,1}X^0$$

$$s_{PDi,N} = P_{Di}(X^N) - t_{PDi,N}X^N$$

The bi-criteria Goal Programming (*GP*) problem for optimising both risk and cost objectives may then be transformed as follows:

$$GP \begin{cases} \min\ Cost = \sum_{i=1}^{n}(C_{Ti} + C_{Li} + C_{Ri} - COST_0 \times BT_{Ti})P_i(X) \\ \qquad + (C_{MLi} + C_{MPi} + C_{MMi} - COST_0 \times BT_{Mi})\frac{T_{PT}}{X} \\ \qquad + \sum_{i=1}^{m}(C_{RLi} + C_{RPi} + C_{RRi} - COST_0 \times BT_{Ri})f_i(X) \\ \qquad + \sum_{i=1}^{c}(\frac{M_i}{P_{Di}(X)} - C_{Di} + COST_0 \times BT_{Di})y_i \\ \min\ Risk = \sum_{i=1}^{n} K_i \times P_i(X) + \sum_{j=1}^{c}(K_{Dj} \times P_{Dj}(X) - y_j) \\ s.t.\ \ X_{\min} \le X \le X_{\max}, \quad Y = [y_1, y_2, \cdots, y_c]^T \\ \qquad 0 \le y_i \le P_{Di}(X), \quad i=1, 2, \cdots, c \\ \qquad X - a_j^+ + a_j^- = X^j \qquad j=1, \cdots, N-1 \\ \qquad a_j^+ \times a_j^- = 0;\ a_j^+, a_j^- \ge 0 \qquad j=1, \cdots, N-1 \end{cases} \tag{8.4}$$

The *GP* as defined in (8.4) can be used to obtain compromise designs and to find the interaction between *Cost* and *Risk*, on the basis of which design decisions can be made regarding the particular requirements of *Cost* and *Risk*. In (8.4), $P_i(X)$, $f_i(X)$ and $P_{Di}(X)$ are represented by (8.1), (8.2) and (8.3), respectively. *GP* defined in (8.4) is a non-linear bi-criteria programming problem.

Let $V = [X, a_1^+, a_1^-, \ldots, a_{N-1}^+, a_{N-1}^-, y_1, \ldots, y_c]^T$. V is referred to as a design vector. The problem as represented by (8.4) is then to search for designs that can attain the two

objectives as closely as possible. As described early, there is generally no single design vector available which could simultaneously minimise the *Cost* and *Risk* objectives. It is therefore significant to search for non-dominated (or efficient) design vectors for evaluation [8.22]. Such efficient design vectors can be obtained using existing MODM techniques [8.14][8.21][8.23].

In the next section, an example will be used to demonstrate how to construct a techno-economic model and generate efficient designs.

8.5. An Example

The diagram of the hydraulic hoist transmission system of a marine crane is shown functionally in Figure 4.3 of Chapter 4. The descriptions of this system and its five constituent subsystems can also be found in Chapter 4.

8.5.1 Top Event-caused Cost Modelling

The top events and the associated prime implicants of the hydraulic transmission system can be identified using the inductive bottom-up methodology incorporating the MBRM and FMECA described in Chapter 4. The final Boolean representation table of this system is shown in Table 4.21 of Chapter 4. Each row in Table 4.21 represents a possible condition for an occurrence of the system's output state. For example, the first row associated with the top event S_1 represents that if "*the output of the control system cannot be closed for lowering motion*" and "*shaft failure of the hydraulic servo transmission system*" simultaneously occur, the top event S_1 will happen.

Three system top events S_1, S_2 and S_3, have been identified from the constructed system Boolean representation table. Let $T_1 = S_1$, $T_2 = S_2$ and $T_2 = S_3$. These three system top events are:

T_1: Hoisting down continuously not as required.

T_2: Hoisting up continuously not as required.

T_3: No output from the package motor of the hydraulic servo transmission system

In Table 4.21 of Chapter 4, there are 10 prime implicants identified to be associated with T_1, 43 prime implicants with T_2 and 14 prime implicants with T_3. The possible consequences resulting from these three identified system top events have been comprehensively described in section 4.5.

The probabilistic assessment of the top events can be carried out on the basis of the obtained final system Boolean representation table. The probability distributions of the top events T_1, T_2 and T_3 with MTBM can be produced from the simulation analysis for the prediction of the probabilities of occurrence of the system failure events. Such probabilities distributions of T_1, T_2 and T_3 are shown in Table 6.9 and Figure 6.11 of Chapter 6. The piecewise linear failure distributions of T_1, T_2 and T_3 with MTBM are shown graphically in Figure 8.1.

In the failure-caused cost model, n is equal to 3 and other parameters are assumed and shown in Table 8.1.

Table 8.1 The parameters in the top event-caused cost model

C_T	*pounds*	C_L	*pounds*	C_R	*pounds*
C_{T1}	200000	C_{L1}	10000	C_{R1}	10000
C_{T2}	600000	C_{L2}	20000	C_{R2}	20000
C_{T3}	100000	C_{L3}	5000	C_{R3}	5000

8.5.2 Maintenance Cost Modelling

The parameters in the maintenance cost model are assumed and shown as follows:

