

METHODOLOGY FOR COMPUTER AIDED FUZZY
FAULT TREE ANALYSIS

CHY. MD. REFAUL FERDOUS



METHODOLOGY FOR COMPUTER AIDED FUZZY FAULT TREE ANALYSIS

BY

CHY. MD. REFAUL FERDOUS © B.Sc. Engg.

A thesis

submitted to the school of Graduate Studies

in partial fulfillment of the requirements for the degree of

MASTER OF ENGINEERING

**FACULTY OF ENGINEERING AND APPLIED SCIENCE
MEMORIAL UNIVERSITY OF NEWFOUNDLAND**

July, 2006
St. John's, Newfoundland, Canada



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 978-0-494-30501-0

Our file Notre référence

ISBN: 978-0-494-30501-0

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.


Canada

Abstract

Process facilities are well known for unplanned chemical emission, toxic release, fire and explosion and operational disruption. These incidents have the potential to cause an industrial accident and environmental damage. From the investigation of all major accidents, it is apparent that most industrial accidents can be avoided or restricted with a systematic risk analysis and safety management strategy. An effective risk analysis strategy always gives preference to minimizing the risk of a process facility at its design stages.

Probabilistic risk assessment (PRA) is a comprehensive, structured and logical method for identifying and assessing risks of complex process systems. It uses fault tree analysis (FTA) as a tool to identify basic causes leading to an undesired event, to represent logical dependency of these basic causes in leading to the event, and finally to calculate the probability of occurrence of this event. Probability data estimation, and large and complex fault trees, are challenging aspects of FTA as applied to process facilities.

Quantitative analysis of a fault tree for a process system requires a fault tree and the system components (basic events) failure data. Sometimes or always it is difficult to have an exact estimation of the failure rate of individual components or the probability of occurrence of undesired events due to a lack of sufficient data. Further, due to

imprecision in basic failure data or the data sufficiency the overall analysis of a fault tree may be questionable. To avoid such conditions, a fuzzy approach may be used with the FTA technique. This reduces the ambiguity and imprecision arising out of the subjectivity of the data.

Fault tree construction for a process facility must accommodate for a wide variation in components, process operations and control mechanisms. It is more scientific to analyze such a large and complex fault tree through proper sub-divisions of the tree. A proper modularization technique (sub-division) can sub divide a tree into its equivalent sub trees and then analyze it for the process facility.

This work is focused on developing a methodology of a fuzzy based computer-aided fault tree analysis tool. The central idea of this methodology is to adopt a suitable algorithm for moduling (sub-dividing) a large and complex fault tree and then evaluate it by using the fuzzy approach. This methodology uses a systematic approach of fault tree development, fault tree modularization, minimal cut sets determination, fuzzy probability analysis, and fuzzy based sensitivity analysis of a system for achieving its objectives. Besides developing a methodology for computer- aided FTA, this study also proposes a procedure of fuzzy approach for the uncertainty analysis, which is used for comparing error robustness of fuzzy FTA and conventional FTA.

Acknowledgements

I would like to express my deepest gratitude to my advisors, Dr. Faisal Khan, Dr. Brian Veitch and Dr. Paul R. Amyotte. It has been my good fortune to have the opportunity of working with them. I want to thank them not only for their financial support but also for their concern and support, whenever I met difficulties. I will never forget their remarkable help of encouraging a student to persistently focus on research work, draft papers and lessons of writing technical paper, which form a confidence of a new researcher.

I am also deeply grateful for the financial support of The Natural Sciences and Engineering Research Council (NSERC) and the School of Graduate Studies, Memorial University. Further, a special thanks to the Faculty of Engineering and Applied Science, without its resources and administrative help it is not possible to pursue my Master's degree at Memorial University. In addition, I am also grateful to the writing center of Memorial University for checking the entire thesis.

I want to express my sincere appreciation to Md. Moshrraf Hossain, Shakila Ibrahim and everyone in St. John's, who gave me mental support and extra care when I was in need. My endless gratitude towards my parents, bothers and sister for unbound love, faith, inspiration, support in my graduate school career.

And finally, looking back over my two years stay at Memorial University, I have received so much help from so many people. This thesis would not be possible without the contributions of these people. Specially, I am grateful to my friends: Shibly Rahaman, Wasimul Bari, Arifujjaman, Jenifar canning, Alan, Shakil Ahmed and Shohag Kabir for their moral support and help. They also have made my life here more joyful and happy.

Nomenclatures

Symbols

s	Hypothetical scenario
c	Estimated consequence(s)
f	Estimated frequency
G_1, \dots, G_n	Gate events of FTA
BE_1, \dots, BE_n	Basic event of FTA
K_1, K_2, \dots, K_n	Minimal cutsets of FTA
n	Total number of minimal cutsets
N	Total number of random samples
$F_i(t)$	Probability of a basic event
$P_{(T)}$	Top event probability
μ	Membership function of a fuzzy set
\tilde{P}_{BE_i}	Fuzzy Probability of basic events
$\underline{\Delta}$	Representation of a trapezoidal fuzzy set
P_{iA}, P_{iB}	The left-hand bounds of trapezoidal set
P_{iC}, P_{iD}	The right-hand bounds of trapezoidal set
$\mu_{\tilde{P}_{BE_i}}(p)$	Membership grade of basic event fuzzy set

\tilde{p}_T^{AND}	Fuzzy top event probability of AND gate
\otimes	Multiplication of two fuzzy set
\tilde{p}_T^{OR}	Fuzzy top event probability of OR gate
$\tilde{C}_1, \tilde{C}_2, \dots, \tilde{C}_n$	Fuzzy Probabilities of Minimal Cutsets
\tilde{P}_T	Top event fuzzy probability,
$P_{A(T)}, P_{B(T)}$	The left-hand bounds of top event trapezoidal fuzzy set
$P_{C(T)}, P_{D(T)}$	The Right-hand bounds of top event trapezoidal fuzzy set
$M(P_T)$	Most Likely fuzzy Top event probability,
$\mu_{\tilde{P}_T}$	Membership grade of fuzzy Top event probability
P_T	Top event probability with Basic event
P_{Ti}	Top event probability without Basic event
$V(P_T, P_{Ti})$	Fuzzy Improvement Index
I_{ci}	Probability of cutsets importance
Q_j	Fuzzy probability of cutsets frequency
Q_0	Most likely top event probability.
μ'	Location Parameter
α	Percentage level of error in basic events
\tilde{Q}	Median value of basic event probability
σ	Scale parameter

Abbreviations

AIChE	American Institute of Chemical Engineer
BE	Basic Event
CC	Closeness Checking
BDD	Binary Decision Diagram
ETA	Event Tree Analysis
FE	First Element
FTA	Fault Tree Analysis
FV	Fussel-Vesely
FWI	Fuzzy Weighted Index
GE	Gate Event
GUI	Graphical User Interface
IM	Intermediate Event
HAZOP	Hazard and Operability Study
HSE	Human Safety Executive
KHIC	Kohda, Henley, and Inoue Comprehensive method
LCC	Local Combination Checking
MOCUS	Method of Obtaining CUt Sets
MICSUP	Minimal Cutsets, UPward
MCSs	Minimal CutSets
NOCGE	Number of Connecting Gate Event
PRA	Probabilistic Risk Assessment
PROFAT	PRObabilistic FAult Tree
PC	Possibility Checking
QRA	Quantitative Risk Analysis
VOC	Volatile Organic Compound

Thesis Contents

Abstract	ii
Acknowledgements	iv
Nomenclatures	v
List of Figures	xii
List of Tables	xiv
Chapter 1 Introduction	1
1.1 Risk analysis for process facility	1
1.2 Significance of risk analysis	2
1.3 Risk analysis methodology	4
1.4 Fault tree analysis (FTA)	6
1.4.1 FTA fundamentals	7
1.4.2 Some basic definitions and concepts of FTA	8
1.5 Statement of the problem	10
1.6 Objectives of present work	11
1.7 Organization of the thesis work	12

Chapter 2 Methodology for Computer-aided FTA	14
2.1 FTA for process facility	14
2.2 Overview of available FTA tools	21
2.3 Procedure for developing FTA methodology	18
2.4 Features of current methodology	25
 Chapter 3 Fault Tree Development	 26
3.1 Basic elements and symbols used in fault tree construction	26
3.2 Fault tree construction	30
3.2.1 Rules for fault tree construction	31
3.3 Illustrative example of a fault tree construction	34
 Chapter 4 Fault Tree Evaluation	 36
4.1 Qualitative evaluation	36
4.1.1 Fault tree modularization	39
4.1.2 Modularization algorithm for computer-aided FTA	41
4.1.3 Minimal cutsets determination	42
4.1.4 Integrated algorithm for MCSs determination	46
4.1.5 Illustrative example for qualitative evolution of fault tree	47
4.2 Quantitative evaluation	51

4.2.1 Fuzzy set fundamentals and its application on FTA	54
4.2.1.1 Fuzzy probability	55
4.2.1.2 Fuzzy arithmetic operation	56
4.2.2 Fuzzy Based Probability Analysis	58
4.2.3 Sensitivity analysis	63
Summary	65
 Chapter 5 Case Study and Uncertainty Analysis	 66
5.1 A case study of proposed methodology	66
5.1.1 System descriptions and hazard identification	67
5.1.2 Fault tree development	67
5.1.3 Qualitative evaluation	69
5.1.4 Quantitative evolution	71
5.1.5 Sensitivity analysis	72
5.2 Uncertainty analysis	74
5.2.1 Conventional probability approach	75
5.2.2 Fuzzy approach	77
Summary	79

Chapter 6 Results and Discussion	81
6.1 Fault tree analysis (FTA)	81
6.2 Comparative study	82
6.1.1 Comparison using methodology	82
6.1.2 Comparison using results of FTA	83
6.1.3 Comparison using Uncertainty analysis	85
Summary	86
 Chapter 7 Conclusions and Future Work	 87
7.1 Conclusions	88
7.2 Future work	89
 References	 91
 Appendix A	 99
 Appendix B	 103
 Appendix C	 106

List of Figures

Figure 1.1 - Risk analysis methodology for process facility	2
Figure 2.1 - Operational steps for FTA (AIChE, 2000)	11
Figure 2.2 - Algorithm of FTA tool	12
Figure 2.3 - Architecture of propose methodology for Fuzzy based FTA tool	27
Figure 3.1 - Fundamental structural diagram of fault tree	29
Figure 3.2 - Standard fault tree symbols	30
Figure 3.3 - Process block diagram of illustrative example	30
Figure 3.4 - Fault tree diagram of illustrative example	33
Figure 3.6 - Rule Network for causes and consequences	35
Figure 4.1a - Original fault tree	40
Figure 4.1b - Modularized Original fault	44
Figure 4.2 - Algorithm for MCSs determination	45
Figure 4.3 - Steps wise process of KHIC algorithm	53
Figure 4.4 - Fuzzy model for quantitative evaluation of FTA	55
Figure 4.6 - 'AND' Gate	40
Figure 4.7 - 'OR' Gate	44

Figure 4.8 - Trapezoidal representation of probability value “around 0.1”	45
Figure 4.9 - Trapezoidal representation of probability value “around 0.6”	53
Figure 4.10 - Fault tree example	55
Figure 5.1 - Fault tree diagram of the case study in the GUI	68
Figure 5.2 - Connection list of gate events and basic events for the fault tree	70
Figure 5.3 - Obtained modules for the fault tree	70
Figure 5.4 - Fuzzified data of basic events	72
Figure 5.5 - Source uncertainty in risk analysis of process facility	75
Figure 5.6 - Uncertainty analysis model for fuzzy FTA	78
Figure 6.1 - Error robustness of fuzzy FTA and conventional FTA	90

List of Tables

Table 3.1 - Fault tree event symbols	45
Table 3.2 - Fault tree gate symbols	46
Table 4.1 - Hierarchy of gate events	48
Table 4.2 - Connection list and attributes	57
Table 4.3 - Boolean Matrix transformation for MCSs determination	58
Table 5.1 - Name of the basic event and their notifications	68
Table 5.2 - Name of the top event (TE) and intermediate event (IM _i)	69
Table 5.3 - Minimal cutsets for the modules	70
Table 5.4 - Minimal cutsets for the fault tree	71
Table 5.5 - Fuzzy top event probability estimation for case study	72
Table 5.6 - FWI for different events	73
Table 5.7 - Cutsets importance for all MCSs	73
Table 5.8 - Location Parameter for Basic events	76
Table 5.9 - Scale Parameter of log normal distribution	77
Table 5.10 -Error robustness of Fuzzy approach and conventional probability approach	79
Table 6.1 - FTA methodology used in existing software packages and in the current work	83
Table 6.2 - Results obtained for case study using different approaches	84

Chapter 1

INTRODUCTION

1.1 RISK ANALYSIS FOR PROCESS FACILITY

In general, risk associated with an event can be defined as the probability of environmental damage, economic loss or human injury, in terms of both the incident's likelihood and the magnitude of the injury, damage, or loss.

CPQRA (Chemical Process Quantitative Risk Analysis) defines risk as a function of probability or frequency of a particular accident scenario, as well as its consequences (AIChE, 2000).

$$\text{Risk} = F(s, c, f)$$

Where s = hypothetical scenario, c = estimated consequence(s), and f = estimated frequency.

According to Kaplan and Garrick (Kaplan, et. al., 1981), risk of a process system is a set of scenarios, each of which has a probability and a consequence.

Risk analysis is a systematic approach, which gathers and integrates all the information about scenarios, frequencies, and consequences of an activity. This is an important part of the risk assessment process that identifies the basic causes that can lead to an accident by developing casual relations between the scenarios, frequencies and consequences of a risk. This casual relation of a risk assessment model acquires all

information about a system and gives an overview of the decision making process for reducing the probability of an accident and improving the system design of the risk management process (Ljungquist, 2003). The risk analysis or risk assessment for a process facility or system is done by the chronological steps shown in Figure 1.1.

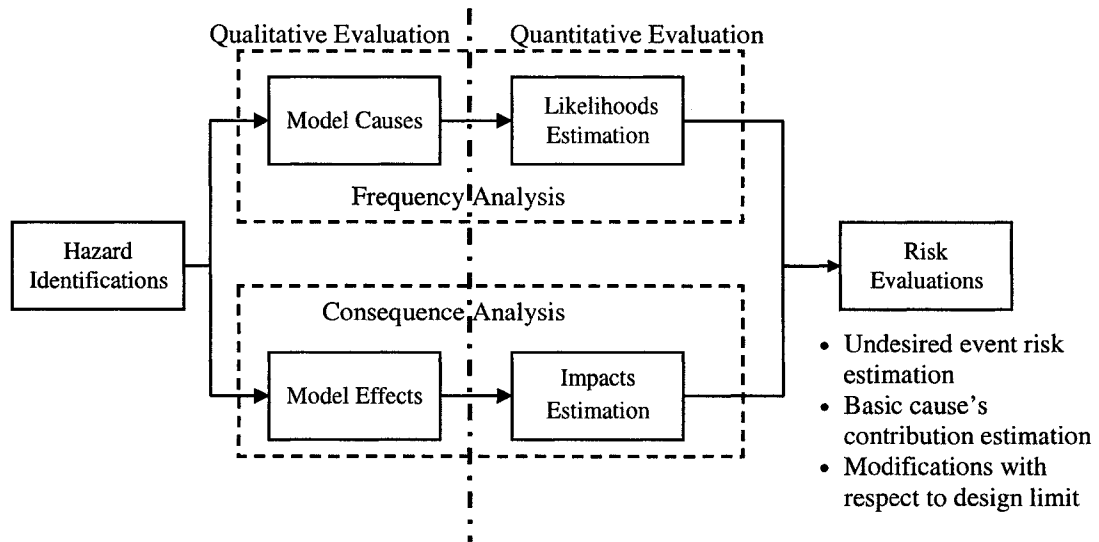


Figure 1.1: Risk assessment methodology for process facility

1.2. SIGNIFICANCE OF RISK ANALYSIS

System safety and reliability are the main parameters to ensure system design, development, and operation for a process facility. It is generally preferred to use risk analysis process for estimating the risk measuring parameters of a process or operation system. These quantitative or qualitative risk parameters enhance the decision task for reducing the different types of major or minor risk incidents probabilities occurring in a process facility or offshore operation system. A study by HSE (1996) and Mansfield et al. (1996a) described that around 80% of industrial accidents have occurred from major or minor risk incidents in a process operation system. The potential sources of these

incidents include riser or process leaks, fires, explosions, pipeline ruptures, vessel ruptures, chemical releases and design faults of a system (Pula, 2005). Some Examples of industrial accidents that have occurred in the last few decades include the Flixborough, England accident, which cost the lives of 28 people, the whole plant and many injuries (Crowl & Louvar, 2002); the Bhopal, India accident, which killed more than 2000 civilians and injured 20,000 more (Crowl & Louvar, 2002); a massive explosion in Pasadena, Texas on Oct. 23, 1989, which resulted in 23 fatalities, 314 injuries, and capital loss of over \$715 million (Lees, 1996). Recently on March 23, 2005, the Isomerization unit explosions of British Petroleum (Mogford, 2005), Texas City, killed 15 people and injured over 170 more persons. The investigation team revealed that an improper level indicator design of Raffinate Splitter was one of the main contributors to this accident. The study of previous industrial accidents shows that most of these accidents occurred due to improper identifications of risk incidents and correlations of these incidents with an accident. However, the major accidents mentioned above occur rarely in process operations, but minor incidents are very common in process facilities, occurring on a day-to-day basis, resulting in many occupational injuries, illnesses, and costing society billions of dollars every year. The investigation of all the major or minor accidents discloses that an effective risk analysis and safety management strategy can easily restrict them.

The world is more conscious for developing a systematic methodology for estimating both financial, safety, and environmental risks of an industry. The ultimate goal of this risk management plan is to control the risk incidents as well as the major or

minor accidents that occur in process facilities on a routine basis. In 2000, the American Institute of Chemical Engineers (AIChE) developed guidelines for quantitative risk analysis strategy for the chemical process industry. Now, all developed countries maintain a specific guideline for industrial safety to maintain a desired risk level for the process facility. Crowl et al. (2002) mentioned that more than 50 federal regulations of a developed country are dedicated, or directly related, to process safety. A few safety management organizations such as Occupational Safety and Health Administration (OSHA), Process Safety Management (PSM), Environmental Protection Agency (EPA) and Risk Management Program (RMP) have generally worked to interpret the industrial risk into the SIL (Safety Integrated Level) for federal or state regulations.

1.3 RISK ANALYSIS METHODOLOGY

Qualitative and quantitative risk analysis are the two types of risk evaluation system that are used in process facilities or any operation system for estimating risk in terms of different risk parameters, i.e., societal risk, individual risk, potential loss of life, probability of an accident, and reliability of a system. Qualitative analysis, performed at each stage of system development, is intended to identify all major hazards with their relevant causes. Most of the traditional qualitative analysis methods, e.g. HAZOP (Hazard and Operability Study), Functional Hazard Analysis, and Failure Modes and Effects Analysis, are descriptive and generally used for identifying possible system hazards. Normally these methods are used in preparation for consequence analysis or failure frequency analysis modeling of a risk analysis process, and also when a more detailed study is not required (Hauptmanns, 1988; Lees, 1996). After identifying the

possible hazard scenarios of a system, the principal task of risk analysis is to find the logical causes and consequences for the identified hazard scenarios. Quantitative analysis is usually applied to this major task for a risk analysis process.

Quantitative risk analysis (QRA) for a process system can either be deterministic or probabilistic. Generally, the deterministic methods focus on consequence assessment (such as worst-case scenario analysis), while the probabilistic approaches consider both frequency and consequence. The probabilistic approach of QRA evaluates risk for a system in terms of its numerical evaluation of consequences and frequencies of an accident or an incident. Probabilistic data and information about the possible hazard scenarios of an accident are the main required parameters of probabilistic QRA. The final outcome of QRA involves a numerical evaluation of all system hazards and their contributions to the overall risk. Therefore, QRA is more aptly defined as a systematic analysis strategy, rather than a well-defined methodology. The main objectives of QRA are to find the answers to question like “How often will it happen?”, “How can this happen?” or “What are the consequences of an accident?”.

The first step of QRA is hazard identification. The identified hazards are needed for further evaluation to find the answers of “how often it will happen?” and “How can this happen?” These types of queries for a system are addressed by quantitative evaluation. QRA finds these answers via developing frequency model among the incidents of an accident and calculating the probability of each incident scenario for a system. Fault tree analysis (FTA), event tree analysis (ETA), and Markov Modeling are usually used in risk

analysis process for developing the frequency model. ETA is used to estimate the distributions of incident outcomes (e.g., frequencies of explosions, pool fires, flash fires, and safe dispersal) while FTA is used to estimate incident frequency (e.g., major leakage of a flammable material). Markov modeling involves large quantities of fundamental mathematics and is generally preferred for dynamic systems where time dependent failure must be considered. The focus of the present work is to develop a systematic methodology of FTA for the risk analysis process.

1.4 FAULT TREE ANALYSIS (FTA)

Fault tree analysis (FTA) was first developed in 1961-1962 by H. A. Watson at Bell Telephone Laboratories, in connection with a US Air Force contract to study the Minuteman Missile launch control system. The first published paper was presented at the 1965 Safety Symposium sponsored by the University of Washington and the Boeing Company. In this paper, D. F. Haasl, R.J. Schroder, and W.R. Jackson described the whole technique of fault tree construction and its application to a wide variety of industrial safety and reliability problem techniques. Since 1965, fault tree analysis has proliferated its applications in every sector, especially where safety and risk management of a system is a major issue.

1.4.1 FUNDAMENTALS OF FTA

A complete FTA has two major parts: one is fault tree development, which represents an accident model, and the other part is the evaluation of an accident. Therefore, a FTA can be defined as a systematic and deductive technique, which allows

for identifying the basic causes of an undesired event, and finally gives a complete analysis for the evaluation of the causes and the undesired event for an accident. It is a deductive tool in the sense that it starts from a defined system failure event, and unfolds its causes backward down to the primary (basic) independent faults. The qualitative analysis of a fault tree identifies all possible paths that lead to an undesired event for a system, while quantitative analysis of a fault tree helps to estimate the probability of a eventual event from the given failure probabilities of the system's components and basic causes (Veseley et al., 1981; Lees 1996; AIChE, 2000). Besides the graphical representations, a complete analysis of a FTA, which is either a qualitative or quantitative evaluation, ensures the following information for the process facility:

- Identifying safety critical components
- Verifying product requirements
- Certifying product reliabilities
- Assessing product risks
- Investigating accidents/incidents
- Evaluating design changes
- Displaying the causes and consequences of events
- Identifying common-cause failures

1.4.2 SOME BASIC DEFINITIONS AND CONCEPTS OF FTA

- **Event:** Any unwanted or unexpected situations i.e., abnormal or deviation from expected state of a system or a component is known as an event in FTA. As an example as ethylene release from a tank, explosions, carbon filter system failure

can be treated as analyzing event for the process facility as well offshore operations system.

- **Top event:** The unwanted event or incident that is analyzed to further for finding the basic cause of an incident or an accident. It places at the top of the fault tree and is traced downward to more basic failures using logic gates.
- **Basic Event:** An event that no further development or definition is judged necessary (e.g., equipment item failure, human failure, external event).
- **Undeveloped Event:** A basic event that cannot be further developed, because of unavailable information or historical data insufficiency.
- **Logic gate:** The gates that are used to express the logical relationships between inputs (lower) events and a single output (Higher event). In most cases, a fault tree uses the AND or OR logic gates to represent the whole logical dependency of higher event and lower events. AND gates combine the input events, all of which have to occur simultaneously for the output event to occur. In the case of OR gates, the output event occurs if at least one of the input events occurs.
- **Intermediate Event:** An event that is a combination of a few more basic events or any gate event. It propagates towards on an initiating (basic) event during the accident sequence (e.g., improper operating action, failure to stop an ammonia leak, but an emergency plan mitigates the consequences).
- **Likelihood:** A quantitative measure of the expected occurrence of an event. This may be expressed as a frequency (e.g., events/year), a probability of occurrence

during some time interval, or a conditional probability (e.g., probability of occurrence given that a precursor event has occurred).

- **Boolean algebra:** Boolean algebra describes the behavior of linear functions of all variables that are binary in nature: fails or working state, on or off, open or closed, true or false. All coherent fault trees can be converted into an equivalent set of Boolean equations.
- **Minimal cutset (MCSs):** Minimal cutsets are basically a combination of basic events and show the shortest pathway to an undesired top event (i.e., the pathway(s) involving the least number of basic events). The final outcome, failure modes and system weak points are obtained from properly assessing all minimal cutsets of a fault tree.
- **Fault tree modularization:** Division of a large fault tree into some small trees is known as fault tree modularization. It accelerates the computational time of fault tree analysis.
- **Boolean Matrix Transformation:** A Boolean matrix represents whole connections between the gate events and basic events of a fault tree.
- **Probability:** Probability is a numerical measure for the degree of certainty (or degree of uncertainty) of the occurrence of an event. It summarizes how likely an event will occur by estimating the ratio of an event outcome to the number of all possible event outcomes. The outcome of the forecast (or likelihood of an event occurring) is expressed as a number between zero (certain not to occur) and one (certain to occur).

- **Fuzzy Probability:** In conventional probability analysis the probability value of an event is considered as a crisp value for the analysis. Fuzzy probability considers an event probability value as a fuzzy number, which is fuzzified on the basis of considered uncertainties with the event probability value.

1.5 STATEMENT OF THE PROBLEM

FTA is an effective and valuable design tool to improve a system safety of a process facility or an operation system. Regrettably, the use of FTA is comparatively limited in the process industry. The two major barriers that restrict the use of FTA for process safety analysis are as follows:

- i. The first obstacle is solving a large and complex fault tree for an operation system. Normally the processes, materials, equipment, and control mechanisms of the process facility or operations system are varied according to the industry and its objectives. Due to these subjective factors, fault tree construction faces much more diversification in the process industries than in the nuclear industry (Wang, 2004). Subsequently, in most cases the fault trees for the process industry become comparatively large and complex, and are difficult to analyze without moduling.
- ii. The second important barrier for FTA is event data precision. The quantitative analysis of a fault tree needs a fault tree along with failure data of the basic events (components). Sometimes it is difficult to have precise estimation of the failure rate of individual components, or the probability of occurrence of undesired events due to a lack of sufficient data. Further, due to imprecision in basic data and the uncertainty of conventional FTA, the overall result may be questionable.

A suitable modularization algorithm and fuzzy set theory applied to computer-aided FTA may simplify the complex network of a fault tree, and also reduce the ambiguity or vagueness of the outcomes of a fault tree, respectively. These two approaches (modularization and fuzzy set theory) would greatly encourage the use of FTA in the process industry, as well as in any operation system.

1.6 OBJECTIVES OF PRESENT WORK

The preceding discussion indicates that FTA is an important tool for a comprehensive risk management study. Coping with large fault trees and imprecise event data are now the main barriers to its applications in the process facility or any operation system. To overcome this difficulty, a methodology for computer-aided FTA has been developed in this research. Then, an uncertainty analysis is used to compare the error robustness of the fuzzy probability approach, along with the conventional probability approach.

The objectives of this research include:

- To develop a revised methodology for computer-aided fault tree analysis by incorporating:
 - fault tree modularization algorithm to module a large and complex fault tree (to save computational time).
 - fuzzy probability theory and its use in performing probabilistic risk assessment (quantitative fault tree analysis).
- To analyze and compare system sensitivity and the error robustness of the fuzzy probability approach, along with the conventional probability approach.

1.7 ORGANIZATION OF THE THESIS WORK

This thesis is divided into seven chapters. The first chapter gives a broad overview of risk analysis methodology and its significance and current practices in the process industry. Further, it describes the FTA technique with some basics and the difficulties of its application in process facilities are discussed, followed by the objectives of this work.

Chapter 2 presents a detailed study of the FTA technique for a process facility. Particularly, FTA steps for computer-aided fault tree analysis are emphasized and the procedures for developing a complete methodology for computer aided FTA have been discussed. Chapter 3 provides the rules and symbols used for fault tree development for any process facility. This chapter also includes an illustrative example for fault tree development that is used in the methodology proposed in this study. Chapter 4 discusses the fault tree evaluation techniques used in the present methodology. This chapter elaborates the extensive literature review carried out in fault tree evaluation modeling to select a suitable model for qualitative and quantitative analysis for computer-aided FTA. Modeling details of the selected model are discussed in detail with an illustrative example as well.

With successful selection of essential and appropriate models for a process facility as discussed in Chapters 3 and 4, computer codes were developed in Visual Basic for fault tree development and Excel simulations were run for the evaluation of the developed fault tree. This is discussed with a case study in Chapter 5. Chapter 6 discusses the simulation results obtained using the proposed methodology for the case study.

Further, the results are also compared and validated with the results obtained from some other commercial packages. Chapter 7 includes the final conclusions of this work and future scope of research in this area.

Chapter 2

METHODOLOGY FOR COMPUTER-AIDED FTA

This Chapter provides an overview of the fault trees analysis (FTA) technique for a process facility. Different available methodologies for FTA are reviewed and finally a stepwise methodology for FTA is developed in this study. The procedure to develop a computer-aided FTA is illustrated and models required to carry out the fault tree analysis are identified and discussed here.

2.1 FTA FOR PROCESS FACILITY

As per the discussion in the previous chapter, risk analysis involves four main basic steps: hazard identification, frequency analysis, consequence analysis, and finally risk evaluation. Hazard identification identifies system hazards. Risk evaluation measures the system risk that arises from the identified hazard. Frequency and consequence model of risk analysis are the two central steps of risk analysis for estimating the qualitative and quantitative risk for a system in terms of human injury, environmental damage, economic loss, the incident likelihood, operational damage or loss, system reliability, as well as system lifetime and safety (Ljungquist, 2003). Risk analysis of a process system uses the FTA approach to model the frequency of the identified process hazards and then evaluates the system risk for the process facility. The evaluation strategy of FTA involves identification of initiating events which may eventually lead to a major accident, shortest

routes (a series of initiating events) that lead to an accident, the probabilities of occurrence of such initiating events, the relative contribution of each of the initiating events, and finally, a means to sort out these initiating events with the greatest potential to cause the major accident (Khan and Abassi, 1999). FTA is now widely used as an effective tool to assess the system performance, reliability and safety of various complex systems as in a nuclear reactor, in aerospace, in the petrochemical industry, the process industry, and in the offshore oil and gas operations system. Nevertheless, the steps and methods for a complete FTA remains the same for all types of process facilities and other systems. Only the specific fault tree developed for a process unit or system that is used in the analysis varies from system to system and process to process.

HSE (1996) and Mansfield et al. (1996) previously found that among all industrial accidents, process accident pose the highest risk to both humans and the industry itself. Accidents in the process facilities can include large quantity of explosive chemical emission, toxic release, and fire or explosion, all potentially resulting from abnormal developments in the course of an industrial activity. These accidents may cause a serious danger to the workers, the public or the environment. A successful risk reduction method, i.e., inherent safety which gives emphasis on minimizing risk at design stages of a process plant, can minimize the system risk from its basic design. Generally, a typical FTA methodology involves several steps, which require experts' time, reliable probability data, and computational capabilities. Haasl (1965), McCormick (1981), Roberts et al. (1981), Hauptmanns (1988), Henley and Kumamoto (1981), Billington and

Allen (1986), Lees (1996), Khan and Abbasi (1999) and AIChE (2000) described the following basic steps for developing a methodology for computer-aided FTA:

1. Knowledge accumulation about the process system and process operation using a process block diagram.
2. Identification of system hazards or undesired top event by analyzing the hazard scenarios for a process.
3. Fault tree construction for a process facility.
4. Estimating or collecting the failure probability data for all basic components or basic events.
5. Qualitative and quantitative evaluation of a developed fault tree.
6. Perform sensitivity analysis of a fault tree.
7. Re-evaluate the fault tree for the corresponding changes.

To optimize these time-consuming steps for analyzing a fault tree of a system or process unit, many computerized FTA tools have been developed, including CARA fault tree, PROFAT, Relex Fault Tree, and Fault tree+. The basic rules for a fault tree development of a system are more or less same for all FTA tools. The difference is only in their evaluation strategy of the fault tree. Figure 2.1 shows the basic steps that are generally used for computer-aided FTA. The following sections of this chapter analyze the methodologies that have been used in the available FTA tools.

2.2 OVERVIEW OF AVAILABLE FTA TOOLS

The first computer based FTA technique was developed in the early 1970's (Henley, 1981). Since then, the use of computer-aided FTA has become an effective tool for in any type of process facility to assess their operational performance and system safety. Automated fault tree generation develops a fault tree for a specific process system on the basis of several techniques, e.g. Diagraph Based Methods (Lapp and Powers, 1977 and 1979), fault tree construction by formal method (Fussell, 1973), Rule Based Methods (Elliott, 1994), and Loop Based Methods (Shafaghi, 1988) .

In process industries or facilities, there exist diversification in between process operations as well as within the process components. In addition, the process output and material production also varies from process to process. These process phenomena make variations in fault tree constructions for a process facility. During the last two decades, many researchers and organizations have been working on computerized fault tree analysis tools, which contain the flexibility to develop a fault tree for diversified systems. A variety of methods and tools have been developed for this purpose. Figure 2.2 shows a general algorithm for developing computer-aided FTA tools. The features of four available commercial tools for FTA are described below.

CARA-Fault Tree: CARA-Fault Tree (CARA-Fault Tree, version 4.1, 1999) is a Microsoft Windows based program for top-down construction of fault trees. The fault tree is constructed from top to bottom using symbols for each event. To minimize computing time and to provide convenient analysis, this FTA tool follows a

modularization technique consisting of scanning the fault tree for so-called super-modules or sub-trees with input events that are not repeated inside or outside the sub-tree. In the modularized tree, the modules are treated as input events and the corresponding probabilities are re-computed for each module by a simple recursive (exact) technique. It should be noted that if the modularization option is chosen, the MOCUS (minimum obtained cutsets) algorithm implemented in the CARA-Fault Tree will produce minimal cutsets only in terms of the input events of the modularized tree; i.e. the modules themselves will appear as input events in the minimal cutsets.

Fault Tree+: Fault Tree+, developed by Isograph Ltd., runs under Microsoft Windows and is capable of analyzing large and complex fault and event trees producing the full minimal cutsets representation for fault tree top events and event tree consequences. It follows a minimal cutsets generation algorithm to analyze large and complex fault and event trees events (Fault Tree+, Version 11.0, Demo).

Relex Fault Tree: Relex Fault Tree provides a flexible user interface that allows the user to create a fault tree on a window. It uses the idea of modeling a whole tree in terms of a series of smaller fault trees for coping with the large fault tree. An analytical approach is used in this tool to calculate and display the probabilities of the events and gates at a given period of time.

PROFAT: The package PROFAT (PRObabilistic FAult Tree analysis) (Khan and Abbasi, 1999) is based on an analytical simulation methodology. This package reduces the imprecision and ambiguity in fault tree by incorporating probability analysis with fuzzy sets. Although this package has the capability to analyze large and complex trees

by using a modularization technique, it has no graphical interface by which a user can draw the whole fault tree on a window.

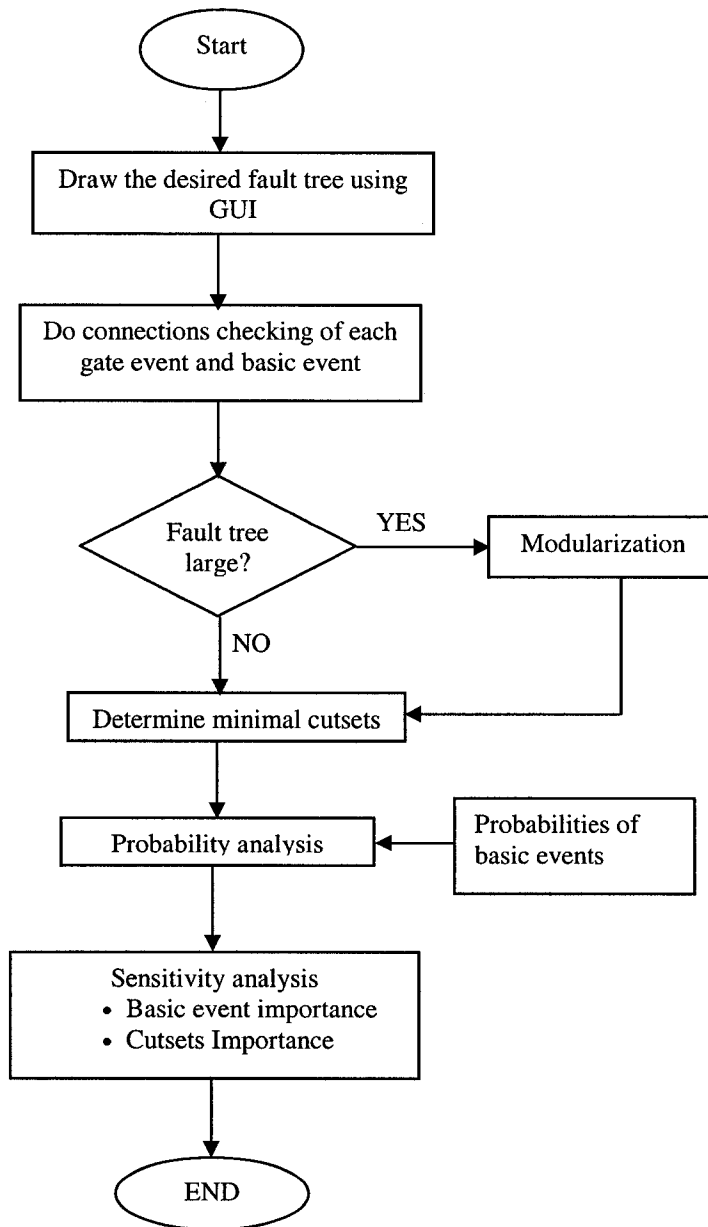


Figure 2.2: Algorithm of FTA tool

Except PROFAT, the remaining FTA tools use the conventional probability approach for the quantitative evaluation of a fault tree. The conventional FTA method considers failure probability data of basic events to be crisp for calculating top event probability. In fact, in real situations the event data cannot be exact values. A great deal of uncertainty is generally associated along with these event's data (Sawyer, 1994; Guimarões et al., 1999; Wu, 2004). Moreover, the accuracy of FTA prediction for a system depends on the precision of the basic component data. In order to reduce the ambiguity and data vagueness, PROFAT uses fuzzy concepts in précising the basic event data. However, PROFAT gives a fuzzy based analysis of a fault tree. It faces some problems on basic event data fuzzification and top event probability calculation. Also, it has no GUI for drawing a fault tree and making a connection list of the tree for FTA. This study addressed these limitations of PROFAT by revising its fuzzy model and methodology for probability analysis. The following sections emphasize a complete methodology for computer-aided FTA.

2.3 PROCEDURE FOR DEVELOPING FTA METHODOLOGY

Based on the above discussion, it is apparent that the steps involved for FTA methodology are fault tree development, qualitative analysis, quantitative analysis and sensitivity analysis. All of these steps are time-consuming, and involve a few brainstorming calculations and are prone to errors-of-omission and inaccuracies. The main objective of a computer- aided FTA tool is to perform an appropriate analysis of a fault (top event) and the causes of this fault. Further, it can optimize the time-consuming

task, and minimize the error of fault tree analysis for a system or process unit. The complete architecture of the proposed methodology of FTA for this study is shown in Figure 2.3 and a brief discussion of each step is given below.

- i. **Fault tree development:** This step of the FTA builds a graphical model of all identified hazard scenarios for a process system. Fault tree construction for a system including preparing a connection list of the whole tree is very significant. Details concerning rules and symbols used for the fault tree development are elaborated in Chapter 3.
- ii. **Qualitative analysis:** A failure or an undesired event occurs as a result of single cause or combination of two or three causes. Qualitative analysis can give a prediction about process system failure characteristics via sorting out the failure modes, i.e., minimal cutsets (MCSs) for a system. The qualitative evaluation for this study is carried out in two steps. The first step identifies the modules of a large fault tree and the second step translates these identified modules into a Boolean matrix to determine the MCSs of a tree. Available algorithms for fault tree modularization and MCSs determination have been reviewed and the most suitable method is identified for large and complex fault trees. Section 4.1 gives the details of qualitative analysis of FTA.
- iii. **Quantitative analysis:** Quantitative analysis evaluates a system numerically. It generally uses probability analysis approach to calculate the probability of an undesired event for a FTA. In order to overcome the vague evaluation of conventional FTA, a fuzzy based probability analysis approach is incorporated in

quantitative evaluation of this methodology. A comprehensive literature review has been carried out to develop a fuzzy model for the probability analysis of FTA. Stepwise descriptions for the fuzzy based quantitative evaluation of FTA are presented in sections 4.2.1, and 4.2.2.

- iv. **Sensitivity analysis:** Sensitivity analysis gives a numerical evaluation for the necessary design modifications, and the weakest link detection of a process system. It can also calculate the quantitative contribution of each cause that leads to an undesired event for the system. A fuzzy weighted index (FWI) and the cutsets importance are used in this study for performing the sensitivity analysis of the system. The details of these two steps are described in section 4.2.3.

However, a few computer tools for FTA are available. Most of these tools use a traditional approach for the probability analysis of a developed fault tree. As previously discussed, basic events data are the input parameter for the quantitative analysis. Events data collection and estimation is now the main barrier for traditional FTA. The aim of this work is to develop a methodology for a computer-aided FTA tool that would overcome the limitations of basic events data estimation in probability analysis (quantitative analysis) of a fault tree, and the problems associated with handling the large and complex tree for MCSs determination of a tree. Fuzzy set theory and modular approach with Boolean matrix transformation are used in this methodology to recover the limitations of traditional FTA. Special features of this methodology are highlighted in the next section of this chapter.

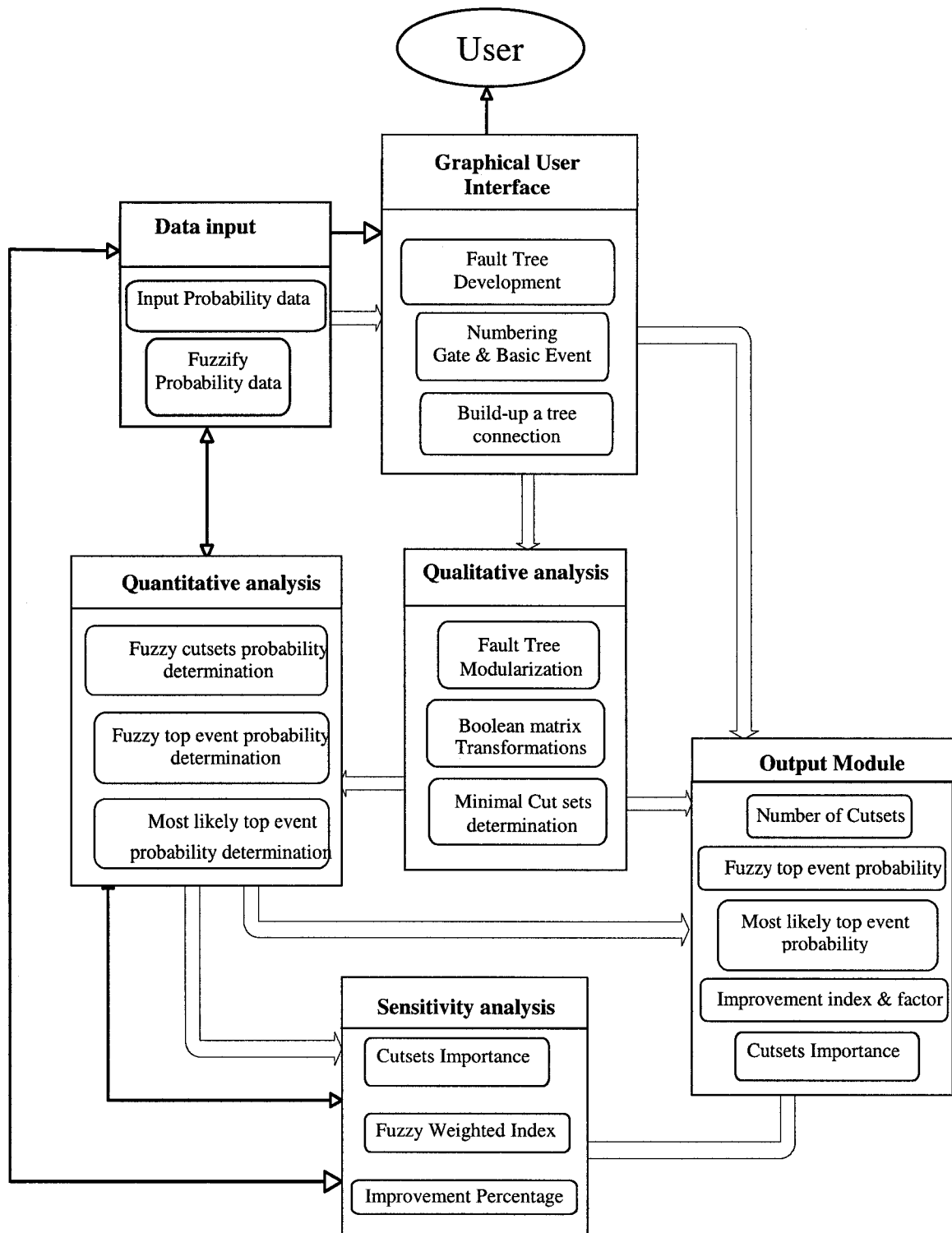


Figure 2.3: Architecture of proposed methodology for fuzzy based FTA tool

2.4 FEATURES OF THE PROPOSED METHODOLOGY

The revised methodology developed for FTA has the following features:

- i. Identifies all possible cutsets through the detected modules of a large fault tree.
- ii. Estimates basic events data through the fuzzy set approach.
- iii. Calculate the probability of an undesired event through fuzzy probability analysis.
- iv. Determine the contribution of each basic cause and MCSs for an undesired event through the numerical estimation of FWI and cutsets importance.