$$C_{ML} + C_{MP} = 4000 \text{ pounds}$$

$$C_{MM} = 500 \text{ pounds}$$

$$T_{PT} = 20 \times 365 \times 24 \text{ hr}$$

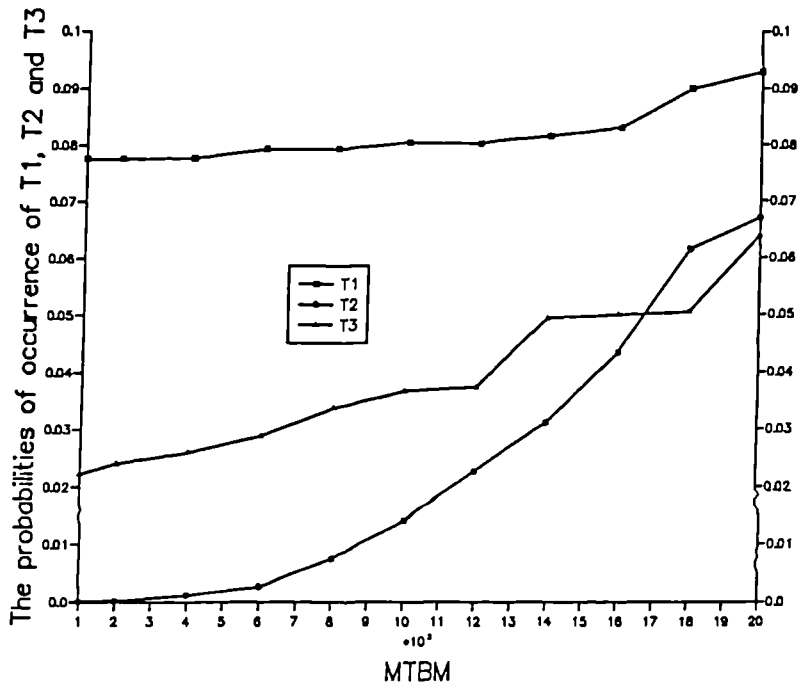


Figure 8.1 Failure distributions of T_1, T_2 and T_3 with MTBM

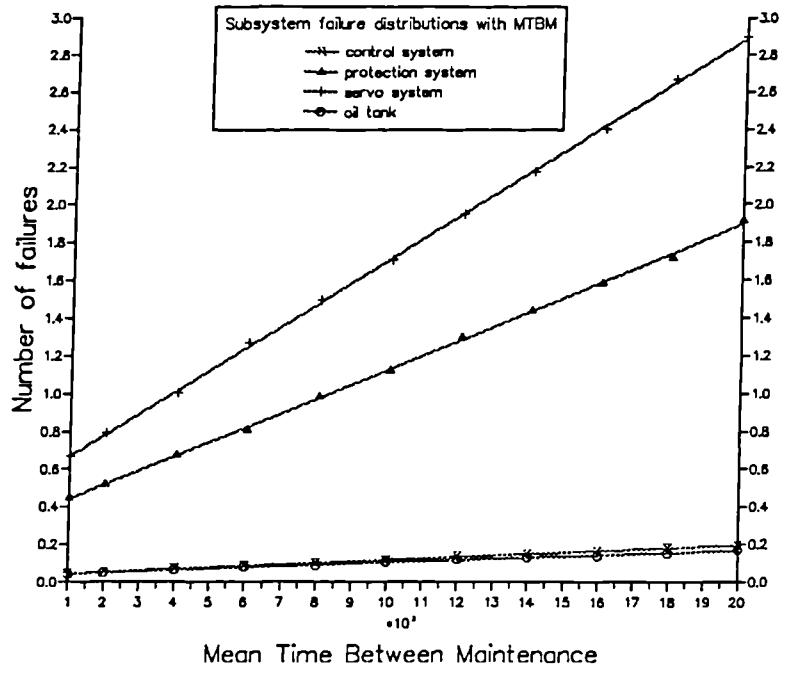


Figure 8.2 Subsystem failure distributions with MTBM

8.5.3 Repair Cost Modelling

As described in Chapter 6, the failure distributions of the subsystems with MTBM can be producted using the component/subsystem failure simulation model. Such distributions are shown in Table 6.7 and Figure 6.10 of Chapter 6. Obviously, these distributions are discrete and nonlinear functions of MTBM because they can only be obtained by simulation at discrete MTBM values. The piecewise linear failure distributions of the subsystems with MTBM are graphically shown in Figure 8.2.

In the repair cost model, m is equal to 4 and other parameters are assumed and shown in Table 8.2.

Table 8.2 The parameters in the repair cost model

C_{RL}	*pounds*	C_{RP}	*pounds*	C_{RR}	*pounds*
C_{RL1}	1000	C_{RP1}	2000	C_{RR1}	2000
C_{RL2}	2000	C_{RP2}	4000	C_{RR2}	4000
C_{RL3}	2000	C_{RP3}	4000	C_{RR3}	4000
C_{RL4}	1000	C_{RP4}	2000	C_{RR3}	2000

8.5.4 Design Review Cost Modelling

The probabilities of occurrence of the prime implicants associated with the system top events T_1, T_2 and T_3 with respect to MTBM can be produced using the simulation model described in section 6.4.3. If six prime implicants with the highest probabilities of occurrence with respect to each MTBM value are taken into account, the total eight prime implicants regarding all MTBM values are identified for reduction or elimination. This is because the six prime implicants may not be the same for different MTBM values. These eight prime implicants are described as follows:

Prime implicant 1: the 5th prime implicant associated with T_1 in Table 4.20.

Prime implicant 2: the 6th prime implicant associated with T_1 in Table 4.20.

Prime implicant 3: the 4th prime implicant associated with T_2 in Table 4.20.

Prime implicant 4: the 1st prime implicant associated with T_3 in Table 4.20.

Prime implicant 5: the 3rd prime implicant associated with T_3 in Table 4.20.

Prime implicant 6: the 5th prime implicant associated with T_3 in Table 4.20.

Prime implicant 7: the 7th prime implicant associated with T_3 in Table 4.20.

Prime implicant 8: the 10th prime implicant associated with T_3 in Table 4.20.

For each MTBM value, the range of the probability reduction of occurrence of each above prime implicant is shown in Table 8.3.

Table 8.3 The range of the probability reduction of occurrence of each prime implicant

MTBM (hr)	Prime implicants							
	P_{D1} 1	P_{D2} 2	P_{D3} 3	P_{D4} 4	P_{D5} 5	P_{D6} 6	P_{D7} 7	P_{D8} 8
1000	.0539	.0236	.0001	.0060	.0020	.0074	.0014	.0036
2000	.0539	.0236	.0002	.0076	.0026	.0090	.0014	.0036
4000	.0539	.0237	.0011	.0076	.0026	.0090	.0014	.0054
6000	.0539	.0253	.0022	.0079	.0026	.0092	.0018	.0054
8000	.0541	.0257	.0058	.0086	.0032	.0104	.0026	.0054
10000	.0553	.0257	.0117	.0088	.0034	.0106	.0034	.0056
12000	.0553	.0257	.0199	.0088	.0034	.0108	.0038	.0094
14000	.0560	.0257	.0253	.0096	.0036	.0110	.0062	.0142
16000	.0564	.0274	.0340	.0098	.0036	.0110	.0062	.0142
18000	.0613	.0286	.0419	.0098	.0036	.0120	.0064	.0142
20000	.0693	.0292	.0507	.0108	.0036	.0130	.0112	.0190

More clearly, the range of the probability reduction of each above prime implicant is shown in Figure 8.3.

In the design review cost model, c is equal to 8 and other parameters are assumed and shown as follows:

$$C_{D1} = C_{D2} = C_{T1} + C_{L1} + C_{R1} = 220{,}000 \ \textit{pounds}$$

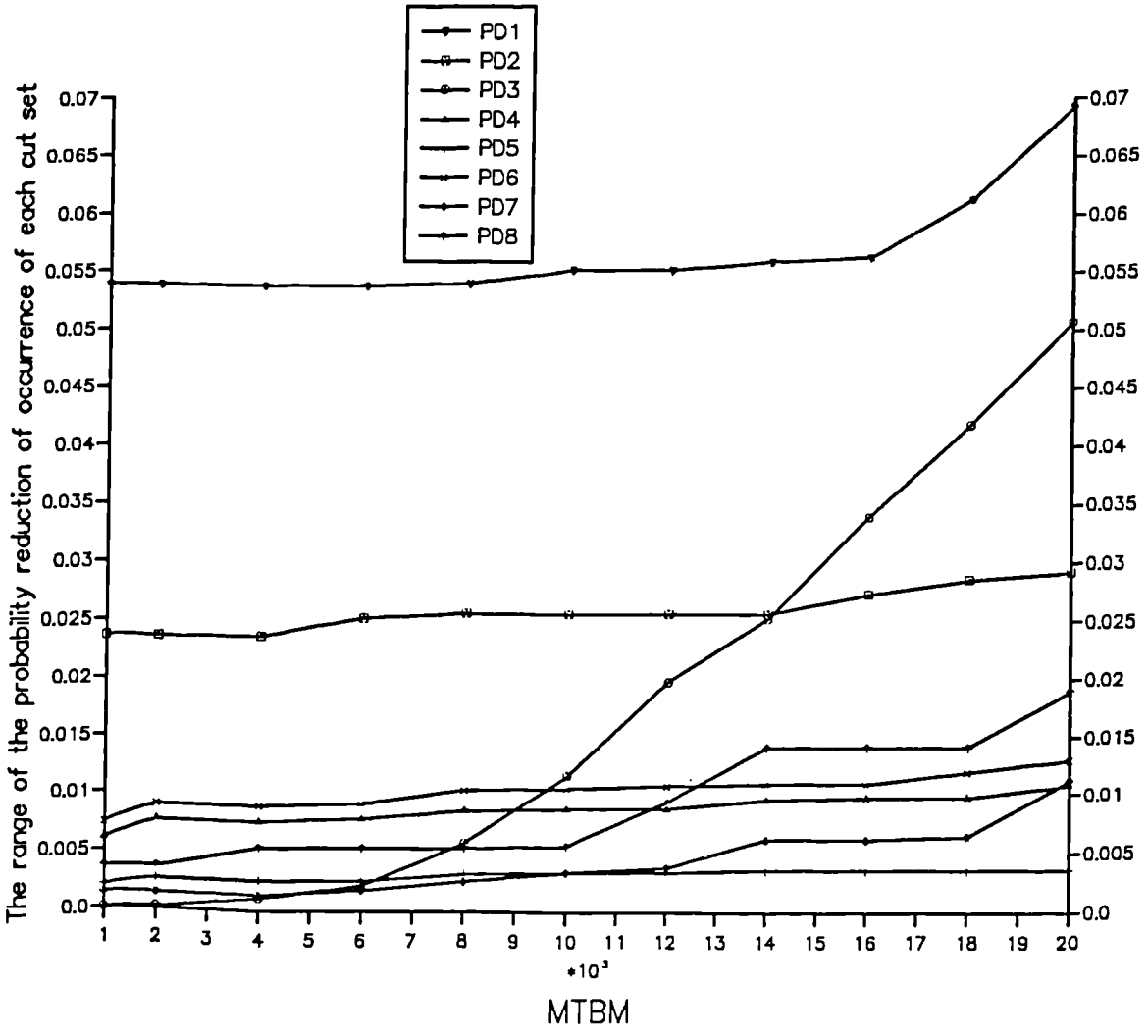


Figure 8.3 The range of the probability reduction of occurrence of each cut set

$$C_{D3} = C_{T2} + C_{L2} + C_{R2} = 640{,}000 \ pounds$$

$$C_{D4} = C_{D5} = C_{D6} = C_{D7} = C_{D8} = C_{T3} + C_{L3} + C_{R3} = 110{,}000 \ pounds$$

$$M_1 = M_2 = M_3 = M_4 = M_5 = M_6 = M_7 = M_8 = 8{,}000 \ pounds$$

8.5.5 Operational Cost Modelling

Assuming that the annual operational cost of this hydraulic hoisting transmission system is 10,000 *pounds*, the daily operational cost $COST_O$ can be obtained by:

$$COST_O = \frac{10000}{365} \ pounds$$

The parameters for the modification of the models of the top event-caused cost, repair cost, maintenance cost and design review cost are assumed and shown in Table 8.4.

Table 8.4 The parameters for the modification of the models

$BT_{R1} = 2$	$BT_{T1} = 5$
$BT_{R2} = 1$	$BT_{T2} = 5$
$BT_{R3} = 2$	$BT_{T3} = 5$
$BT_{R4} = 1$	$BT_{Mi} = 5$
$BT_{D1} = BT_{T1} = 5$	$BT_{D5} = BT_{T3} = 5$
$BT_{D2} = BT_{T1} = 5$	$BT_{D6} = BT_{T3} = 5$
$BT_{D3} = BT_{T2} = 5$	$BT_{D7} = BT_{T3} = 5$
$BT_{D4} = BT_{T3} = 5$	$BT_{D8} = BT_{T3} = 5$

where i = 1, 2, $\cdots$, $\frac{T_{PT}}{X}$

8.5.6 Techno-economic Modelling

Other parameters in the techno-economic model are shown as follows:

$$K_{D1} = K_{D2} = K_{D4} = K_{D5} = K_{D6} = K_{D7} = K_{D8} = K_1 = K_3 = 1$$

$$K_{D3} = K_2 = 2$$

X_{min} = 1000 hr

X_{max} = 20000 hr

All parameters have been given for the *Cost* and *Risk* models of the crane hoist transmission system. The nonlinear *GP* shown in (8.4) can be solved using the Integrated MCDM-Based Decision Support System [8.14][8.21][8.23] written in "*C*" computer language.

8.5.7 Optimisation Results

The optimisation results are shown in Figure 8.4 and discussed as follows:

If only the *Cost* objective is optimised, the minimum *Cost* is equal to 121,631 pounds and the design is located at point 2 as shown in Figure 8.4. In this case, the *Risk* objective is equal to 0.32, *X* or MTBM is equal to 18000 hr, and prime implicants 1 and 3 are required to be eliminated. Elimination of such prime implicants can be made by the use of more reliable components, the provision of protection systems, sensors and alarm systems, or a combination of such measures, as described previously. A detailed study in this area would be necessary to move further in this area.

If only the *Risk* objective is minimised, the minimum *Risk* is equal to 0.10 and the design is located at point 1. In this case, the *Cost* objective is equal to 839,600 pounds, *X* is equal to 1000 hr, and prime implicants 1, 2, 3, 4, 5, 6, 7 and 8 are all required to be eliminated.

Each point in the curve shown in Figure 8.4 is an efficient design with regard to both *Cost* and *Risk* objectives. A design is efficient or Pareto optimal if it is not dominated by any other feasible designs in terms of the two objectives. At point 5, for example, the *Cost* and *Risk* objectives are equal to 262,364 pounds and 0.1082, respectively, *X* is equal to 4241 hr, and all eight prime implicants are required to be eliminated. There is no other design available which could have the *Cost* and *Risk* values lower than 262,364 pounds and 0.1082 simultaneously. At point 6, the *Cost* and *Risk* objectives are equal to 139,516 pounds and 0.1696, respectively, *X* is equal to 10000 hr, and prime implicants 1, 2, 3 and 6 are required to be eliminated.