Chapter 3

FAULT TREE DEVELOPMENT

Fault tree analysis (FTA) starts with the specified undesired state of a system (usually known as top event/undesired event e.g., hazardous event, equipment failure) and then the tree is developed from the top-down to find the all credible ways in which the undesired event can occur. All identified credible ways or basic causes are interlinked with each other by Boolean logic gates (AND gate or OR gate). Therefore a fault tree itself is a graphical model of various parallel and sequential combinations of faults that will result in the occurrence of a predefined undesired event. The faults commonly known as basic events of a fault tree can be component failures, human error, environmental conditions, design error, improper device control and so on. Simply, a fault tree depicts a logical relationship between the top event and basic events. The following sections of this chapter depict the necessary symbols and rules for fault tree development.

3.1 BASIC ELEMENTS AND SYMBOLS USED IN FAULT TREE CONSTRUCTION

Two types of symbol generally preferred for tree development are: (1) event symbols; and (2) logic gate symbols. Event symbols are used for representing a top event, basic events, undeveloped events, external events, and intermediate events. Logic gate symbols are used for demonstrating AND or OR gates of a fault tree. The commonly used

event and gate symbols for composing a fault tree are primarily collected from McCormick (1981), Kumamoto and Henley (1981), Veseley et al. (1981) AIChE (2000), Lees (1996) and these are presented in Tables 3.1 and 3.2 respectively.

Table 3.1: Fault tree event symbols










Graphical Symbol	Shape Name	Representing Event
	Rectangle	It is used for representing Intermediate event or top-event.
	Circle	Represents the basic event
	Diamond	Undeveloped Event
	Oval	Conditional event-use for representing any conditions
	House	External Events

Table 3.2: Fault tree gate symbols

Graphical Symbol	Shape Name	Representing logic
	AND gate	AND gates combine the input events, all of which has to occur simultaneously for the output event to occur.
	OR gate	OR gates combine the output event that occurs if at least one of the input events occurs.
	INHABIT gate	Input event produces output event when conditional event occurs.
	TRANSFER gate	Transferring gate information or event information under a sub tree.

The structural diagram for constructing a fault tree described by Henley et al. (1981) is demonstrated in Figure 3.1. According to this figure, the undesired event or incident, which needs further analysis, is positioned on the top of a fault tree. For example, the most typical top events for a process facility are toxic or flammable gas or liquid release, fire, explosions, component ruptures or malfunctions. The basic causes are those responsible for the top event and represented as basic events. A basic event is placed on a tree when it does not require further analysis. The intermediate events are the combinations of basic events or gate events. They appear on the tree when two or three basic events or gate events need to be represented by only one event. Transfer gates show the continuation of a large fault tree to the corresponding tree divisions. An event with unavailable information is generally symbolized as an undeveloped event in a fault tree. Using the denoted events and gate symbols the graphical model of a fault tree is finally built up for a process facility. This model shows a connection among the top event and basic events along with intermediate, external, or undeveloped events. Each connection of this tree expresses the logical dependency of an event with any other events. In most cases, fault tree construction uses AND or OR gate events to express the dependency of the top event with the basic/other events. Figure 3.2 shows a fault tree developed using the standard symbols.

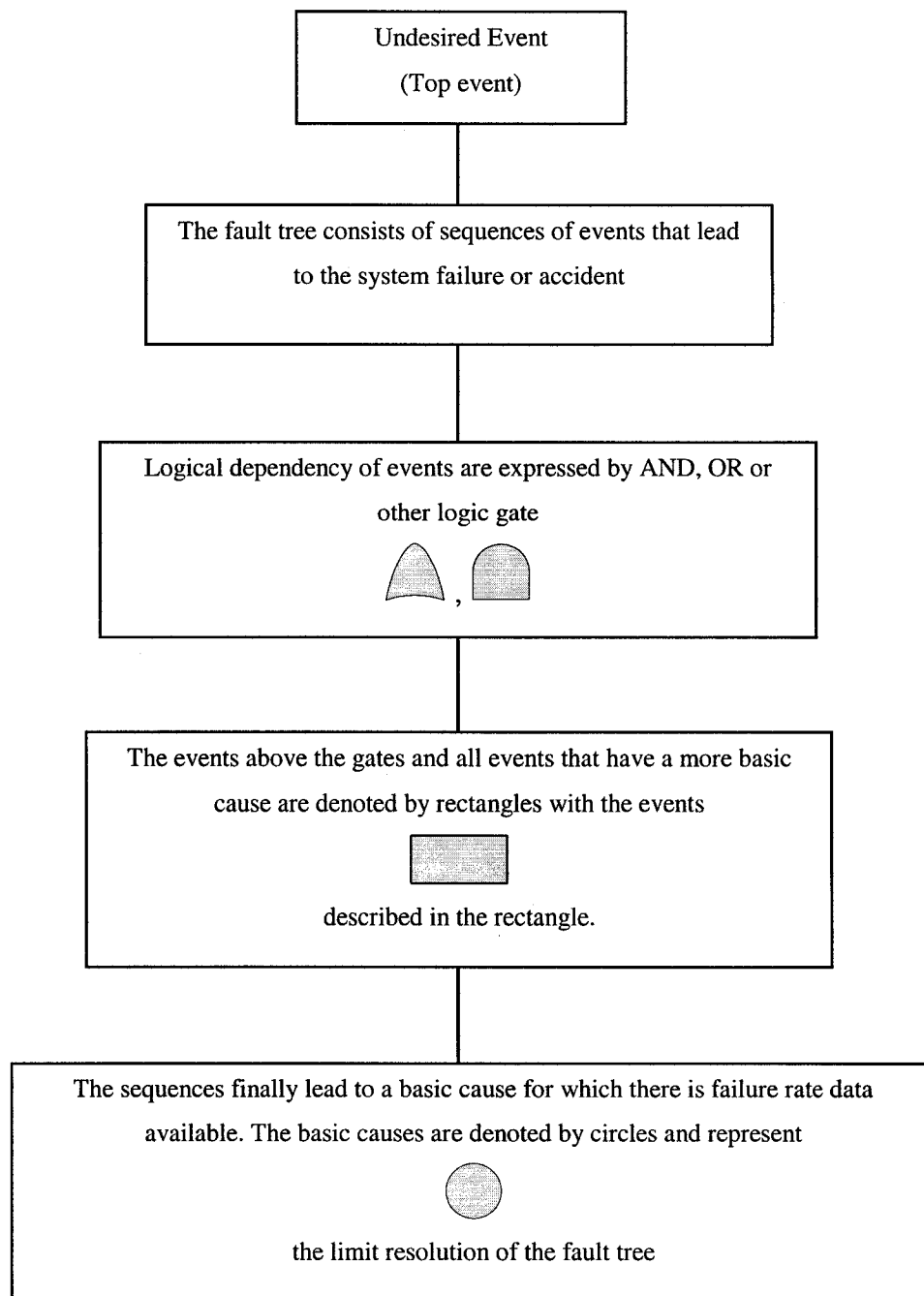


Figure 3.1: Fundamental structural diagram of fault tree (Henley et al., 1981)

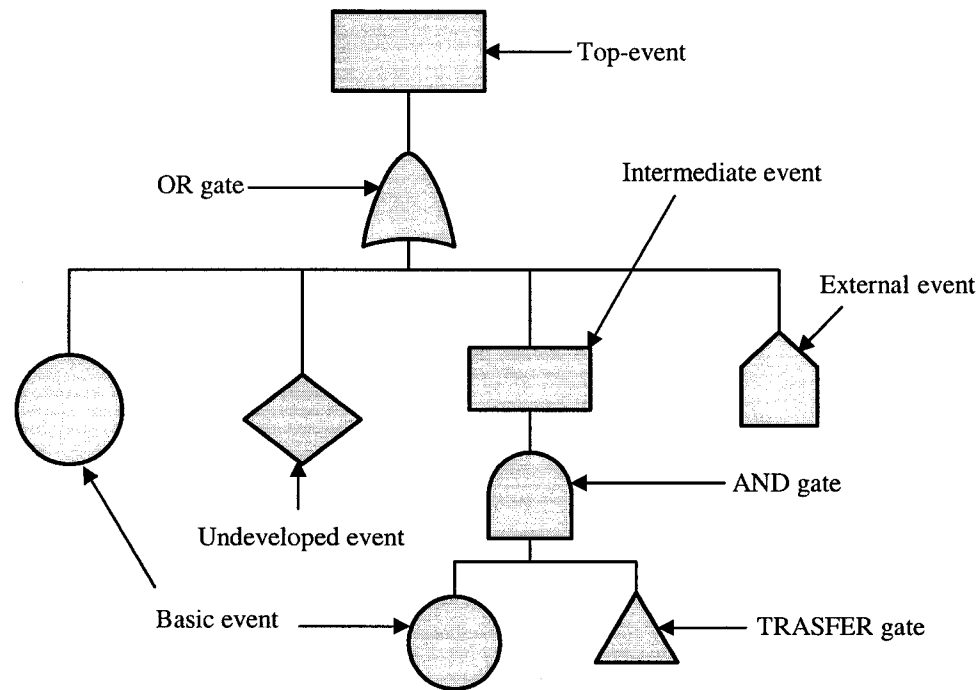


Figure 3.2: Standard fault tree symbols

3.2 FAULT TREE CONSTRUCTION

AICHe (2000) depicts the three approaches for a fault tree construction: 1) manual fault tree development; 2) algorithmic fault tree development; and 3) automatic fault tree development. An algorithmic fault tree develops a fault tree for a process system on the basis of several techniques, e.g. Diagraph Based Methods (Lapp and Powers, 1977 and 1979), Fault Tree construction (Fussell, 1973), Rule Based Methods (Elliott, 1994), and Loop Based Methods (Shafaghi, 1988). For automatic fault tree development, Salem et al (1981) developed CAT code, Taylor (1982) developed RIKKE code and Martin-Soils et al. (1980) developed the fault propagation code. Algorithmic or automatic fault tree construction is only able to construct a fault tree for a specific system. The variation of process components and process operation allows a wide variation in the fault tree

construction for a process unit. Further, the operation of these components is not unique for all process facilities, or industries. It is varied according to the goal and the process output of a facility/industry. Because of these variations in components and operation systems, neither algorithmic nor automatic fault tree construction can build the actual fault tree for the process system. For these reasons, automatic fault tree constructing has not been widely preferred in fault tree analysis at yet.

Manual fault tree construction has user flexibility to construct a fault tree and gives more emphasis to user ideas for developing a fault tree. CARA fault tree, Relex fault tree, Fault tree+ all of these fault tree tools have a graphical user interface for constructing a fault tree by drag and drop event symbols or gate symbols from a toolbar menu. Fault tree construction for a process facility follows some specific rules and regulations. Henley et al. (1981), Veseley et al. (1981), AIChE (2000), Lees (1996), Khan and Abbasi (1999) and Wang (2004) have described the rules for fault tree development.

3.2.1. RULES FOR FAULT TREE CONSTRUCTION

A fault tree demonstrates the causal relationship among basic failures (basic events) that contribute to a predetermined system failure (top event). To complete the construction of a fault tree manually for a complicated system, it is important to first understand how the process works. Process description gives an overall idea about the process and component behavior, as well as the logical dependency of each component of a system. On the other hand, failure scenarios (hazard identification) help to sort out the undesired event and the top event of a fault tree. Many methods could be used for

studying failure scenarios of a system, such as preliminary hazard analysis (PHA), hazard and operability (HAZOP) studies and failure mode effect analysis (FMEA) (AIChE, 2000). Once failure scenarios are identified, the fault tree is developed in the form of a logical diagram for the system. The causal relationship among the basic events and top event is expressed using a logic symbol such as an AND-gate or an OR-gate. In the case of large fault tree constructions for process systems each logic gate and basic event has a unique identifier. Generally the logic gates are labeled with G1, G2, G3, and so on. Each basic event or undeveloped event is labeled with BE1, BE2, BE3, and so on. While a fault tree construction is inherently subjective, it nevertheless some specific guidelines for constructing a high-quality fault tree model of a process system. US Nuclear Regulatory Commissions (1981) examined and listed the guidelines for fault tree development in the Fault Tree Handbook. They have subdivided the guidelines as ground rules and fault propagation rules, which are highlighted below.

- *Ground Rule 1*

Write accurately in event statement boxes about what the fault is and when it occurs. Try to use simple words and avoid the word that might lead to ambiguous meaning.

- *Ground Rule 2*

Classify the fault events accurately. If a specific fault consists with a component failure; classify it as a “state-of-component fault”. Otherwise, classify it as a “state-of-system fault”.

- *Fault Propagation Rule 1 (No Miracles Rule)*

If the normal functioning of a component propagates a fault sequence, then it is assumed that the component functions normally.

- *Fault Propagation Rule 2 (Complete-the-Gate Rule)*

All inputs to a particular intermediate gate should be completely defined before further analysis of any one of them is undertaken.

- *Fault Propagation Rule 3 (No Gate-to-Gate Rule)*

All gate inputs should be properly defined, and no gate should directly feed into another gate.

The more accurate fault tree model gives a more conservative analysis for a system. Furthermore, the accuracy of fault tree construction fully depends on user ideas and expert inputs. Manual fault tree construction has the option to update the user idea and inputs at any time.

This study builds a GUI (Graphical User Interface) to develop a fault tree which has the facility to modify the tree construction by users. The rules and elements for the fault tree development described in this chapter have been used to generate the computer code for the GUI. The following section of this chapter shows an illustrative example of fault tree construction using the rules and elements of fault tree development.

3.3 ILLUSTRATIVE EXAMPLE OF A FAULT TREE CONSTRUCTION

This process is adapted from AIChE (2000), which deals with a control unit of a reactor operation system. Proper card signals from temperature elements (TE) and pressure transmitters (PT) control the shutdown period of the reactor unit. The identified hazard for the system is loss of capability to shut down the reactor system. The process diagram is shown in Figure 3.3

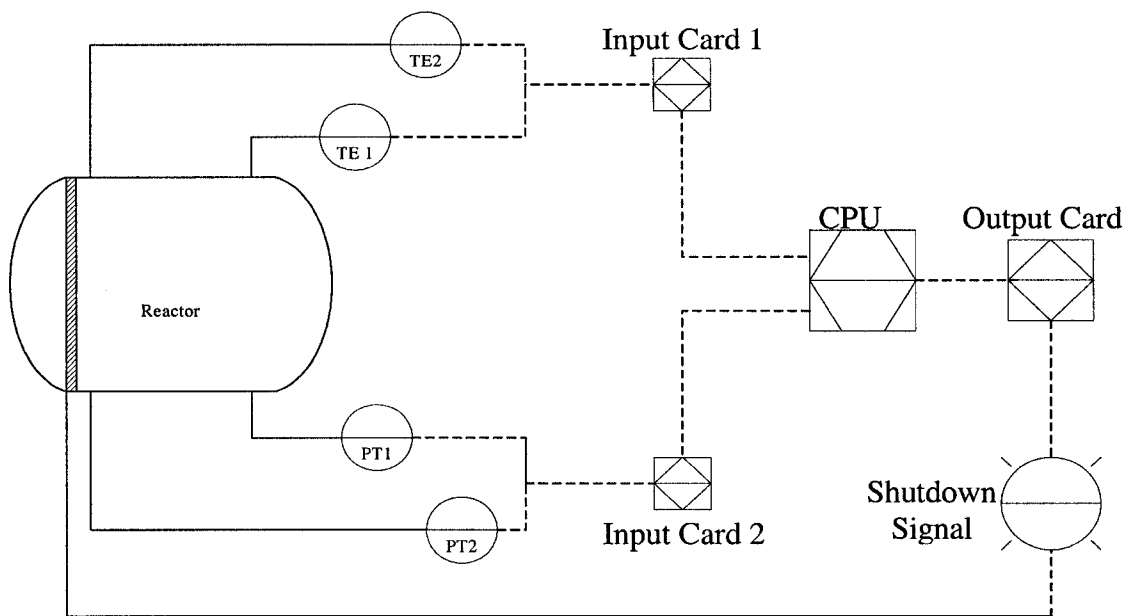


Figure 3.3: Process block diagram of illustrative example (AIChE, 2000)

The fault tree is constructed for this system based on the fault tree construction rules. Respective logic gates are used to express the logical dependency of possible failure modes for the system. In total seven basic causes were identified that lead to loss of capability of system shutdown. According to the rule all basic events are labeled with BE1, BE2, BE3, BE4, BE5, BE6 and BE7 respectively. A total of six logic gates are

labeled with G1, G2, G3, G4, G5 and G6. The developed fault tree for loss of capability to shutdown the reactor system is shown in Figure 3.4.

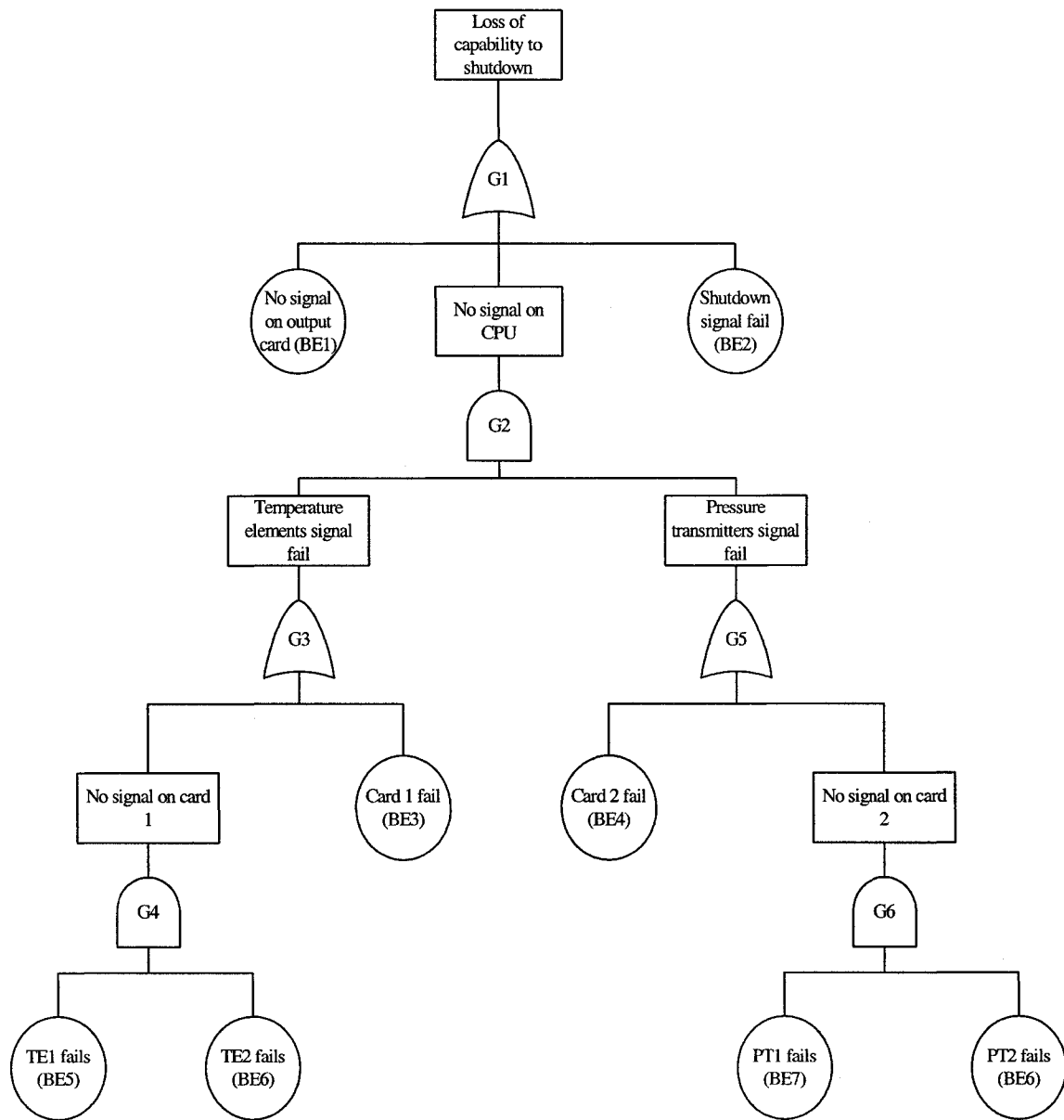


Figure 3.4: Fault tree diagram of illustrative example

Chapter 4

FAULT TREE EVALUATION

This chapter describes the fault tree evaluation techniques for process facility. Once a fault tree is constructed for a process system it needs qualitative or quantitative evaluations for predicting the system's reliability and safety (Veseley, 1981; AIChE, 2000). A fault tree that consists of a few gates and basic events can be easily evaluated manually. However, large and complex fault trees for a process facility need a computer code and a systematic algorithm for a complete evaluation. This chapter discusses the qualitative and quantitative evaluation technique of the proposed methodology for a fault tree.

4.1 QUALITATIVE EVALUATION

When a fault tree has been constructed for a process system the qualitative evaluation can be performed by using the structure of the tree and Boolean algebra operations. Boolean expressions in qualitative analysis have been carried out to express a tree as a combination of basic failure modes of a system that are sufficient to cause an undesired top event to occur. These expressions are sufficient enough to model the failure mechanism of a system, possible failure modes, and identification of critical events for a system. The reliability and safety analysis of a system utilizes the information of qualitative analysis for improving the system design and modifications. According to

Veseley (1981), AIChE (2000), Henley et al. (1981) the qualitative evaluation of a fault tree includes: i) the minimal cutsets (MCSs) determination, ii) qualitative basic events importance estimation, and iii) common-cause failures detection. As previously mentioned, MCSs are basically combinations of basic events that shows the shortest pathway to an undesired top event. Qualitative importance provides a relative ranking of all basic events as per their contribution to system failure. Common-cause identifies those MCSs potentially susceptible to a single failure cause. Therefore, a systematic minimal cutsets analysis can reveal all the information about the failure mechanism for a system.