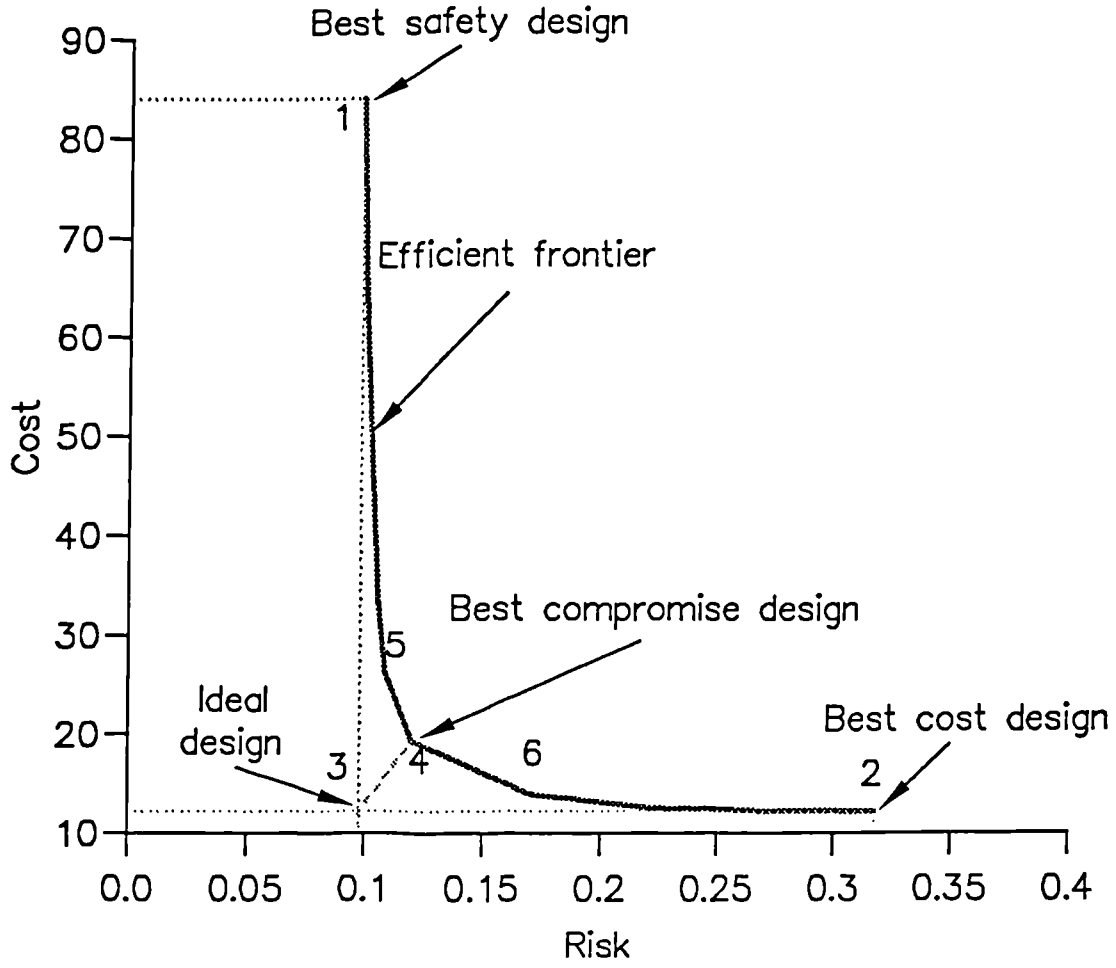


Figure 8.4 The optimisation results

The ideal design is located at point 3 where both the *Cost* and *Risk* objectives are simultaneously minimised. However, such a design is not feasible. Therefore, only compromise designs can be obtained. The best compromise design is located at a point in the frontier, which is nearest to the ideal design point. If the *Cost* and *Risk* objectives are of equal importance, such a best compromise design (i.e. point 4) can be obtained using minimax approach [8.14][8.23]. At point 4, *Cost* and *Risk* are equal to 193,020 pounds and 0.1198, respectively, X (MTBM) is equal to 6269 hr, and prime implicants 1, 2, 3, 4, 6 and 8 are required to be eliminated.

It can be noted, from Figure 8.4, that *Cost* is significantly reduced with a slight increase of *Risk* from point 1 to point 5 in the efficient frontier, and that *Risk* is significantly reduced with a slight increase of *Cost* from point 2 to point 6. These two sections should obviously be avoided in the design. A practical efficient design can be at some point in the section between 5 and 6, depending on the particular requirements on cost and safety to be considered. For instance, if safety is a comparatively important factor, an efficient design may be chosen from the section between points 5 and 4; and if cost is a comparatively important factor, an efficient design may be chosen from the curve between points 4 and 6. Each point corresponds to a fixed design vector V.

From the the above analysis, it is obvious that the optimisation results as illustrated by Figure 8.4 can assist the designer in understanding the problem in hand and making a decision as to what maintenance policies and design review actions should be taken.

8.6. Concluding Remarks

A techno-economic modelling methodology is proposed in this chapter for decision making based on safety analysis. The techno-economic modelling methodology proposed can be used to process the information produced using the safety analysis methodologies developed in Chapters 4, 5 and 6 to construct a bi-criteria techno-economic model. MODM techniques can then be applied to deal with the constructed model. Such a techno-economic modelling methodology provides the safety analyst with a rational tool to make full use of the information produced in safety analysis and to take into consideration both design aspects and maintenance policies simultaneously.

In the illustrative example, there are two competing demands of safety and economy. The decision as to which one is to be stressed may be dependent on the particular

situation in hand. The proposed techno-economic modelling methodology can be used to assist designers in understanding the interaction between safety and economic considerations, so as to balance and best utilise resources to design a large MTO product.

This chapter does not deal with how protection systems, alarm systems and more reliable components are to be added to the system to reduce or eliminate the prime implicants considered in the design review process. This could be a subject of further research. In addition, the following areas are also considered worthwhile for further research:

i. A practical and real "safety case" would help to validate the developed methodology, and realise where improvements can be made, as will be described in Chapter 9.

ii. The extension of the techno-economic modelling methodology to deal with more objectives which may be involved in the design process.

iii. The modification of the techno-economic modelling methodology to taken into account the rearrangement of the system design.

REFERENCES - CHAPTER 8

[8.1] Carpenter S. J., Fleming J., M., *An integrated approach to the safety assessment of offshore production facilities,* APE Asia-Pacific Conference, Perth, Western Australia, November, 1991, 693-704.

[8.2] DeGarmo E. P., Sullivan W. G., Bontadelli J. A., *Engineering economy,* Macmillan Publishing Company, 1989.

[8.3] Department of Energy, *The public inquiry into the Piper Alpha disaster (Cullen Report),* HMSO, ISBN 0 10 113102, 1990.

[8.4] Goss R., *Rational approach to maritime safety,* Transaction of North East Institute of Engineers and Ship Builders", Vol.105, No.3, 97-110.

[8.5] Henley E. J., Kumamoto H., *Probabilistic risk accessment,* IEEE Press, New York, 1992.

[8.6] House of Lords, *Safety aspects of ship design and technology,* Select Committee on Science and Technology, 2nd Report, HL Paper 30-I, February 1992.

[8.7] Hurst N. W., Nussey C., Pape R. P., *Developed and application of a risk assessment tool (RISKAT) in the health and safety executive,* Chem Eng Res Des, Vol.67, July 1989, 362-372.

[8.8] Kriger G., Piermattei E., *Risk analysis applied to offshore platforms during the unpiled installation phase,* 15th Annual OTC, Houston, Texas, May 1983, 9-17.

[8.9] McNichols G. R., *Cost-risk procedures for weapon system risk analysis,* Proceeding of Annual Reliability and Maintainability Symposium, 1981, IEEE, 86-94.

[8.10] NEL, *FMECA of NEI pedestal crane,* Report No. NECL/01, May 1987.

[8.11] Rasmussen M., *Lower maintenance cost through maintenance optimisation in design and operation,* Paper 5, ICMES, 90, Marine Management (Holdings) Ltd, 1990, 53-58.

[8.12] Ruxton T., Wang J., *Advances in marine safety technology applied to marine engineering systems,* Proceeding of First Joint Conference on Marine Safety and Environment, Delft, The Netherlands, June 1992, 421-432.