Minimal cutsets analysis has been carried out either by direct simulation method or analytical method. Direct simulation methods use the Monte Carlo method, which can only determine those cutsets that have a major contribution to system unreliability (Hauptmanns, 1988). Because of this limitation, i.e. being unable to calculate all possible cutsets for a tree, most computer codes have preferred to use the analytical method for minimal cutsets analysis. The analytical method uses Boolean algebra operations in order to express a fault tree in terms of its MCSs (Hauptmanns, 1988; AIChE, 2000). A top down approach or a bottom up approach with Boolean expressions determines all the possible cutsets for a fault tree (Hauptmanns, 1988; Henley, et al., 1996; Lees, 1996; Khan and Abbasi, 1999). The basic principle of the top down approach is that it starts with the top event and works its way down to the basic events. The bottom up approach follows the reverse order of the top down algorithm i.e., its starts from basic events and ends with the top-event. Since 1970, a few computer codes based on these two algorithms have been developed. In 1974, Fussell developed the MOCUS (method of obtaining

cutsets) code (Fussell, et al., 1974b), which can automatically determine MCSs for a fault tree. The MOCUS uses the top down algorithm for generating MCSs of a tree. Another computer code MICSUP (minimal cutsets, upward), developed by Pande (Henley, et al., 1996), calculates the number of minimal cutsets by using the bottom up algorithm. MOCUS or MICSUP are restricted for determining the cutsets only for small fault trees. The fault tree construction for a process facility has wide diversification. Moreover, the process operations and its internal component variations always make a fault tree for the system is complicated in network and large in shape. Neither MOCUS nor MICSUP are capable of solving the MCSs for a large and complex tree. In order to solve all cutsets for a large tree it is essential to sub-divide the tree. The division of a large tree into its equivalent sub trees is known as fault tree modularization. Chatterjee (1975), Birnbaum et al. (1965), Locks (1981), Yllera (1988), Reay et al. (2002), Kohda et al. (1989) developed fault tree modularization algorithms for computer-aided FTA. Once all modules for a tree are determined, the MCSs for the tree can be determined by using the Boolean matrix transformation. The present study developed an integrated approach of modularization technique with Boolean matrix transformations for determining the exact number of minimal cutsets involved in a fault tree. The suitable modularization approach is adopted for this methodology on the basis of pros and cons analysis of existing modularization algorithm. The next section discusses details about the modularization and MCSs determination.

4.1.1 FAULT TREE MODULARIZATION

The main problem with large fault trees is that the number of possible cutsets increases exponentially with the size of the tree (Henley and Kumamoto, 1996). Fault tree modularization permits a separate evaluation of the fault tree branches without changing the basic rules for the fault tree evaluation technique. Henley et al. (1996) identified the following problems to handle a large and complex fault tree:

1. Manually it is impossible to determine the exact number of MCSs for a very large fault tree.
2. It is difficult to estimate the cutsets importance of a large fault tree by manual calculations.
3. Safety software requires high memory to run a large fault tree for detecting all failure modes of a system
4. For large and complex fault trees, producing and analyzing the minimal cutsets only by top down or bottom up approaches may be a time-consuming process even for modern computers.

The modularization technique first reduces the size of a fault tree by dividing the tree into equivalent independent sub trees which are known as independent modules for the tree. These modules are later analyzed with the top down or bottom up approach to enumerate all cutsets for the tree. Thus, fault tree modularization accelerates the computational time for evaluating a fault tree and at the same time it assists in module-

wise analysis of a fault tree. Han (1988) and Henley et al. (1996) identified the following basic steps for modularizing a large fault tree:

Step 1: Detect the unrepeated events in a fault tree.

Step 2: Replace a gate with a module if the gate is composed of unrepeated events

Step 3: In case of a gate composed of repeated and unrepeated events, replace this gate with a module, which contains unrepeated events.

Step 4: Rearrange the fault tree with identified module.

Step 5: Repeat the above procedures until no more modularization can be performed.

Figure 4.1a and Figure 4.1b shows an illustrative example of a simple modularization technique used in large fault tree analysis.

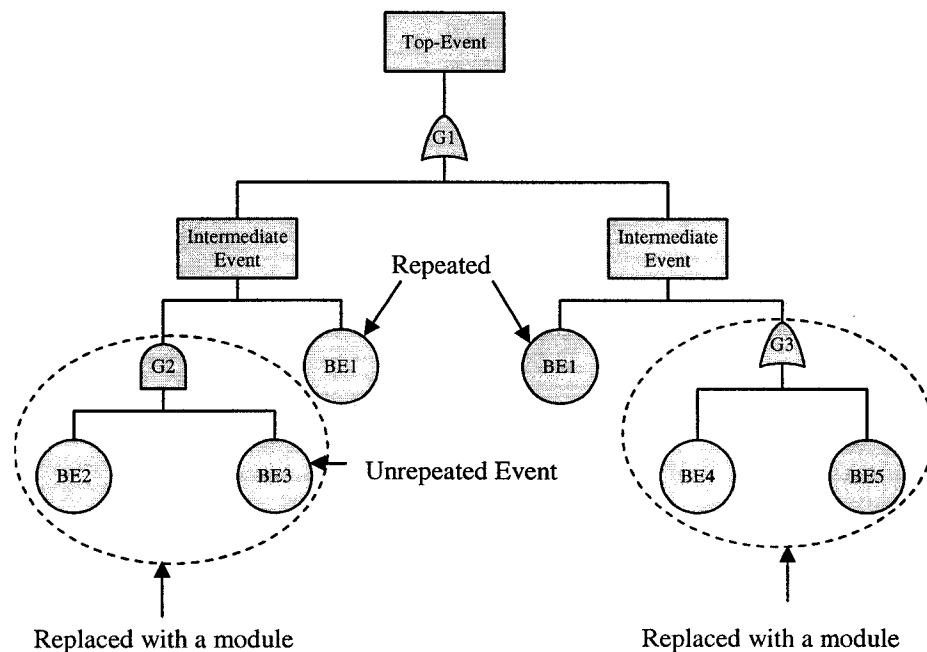


Figure 4.1a: Original fault tree

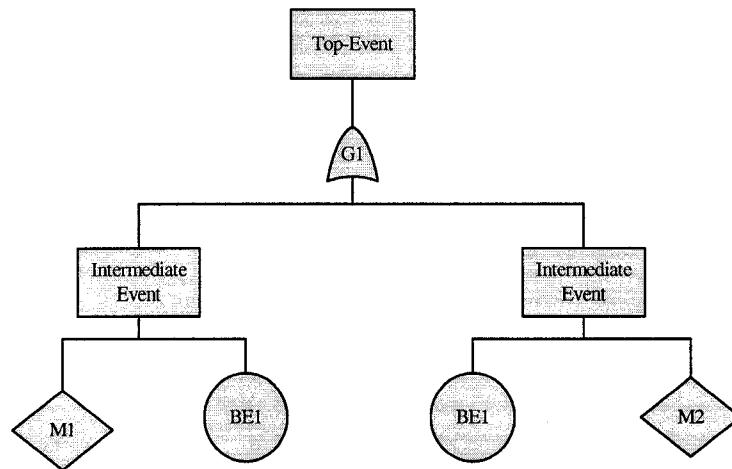


Figure 4.1b: Modularized Original fault tree

4.1.2 MODULARIZATION ALGORITHM FOR COMPUTER-AIDED FTA

A few algorithms have been developed specially for detecting the independent modules of a fault tree in computer-aided FTA. Chatterjee (1975) and Birnbaum et al. (1965) describe the properties of fault tree modularizing and its use in the fault tree analysis. Later on, Locks (1981) implemented these properties into non-coherent fault tree analysis. Chatterjee's algorithm requires all MCSs information as an input for a fault tree modularization. This algorithm is not able to find out all modules for a fault tree, if the fault tree has two or more repeated events. For these reasons this algorithm is not useful for the purpose of fault tree modularization. On the other hand, Locks' (1981) algorithm for fault tree modularization is restricted only for non-coherent fault tree analysis. Besides these two algorithms some other methods, such as super-modularizing (Yllera, 1988), the Binary Decision Diagram (BDD) (Reay et al., 2002), KHIC algorithm

(Kohda et al., 1989) have also been developed for identifying the modules of a fault tree. Reay's algorithm attempts to incorporate the features of neural networks to select the most ordering scheme for each module of a fault tree, based upon its individual characteristics. The BDDs for each module are constructed and culminated in a set of BDDs, which altogether represents the original system. The incorporation of neural-network with the BDD diagram of Reay's algorithm makes it complicated and difficult for applying on computer-aided fault tree analysis. The super-moduling algorithm decomposed a fault tree and expresses the tree in terms of a complex mathematical function, which is called structure function of a fault tree. This algorithm follows some brainstorming rules for labeling the basic events and gate events. Moreover, either BDDs or the super-moduling algorithm are not capable to analyze a non-coherent fault tree. KHIC algorithm is applicable for both coherent and non-coherent fault tree analysis. Further, this algorithm is easy to understand and does not add much complication for basic-events or gate events labeling. For these reasons, in present work, the KHIC algorithm has been incorporated in the computer-aided fault tree analysis methodology.

4.1.3 MINIMAL CUTSETS DETERMINATION

This methodology uses KHIC (Kohda et al., 1989) and the top down algorithm with Boolean matrix transformation (Hauptmanns, 1988) to determine the exact number of minimal cutsets. Figure 4.2 shows the algorithm for MCSs determination implemented in this study and the main steps of this algorithm are described in the following sections.

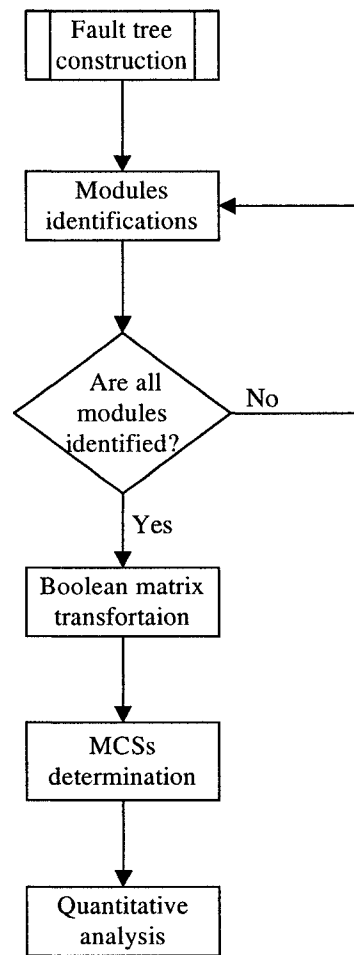


Figure 4.2: Algorithm for MCSs determination

KHIC Method for fault tree moduling: Kohda et al. (1989) developed KHIC algorithm for coherent and non-coherent fault tree analysis. The KHIC method involves four basic steps (Kohda et al., 1989): preparing a connection list, Possibility Checking (PC), Closeness Checking (CC), and Local Combination Checking (LCC). A connection list shows the attributes of the basic event and gates of the fault tree. PC examines whether the first element in its connection list is the same as the current gate event. CC examines whether the upper gate events that connect to input events appearing in the expansion

procedure is included in the sub-tree being examined. Finally, LCC looks for the existence of any logical combinations on the tree. To make this closeness check systematic, the method first allocates hierarchical levels to all gate events and examines them in ascending order. The KHIC method tries to obtain modules whose output event is not expressed by gate events. The stepwise modularization technique of KHIC algorithms are presented in Figure 4.3 The modules obtained from the KHIC algorithm are then used in Boolean matrix transformations to calculate minimal cutsets for a modularized fault tree. The basic steps involved in the KHIC algorithm for coherent fault tree moduling are as follows:

- i. Labeling the gate events and basic events of constructed fault tree.
- ii. Prepare a connection list of the fault tree.
- iii. Check the basic events under gate events.
- iv. Check the repeated basic events or gate events on the tree.

Boolean matrix transformation: The modular approach expresses a fault tree in terms of equivalent sub trees. These modules are further expanded for developing a logic structure of the tree by using Boolean algebra operations. The logic structure of a fault tree can be induced from all possible MCSs of a fault tree. The top down or bottom up approach mentioned earlier, usually determines all the MCSs of a fault tree. Top down algorithms work on the principle that an OR gate increases the number of cutsets, while an AND gate enlarges the size of the cutsets (Henley and Kumamoto, 1996). Hauptmanns (1988) used the top down algorithm to develop a Boolean matrix, which expresses a logic

structure of a fault tree in terms of MCSs. A Boolean matrix represents the connections between the gate events and basic events of a fault tree.

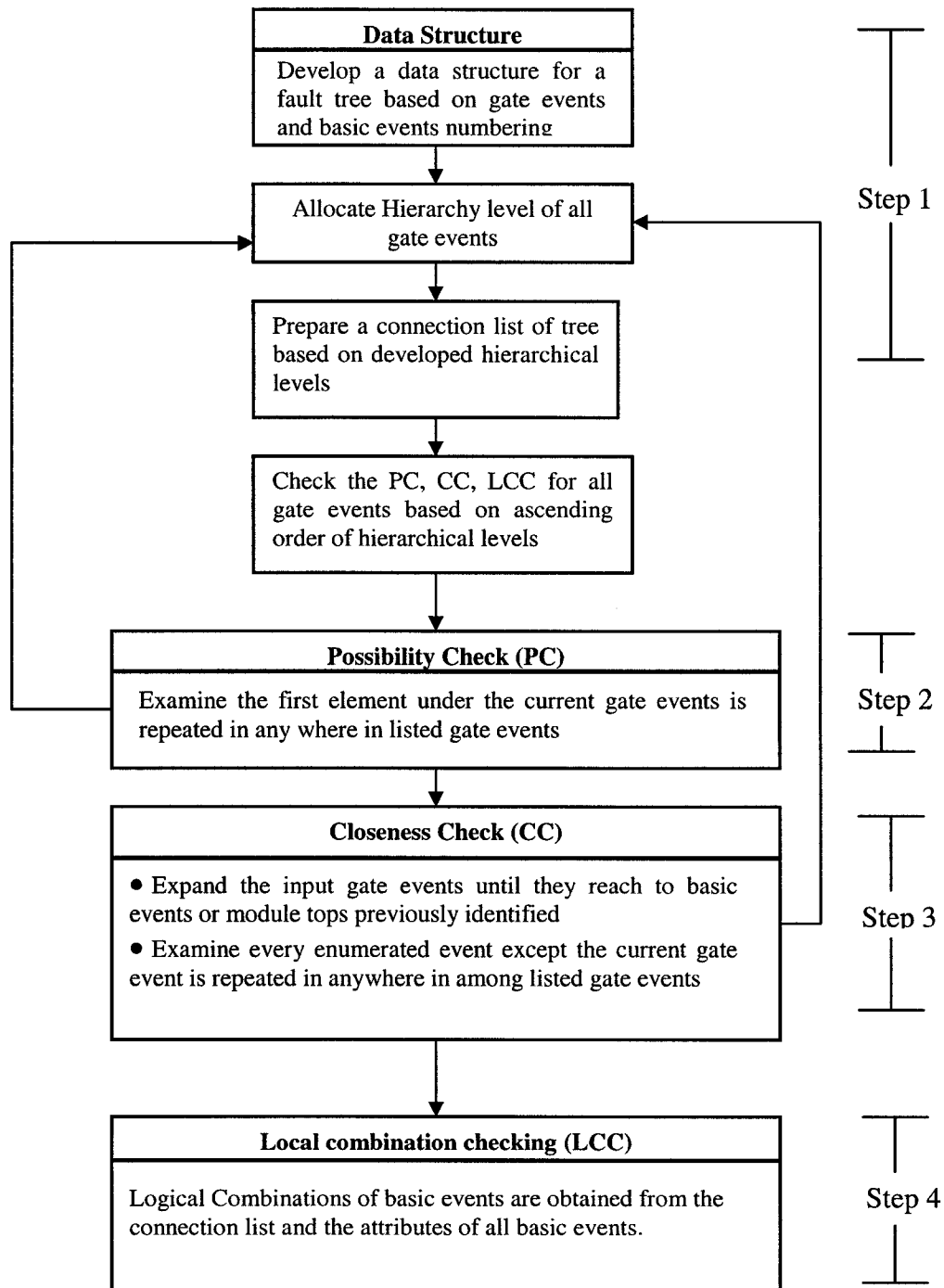


Figure 4.3: Steps wise process of KHIC algorithm (Kohda et al., 1989)

4.1.4 INTEGRATED ALGORITHM FOR MCSs DETERMINATION

As discussed in the previous section, it is apparent that, to cope with the large and complex network of a fault tree, it is required to find out the possible modules for a tree and then the MCSs of the tree are determined. The current study developed an integrated approach of KHIC algorithm and Boolean matrix transformation for determining the exact number of cutsets for a fault tree. KHIC algorithm finds out the possible equivalent modules of a fault tree, and a Boolean matrix sort out the exact number of cutsets for the tree. The steps followed for the proposed algorithm are given below:

- i. Find all modules obtained by KHIC algorithm for the developed fault tree.
- ii. The total number of gates represents the total number of rows of the matrix.
- iii. The columns of this matrix are divided into three blocks containing basic events in the first block, OR-gates in the second block and AND-gates in the third block.
- iv. Using “1” for a basic events or gate events connection and “0” for no connection fill the matrix.
- v. Replace each gate with corresponding basic events by using the top down algorithm.
- vi. Repeat the above procedures until all gate events are replaced with basic events.

The final matrix is then solved for finding the number of cutsets involved in a tree. The rows with only basic events in the matrix represent minimal cutsets of the developed fault tree. The following section illustrates an example of qualitative evaluation of a fault tree as an application of the developed algorithm.

4.1.5 ILLUSTRATIVE EXAMPLE FOR QUALITATIVE EVALUATION OF FAULT TREE

Consider again the fault tree in Figure 3.3 in chapter 3 for the illustration of a complete methodology of qualitative evaluations of a fault tree that is developed in this study.

Step 1: KHIC ALGORITHM FOR FAULT TREE MODULARIZATION

The fault tree example in Figure 3.3 consists of three AND gates and three OR gates. The results obtained by the KHIC methodology are as follows:

- With respect to connection list preparation, hierarchical levels are shown in Table 4.1. The order of G6, G5, G4, G3, and G2 is not important because they are all bottom gate events. The hierarchical level of a gate event with input gate events is larger than those of its input gate events. For example, the number assigned to G1 is larger than for G2, G3, and G5.
- Based on the above step (hierarchical level determination) – connection lists are obtained as shown in Table 4.2 where their attributes are also shown. This ordering process makes it easy to compare connection lists and their attributes.

Table 4.1: Hierarchy of gate events

Gate level 1	G6
Gate level 2	G5
Gate level 3	G4
Gate level 4	G3
Gate level 5	G2
Gate level 6	G1

Table 4.2: Connection list and attributes

G2	(G1, 1)	BE1	(G1, 1)
G3	(G2, -1)	BE2	(G1, 1)
G4	(G3, 1)	BE3	(G3, 1)
G5	(G2, -1)	BE4	(G5, 1)
G6	(G5, 1)	BE5	(G4, -1)
		BE6	(G4, -1)
		BE7	(G4, -1)

- The results of the checking process for gate events (possibility, closeness, and local combination checks) show that no logical combinations are obtained from the fault tree in Figure 3.3. Module tops G3, G5, G2, and G1 result from the decomposition of the fault tree by modules. These results are captured in the following listing:

i) For gate event G6:

Possibility Checking (PC): The first element (FE) is G6 for BE6 and BE7.

Closeness Checking (CC): The number of connecting gate events (NOCGE) is 2 for enumerated basic event BE6. Thus, G6 cannot be a module top.

ii) For gate event G4:

PC: FE is G4 for BE5 and BE6.

CC: NOCGE is 2 for BE6. Thus, G4 cannot be a module top.

iii) For gate event G5:

PC: FE is G5 for BE4 and G6.

CC: Appearing events in the expansion procedure (EP) are G5, G6, BE4, BE6, and BE7.

Elements of their connection lists are G5, G6, and BE4. Thus, the closeness condition holds and G5 can be a module top.

Local Combination Checking (LCC): Connection lists and their attributes for BE6 and BE7 are different, and no combination module is found.

iv) For gate event G3:

PC: FE is G3 for BE3 and G4.

CC: Appearing events in the EP are G3, G4, BE3, BE5, and BE6. Elements of their connection lists are G3, G4, and BE3. Thus, the closeness condition holds and G3 can be a module top.

LCC: Connection lists and their attributes for BE5 and BE6 are different, and no combination module is found.

v) For gate event G2:

PC: FE is G2 for G3 and G5.

CC: Appearing events in the EP are G2, G3, G5, G4, G6, BE3, BE4, BE5, BE6, and BE7. Elements of their connection lists are G2, G3, and G5. Thus, the closeness condition holds and G3 can be a module top.

LCC: Connection lists and their attributes for BE3, BE4, BE5, BE6, and BE7 are different and no combination module is found.

vi) For gate event G1:

PC: FE is G1 for BE1, BE2, and G2.

CC: Appearing events in EP are G1, G2, G3, G5, G4, G6, BE1, BE2, BE3, BE4, BE5, BE6, and BE7. Elements of their connection lists are G1, G2, BE1, and BE2. Thus, the closeness condition holds and G1 can be a module top.

LCC: Connection lists and their attributes for G2, G3, G5, G4, G6, BE1, BE2, BE3, BE4, BE5, BE6, and BE7 are different, and no combination module is found.

Step 2: BOOLEAN MATRIX TRANSFORMATION

KHIC algorithm identified 4 modules for the fault tree: G1, G2, G3, and G5. Table 4.3 shows the Boolean matrix transformations of these modules. MCSs for each module and the whole tree are highlighted with different colors in this matrix.

Table 4.3: Boolean Matrix transformation for MCSs determination

Modules	Basic Events							Gate events					
	BE1	BE2	BE3	BE4	BE5	BE6	BE7	G1	G3	G5	G2	G4	G6
Module 1 (G5)	0	0	0		0	0	0	0	0	1	0	0	0
	0	0	0	1	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	1
	0	0	0	0	0	1	1	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0
Module 2 (G3)	0	0	0	0	0	0	0	0	1	0	0	0	0
	0	0	1	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	1	0
	0	0	0	0	1	1	0	0	0	0	0	0	0
Module 3 (G2)	0	0	0	0	0	0	0	0	0	0	1	0	0
	0	0	0	0	0	0	0	0	1	1	0	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0
	0	0	0	0	1	1	0	0	0	1	0	0	0
	0	0	1	1	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	1	1	0	0	0	0	0	0
	0	0	0	1	1	1	0	0	0	0	0	0	0
	0	0	0	0	1	1	0	0	0	0	0	0	0
Module 4 (G1)	0	0	0	0	0	0	0	1	0	0	0	0	0
	1		0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	1	0	0
	0	0	1	1	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	1	1	0	0	0	0	0	0
	0	0	0	1	1	1	0	0	0	0	0	0	0
	0	0	0	0	1	1	0	0	0	0	0	0	0

4.2 QUANTITATIVE EVALUATION

The quantitative evaluation of a fault tree includes a) absolute probabilities of the top event, b) quantitative importance of basic events and MCSs, and c) sensitivity evaluations. Top event probability estimates the frequency of an undesired event of a fault tree if all basic events occurred together. Quantitative importance of basic components and MCSs determine the percentage contributions of each basic event or cutsets to cause the undesired event. Sensitivity analysis estimates the changing effect of components in a system as well as the necessary design modifications for the system.

The first step of quantitative analysis of a fault tree is top event probability calculation. A fault tree structure and estimated failure probabilities of all basic events are the two important parameters for calculating the top event probability of a fault tree. The calculation of top event probability is done either using minimal cutsets approach or gate-by-gate approach in the Boolean expressions (AIChE, 2000). Gate-by-gate approach is simpler and requires simple Boolean calculation. This technique starts with the basic events and proceeds upward to the top event (Lawely, 1980). However, this approach calculates the top event probability without determining all cutsets of a tree. In this approach the top event probability suspects to have some percentage of error if the fault tree has a few more repeated basic events in different branches of an AND gate (AIChE, 2000). Moreover, this approach performs better if the fault tree is small and simple in size. On the other hand, the minimal cutsets approach always gives a conservative estimation. Minimal cutsets approach represents the logical structure of the fault tree. Once the probabilities for all basic events and MCSs are estimated, the top event

probability by minimal cutsets approach is then calculated by using either equation 4.1 (Yuhua et al., 2005) or equation 4.2 (Hauptmanns, 1980).

$$P(T) = P\left(\bigcup_{j=1}^n K_j\right) = \sum_{i=1}^n P(K_i) - \sum_{i < j=2}^n P(K_i K_j) + \sum_{i < j < k=3}^n P(K_i K_j K_k) + \dots \dots \dots + (-1)^{n-1} P(K_1 K_2 \dots K_n) P(K_j) = \prod_{i \in K_j} F_i(t) \quad [4.1]$$

$$P(T) = 1 - \prod_{i=1}^n [1 - K_i] \quad [4.2]$$

In the above equation, K_1, K_2, \dots, K_n represent the minimal cutsets, n is the total number of minimal cutsets and $F_i(t)$ is the probability of a basic event BE_i . Due to a low probability of occurrence, the first part of the equation 4.1 is generally used to calculate the top event probability of a tree (Yuhua et al., 2005). Equation 4.1 gives exact estimation of top event probability if the fault tree is large and consists of a large number of cutsets. Whereas equation 4.2 always gives a conservative result in cases of both small or large fault tree.

Conventional FTA uses crisp basic events data to be used in equation 4.1 or equation 4.2 for quantitative evaluation of a fault tree. This quantitative evaluation of a fault tree can only give an approximation of the reality. Because of, variant failure modes, failure data collection error, design faults, poor understanding of failure mechanism, as well as the vagueness of system phenomena, it is a difficult task to get precise failure probability data of basic events. Therefore, the conventional FTA analysis (dependent on precise failure probability data of basic events) cannot give reliable results for process systems. Liang et al., (1993), Yuhua, et al. (2005) Ying, et al.(1998), Suresh

et. al. (1996), Wu (2004), Pan, et al. (1997) have described the limitations of conventional FTA and also identified the following reasons for arising uncertainty in estimation of basic events data:

- Human error on data collection
- Data sufficiency of new components
- Change of operational and environmental conditions of a system
- Lack of knowledge about the system and its failure mechanism

Further, it is difficult task to get precise reliability data for all basic components at one time and many components of a fault tree may not have quantitative data at all. This limitation actually makes the whole fault tree analysis for a system questionable. In order to overcome such limitations, a fuzzy based methodology is developed in this study instead of using the normal probabilistic approach for quantitative evaluation of a fault tree. The fuzzy model for quantitative evaluation of FTA is shown in Figure 4.4. The following sections of this chapter describe the fuzzy model for quantitative analysis of a fault tree with regards to fuzzy set theory fundamentals.

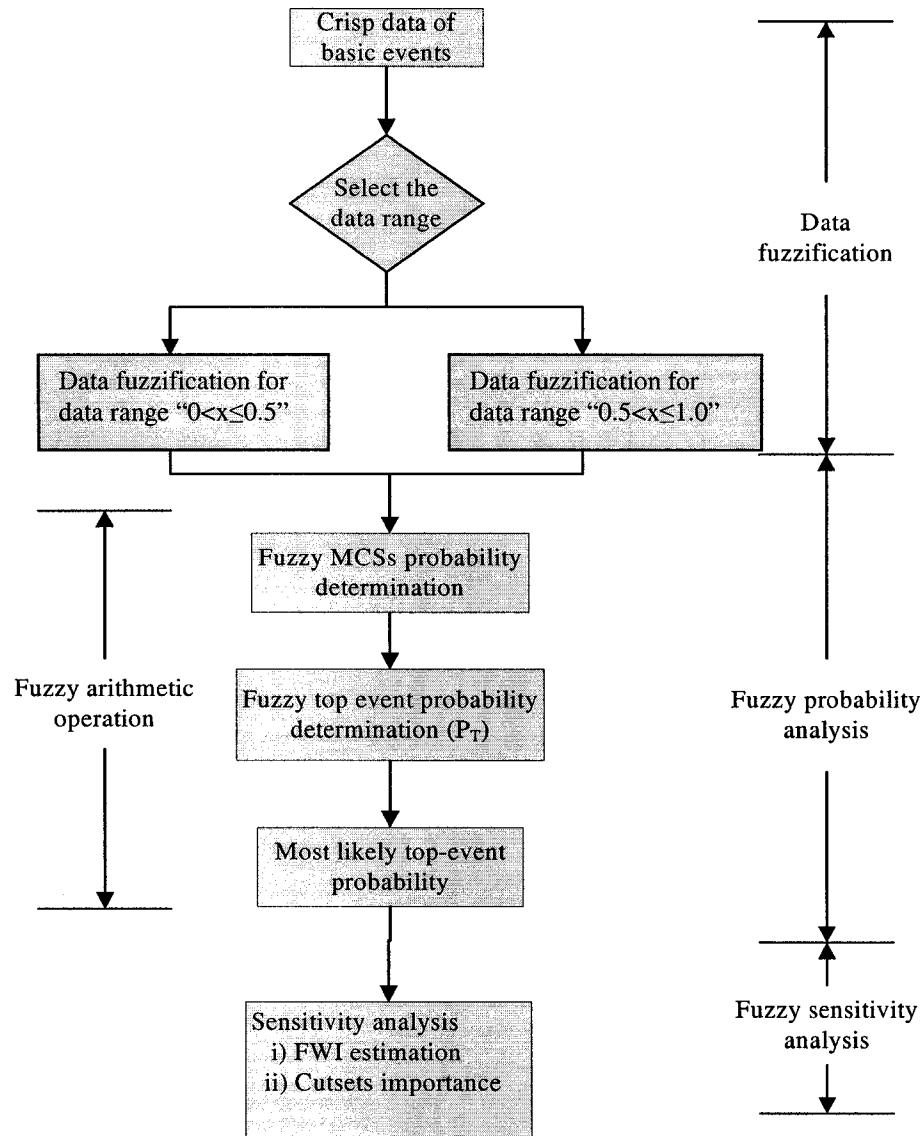


Figure 4.4: Fuzzy model for quantitative evaluation of FTA

4.2.1 FUZZY SET THEORY FUNDAMENTALS AND ITS APPLICATION TO FTA

In conventional FTA, failure probability of the top event is calculated by considering failure probability data of basic components of a system to be exact values (Wu, 2004; Yuhua et al., 2005). However, in practice, ambiguity of the system and component behavior, working environment of a system, as well as lack of sufficient statistical inference raise the difficulties during estimation of exact failure probability of

basic components (Singer, 1990; Liang et al., 1993; Ying et al., 1998; Wu, 2004; Yuhua et al., 2005). In order to avoid such uncertainty in probabilistic risk assessment, Lai et al. (1988) and Singer (1990) introduced the fuzzy set theory to safety and reliability problems. Later, Liang (1993), Sawyer (1994), Ying et al. (1998), Khan and Abbasi (1999), Shengping et al. (2000) implemented it into the FTA technique.

4.2.1.1 FUZZY PROBABILITY

The imprecise probability value of a basic event may be defined as “about 0.5” or “around 0.5”. For the estimating of such vague quantities or linguistic ideas on probability estimation, fuzzy probability analysis is appropriate. Fuzzy probability uses the fuzzy number, which is expressed by a fuzzy set and characterized by its membership function, μ . Its can be represented by a triangular or trapezoidal shape or bell shaped membership function (Cheng et al., 2000). As an example, Figure 4.5 represents the trapezoidal representation of an event probability “around 0.4” (Misra et al., 1990; Lai et al., 1988). Thus, in trapezoidal representation, the fuzzy probability of an event BE_i can be denoted by the $\tilde{P}_{BE_i} \triangleq$ four-tuple $(P_{iA}, P_{iB}, P_{iC}, P_{iD})$ (Figure 4.5). The corresponding membership functions are:

$$\mu_{\tilde{P}_{BE_i}(p)} = \begin{cases} 0 & 0 \leq p \leq P_{iA} \\ 1 - \frac{P_{iB} - p}{P_{iB} - P_{iA}} & P_{iA} \leq p \leq P_{iB} \\ 1 & P_{iB} \leq p \leq P_{iC} \\ 1 - \frac{p - P_{iC}}{P_{iD} - P_{iC}} & P_{iC} \leq p \leq P_{iD} \\ 0 & P_{iD} \leq p \leq 1 \end{cases} \quad [4.3]$$

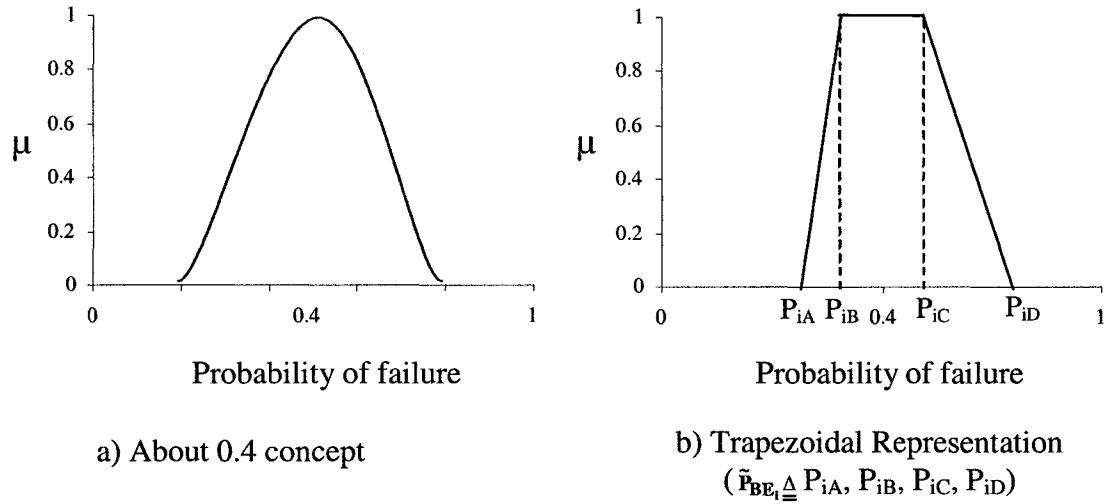


Figure 4.5: Fuzzy probability representation

4.2.1.2 FUZZY ARITHMETIC OPERATION

In fuzzy fault tree analysis, probability of all basic events is expressed in terms of fuzzy numbers. Hence, in order to estimate the fuzzy top event probability, it is necessary to use fuzzy arithmetic operations for the “AND” gate and the “OR” gate operation of a fault tree. Fuzzy arithmetic operations follow the rules of fuzzy set theory and the use of the extension principle. Based on this extension principle Misra et al. (1990), Lai et al. (1988) and Liang et al. (1993) have described the fuzzy arithmetic operations for fault tree analysis. The fuzzy arithmetic operations for determining failure possibilities under the AND or OR gate are:

1. The fuzzy probability under the n-array and the AND gate with inputs BE_1, BE_2, \dots, BE_n (Figure 4.6) is:

$$\tilde{P}_T^{AND} = \tilde{P}_{BE_1} \otimes \tilde{P}_{BE_2} \otimes \dots \otimes \tilde{P}_{BE_n} \quad [4.4]$$

Tanaka et al. (1981) provide an approximation procedure for the multiplication of two fuzzy numbers. If \tilde{P}_{BE_1} and \tilde{P}_{BE_2} are two fuzzy probabilities of basic events then the fuzzy multiplication rule is defined as

$$\tilde{P}_{BE_1} \otimes \tilde{P}_{BE_2} = (P_{1A} P_{2A}, P_{1B} P_{2B}, P_{1C} P_{2C}, P_{1D} P_{2D}) \quad [4.5]$$

where, $P_{1A}, P_{1B}, P_{1C}, P_{1D}$ and $P_{2A}, P_{2B}, P_{2C}, P_{2D}$ are the four-tuple values of each basic event.

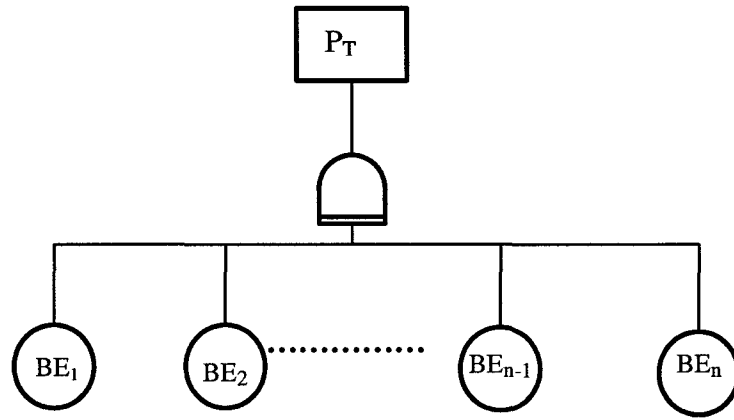


Figure 4.6: 'AND' Gate

2. The fuzzy probability under the n-array in the OR gate with inputs BE_1, BE_2, \dots, BE_n (Figure 4.7) is:

$$\tilde{P}_T^{OR} = 1 - \left[(1 - \tilde{P}_{BE_1}) \otimes (1 - \tilde{P}_{BE_2}) \otimes \dots \otimes (1 - \tilde{P}_{BE_n}) \right] \quad [4.6]$$

Similarly, again if \tilde{P}_{BE_1} is a fuzzy set probability of a basic event then the fuzzy complementation rule is defined as

$$1 - \tilde{P}_{BE_1} = 1 - P_{1A}, 1 - P_{1B}, 1 - P_{1C}, 1 - P_{1D} \quad [4.7]$$

where, $P_{1A}, P_{1B}, P_{1C}, P_{1D}$ are the four-tuple values of the basic event.

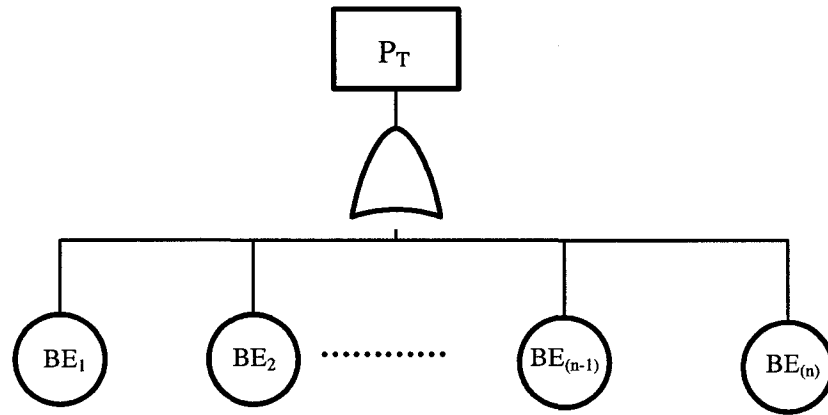


Figure 4.7: 'OR' Gate

4.2.2 Fuzzy Based Probability Analysis

The minimal cutsets obtained from qualitative evaluation of a fault tree are used for probability analysis of FTA. In the probabilistic approach, the uncertainties in component data propagate through these cutsets to the top event failure probability, further it affect the sensitivity analysis of a fault tree. Hence, if the basic events probability data are not precise, then the whole fault tree analysis will give a wrong prediction about the system reliability. Fuzzy based probability analysis attempts to define a basic event data into a fuzzy set and uses it in subsequent computations. Finally, the value is defuzzified to get a precise top event probability. The procedure for the fuzzy based probability analysis consists of the following steps:

Conversion of Basic Events Probability Data to Fuzzy Probability Data: In fuzzy based probability analysis, the imprecise failure probabilities of basic events are refined by characterizing the basic event data with a suitable membership function. In this paper, trapezoidal membership function is recommended for converting the basic event data.

P_{iA} , P_{iB} , P_{iC} and P_{iD} are the left-hand and right-hand bounds of this function. Two approaches can be applied to obtain left-hand and right-hand bounds: i) from the point median value and the error factor; and ii) from the direct assignment based on expert assessment (Liang et al., 1993). PROFAT (Khan and Abbasi, 1999) uses one trapezoidal function for data fuzzification, which under limit the reliability predictions in extreme condition (basic events having high failure probability value) and also gives a wrong estimation of top event probability. To overcome this difficulty, the proposed methodology uses two trapezoidal membership functions for the different conditions of basic event probability data range. The first trapezoidal condition is used for the probability data lies in the range of “0 to 0.5”, and the second one is used for the values between the ranges of 0.5 to 1.0. The calculating strategy for the lower bound and the unbound values of each trapezoidal membership function are given below with the examples.

Condition 1: $0 \leq \text{Probability value} \leq 0.5$

$$\text{Lower bound value } P_{iA} = \text{Probability value} \times 0.5$$

$$\text{Lower bound value } P_{iB} = \text{Probability value} \times 0.75$$

$$\text{Upper bound value } P_{iC} = \text{Probability value} \times 1.25$$

$$\text{Upper bound value } P_{iD} = \text{Probability value} \times 1.5$$

Example: The conversion of the probability value “around 0.1” is given below and its trapezoidal representation is shown in Figure 4.8.

$$P_{iA} = 0.1 \times 0.5 = 0.05 \quad P_{iB} = 0.1 \times 0.75 = 0.075$$

$$P_{iC} = 0.1 \times 1.25 = 0.125 \quad P_{iD} = 0.1 \times 1.5 = 0.15$$

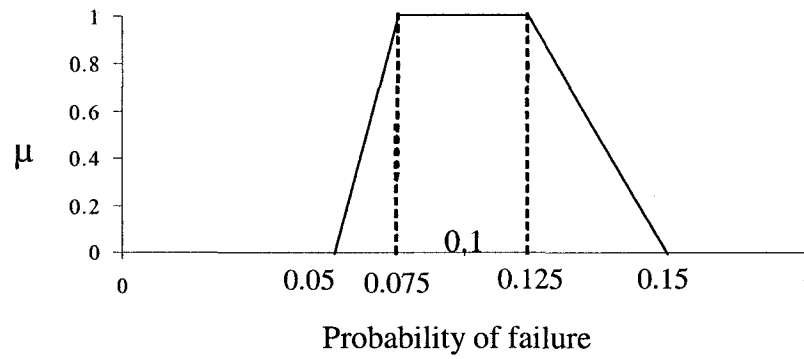


Figure 4.8: Trapezoidal representation of probability value “around 0.1”

Condition 2: $0.5 \leq \text{Probability value} \leq 1.0$

$$\Delta = (1 - \text{Probability value})/4$$

$$\text{Lower bound value } P_{iA} = (\text{Probability value} - (2 \times \Delta))$$

$$\text{Lower bound value } P_{iB} = (\text{Probability value} - \Delta)$$

$$\text{Upper bound value } P_{iC} = (\text{Probability value} + \Delta)$$

$$\text{Upper bound value } P_{iD} = (\text{Probability value} + 2 \times \Delta)$$

Example: The conversion technique for probability value “around 0.6” is given below and its trapezoidal representation is shown in Figure 4.9.

$$\Delta = (1 - 0.6)/4 = 0.1$$

$$P_{iA} = (0.6 - (2 \times 0.1)) = 0.4 \quad P_{iB} = (0.6 - 0.1) = 0.5$$

$$P_{iC} = (0.6 + 0.1) = 0.7 \quad P_{iD} = (0.6 + (2 \times 0.1)) = 0.8$$

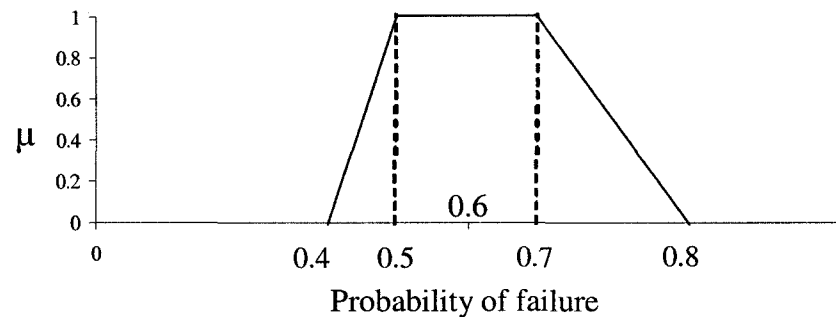


Figure 4.9: Trapezoidal representation of probability value “around 0.6”

PROFAT uses one trapezoidal function to convert the basic event crisp data to fuzzy data. Hence it performs better when the basic event has lower probability values, i.e., values “around 0.5”. However, in cases like a fault tree example in Figure 4.10, which has two gates and four basic events, which have the probability values “around 0.4”, “around 0.7”, “around 0.8” and “around 0.9” respectively, PROFAT estimates the top event probability for this tree as 0.833. The calculated exact top event probability for this tree is 0.949. The top event probability estimated by the present algorithm for this example is 0.943, which is close to the exact value.

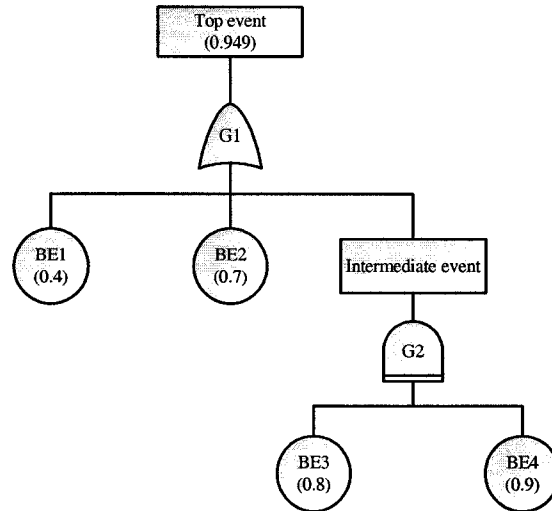


Figure 4.10: Fault tree example

Fuzzy Top event Probability Calculation: Quantitative analysis of a fault tree attempts to calculate the probabilities of the top event and the minimal cutsets (MCSs). To minimize the error due to uncertainty in the basic events probability data, the present algorithm used fuzzified probability data for quantification of a fault tree. Once the fuzzy probability for all basic events and MCSs are estimated, the fuzzy top event probability is then calculated by using equation 4.8. Fuzzy arithmetic operations rules are employed to

estimate top event as well as minimal cutset probability estimation. The obtained results (the top event and minimal cutsets probability) are also a continuous fuzzy number with a membership function that is defined by a trapezoidal function.

$$\tilde{P}_T = 1 - \left[(1 - \tilde{C}_1) \otimes (1 - \tilde{C}_2) \otimes \dots \otimes (1 - \tilde{C}_n) \right] \quad [4.8]$$

Here, $\tilde{C}_1, \tilde{C}_2, \dots, \tilde{C}_n$ are the fuzzy probabilities of all minimal cutsets. And \tilde{P}_T represent the four-tuple values of top event fuzzy probability, e.g., $(\tilde{P}_T \triangleq P_{A(T)}, P_{B(T)}, P_{C(T)}, P_{D(T)})$.