[8.13] Sen P, Labrie C. R., Wang J., Ruxton T., Chan J., *A general design for safety framework for large Made-To-Order engineering products,* First Newcastle International Conference on Quality and Its Applications, 1-3 Sep 1993; Newcastle. Sponsored by I.Mar.E., Institute of Quality Assurance, et al. 499-505.

[8.14] Sen P., Yang J. B., *A multiple criteria decision support environment for engineering design,* Proceedings of 9th International Conference on Engineering Design, Hague, The Netherlands, August 1993.

[8.15] Sen P., Yang J. B., Wang J., *Bi-criteria Modelling Based Design Methodology for Safety and Cost Optimisation,* Submitted February 1994 to: SARSS'94: Risk Management and Critical Protective Systems, October 1994, Altrincham, Cheshire, UK.

[8.16] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Design Conference, March 7-11, Chicago, 1-12.

[8.17] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), Vol.105, Marine Management (Holdings) LTD, 1993, 21-34.

[8.18] Wang J., Ruxton T., Thompson R. V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, The Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, December 1993, 1-10.

[8.19] Wang J., Ruxton T., Labrie C. R., *Design for safety of the engineering systems with multiple failure state variables,* Accepted March 1994 for Publication by Reliability Engineering and System Safety, (Research Report EDCN/SAFE/RESC/10/1, EDC, October 1991).

[8.20] Wang J., Yang J. B., Sen P., *Techno-economic Modelling for Design and Maintenance Optimisation Based on Safety Analysis,* Submitted March 1994 to Quality and Reliability Engineering International, (Research Report, EDCN/SAFE/RESC/19/1, Engineering Design Centre, February 1994).

[8.21] Yang J. B., *An integrated MCDM-based Decision Making System for Efficient Engineering Design,* Research Report, EDCN/MCDM/PAPERS/3/2, Engineering Design Centre, University of Newcastle upon Tyne, January 1992.

[8.22] Yang J. B., Chen C., Zhang Z.J., *The interactive step trade-off method (ISTM) for multiobjective optimization,* IEEE Transactions on Systems, Man, and Cybernetics, Vol.20, No.3, 1990, 688-695.

[8.23] Yang J. B., Sen P., *An interactive MODM method for design synthesis with assessment and optimization of local utility functions,* presented at the PEDC Seminar on Adaptive Search and Optimization in Engineering Design, Plymouth University, December 1993 (also submitted to European Journal of Operational Research, 1993).

CHAPTER 9

Conclusions and Further Work

SUMMARY

This chapter summarises the results of the research project carried out and indicates where the developed safety analysis methodologies would be of benefit in the "design for safety" process. The areas where further effort is required to improve the developed methodologies are outlined, as those areas are considered suitable for possible further study. Finally, other important topics related to safety analysis methodologies are discussed with reference to further development.

9.1 Conclusions

The previous chapters of this thesis have developed a range of safety analysis methodologies and the reasons behind the development of such methodologies have been explained. The many valid reasons for using the developed safety analysis methodologies in the "design for safety" process of marine and other large MTO products have also been discussed, and will not be repeated here. However, it is necessary to summarise in general terms the developed safety analysis methodologies.

The "design for safety" methodology has been developed in a generic sense to be theoretically applicable to all designs of marine and other large MTO products. Such a

methodology can be used as a basis for the development of various safety analysis methods and decision making procedures for effective use to make "design for safety" more objective, efficient and effective.

The MBRM developed in Chapter 4 can benefit fully from the information produced from FMECA. Since top events of MTO products may not be available from previous accidents and incident reports of similar products and since a complete identification of all failure causes associated with system top events is required, it will be very effective for the developed MBRM to be applied together with FMECA to identify and evaluate risks of MTO products. Risk identification and risk evaluation at a higher indenture level can directly make use of the information produced at lower indenture levels using the methodology incorporating the MBRM and FMECA. Complex interactions of the subsystems of a large MTO product can be considered properly, and system top events and associated causes can be identified with less omissions using this methodology.

The proposed qualitative reasoning and simulation modelling approaches can greatly extend the use of the MBRM. The former has been combined with the MBRM to form a mixed safety modelling methodology. Such a mixed methodology can be used to model large systems for which component input-output relationships are difficult to obtain. Precise Boolean representation descriptions of such systems can easily be obtained using this mixed safety modelling methodology. The simulation modelling approach has been developed to take into account maintenance factors, different distributions of basic failure events, and covert and revealed failures, to estimate safety parameters.

The developed subjective reasoning methodology incorporating fuzzy set modelling and evidential reasoning provides the safety analyst with the flexibility in articulating non-numerical safety data and in assessing the safety of engineering systems for which great uncertainty is involved and failure distributions of variables for use in probabilistic risk analysis are difficult or impossible to obtain.

The proposed techno-economic modelling methodology can make full use of the information produced using FMECA, the MBRM and the proposed simulation models to construct a techno-economic model for decision making purposes. Such a techno-economic modelling methodology provides the safety analyst with a rational tool to incorporate safety into the design process from the initial stages by optimising both design aspects and maintenance policies.

Obviously, it could be time-consuming to conduct safety analysis of complex MTO products using the developed safety analysis methodologies and it may take time to learn how to use such methodologies although today's powerful computers and flexible man-machine interfaces may solve such problems. In addition, common cause failures have not been dealt with using the MBRM. In some circumstances, common cause failures even in higher-order prime implicants may play an important role in safety analysis. Therefore, the MBRM needs to be further investigated to be capable of dealing with common cause failures.

The safety of large MTO products such as offshore topsides is usually affected by process system failures, structure failures, fire, etc. Therefore, design for safety of large MTO products should involve studying all such aspects. However, structural safety and fire safety have not been studied in this thesis. The safety analysis methodologies developed in this thesis are in nature capable of processing and synthesising the structural and fire safety information and the safety information of process systems to obtain comprehensive assessments of MTO artefacts. As will be described in the next section, it is required to apply the developed safety analysis methodologies to a practical MTO product so that the architectural and fire aspects and process systems can be studied together to further modify the developed safety analysis methodologies.

It is believed that modification of such methodologies may extend the use of them. Apart from the required modification discussed above, the other areas required to be investigated further are discussed in section 9.2.

This thesis is not concerned with how alarm systems, sensors, protection systems and more reliable components are designed and provided to reduce or eliminate high risks although such areas are considered to be worthwhile ones for exploration and exploitation in the future.

It is believed that the methodologies developed in this thesis possess enormous potential as valuable aids and effective alternatives in the areas of "design for safety", and will gain increased usage in the design of marine and the other large MTO products. It is also believed that practical applications of these methodologies will result from utilisation by organisations who deal with safety problems with high uncertainty and insufficient safety data. In such cases, the implementation of the developed methodologies could have a highly beneficial effect. In fact, it is widely accepted that any developed safety analysis methodology should preferably be introduced into a

commercially stable environment in order that the applications have the chance to become established in order to prove feasible, otherwise it is more likely that its full potential will not be realised.

9.2 Further Work

9.2.1 Further Work Required to Improve the Developed Safety Analysis Methodologies

The following areas may be worthwhile to be further explored and exploited on the basis of the methodologies developed in this thesis.