Most Likely Failure Probability Estimation: After fuzzy arithmetic operations, the result of a fault tree becomes a fuzzy variable, which further needs to be translated into a crisp value (Klir et al., 2001). The objective is to derive a single crisp numeric value that represents the most inferred fuzzy values of the estimated fuzzy variable. Defuzzification is an inverse transformation which maps the output from the fuzzy domain back into the crisp domain (Klir et al., 2001). Several methods exist for the defuzzification process: the centre of area method, the centre of maxima method, mean of maxima method, and the weighted average method. The methodology here uses the weighted average method for determining the most top event probability of a fault tree. The weighted average method estimates the most inferred top event fuzzy value using the following equation:

$$M(P_T) = \frac{P_{A(T)} \cdot \mu_{P_{A(T)}} + P_{B(T)} \cdot \mu_{P_{B(T)}} + P_{C(T)} \cdot \mu_{P_{C(T)}} + P_{D(T)} \cdot \mu_{P_{D(T)}}}{\mu_{P_{A(T)}} + \mu_{P_{B(T)}} + \mu_{P_{C(T)}} + \mu_{P_{D(T)}}} \quad [4.9]$$

where, $M(P_T)$ is the most likely fuzzy top event probability; $P_{A(T)}$, $P_{B(T)}$, $P_{C(T)}$, $P_{D(T)}$ are left and right bounds of top event fuzzy probability and $\mu_{\tilde{P}_T}$ is the corresponding membership grade of each value.

The fuzzy probability analysis of this methodology uses three steps to convert the basic events data into fuzzy sets and calculates top event probability for a FTA. The three consecutive steps are:

- i. Crisp data fuzzification of basic events.
- ii. Fuzzy top event probability calculation.
- iii. Defuzzification of Fuzzy top event probability.

4.2.3 SENSITIVITY ANALYSIS

Top event probability provides only the idea about the system conditions, for example, system success or failure states for a given time period. Sensitivity analysis helps to evaluate the percentage contribution of each basic event that leads to a system failure (top event) and also estimates unavailability and failure frequencies of the basic event, which have to be changed in order to maintain a predefined system's top event probability. In addition, sensitivity analysis also helps to identify three important decisions for the design modifications of a system: the weakest link of the system; a better design alternative; and how to evaluate the effect of the adopted solution on system safety (Contini et al., 2000). In this study the sensitivity analysis for a system is evaluated on the basis of investigating the fuzzy weighted index (FWI) of each basic event, and the cutsets importance of a fault tree.

Fuzzy Weighted Index Estimation: In FTA, the contribution of basic events that leads the top event failure is generally measured in terms of the improvement index of the system. Fuzzy weighted index is another form of estimating the improvement index of a basic event, when the failure probability of a basic event is defined through fuzzy functions. This is estimating by eliminating each basic event from the tree and evaluating its impact (in terms of weight) on the tree (Tanaka et al., 1983; Misra et al., 1990; Liang et al., 1993; Yiang et al., 1998; Cheong, 2004). In the present work, the following modified equation is used for measuring fuzzy improvement or weighted index of a basic event:

$$V(P_T, P_{T_i}) = (P_{IA(T)} - P_{IA(T_i)}) + (P_{IB(T)} - P_{IB(T_i)}) + (P_{IC(T)} - P_{IC(T_i)}) + (P_{ID(T)} - P_{ID(T_i)}) \quad [4.10]$$

where, P_T refer to top event probability with all event occurring, P_{T_i} refer to top event probability without $P_{IA(T_i)}$.

Cutsets Importance: The additional feature of measuring cutsets importance is added in this methodology for identifying the most likely path that leads to the top-event. In order to measure the cutsets importance, the output fuzzy function of each minimal cutset is needed to convert into crisp value through the defuzzification method (Klir et al., 2001).

The cutset contribution to the top event is then estimated by using the following equation:

$$I^{ci} = \frac{Q_j}{Q_0} \times 100 \quad [4.11]$$

where, I^{ci} = the probability of cutsets importance, Q_j = the fuzzy probability of cutsets frequency; and Q_0 = most likely top event probability.

SUMMARY

The overall methodology for a fault tree evaluation has been described in this chapter. The qualitative evaluation of this methodology follows fault tree modularization and Boolean matrix transformation for determining all possible MCSs for a tree. And the quantitative evaluation of the methodology uses the fuzzy set theory for the probability analysis and sensitivity analysis of the fault tree.

KHIC algorithm moduled a large fault tree into the equivalent sub trees and Boolean matrix transformed these trees into the Boolean functions and determines the possible MCSs for the fault tree. Once all MCSs have been elucidated, the fuzzy probability analysis follows data fuzzification, fuzzy MCSs probability estimation, fuzzy top event probability calculation and defuzzification process to calculate the most likely top event probability of the tree. Further, the FWI and cutsets importance in the present methodology estimates a fuzzy based basic events and cutsets contribution to an undesired event for a fault tree.

Chapter 5

CASE STUDY AND UNCERTAINTY ANALYSIS

In order to verify the methodology of computer-aided FTA, a case study is presented in this chapter to illustrate the proposed methodology. Further, an uncertainty analysis of this case is also carried out to make the comparisons between the proposed methodology and the existing strategy of FTA. This case study was previously studied by Wang et al. (2005). He used a FTA in this case study for improving the design of an activated carbon filter safeguard system, whereas we have used this case study for comparison and uncertainty purposes. The subsequent section of this chapter will give a detailed fault tree analysis and the uncertainty quantification of this case study, which was obtained by using the proposed methodology for the fuzzy computer-aided FTA tool.

5.1 A CASE STUDY

A FTA, based on the proposed methodology, is conducted for an activated carbon filter safeguard system. The objectives of the study are to a) identify all possible MCSs that may cause the top event to occur, b) determine the fuzzy top event probability and the most likely fuzzy value of the top event, and c) calculate the contribution of each event in terms of FWI and the cutsets importance that are causing the top event. The stepwise analysis of the described methodology of fuzzy computer-aided FTA tool is given below.

5.1.1 SYSTEM DESCRIPTIONS AND HAZARD IDENTIFICATION

O-ethyl S- (2-diisopropylaminoethyl) methyl phosphonothiolate ($C_{11}H_{26}NO_2PS$) is the chemical name of VX. The US Army Safety System defines three major hazard scenarios of the VX neutralization process, which are VX agent release, personal injury/illness, and system loss. The vent streams from the process unit contain trace amounts of VX agent and volatile organic compounds (VOCs). These are passed through the cascade ventilation system, which consists of four-supply air handling units and eight exhaust activated carbon filter units, to remove VOCs and VX agents from the streams before transferring into the building exhaust system.

5.1.2 FAULT TREE DEVELOPMENT

The identified undesired top event by Wang et al. (2005) for this system was that *“fails to capture VX and VOCs release agents due to the failure of carbon filter system”*. Wang et al. (2005) already identified all the possible hazard scenarios and their logical dependency for causing the top event of the fault tree. Using these identified hazards and their information, a fault tree for the VX neutralization process was constructed in the GUI. Figure 5.1 shows the fault tree for the case study. Basic events, intermediate events, top event, and gate events (Figure 5.1) are shown in Tables 5.1 and 5.2 respectively.

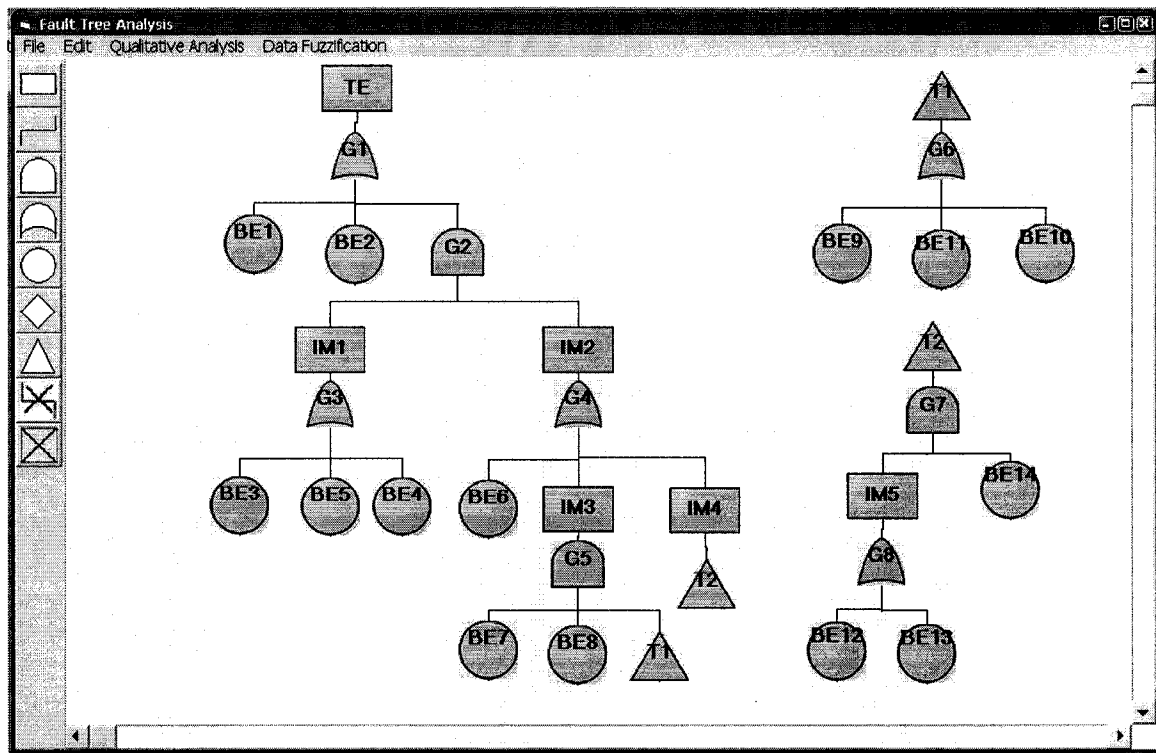


Figure 5.1: Fault tree diagram of the case study in the GUI

Table 5.1: Name of the basic event and their notifications

Basic Events Notification	Name of the Basic Event
BE1	Carbon Filter System Improperly Designed
BE2	Carbon bed filters become saturated with HC
BE3	Both of moisture indicators MIT-1905 A and B fails to operate
BE4	Supply air Heater elements fails to operate
BE5	The Exhaust air high humidity interlock controller fails to respond
BE6	Process heat Loads do not heat saturated supply air because process is shut down
BE7	Ton container stream cleaning is occurring
BE8	TCC stream cleaning flow rate is two times normal
BE9	Loss of chilled cooling water supply
BE10	1 of 2 cooling water isolation valves is inadvertently closed
BE11	1 of 2 cooling water isolation valves is plugged
BE12	Air supply dehumidification system improperly deigned
BE13	Loss of chilled cooling water supply
BE14	Ambient air relative humidity >70%

Table 5.2: Name of the top event (TE) and intermediate event (IM_i)

Basic Events Notification	Name of the Basic Event
TE	Fails to capture VX and VOCs release agents due to the failure of carbon filter system
IM1	Supply air Heater elements fails to operate on high humidity
IM2	Exhaust air received humidity >>70%
IM3	TCC stream cleaning flow rate is too high and condenser fails
IM4	Loss of supply air dehumidification when ambient air > 70% relative humidity
IM5	Loss of supply air dehumidification system

5.1.3 QUALITATIVE EVALUATION

The fault tree for this identified top event, i.e., failure of carbon filter system to capture VX and VOCs release agents from the exhaust (Figure 5.1), consists of eight gates and fourteen basic events. The generated connection list for this fault tree is shown in Figure 5.2. This list is further used in determining the modules of the fault tree. The modularizing algorithm of the methodology identifies eight modules, which are shown in Figure 5.3. After sorting out all possible modules for the tree, the Boolean matrix transformation was then used for finding the MCSs (Figure 5.1). The Boolean matrix transformation of these modules gave twenty minimal cutsets (MCSs). Tables 5.3 and 5.4 listed all the modules and the MCSs for the fault tree along with the minimal cutsets and their number in each module.

Connectionlist		
Gate Events	Gate Type	Elements Under Gate Events
G1	OR	BE1 BE2 G2
G2	AND	G3 G4
G3	OR	BE3 BE4 BE5
G4	OR	BE6 G5 G7
G5	AND	BE7 BE8 G6
G7	AND	G8 BE14
G6	OR	BE10 BE11 BE9
G8	OR	BE13 BE12

Figure 5.2: Connection list of gate events and basic events for the fault tree

Module of fault tree		
Gate Events	Gate Type	Elements Under Gate Events
G1	OR	BE1 BE2 G2
G2	AND	G3 G4
G3	OR	BE3 BE4 BE5
G4	OR	BE6 G5 G7
G5	AND	BE7 BE8 G6
G7	AND	G8 BE14
G6	OR	BE9 BE10 BE11
G8	OR	BE12 BE13

Figure 5.3: Obtained modules for the fault tree

Table 5.3: Minimal cutsets for the modules

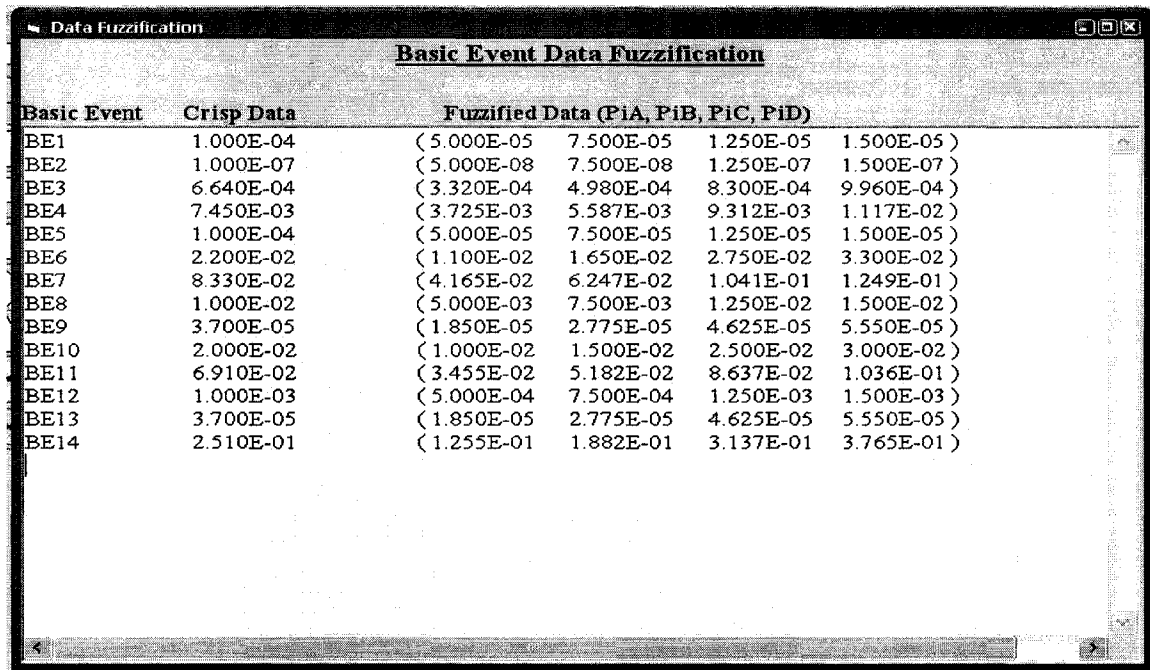
Module Top	Gate Type	Minimal Cutsets	Cutsets in Each module
<u>G8</u>	OR	(BE12), (BE13)	2
<u>G7</u>	AND	(BE12, BE14)	2
		(BE13, BE14)	
<u>G6</u>	OR	(BE9), (BE10), (BE11)	3
<u>G5</u>	AND	(BE7, BE8, BE9)	3
		(BE7, BE8, BE10)	
		(BE7, BE8, BE11)	
<u>G4</u>	OR	(BE6), (G5), (G6)	3
<u>G3</u>	OR	(BE3), (BE4), (BE5)	3
<u>G2</u>	OR	(G3, G4)	1
<u>G1</u>	OR	(BE1), (BE2), (G2)	20

Table 5.4: Minimal cutsets for the fault tree

MCSs			
BE1			
BE2			
BE3	BE6		
BE4	BE6		
BE5	BE6		
BE3	BE7	BE8	BE9
BE4	BE7	BE8	BE9
BE5	BE7	BE8	BE9
BE3	BE12	BE14	
BE4	BE12	BE14	
BE5	BE12	BE14	
BE3	BE7	BE8	BE10
BE4	BE7	BE8	BE10
BE5	BE7	BE8	BE10
BE3	BE7	BE8	BE11
BE4	BE7	BE8	BE11
BE5	BE7	BE8	BE11
BE3	BE13	BE14	
BE4	BE13	BE14	
BE5	BE13	BE14	

5.1.4 QUANTITATIVE EVALUATION

This study uses the fuzzy concept in probability analysis of the fault tree. The fuzzified data for the basic events are shown in Figure 5.4. Fuzzy probability analysis of the current work uses these fuzzified data for the fault tree evaluation. The most likely top event probability estimated for this tree is 2.954E-04. Table 5.5 shows the fuzzy top event probability analysis results for the case study.



Basic Event	Crisp Data	Fuzzified Data (PiA, PiB, PiC, PiD)
BE1	1.000E-04	(5.000E-05 7.500E-05 1.250E-05 1.500E-05)
BE2	1.000E-07	(5.000E-08 7.500E-08 1.250E-07 1.500E-07)
BE3	6.640E-04	(3.320E-04 4.980E-04 8.300E-04 9.960E-04)
BE4	7.450E-03	(3.725E-03 5.587E-03 9.312E-03 1.117E-02)
BE5	1.000E-04	(5.000E-05 7.500E-05 1.250E-05 1.500E-05)
BE6	2.200E-02	(1.100E-02 1.650E-02 2.750E-02 3.300E-02)
BE7	8.330E-02	(4.165E-02 6.247E-02 1.041E-01 1.249E-01)
BE8	1.000E-02	(5.000E-03 7.500E-03 1.250E-02 1.500E-02)
BE9	3.700E-05	(1.850E-05 2.775E-05 4.625E-05 5.550E-05)
BE10	2.000E-02	(1.000E-02 1.500E-02 2.500E-02 3.000E-02)
BE11	6.910E-02	(3.455E-02 5.182E-02 8.637E-02 1.036E-01)
BE12	1.000E-03	(5.000E-04 7.500E-04 1.250E-03 1.500E-03)
BE13	3.700E-05	(1.850E-05 2.775E-05 4.625E-05 5.550E-05)
BE14	2.510E-01	(1.255E-01 1.882E-01 3.137E-01 3.765E-01)

Figure 5.4: Fuzzified data of basic events

Table 5.5: Fuzzy top event probability estimation for case study

Fuzzy probability analysis	$P_{A(T)}$	$P_{B(T)}$	$P_{C(T)}$	$P_{D(T)}$
Top Event Fuzzy set	9.553E-05	1.778E-04	4.131E-04	5.669E-04
Most likely Top Event	2.954E-04			

5.1.5 SENSITIVITY ANALYSIS

The cutsets importance module in the sensitivity analysis revealed that path [BE1 and BE4-BE6] has the maximum probability of occurrence, while paths [BE5-BE13-BE14], [BE3-BE7-BE8-BE9], [BE4-BE7-BE8-BE9], [BE5-BE7-BE8-BE9] and [BE5-BE7-BE8-BE11] have the least. The fuzzy weighted index (FWI) of each basic events helps to conclude that particular attention must be given to the basic events BE1, BE4, and BE6, as these are most likely to cause the top event. Tables 5.6 and 5.7 shows the detailed sensitivity analysis for the case study.

Table 5.6: FWI for different events

Event not occurring	Probability Factor	FWI	Improvement
0	2.954E-04	0.000E-00	0.00
BE1	1.955E-04	3.999E-04	13.54
BE2	2.954E-04	3.998E-07	0.01
BE3	2.797E-04	6.894E-05	2.33
BE4	1.183E-04	7.737E-04	26.19
BE5	2.931E-04	1.038E-05	0.35
BE6	1.035E-04	8.356E-04	28.29
BE7	2.946E-04	4.805E-06	0.16
BE8	2.946E-04	4.805E-06	0.16
BE9	2.955E-04	1.995E-09	0.00
BE10	2.953E-04	1.078E-06	0.04
BE11	2.948E-04	3.725E-06	0.13
BE12	2.930E-04	1.211E-05	0.41
BE13	2.954E-04	4.480E-07	0.02
BE14	2.929E-04	1.255E-05	0.43

Table 5.7: Cutsets importance for all MCSs

MCSs	Fuzzy MCSs Probabilities	MCSs Importance (in percentage)
BE1	1.000E-04	33.85
BE2	1.000E-07	0.03
BE3-BE6	1.552E-05	5.25
BE4-BE6	1.741E-04	58.94
BE5-BE6	2.338E-06	0.79
BE3-BE7-BE8-BE9	2.822E-11	0.00
BE4-BE7-BE8-BE9	3.166E-10	0.00
BE5-BE7-BE8-BE9	4.250E-12	0.00
BE3-BE12-BE14	1.979E-07	0.07
BE4-BE12-BE14	2.221E-06	0.75
BE5-BE12-BE14	2.981E-08	0.01
BE3-BE7-BE8-BE10	1.525E-08	0.01
BE4-BE7-BE8-BE10	1.711E-07	0.06
BE5-BE7-BE8-BE10	2.297E-09	0.00
BE3-BE7-BE8-BE11	5.270E-08	0.02
BE4-BE7-BE8-BE11	5.913E-07	0.20
BE5-BE7-BE8-BE11	7.937E-09	0.00
BE3-BE13-BE14	7.323E-09	0.00
BE4-BE13-BE14	8.216E-08	0.03
BE5-BE13-BE14	1.103E-09	0.00

5.2 UNCERTAINTY ANALYSIS

Risk assessment methodology uses the available information of a risk event and then utilizes it to make the decisions for minimizing the risk right from the source. Uncertainties include data uncertainty, model uncertainty, human error uncertainty, and so on (McCormick, 1981; Smith, 2002; AIChE, 2000). Further, uncertainty is a central issue in the utilization of the risk management. Hence, uncertainty quantifications should proceed before making any decision regarding risk estimation methodology or a developed model for risk assessment management. Uncertainty analysis is the part of the risk assessment process, which numerically or graphically estimates the effect of data error and model inaccuracy on the risk estimation process. Past studies have also shown that model uncertainty, data uncertainty, and quality uncertainty are the main sources of uncertainties for the risk analysis of process facilities (Henley et al., 1996; AIChE, 2000, Smith, 2002). Figure 5.5 represents the types of uncertainty associated with each source. Among all of the uncertainty sources to date, the data uncertainty is the most critical issue for the risk assessment process (AIChE, 2000). However, there is no specific mathematical model for uncertainty analysis. Veseley, et al. (1981), Henley and Kumamoto (1996) and Abrahamsson (2002) describe a few methods for the uncertainty analysis of a FTA.