- The developed safety analysis methodologies need a sufficiently large and realistic test bed for detailed evaluation. A practical MTO product such as an offshore topside may be taken as a test case to modify and validate the proposed methodologies. Transfer of the technology to industry may then be possible.

- The safety analysis methods outlined in Chapter 3 are required to be studied in more detail regarding data flows and interrelations in order to fully make use of the advantages of each method and to effectively utilise the safety information produced using each method.

- A combination of computer databases, expert system and safety analysis could be used to maximise the safety of large MTO products within both technical and economic constraints.

  A knowledge based expert system may utilise the results produced using the methodologies developed in this thesis, to arrive at design rules that provide guidance on the design changes that can be made to improve safety. Such an expert system may be designed to interact with safety analysis using the MBRM and the qualitative reasoning approach to deduce and determine system behaviour in order to take effective design actions.

- Further studies in the development of more flexible and objective bottom-up approaches should be carried out to face the challenge imposed by the increasing complexity of large MTO products and the increasing public concern for safety. Further studies of combining bottom-up and deductive top-down safety analysis

methods should also be carried out to achieve more realistic, convenient and effective safety analysis.

- For the MBRM and the qualitative reasoning approach, further studies may be required in the following areas:

    i. Integrate more aspects of these two approaches with other formal safety analysis methods.

    ii. Construct a module library so that given the description of a system its component models can directly be obtained by referring to the library and the system behaviour description can then be easily obtained by studying the interrelations of the components and applying the rules developed in Chapters 4 and 5.

- As far as computer simulation is concerned, it is believed that the application and integration of simulation techniques to the established safety analysis modelling methodologies described in this thesis, including the construction of simple and flexible simulation models, will need to be developed further.

- For the subjective reasoning methodology developed in Chapter 7, further studies may beneficially be carried out in the following areas:

    i. Modification of the developed methodology. This may be achieved by applying this methodology to a reasonably sizable practical test case.

    ii. Development of a decision making approach incorporating evidential reasoning [9.14] to process the information produced using the methodology, to rank the design proposals of the system and to make design decisions. Multiple objectives represented by the methodology may be dealt with using formal decision making approaches.

    iii. The decision making analysis may be further extended to combine evidential reasoning and formal Multiple Objective Decision Making (MODM) tools [9.13] to study the effect of a design review on system safety, and to optimise design aspects and maintenance activities.

- The techno-economic methodology proposed in Chapter 8 may be modified to take into account the initial cost of a MTO product, to deal with the rearrangement of

the system design and perhaps to optimise more objectives such as operability. Such a modification may provide a practical tool with which design decisions can be made effectively in the design process.

9.2.2 **Other Further Work**

In author's view, further work required in the areas which are related to the safety analysis methodologies developed in this thesis can be described as follows:

- **Human behaviour**

  The scope and precision of engineering modelling have increased in the pursuit of safety. One area in particular has received scant attention from engineers, given its importance: human behaviour. It is realised that human beings are crucial components in most MTO products, and they are also, historically, the most unreliable [9.12].

  Human error is one of the major sources of accidents — not from malicious intent, but from ignorance, overstress, misinterpretation and fatigue, among other factors [9.12]. Human error is now receiving increasing attention, particularly from industries concerned with the design and use of marine and other large MTO products.

  Although human error can be reduced by the introduction of safety warning devices such as sensors and alarms for the timely detection of the condition as described in Chapter 3, it may also be greatly altered by better education and training since safety is very much a matter of attitude and a way of thinking, and also by better design. Far more attention is required to devote to studying human behaviour in the future, especially in the areas of:

  i. Human performance prediction.

  ii. Performance analysis of man-machine systems.

  iii. Reliability allocation to human performance.

- **Reliability data**

  Quantitative risk assessment of large MTO products is frequently inhibited by the lack of representative failure and repair statistics [9.1]. It has been realised that the

collection of failure and repair data of components and systems, already practised in various industries, needs to be more widespread. Individual companies should be persuaded to release their data to a general pool and this larger quantity of data should be available for the benefit to all industries. More effort should be devoted to the reliability data management systems to collect failure and repair data in order to estimate and evaluate system safety more confidently and reliably.

- **Education**

  For many engineers, design education is oriented towards using prescriptive regulations which are applied in a systematic and often routine way. However, it is realised that the shift to more goal-setting regulations may offer more explicit consideration of safety and a clear understanding of the underlying principles involved in design.

  Although such a shift may make engineering design more difficult, it will give much more rewarding results, particularly for the design of marine and other large MTO products, which involves the broadest range of engineering skills and requires a great deal of innovation.

- **Observability and controllability**

  The concepts of observability and controllability used in control engineering may beneficially be introduced to safety analysis. Such a study may produce a general framework with which the observability and controllability of each failure variable of a MTO product can be determined in order to monitor and reduce high risk areas. Such a framework may also be used to optimally determine where alarm systems, sensors and protection systems are required to make all serious failure events observable and controlled.

REFERENCES - CHAPTER 9

[9.1] Moss T. R., Strutt J. E., *Data sources for reliability design analysis,* Proc Instn Mech Engrs, Vol 207, 13-19.

[9.2] Ruxton T., *Safety analysis required for safety assessment in the shipping industries,* Presented to NEVJB, Institute of Marine Engineers and the Royal Institute of Naval Architects, December, 1992.

[9.3] Ruxton T., Wang J., *Advances in marine safety technology applied to marine engineering systems,* Proceeding of First Joint Conference on Marine Safety

and Environment, Delft, The Netherlands, June 1992, 421-432.

[9.4] Sen P., Labrie C. R., Wang J., Ruxton T., Chan J., *A general design for safety framework for large made-to-order engineering products,* Proceeding of First Newcastle International Conference on Quality and Its Applications, Newcastle, September 1993, 499-505.

[9.5] Wang J., Ruxton T., *Design for safety of Made-To-Order (MTO) products,* ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12

[9.6] Wang J., Labrie C. R., Ruxton T., *Computer simulation techniques applied to the prediction and control of safety in maritime engineering,* Institute of Marine Engineers, Transactions (C), Vol.105, 1993, 21-34.

[9.7] Wang J., Ruxton T., Labrie C. R., *Design for safety of marine engineering systems with multiple failure state variables",* Accepted for Publication by Journal of Reliability Engineering and System Safety (Research Report EDCN/SAFE/RESC/10/1, EDC, October 1991).

[9.8] Wang J., Sen P., Thompson R. V., *A mixed modelling approach for safety analysis,* Proceeding of the SRA - Europe 4th Conference: European Technology & Experience in Safety Analysis and Risk Management, Rome, 18 - 20 October, 1993, 7 p.

[9.9] Wang J., Ruxton T., Thompson R. V., *Failure analysis of Made-To-Order (MTO) products,* ASME Publication, 93-WA/DE-8, Presented at the Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, December 1993, 1-10.

[9.10] Wang J., Yang J. B., Sen P., *Safety analysis and synthesis using fuzzy set modelling and evidential reasoning,* Accepted July 1994 for Publication by Reliability Engineering and System Safety.

[9.11] Wang J., Yang J. B., Sen P., *Techno-economic modelling for design and maintenance optimisation based on safety analysis,* Submitted March 1994 to Quality and Reliability Engineering International, (Research Report, EDCN/SAFE/RESC/19/1, Engineering Design Centre, February 1994).

[9.12] Wolfram J., *Safety and risk: models and reality,* Proc Instn Mech Engrs, Vol 207, 3-11.

[9.13] Yang J. B., *An evidential reasoning approach for multiple attribute decision making with uncertainty,* Transactions on Systems, Man, and Cybernetics, Vol.23, No.6, 1993.

[9.14] Yang J. B., Sen P., *A hierarchical evaluation process for multiple attribute design selection with uncertainty,* Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE-93), Gordon and Breach Science Publishers, 1993, 484-493.

[9.15] Yang J. B., Sen P., *Evidential reasoning based hierarchical analysis for design selection of ship retro-fit option",* Third International Conference on Artificial Intelligence in Design, Lausanne, Switzerland, 15-18 August 1994.

[9.16] Yang J. B., Sen P., *An interactive MODM method for design synthesis with assessment and optimization of local utility functions,* Seminar on Adaptive Search and Optimization in Engineering Design, Plymouth University, December 1993 (also submitted to European Journal of Operational Research, 1993).

[9.17] Yang J. B., *An integrated MCDM-based Decision Making System for Efficient Engineering Design,* Research Report, EDCN/MCDM/PAPERS/3/2, Engineering Design Centre, University of Newcastle upon Tyne, January 1992.

APPENDIX 1

Publications Arising from the Work

Refereed papers published and waiting to be published

1. Ruxton T., Wang J., *Advances in Marine Safety Technology Applied to Marine Engineering Systems*, Proceeding of First Joint Conference on Marine Safety and Environment, Delft, The Netherlands, 1-5 June 1992, 421-432.
2. Wang J., Ruxton T., *Design for Safety of Made-To-Order (MTO) Products*, ASME Publication, 93-DE-1, 1993 National Engineering Design Conference, Chicago, March 1993, 1-12.
3. Wang J., Labrie C. R., Ruxton T., *Computer Simulation Techniques Applied to the Prediction and Control of Safety in Maritime Engineering*, Institute of Marine Engineers, Transactions (C), Vol.105, Marine Management (Holdings) Ltd, London, 1993, 21-34.
4. Sen P., Labrie C. R.., Wang J., Ruxton T., *A General Design for Safety Framework for Large Made-To-Order Engineering Products, Proceeding of First Newcastle International Conference on Quality and Its Applications*, Newcastle, 1-3 September, 1993, 499-505.
5. Wang J., Ruxton T., Thompson R. V., *Failure Analysis of Made-To-Order (MTO) Products*, ASME Publication, 93-WA/DE-8, Presented at the Winter Annual Meeting on Failure Analysis/Failure Prevention, New Orleans, Louisiana, 29 November-3 December, 1993, 1-10.
6. Wang J., Sen P., Thompson R. V., *A Mixed Modelling Approach for Safety Analysis*, Proceeding of the SRA - Europe 4th Conference: European Technology & Experience in Safety Analysis and Risk Management, Rome, 18 - 20 October, 1993, 7pp.
7. Wang J., Ruxton T., Labrie C. R., *Design for Safety of Marine Engineering Systems with Multiple Failure State Variables*, Accepted March 1994 for Publication by Reliability Engineering and System Safety.
8. Wang J., Yang J. B., Sen P., *Safety Analysis and Synthesis Using Fuzzy Set Modelling and Evidential Reasoning*, Accepted July 1994 for Publication by Reliability Engineering and System Safety.

Workshop papers

9. Ruxton T., Wang J., *Safety Prediction Model for a Ship Steering Gear, Presented at the* Workshop on Safety Analysis and Techniques Required for Formal Safety Assessments in the Shipping and Offshore Industries, Paper 12, 16-18 December 1992, London, Sponsored by I.Mar.E., et al., 30 p.
10. Wang J., *"Design for safety: a risk identification and risk estimation tool"*, Presented at the Design for Safety Seminar, University of Newcastle upon Tyne, 13 July 1994, Sponsored by Tyneside Training and Enterprise Council Ltd, 40 p.

Paper in hand

11. Wang J., Yang J. B., Sen P., *Techno-economic Modelling for Design and Maintenance Optimisation Based on Safety Analysis*, Submitted September 1994 to: IEEE Transactions on Reliability, (Research Report, EDCN/SAFE/RESC/19/1, Engineering Design Centre, University of Newcastle upon Tyne, February 1994).

APPENDIX 2

MODSIM II™: The Language for Object-Oriented Programming

MODSIM II™ is a modular, object-oriented, strongly typed, block-structured simulation language. The characteristics of *MODSIM II™* are described as follows [A2.1]:

— **Modular:** *MODSIM II™* programs may be divided into "modules", each of which can be stored in a separate file.

— **Object-oriented:** An object is an encapsulation of a data record which describes the state of the object and the associated procedures, called methods, which describe the object's behaviour.

— **Strongly-typed:** Every expression, assignment statement and parameter is type checked at compile time for consistency.

— **Block-structured:** A block is made up of declarations and executable statements. The block-structured feature of this language is that the scope or visibility of variables is restricted to the block in which they are declared and any subsidiary blocks.

— **Simulation:** Simulation capabilities are provided in library modules. The modules provide direct support for all capabilities needed to program discrete event simulation models.

Structure of *MODSIM II™* programs

Most large programs written in *MODSIM II™* consist of a number of modules in separate files. Modular structure allows programs to be constructed from library modules. Any part of a program can import types, variables, constraints and procedures from library modules as needed. There are three types of modules MAIN, DEFINITION, and IMPLEMENTATION, each of which is named with a identifier and can be compiled separately to facilitate program maintenance and to reduce

development time. Any constant, type, variable or procedure declared in a DEFINITION module is implicitly visible in the accompanying IMPLEMENTATION module. Constants, types, variables, procedures and objects defined in a DEFINITION module can be imported to other DEFINITION modules, IMPLEMENTATION modules or MAIN modules.

The program structure of *MODSIM II™* is similar to that of the languages such as Algol, Pascal, Modula-2 or Ada. A typical structure of a simple *MODSIM II™* program is shown as follows:

```
MAIN MODULE MODSIM_Example;
    FROM Definition_Example IMPORT Object_Example;
    ... ...;
CONST
    ... ...;
TYPE
    ... ...;
VAR
    ... ...;
PROCEDURE Procedure_Example();
    ... ...;
END PROCEDURE;

BEGIN           { main program code starts here }
    Procedure_Example;
    ... ...;
END MODULE.

DEFINITION MODULE Definition_Example;
TYPE
    Object_Example = OBJECT;
        ... ...;
    END OBJECT;
```

```
        ... ...;
END MODULE.

IMPLEMENTATION MODULE Definition_Example;
OBJECT
  Object_Example;
        ... ...;
END OBJECT;
        ... ...;
END MODULE.
```

Object-Oriented Programming (OOP)

Objects in *MODSIM II™* are dynamically allocated data structures which add several new programming capabilities to the programmer's toolbox. Such capabilities include:

— **Encapsulation of data and code:** Tying together the fields which describe the object's state with the procedures (called methods) which define its behaviour. Controlling access to the fields.

— **Inheritance:** New types can be defined based on the existing types. Each descendant in the hierarchy can add its own fields and method definitions to those of its ancestors.

— **Message passing:** An object's method is invoked by sending a message to the object asking it to perform a specific method.