In present study an uncertainty analysis for the case study has been carried out to determine the cumulative error of imprecise basic events data that accumulates on the top event of a fault tree. Both conventional probability approach and fuzzy approach are used for this purpose. The uncertainty analysis for this case study is finally used for comparing

the conventional FTA approach and fuzzy FTA approach with respect to their error adjustment in computer-aided FTA. The detailed procedures of these two approaches are given in the following sections.

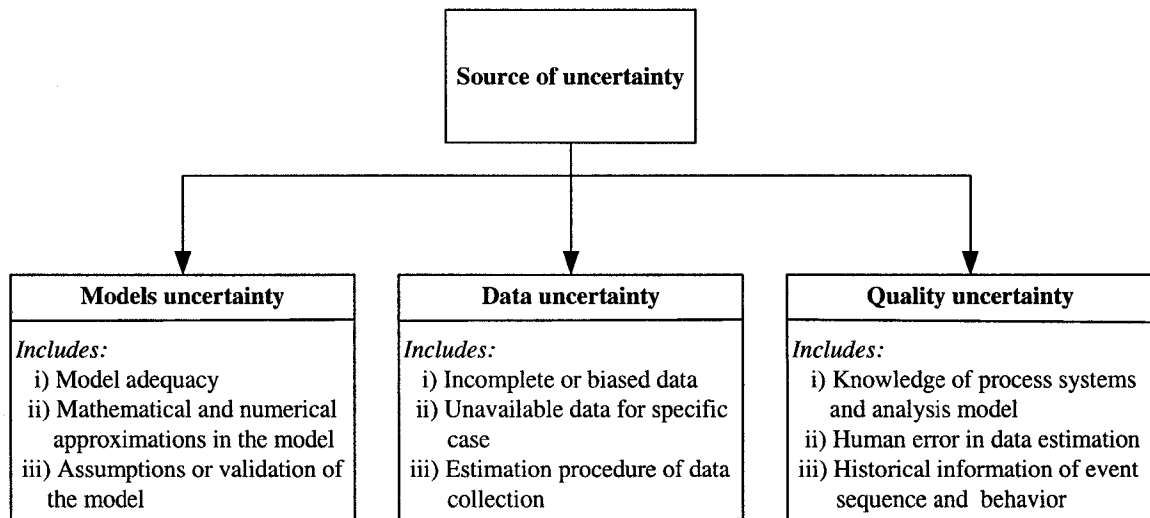


Figure 5.5: Source uncertainty in risk analysis of process facility (AIChE, 2000)

5.2.1 CONVENTIONAL PROBABILITY APPROACH

In the conventional approach, Monte Carlo simulation technique is used for the uncertainty analysis of a complex fault tree network (AIChE, 2000; Abrahamsson, 2002).

It uses the following steps for assessing parameters uncertainty:

- i. Select a distribution to describe possible values of a parameter.
- ii. Generate data from this distribution.
- iii. Use the generated data as probable values of the parameters in the model to produce output.

In this study, log-normal distribution is used for generating basic event data, assuming the error percentage in all basic events is α amount. The location and scale parameters for each error in the basic events of this case study are shown in Tables 5.8 and 5.9 respectively. The following two equations are used for calculating these two parameters of log-normal distribution (Henley and Kumamoto, 1996):

$$\mu = \ln(\tilde{Q}) \quad [5.1]$$

$$\alpha = \sqrt{e^{\sigma^2} (e^{\sigma^2} - 1)} \quad [5.2]$$

where, μ' = location Parameter; \tilde{Q} = median value of basic event probability; α = percentage level of error in basic events i.e., 5%, 10%, 15% and 20% ; σ = scale parameter.

Table 5.8: Location parameter for basic events

Basic Events	Basic Event data (\tilde{Q})	Location Parameter (μ')
BE1	1.000E-04	-9.210
BE2	1.000E-07	-16.118
BE3	6.640E-04	-7.317
BE4	7.450E-03	-4.900
BE5	1.000E-04	-9.210
BE6	2.200E-02	-3.817
BE7	8.330E-02	-2.485
BE8	1.000E-02	-4.605
BE9	3.700E-05	-10.205
BE10	2.000E-02	-3.912
BE11	6.910E-02	-2.672
BE12	1.000E-03	-6.908
BE13	3.700E-05	-10.205
BE14	2.510E-01	-1.382

Table 5.9: Scale parameter of log-normal distribution

Error in basic event data (%)	Scale parameter (□)
5%	0.2223
10%	0.3125
15%	0.3803
20%	0.4366

After generating 8000 random samples of each basic event, the top event probability is calculated using the minimal cutsets approach. Further, the percentage deviation with respect to exact top event probability for each α level of error is also calculated by using equation 5.3. Results are shown in Table 5.10. Normal error distribution approach is commonly used in most of the commercial software such as CARA faultTree, Relax fault Tree, FaultTree+.

$$\varepsilon = \frac{P_{T(\text{calculated})} - P_{T(\text{actual})}}{P_{T(\text{actual})}} \times 100 \quad [5.3]$$

In this equation, ε is percentage of deviation in top event probability, $P_{T(\text{calculated})}$ is estimated top event probability, $P_{T(\text{actual})}$ is actual value of top event probability.

5.2.2 FUZZY APPROACH

Khan and Abbasi (1999) developed an approach for uncertainty analysis of fuzzy FTA. In this approach, the events data are initially fuzzified by considering a definite amount of error in all basic event data and the top event probability is then calculated by using these fuzzified data. Besides this approach of uncertainty analysis, the present study has also developed an uncertainty analysis model for fuzzy FTA. This model generates a number of random samples for each basic event using two distributions in the whole trapezoidal region. The trapezoidal region of each basic event in this model first

subdivided into three sections and then for generating random samples, triangular distribution is used for the first and third sections, and uniform distribution is used for the second section, of the trapezoidal region. Figure 5.6 shows the model used for generating random sample of the basic events.

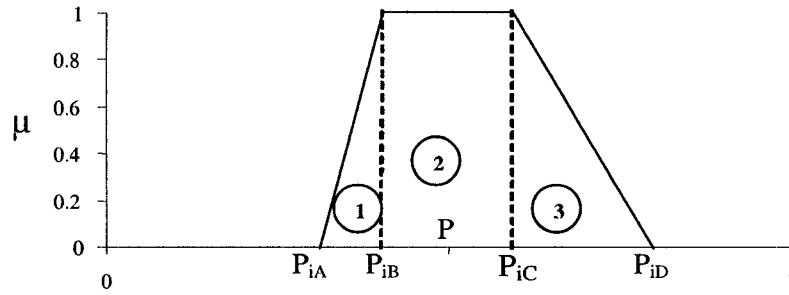


Figure 5.6. Uncertainty analysis model for fuzzy FTA

In this figure the triangular section 1 and 3 uses the triangular distributions and rectangular section 2 uses the uniform distributions for generating random samples for basic events. The lower bound and upper bound value (i.e., P_{iA} , P_{iB} , P_{iC} , P_{iD}) of each basic event (trapezoidal fuzzy set) is used to estimate the distribution parameters.

To compare the error robustness of fuzzy FTA with conventional FTA, this study uses both approaches for uncertainty quantifications. In the first approach (Khan and Abbasi, 1999), basic data are fuzzified considering all basic events with 5%, 10%, 15%, 20% error. These fuzzified data are then used to calculate the top event probability. The deviation of top event probability is then calculated by using equation 5.3. In the second approach of this study, different levels (5%, 10%, 15%, 20% error) of error are considered in basic event data. Then the random data for the trapezoidal fuzzy set of each basic event are generated using triangular and uniform distributions. The top event probability for the fault tree and its deviations from the exact value are calculated by

using equation 5.3.

As expected, both approaches almost predict the same results. The results could get significantly different in case of a very complex network. Table 5.10 presents a detailed comparison study of uncertainty propagation for both approaches. It also illustrates that if basic events data are not accurately measured, then error will accumulate throughout the top event probability calculation.

Table 5.10: Error robustness of fuzzy approach and conventional probability approach

Considered error in data	Approach		Top event probability [$P_{T(\text{calculated})}$]	Deviation (%)
5%	Fuzzy approach	First approach	2.959E-04	~2.0%
		Second approach	2.952E-04	
	Conventional Probability approach		2.920E-04	1.0%
10%	Fuzzy approach	First approach	2.975E-04	~3.0%
		Second approach	2.961E-04	
	Conventional Probability approach		3.327E-04	13.3%
15%	Fuzzy approach	First approach	2.985E-04	~3.5%
		Second approach	3.001E-04	
	Conventional Probability approach		3.486E-04	20.5%
20%	Fuzzy approach	First approach	3.036E-04	~5.0%
		Second approach	3.027E-04	
	Conventional Probability approach		4.630E-04	60%
No Error	Actual top event probability [$P_{T(\text{actual})}$] (considering all basic event data has accurately measured)		2.892 E-04	

SUMMARY

A case study has been discussed in this chapter to demonstrate the applications of the proposed methodology. This case study is a VX neutralization process adapted from the Wang et al. (2005), which is extensively discussed in the literature. Process description, fault tree development in the GUI, fault tree evaluation, and sensitivity

analysis of this case study are presented under section 5.1. The developed model for uncertainty analysis of fuzzy FTA has been discussed in section 5.2.2. The comparison of conventional approach with fuzzy approach for FTA has also been shown in this chapter. The results from the uncertainty analysis show that this methodology gives a more consistent result for FTA, even when the basic events have error during their data estimation.

Chapter 6

RESULT AND DISCUSSION

This chapter presents results and discussion of the proposed methodology and the case study illustrated in the previous chapter. In this chapter FTA results were compared with that of commercial software packages. Besides the comparison of the results, this chapter also gives a brief account of the current work and existing methodology with respect to the analysis strategy of FTA, conventional FTA and fuzzy FTA with regards to the uncertainty analysis.

6.1 FAULT TREE ANALYSIS (FTA)

A complete FTA for the process facility takes MCSs analysis, probability analysis, and sensitivity analysis into account. The MCSs are the minimal combinations of basic events that can result in the top event. Probability analysis estimates the probability of occurrence of the top event and the MCSs. The sensitivity analysis gives a numerical evaluation of the relative contribution of each basic event and MCSs to cause the top event. The complete analysis of a fault tree for the case study was already shown in section 5.1. The significant analyses of this case study obtained by using the described methodology are given below.

Fault tree evaluation:

Number of MCSs = 20

Most likely top event probability = 2.954E-04

Most important cutsets:

- i. BE4-BE6 has 58.94% contribution to cause the top event
- ii. BE1 has 33.85% contribution to cause the top event

Basic events improvement:

- i. The improvement value for BE6 is 28.29.
- ii. The improvement value for BE6 is 26.19.

The following sections use these FTA results for the comparison of the proposed methodology and the available strategy for FTA.

6.2 COMPARATIVE STUDY

Three types of comparisons between the proposed and existing methodology have been carried out in this chapter. The first comparison, given in section 6.2.1, is based on the models used in the current work and existing commercial packages. The second comparison, in section 6.2.2, is made by using the results obtained from the described and available methodologies. Finally, uncertainty analysis is conducted to compare these methodologies with respect to their error robustness. This is given in section 6.2.3.

6.2.1 COMPARISON USING METHODOLOGY

As discussed earlier, few computer-aided tools exist for FTA. The current study developed a revised methodology for the fuzzy based computer-aided FTA tool to yield

more efficient and accurate analysis from a fault tree. A comparison of this methodology with the ones used by existing software packages for the fault tree analysis has been depicted in Table 6.1. It is evident from the table that, for the most part, the proposed methodology is more advanced than the counterpart. The developed methodology should give a more accurate estimation for a fault tree and the risk analysis as well.

Table 6.1: FTA methodology used in existing software packages and in the current work

Sl. No	Fault tree analysis	Used in existing software packages	Used in current work
1	Modules finding for a fault tree	BDD, super-moduling, etc.	KHIC algorithm
2	MCSs determination for large fault tree	MOCUS or MICSUP with BDD or super moduling approach	KHIC algorithm with Boolean matrix transformation
3	Data precision	N/A	Fuzzified basic events data
4	Probability analysis	Conventional probability approach	Fuzzy approach
	Top event probability estimation	Use crisp data for the top event probability calculation	Use fuzzy data for the fuzzy top event probability calculation
5	Most likely top event probability estimation	N/A	Weighted average defuzzification method
6.	Basic events importance	FV importance, Brinbaum's importance, criticality importance	FWI
7	Cutsets impotance	FV cutsets importance,	Fuzzy based cutset importance
8	Uncertainty analysis	Normal probability approach	Fuzzy approach

6.2.2 COMPARISON USING RESULTS OF FTA

PROFAT and the proposed methodology give more accurate analysis for a fault tree. For the case study, the top event probability estimated by PROFAT is 3.131E-04.

But this is found to be 2.954E-04 by the developed methodology, which is almost the same as the probability obtained by Wang et al. (2005). PROFAT uses the centroid method for the top event probability defuzzification, which estimates the top event probability by giving equal emphasis in all membership values. The current study attempts to revise this limitation of PROFAT by defuzzifying the top event probability with weighted average method, which calculates the top event probability for a fault tree by weighting each membership function in the output by its respective maximum membership value. Detailed comparison studies of all results are presented in Table 6.2. The remaining analysis of a fault tree (e.g., the number of minimal cutsets, important basic event and important cutsets) predicts the same results as PROFAT or Relax Fault Tree.

Table 6.2: Results obtained for the case study using different approaches

Approach	Minimal Cutsets
Proposed Algorithm (current work)	20
PROFAT simulation	20
Relax Fault Tree	20
Approach	Important Basic Event
Proposed Algorithm (current work)	BE1,BE3,BE4,BE6
PROFAT simulation	BE1,BE3,BE4,BE6
Relax Fault Tree	It has no module to estimate system sensitivity
Approach	Top Event Probability
Proposed Algorithm (current work)	2.954E-04
PROFAT simulation	3.131E-04
Relax Fault Tree	2.892 E-04

6.2.3 COMPARISON USING UNCERTAINTY ANALYSIS

Conventional FTA (Conventional probability approach) uses crisp data for the probability analysis of a fault tree. It is apparent that if the basic events data has some percentage of error in estimation, it ultimately accumulates in the top event probability calculation of a fault tree. Fuzzy FTA (Fuzzy probability approach) analysis attempts to recover this limitation by fuzzifying the crisp data of basic events to fuzzy data. These fuzzified basic events data give a trapezoidal fuzzy set for the top event, which minimizes the error during the top event probability calculation. The uncertainty analysis in section 5.2 of the current study indicates that the fuzzy FTA (described methodology) gives a better result as compared to the conventional FTA (existing methodology), as even the basic events have error in their estimation. The results of the uncertainty analysis are shown in Figure 6.1. This figure depicts that the percentage of cumulative error in the top event probability, calculated by the conventional approach, increases abruptly with the increases of error in the basic events data. On the other hand, in the case of the proposed fuzzy FTA, the accumulation error on the top event probability appears to be negligible over the ranges of error in the basic events.

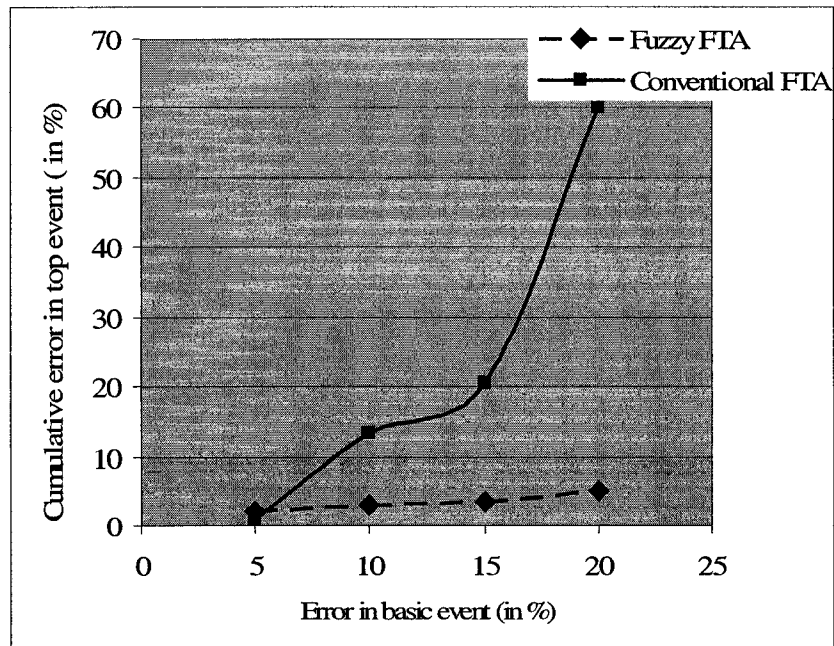


Figure 6.1: Error robustness of fuzzy FTA and conventional FTA

SUMMARY

The results obtained by simulating the case study with the proposed methodology have been discussed. The complete analysis of a fault tree for the case study provides a numerical evaluation for the top event probability calculation, as well as the system's weakest link, and weakest components detection. FTA helps to design a proper strategy to increase a system reliability and safety of a process facility. An uncertainty analysis has also been carried out to emphasize that the fuzzy based FTA handle imprecise basic events better compared to conventional fault tree analysis.

Chapter 7

CONCLUSIONS AND FUTURE WORK

FTA is widely used to assess the operational performance, reliability predictions, lifetime, and system safety of various complex systems as in a nuclear reactor, aerospace system, petrochemical industry, process industry, or oil and gas transmission system. Model and parameter uncertainties are the main barriers for achieving precise results from a fault tree. Fuzzy set theory used in FTA attempts to remove these uncertainties from the conventional fault tree analysis. The proposed methodology is a revised version of the PROFAT algorithm, revisions aimed to improve fuzzy number characterization, fuzzy based top event probability calculation and uncertainty propagation. Further, the fuzzy weighted index and the cutsets importance measuring technique of this methodology provide valuable information about the basic event sensitivity, paths sensitivity and the probable scope for improving overall system performance. The following are the key features of the described methodology.

Features in FTA methodology:

- ***Ability to Handle Large and Complex trees:*** An efficient KHIC algorithm is used to modularize the fault tree into sub-trees. This is the key to handle large and complex fault trees.

- ***Adjustment of Data Uncertainty:*** The fuzzy model in the probability analysis module minimizes the uncertainty in the basic event data by distributing the error to a trapezoidal membership function.
- ***Reliable Analysis:*** Basic event data fuzzification and fuzzy arithmetic operations in probability calculation assist to get a more realistic and reliable analysis (tilting towards the conservative side) of a complete fault tree.
- ***Sensitivity Analysis:*** The two integrated features, i.e., fuzzy weighted index and cutsets importance, in sensitivity analysis give more robust predictions of a system reliability/failure probability.

To illustrate the comparisons of fuzzy FTA and conventional FTA, an uncertainty analysis was carried out for estimating the cumulative error in the top event of a fault tree if the basic events have error in data estimation. The uncertainty analysis of the fuzzy based uncertainty quantification and its comparisons with the normal probabilistic uncertainty quantification have shown that this approach (fuzzy FTA) is more realistic and robust to handle the imprecise basic event data of FTA.

Features of fuzzy approach in uncertainty analysis:

- It distributes all basic event errors in the whole trapezoidal region and thus attempts to represent a more realistic scenario when the actual amounts of data uncertainty are not known with sufficient confidence.

- It could be computationally efficient, as it would avoid data eclipsing by dividing a complex fuzzy membership function into different regions and calculate error using these regions.

7.2 FUTURE WORK

This work proposes a fuzzy based computer-aided methodology for fault tree analysis. The following recommendations have been suggested for the future improvement of the proposed study:

- i. The fuzzy approach in this methodology is a new approach for the evaluation technique of FTA. Hence, in order to make the methodology more reliable and competitive with the existing methodology, it is necessary that the evaluation strategy of FTA in this study be properly compared and validated with the analysis of some more FTA case studies of process facilities.
- ii. Conventional FTA cannot reflect the real situation of basic events data estimation, which is recovered in this study by using a fuzzy model for probability analysis of FTA. This model can be further modified by incorporating expertise elicitation criteria for evaluating the basic events data, more precisely.
- iii. The present fault tree analysis is static in nature. Attempts need to be made to bring dynamic characteristics into fault tree analysis. This would help in carrying out time dependent analysis.

- iv. The developed computer code in VISUAL BASIC needs further modification to make it more user friendly and reliable computer aided FTA tool for the process facility. Then, the developed methodology, along with the supporting tools of FTA, can be used to enhance the application of FTA tools in the risk analysis of the process facility.

REFERENCES

- Abrahamsson, M. (2002). "Uncertainty in Quantitative Risk Analysis –Characterization and Methods of Treatment", *Report # 1024(ISSN: 1402-3504), Brandteknik, Lunds tekniska högskola, Lunds universitet, Lund*
- AICHE (2000). *Guidelines for chemical process quantitative risk analysis*, Second Edition, New York: AIChE.
- Billington, R. and Allen, R.N. (1986). *Reliability evaluation of engineering system*, Marshfield, MA: Pitman Publishing Inc.
- Birnbaum, Z.W. and Esary, J.P. (1965). "Modules of coherent binary systems", *Journal of Applied Mathematics*, **13**, 442-462.
- CARA-Fault Tree light edition 4.1 SR1. (1999). Sysdvest software (www.sysdvest.com).
- Chatterjee, P. (1975). "Modularization of fault trees: a method to reduce the cost of analysis", *Reliability and Fault Tree Analysis*, SIAM, 101-137.
- Cheng, Y. (2000). "Uncertainties in Fault Tree Analysis", *Tamkang Journal of Science and Engineering*, **3**(1), 23-29.