— **Polymorphism:** Allowing different object types in a hierarchy to share the same method name but provide their own definitions.

— **Hierarchical types:** A descendant is type compatible with any of its ancestors.

Simulation

MODSIM II™ has powerful and flexible capabilities for dealing with discrete-event simulation. Each object is capable of carrying on multiple and concurrent activities, each of which can elapse simulation time. The activities can operate autonomously or

they can synchronise their operation. Any or all activities of an object can be interrupted if necessary.

In the *MODSIM II™* simulation language, objects can be selectively added to or removed from a group which contains objects queuing for a resource or a series of events scheduled to happen at a specific time.

Pseudo-random number generators are available in *MODSIM II™*.

Input/Output

There are a number of ways in which to do input and output in *MODSIM II™*. A standard library module, which contains the stream I/O object called SteamObj, is provided in *MODSIM II™*. This object allows the user to do formatted stream oriented input and output to other devices and files.

Graphics

SIMGRAPHICS II is a graphical tool kit built on *MODSIM II™*. Using *SIMGRAPHICS II*, animation, presentation graphics and graphical user interfaces can be easily incorporated into a *MODSIM II™* program.

REFERENCE - APPENDIX 2

[A2.1] CACI Products Company, *MODSIM II™: The Language for Object-Oriented Programming (OOP) and SIMGRAPHICS II™, Reference Manual,* La Jolla, USA, May 1991.

APPENDIX 3

Representation of Piecewise Linear Functions

An optimisation problem (OP) may generally be represented as follows [A3.1]:

$$OP \begin{cases} \max & f(X) \\ s.t. & X \in \Omega \end{cases} \tag{A.1}$$

$$\Omega = \left\{ X \;\middle|\; \begin{array}{l} g_k(X) \le 0 \quad k=1, \cdots, m_1 \\ h_j(X) = 0 \quad j=1, \cdots, m_2 \\ X_o \le X \le X_N \end{array} \right\}$$

where X is a design variable, $f(X)$ is a piecewise linear objective function, and $g_k(X)$ and $h_j(X)$ are nonlinear inequality and equality constraint functions.

Suppose the interval (X_o, X_N) is divided into N sections, and X_{i-1} and X_i are the end points of the ith section. $f(X)$ is a linear function of X in the interval (X_{i-1}, X_i) and can be represented by the following equivalent form [A3.1]:

$$f(X) = \sum_{i=1}^{N-1} \alpha_i |X - X_i| + \beta X + \gamma \quad \text{for } X \in \Omega \tag{A.2}$$

where

$$\alpha_i = \frac{1}{2}(t_{i+1} - t_i), \;\; \beta = \frac{1}{2}(t_1 + t_N) \text{ and } \gamma = \frac{1}{2}(s_1 + s_N) \tag{A.3}$$

t_i and s_i are the slope and the y-intercept of the ith section of the piecewise linear function $f(X)$, respectively.

$$t_i = \frac{f(X_i) - f(X_{i-1})}{X_i - X_{i-1}} \tag{A.4}$$

$$s_1 = f(X_0) - t_1 f(X_0); \quad s_N = f(X_N) - t_N f(X_N) \tag{A.5}$$

For instance, Figure A.1 shows a piecewise linear function $f(X)$ with the feasible interval of X being divided into three equal sub-intervals.

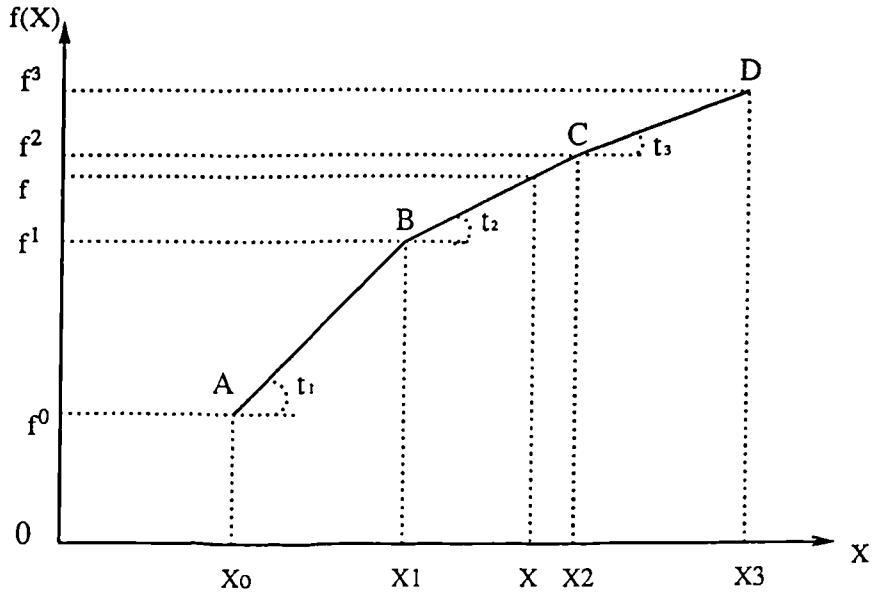


Figure A.1 A Piecewise Linear Function

$f(X)$ can be calculated by

$$f(X) = \frac{1}{2}\left\{f^0 + t_1(|X-X_0|-|X-X_1|) + t_2(|X-X_1|-|X-X_2|) + t_3(|X-X_2|-|X-X_3|) + f^3)\right\}$$

$$= \frac{1}{2}\left\{\left[(t_2-t_1)|X-X_1| + (t_3-t_2)|X-X_2|\right]+\left[(t_1+t_3)X\right]+\left[(f^0-t_1X_0) + (f^3-t_3X_3)\right]\right\}$$

Let's introduce the following auxiliary variables a_i^+ and a_i^-,

$$a_i^+ = \frac{1}{2}\left\{|X - X_i| + (X - X_i)\right\} \text{ and } a_i^- = \frac{1}{2}\left\{|X - X_i| - (X - X_i)\right\} \qquad \text{(A.6)}$$

Then $f(X)$ can be represented by

$$f(X) = \sum_{i=1}^{N-1} \alpha_i (a_i^+ + a_i^-) + \beta X + \gamma \quad \text{for } X \in \Omega \qquad \text{(A.7)}$$

under the restrictions

$$a_i^+ - a_i^- = X - X_i;\ \ a_i^+ \times a_i^- = 0;\ \ a_i^+, a_i^- \geq 0, \quad i=1, \cdots, N-1 \tag{A.8}$$

The problem *OP* may then be obtained by solving the following auxiliary goal programming (*GP*) problem

$$GP \begin{cases} \max\ f(X) = \sum_{i=1}^{N-1} \alpha_i (a_i^+ + a_i^-) + \beta X + \gamma \\ s.t.\ \ X \in \Omega \\ \qquad X - a_i^+ + a_i^- = X_i \quad i=1, \cdots, N-1 \\ \qquad a_i^+ \times a_i^- = 0;\ \ a_i^+, a_i^- \geq 0 \quad i=1, \cdots, N-1 \end{cases} \tag{A.9}$$

REFERENCE - APPENDIX 3

[A3.1] Yang J. B., Sen P., *Preference modelling by estimating local utility functions for multiobjective optimization,* Accepted 1994 by European Journal of Operational Research.