- Contini, S., Scheer, S. and Wilikens, M. (2000). "Sensitivity analysis for system design improvement", *Joint Research Centre, Institute for Systems, Informatics and Safety*, T.P. 210, I-21020 Ispra (VA), Italy.
- Cheong W.C. and Lan-Hui L.A. (2004). "Web access failure analysis – fuzzy reliability approach." *International Journal of the Computer, the Internet and Management*, **12**, 65-73.
- Crowl D.A., Louvar J.F. (2002). "*Chemical Process Safety, Fundamentals with Applications – 2nd edition*", Upper Saddle River, N.J.: Prentice Hall PTR.
- Elliott, M.S. (1994). "Computer-assisted fault-tree construction using a knowledge-based approach", *IEEE Transactions on Reliability*, **R43**, 112-120.
- FaultTree+ Version 11.0 Demo, Isograph Software Ltd., (<http://www.isograph-software.com>).
- Fussell, J.B. (1973). "A formal methodology for fault tree construction", *Nuclear Science & Engineering*, **52**, 421-432.
- Fussell, J.B., Henry, E.B., and Marshall, N.H. (1974b). "MOCUS: A computer program to obtain Minimal Cut Sets from Fault Tree." Report ANCR-1156, Idaho falls, ID: Aerojet Nuclear Company.

- Guimariães, C.F. Anonio and Ebecken, F.F. Nelson (1999). "FuzzyFTA:a fuzzy fault tree system for uncertainty analysis". *Annals of Nuclear Energy, Elsevier Science Ltd.*, **26**, 523-532.
- Hassal, D.F. (1965). "Advanced concepts in fault tree analysis", *System Safety Symposium, Seattle, Boeing Company*, 8-9.
- Han, H. S., Kim, W.T., and Yoo, J. K. (1988). "Development of an Integrated Fault tree Analysis Computer Code Module by Modularization Technique". *Reliability Engineering & System Safety*, **21**, 145-154.
- Hauptmanns U. (1980). "Fault tree analysis of a proposed ethylene vaporization unit." *Industrial Engineering Chemical Fundamentals*, **19**, 301.
- Hauptmanns, U. (1988). "Fault tree analysis for process industries engineering risk and hazard assessment", *Engineering Risk and Hazard Assessment, CRC Press Inc., Florida*, **V1**, 21-59.
- Henley, E.J. and Kumamoto, H. (1981). *Reliability engineering and risk assessment*, New Jersey: Prentice-Hall Inc.
- Henley, E.J. and Kumamoto, H. (1996). *Probabilistic risk assessment and management for engineers and scientists*, Second Edition, New York: IEE Press.
- HSE (1996). "Offshore accident/incident statistics report".OTO96.954, Health and Safety Executive, London, UK.

- Kaplan, S., Garrick, B.J. (1981). "On the quantitative definition of risk". *Risk Analysis*. **1** (1), 11-27.
- Khan, F.I. and Abbasi S.A. (1999). "PROFAT: A user friendly system for probabilistic fault tree analysis", *Process Safety Progress*, **18**.
- Klir, J. G. and Yuan, B. (2001). *Fuzzy Sets and Fuzzy logic Theory and Applications*, Prentice, Hall of India Private ltd.
- Kohda, T., Henley, E.J. and Inoue, K. (1989). "Finding modules in fault trees", *IEEE Transactions on Reliability*, **R38**, 165-176.
- Lai, F. S., Sheno, S. and Fan, T.L. (1993). "Fuzzy fault tree analysis theory and applications", *Engineering Risk and Hazard Assessment*, CRC Press Inc., Florida, **V1**, 117-137.
- Lapp, S.A. and Powers, G.J. (1977). "Computer-aided synthesis of fault trees", *IEEE Transactions on Reliability*, **R26**, 2-13.
- Lapp, S.A. and Powers, G.J. (1979). "Update of Lapp-Powers fault-tree synthesis algorithm", *IEEE Transactions on Reliability*, **R28**, 12-15.
- Lawley, H.G. (1980). "Safety technology in chemical industry: A problem in Hazard analysis with solution ".*Reliability engineering*, **1**, 89-113

- Lees, F. P. (1996). *Loss prevention in the process industries*, Second Edition, 1, London: Butterworths.
- Liang, G. and Wang, J. M. (1993). "Fuzzy fault tree analysis using failure possibility", *Microelectronics and Reliability*, **33(4)**, 583-597.
- Ljungquist, K. (2003). "Probabilistic Design for Evaluation of Indoor environment". Licentiate thesis, Submitted to LULEÅL University of Technology
- Locks, M.O. (1981). "Modularizing, minimizing, and interpreting the K & H fault-tree." *IEEE Transactions on Reliability*, **R30**, 411-415.
- Mansfield, D.P., Kletz, T.A., and Al-Hassn, T. (1996a). "Optimizing safety by inherent offshore platform design". *Proceedings of 1996 OMAE conference-Volume II) Safety and Reliability*), June 16-20, Florence, Italy.
- McCormick, N.J. (1981). *Reliability and risk analysis*, New York: Academic Press.
- Misra, B. K. and Weber, G. G. (1990). "Use of Fuzzy set theory for level-1 studies in probabilistic risk assessment", *Fuzzy Sets and system*, **37**, 139-160.
- Mogford, J. (2005). "Isomerization Unit Explosion Interim Report". Texas City, Texas, USA
- Pan, H. and Yun, W. (1997). "Fault tree analysis with fuzzy gates". *Computers Industrial Engineering*, Elsevier Science Ltd., **33 (3-4)**, 569-572.

- Pula, C, R, (2005). "An integrated system for fire and explosion consequence analysis of offshore process facilities ".A thesis submitted to Memorial university of Newfoundland in partial fulfillment of the requirements for the degree of Master of Engineering.
- Reay, K. and Andrews, J.D. (2002). "A fault tree analysis strategy using binary decision diagrams", *Reliability Engineering and System Safety*, **78**, 45-56.
- Relax Reliability Software V7.7, (www.relaxsoftware.com.)
- Sawyer, P. J. and Rao, S. S. (1994). "Fault tree analysis of Fuzzy Mechanical system", *Microelectronics and Reliability*, **34(4)**, 653-667.
- Shafaghi, A. (1988). "Structure modeling of process system for risk and reliability analysis", *Engineering Risk and Hazard Assessment, CRC Press Inc., Florida*, **V2**, 45-64.
- Shengping, X., Wenxian, Y. and Zhaowen, Z. (2000). "Fuzzy fault tree analysis based on failure rate as fuzzy number", *Proceedings of 7th International Conference on Industrial Engineering and management*, 505-510.
- Singer, D. (1990). "A fuzzy approach to fault tree and reliability analysis", *Fuzzy Sets and system*, **34**, 145-155.
- Suresh, V. P., Babar, A. K. and Raj, V. V. (1996). "Uncertainty in Fault tree analysis: A fuzzy approach", *Fuzzy Sets and system*, **83**, 135-141.

- Tanaka, H., Fan, T. L., Lai, F. S & Toughi, K. (1983). "Fault tree analysis by fuzzy probability". *IEEE Transactions on reliability*, **32(5)**, 455-457.
- Veseley, W. E., Goldberg, F. F., Roberts, N. H. and Haasl, D. F. (1981). *Fault tree handbook*, U.S. Nuclear Regulatory Commission, NUREG-0492, Washington, DC.
- Wang, Y. (2004). "Development of a computer-aided fault tree synthesis methodology for quantitative risk analysis in the chemical process industry", Submitted to Texas A&M University in partial fulfillment of the requirements for the degree of Doctor of Philosophy.
- Wang, Y., West, H. H., Hasan, N. and Mannan, M. S. (2005). "QRA study of an activated carbon filter safeguard system", *Process Safety and Environmental Protection*, **83 (B2)**, 191-196.
- Wu, C. (2004). "Fuzzy reliability estimation using Bayesian approach", *Computer & Industrial Engineering*, **46**, 467-493.
- Ying, H., Chaozhen, H. and Shuangxi, L. (1998). "Application of fuzzy set theory in fault tree Analysis", *Chinese Journal of mechanical Engineering*, **11(4)**, 326-332.
- Yllera, J. (1998). "Modularization methods for evaluating fault tree of complex technical system", *Engineering risk and hazard assessment*, CRC Press Inc, Florida, **V2**, 81-99.

Yuhua, D. and Datao, Y. (2005). "Estimation of failure probability of oil and gas transmission pipelines by Fuzzy fault tree analysis", *Journal of Loss prevention in the process industries*, **18**, 83-88.

Table A1.1: Basic events and its symbols in the fault tree (Hauptmanns, 1980)

Basic events Name	Symbols	Basic event Name	Symbols
Pressure measurement P1 fails	X-1	S1 fails closed	X-24
Valve positioner V1 fails	X-2	S1 fails open	X-25
Signal transmission P1-V1 fails	X-3	S1 set point too high	X-26
V1 fails closed	X-4	S2 fails closed	X-27
V1 fails open	X-5	S2 fails open	X-28
Valve positioner V2 fails	X-6	S2 set point too high	X-29
Signal transmission P1-V2 fails	X-7	Ethylene pump fails	X-30
V2 fails closed	X-8	Spontaneous rupture of deposit	X-31
Instrument air supply fails	X-9	Pipe work fire	X-32
Temperature measurement T1 fails	X-10	External & secondary effects	X-33
Valve positioner V3 fails	X-11	Ethylene vaporizer functioning	X-34
Signal transmission T1-V3 fails	X-12	Pressure vaporizer not functioning	X-35
Pressure measurement P2 fails	X-13	Heater not functioning	X-36
Signal transmission P2-V3	X-14	Ethylene pump demanded	X-37
Flow measurement F1 fails	X-15	Exit to process closed	X-38
Signal transmission F1-V3 fails	X-16	Exit to recompression closed	X-39
V3 fails closed	X-17	No discharge via V2	X-40
V3 fails open	X-18	Pressurization via V1	X-41
Level measurement L1 fails	X-19	Supply to deposit functioning	X-42
Signal transmission L1-V4 fails	X-20	Exit temperature below -10°C	X-43
Valve positioner V4 fails	X-21	Exit manometric pressure > 16.18 bar	X-44
V4 fails closed	X-22	Exit flow > demand	X-45
V4 fails open	X-23	Deposit manometric pressure < 1.96 bar	X-46

Table A 1.2: Connection list of the large fault tree

Sl. No.	Gate event	Gate type	Connected events		
1	G1	OR	G2	X-31	X-32
2	G2	AND	G3	G4	G5
3	G3	OR	G6	G7	X-32
4	G6	AND	G10	X-35	
5	G10	OR	G14	X-5	
6	G14	AND	G17	X-9	X-4
7	G17	AND	G19	X-46	
8	G19	AND	X-1	X-2	X-32
9	G7	AND	G11	G12	
10	G11	AND	X-30	X-37	
11	G12	OR	G15	X-9	X-17
12	G15	AND	G18	X-9	X-17
13	G18	OR	G20	G21	G22
14	G20	AND	G23	X-43	
15	G23	AND	X-10	X-11	X-12
16	G21	AND	G24	X-44	
17	G24	AND	X-11	X-13	X-14
18	G22	AND	G25	G45	
19	G25	AND	X-11	X-15	X-16
20	G4	OR	X-24	X-26	
21	G5	OR	G8	G9	X-40
22	G8	AND	G13	X-40	X-9
23	G13	OR	G16	X-8	
24	G16	OR	X-1	X-6	X-7
25	G9	AND	X-40	X-9	

Table A1. 3: Identified modules and Minimal cutsets for the fault tree

Modules	Minimal Cutsets	Cutsets in Each Module
<u>G13</u>	(G16) (X-8) (X-21) (X-6) (X-7) (X-8)	4
<u>G4</u>	(X-24) (X-26)	2
<u>G22</u>	(G25, X-45) (X-15, X-11, X-16, X-45)	1
<u>G21</u>	(G24, X-43) (X-13, X-11, X-14, X-44)	1
<u>G20</u>	(G23, X-43) (X-10, X-11, X-12, X-43)	1
<u>G18</u>	(G20) (G21) (G22)	3
<u>G11</u>	(X-30, X-37)	1
<u>G7</u>	(G11, G12) [(X-30, X-37), (G15), (X-9), (X-17)] [(X-30, X-37), (G18, X-9, X-17), (X-9), (X-17)] [(X-30, X-37), [(G20)(G21)(G22), (X-9), (X-17)], X-9, X-17],	5
<u>G17</u>	(G19, X-46) (X-1, X-2, X-3, X-46)	1
<u>G10</u>	(G14) (X-5) (G17, X-9, X-4)(X-5)	2
<u>G6</u>	(G10, X-35)	2
<u>G3</u>	(G6) (G7) (X-32)	8
<u>G2</u>	(G3, G4, G5)	78
<u>G1</u>	(G2) (X-31) (X-33)	80

APPENDIX B

FAULT TREE ANALYSIS BY PROFAT TOOL

B1: MCSs determination by PROFAT tool for the case study

PROFAT (PRObability FAult Tree analysis)
F.I.Khan & S.A.Abbasi - Pondicherry 605014

MINIMAL PATH WAYS

```
1
2
3 6
4 6
5 6
3 7 8 9
3 12 14
4 7 8 9
4 12 14
5 7 8 9
5 12 14
3 7 8 10
3 7 8 11
3 13 14
4 7 8 10
4 7 8 11
4 13 14
5 7 8 10
5 7 8 11
5 13 14
```

N.B: PROFAT uses 1, 2, 3.....n for the basic events labeling of a fault tree.

B2: Probability analysis by PROFAT tool for the case study

PROFAT (PRObability FAult Tree analysis)
 F.I.Khan & S.A.Abbasi - Pondicherry 605014

PROBABILITY/ FREQUENCY (/yr)	MINIMAL PATH WAY (Event Numbers)
1.000000e-04	1
0.000000e+00	2
1.689050e-05	3 6
1.895094e-04	4 6
2.543750e-06	5 6
4.033072e-11	3 7 8 9
2.447877e-07	3 12 14
4.525058e-10	4 7 8 9
2.746489e-06	4 12 14
6.073904e-12	5 7 8 9
3.686562e-08	5 12 14
2.180039e-08	3 7 8 10
7.532036e-08	3 7 8 11
9.057148e-09	3 13 14
2.445977e-07	4 7 8 10
8.450853e-07	4 7 8 11
1.016201e-07	4 13 14
3.283191e-09	5 7 8 10
1.134343e-08	5 7 8 11

Total Probability: 3.132844e-04

B3: Fuzzy based probability analysis by PROFAT tool for the case study

PROFAT (PRObability FAult Tree analysis)
F.I.Khan & S.A.Abbasi - Pondicherry 605014

IMPROVEMENT INDEX RESULTS

Event not- occurring	Probability	Improvement	Improvement Index
0	3.131777e-04	0.000000e+00	0.000000
1	2.131909e-04	3.999473e-04	18.797096
2	3.131628e-04	5.966285e-08	0.002804
3	2.958924e-04	6.914145e-05	3.249575
4	1.197904e-04	7.735491e-04	36.355988
5	3.106445e-04	1.013288e-05	0.476235
6	1.042634e-04	8.356571e-04	39.274998
7	3.120005e-04	4.708869e-06	0.221312
8	3.120005e-04	4.708869e-06	0.221312
9	3.131628e-04	5.966285e-08	0.002804
10	3.129095e-04	1.073029e-06	0.050431
11	3.122538e-04	3.695532e-06	0.173686
12	3.101379e-04	1.215933e-05	0.571476
13	3.130883e-04	3.576279e-07	0.016808
14	3.100634e-04	1.245744e-05	0.5854877

APPENDIX C

UNCERTAINTY ANALYSIS

C1: 5% ERROR IN BASIC EVENTS

C1.1 Uncertainty analysis for conventional probability approach

Table C1.1: MiniTab output

Variable	N	Mean	SE Mean	StDev	Median
Top event	8000	0.0002926	0.000000707	0.0000632	0.000289

C1.2 Uncertainty analysis for fuzzy probability approach

Table C1.2.1: Fuzzy probability with -5.0 % error in basic events data

Fuzzy Probability	Fuzzy Number with -5% error ('around')	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	9.500E-05	4.750E-05	7.125E-05	1.188E-04	1.425E-04
P_{BE2}	9.500E-08	4.750E-08	7.125E-08	1.188E-07	1.425E-07
P_{BE3}	6.308E-04	3.154E-04	4.731E-04	7.885E-04	9.462E-04
P_{BE4}	7.078E-03	3.539E-03	5.308E-03	8.847E-03	1.062E-02
P_{BE5}	9.500E-05	4.750E-05	7.125E-05	1.188E-04	1.425E-04
P_{BE6}	2.090E-02	1.045E-02	1.568E-02	2.613E-02	3.135E-02
P_{BE7}	7.914E-02	3.957E-02	5.935E-02	9.892E-02	1.187E-01
P_{BE8}	9.500E-03	4.750E-03	7.125E-03	1.188E-02	1.425E-02
P_{BE9}	3.515E-05	1.758E-05	2.636E-05	4.394E-05	5.273E-05
P_{BE10}	1.900E-02	9.500E-03	1.425E-02	2.375E-02	2.850E-02
P_{BE11}	6.565E-02	3.282E-02	4.923E-02	8.206E-02	9.847E-02
P_{BE12}	9.500E-04	4.750E-04	7.125E-04	1.188E-03	1.425E-03
P_{BE13}	3.515E-05	1.758E-05	2.636E-05	4.394E-05	5.273E-05
P_{BE14}	2.385E-01	1.192E-01	1.788E-01	2.981E-01	3.577E-01

Table C1.2.2: Fuzzy probability of MCSs (-5% error in basic events)

MCSs	Trapezoidal representations ($P_{iA}, P_{iB}, P_{iC}, P_{iD}$)			
BE1	4.750E-05	7.125E-05	1.188E-04	1.425E-04
BE2	4.750E-08	7.125E-08	1.188E-07	1.425E-07
BE3 BE6	3.296E-06	7.416E-06	2.060E-05	2.966E-05
BE4 BE6	3.698E-05	8.320E-05	2.311E-04	3.328E-04
BE5 BE6	4.964E-07	1.117E-06	3.102E-06	4.467E-06
BE3 BE7 BE8 BE9	1.042E-12	5.274E-12	4.070E-11	8.439E-11
BE4 BE7 BE8 BE9	1.169E-11	5.918E-11	4.566E-10	9.468E-10
BE5 BE7 BE8 BE9	1.569E-13	7.943E-13	6.129E-12	1.271E-11
BE3 BE12 BE14	1.786E-08	6.028E-08	2.791E-07	4.823E-07
BE4 BE12 BE14	2.004E-07	6.764E-07	3.131E-06	5.411E-06
BE5 BE12 BE14	2.690E-09	9.079E-09	4.203E-08	7.263E-08
BE3 BE7 BE8 BE10	5.631E-10	2.851E-09	2.200E-08	4.561E-08
BE4 BE7 BE8 BE10	6.318E-09	3.199E-08	2.468E-07	5.118E-07
BE5 BE7 BE8 BE10	8.481E-11	4.294E-10	3.313E-09	6.870E-09
BE3 BE7 BE8 BE11	1.946E-09	9.850E-09	7.600E-08	1.576E-07
BE4 BE7 BE8 BE11	2.183E-08	1.105E-07	8.527E-07	1.768E-06
BE5 BE7 BE8 BE11	2.930E-10	1.483E-09	1.145E-08	2.373E-08
BE3 BE13 BE14	6.609E-10	2.230E-09	1.033E-08	1.784E-08
BE4 BE13 BE14	7.415E-09	2.503E-08	1.159E-07	2.002E-07
BE5 BE13 BE14	9.953E-11	3.359E-10	1.555E-09	2.687E-09

Table C1.2.3: Fuzzy probability with 5.0 % error in basic events data

Fuzzy Probability	Fuzzy Number with 5% error ("around")	Trapezoidal representations ($P_{iA}, P_{iB}, P_{iC}, P_{iD}$)			
P_{BE1}	1.050E-04	5.250E-05	7.875E-05	1.313E-04	1.575E-04
P_{BE2}	1.050E-07	5.250E-08	7.875E-08	1.313E-07	1.575E-07
P_{BE3}	6.972E-04	3.486E-04	5.229E-04	8.715E-04	1.046E-03
P_{BE4}	7.823E-03	3.911E-03	5.867E-03	9.778E-03	1.173E-02
P_{BE5}	1.050E-04	5.250E-05	7.875E-05	1.313E-04	1.575E-04
P_{BE6}	2.310E-02	1.155E-02	1.733E-02	2.888E-02	3.465E-02
P_{BE7}	8.747E-02	4.373E-02	6.560E-02	1.093E-01	1.312E-01
P_{BE8}	1.050E-02	5.250E-03	7.875E-03	1.313E-02	1.575E-02
P_{BE9}	3.885E-05	1.943E-05	2.914E-05	4.856E-05	5.828E-05
P_{BE10}	2.100E-02	1.050E-02	1.575E-02	2.625E-02	3.150E-02
P_{BE11}	7.256E-02	3.628E-02	5.442E-02	9.069E-02	1.088E-01
P_{BE12}	1.050E-03	5.250E-04	7.875E-04	1.313E-03	1.575E-03
P_{BE13}	3.885E-05	1.943E-05	2.914E-05	4.856E-05	5.828E-05
P_{BE14}	2.636E-01	1.318E-01	1.977E-01	3.294E-01	3.953E-01

Table C1.2.4: Fuzzy probability of MCSs (5% error in basic events)

MCSs	Trapezoidal representations ($P_{iA}, P_{iB}, P_{iC}, P_{iD}$)			
BE1	5.250E-05	7.875E-05	1.313E-04	1.575E-04
BE2	5.250E-08	7.875E-08	1.313E-07	1.575E-07
BE3 BE6	4.026E-06	9.059E-06	2.516E-05	3.624E-05
BE4 BE6	4.517E-05	1.016E-04	2.823E-04	4.066E-04
BE5 BE6	6.064E-07	1.364E-06	3.790E-06	5.457E-06
BE3 BE7 BE8 BE9	1.555E-12	7.871E-12	6.073E-11	1.259E-10
BE4 BE7 BE8 BE9	1.744E-11	8.831E-11	6.814E-10	1.413E-09
BE5 BE7 BE8 BE9	2.341E-13	1.185E-12	9.146E-12	1.897E-11
BE3 BE12 BE14	2.412E-08	8.139E-08	3.768E-07	6.512E-07
BE4 BE12 BE14	2.706E-07	9.132E-07	4.228E-06	7.306E-06
BE5 BE12 BE14	3.632E-09	1.226E-08	5.675E-08	9.807E-08
BE3 BE7 BE8 BE10	8.404E-10	4.254E-09	3.283E-08	6.807E-08
BE4 BE7 BE8 BE10	9.429E-09	4.773E-08	3.683E-07	7.638E-07
BE5 BE7 BE8 BE10	1.266E-10	6.407E-10	4.944E-09	1.025E-08
BE3 BE7 BE8 BE11	2.904E-09	1.470E-08	1.134E-07	2.352E-07
BE4 BE7 BE8 BE11	3.258E-08	1.649E-07	1.273E-06	2.639E-06
BE5 BE7 BE8 BE11	4.373E-10	2.214E-09	1.708E-08	3.542E-08
BE3 BE13 BE14	8.923E-10	3.012E-09	1.394E-08	2.409E-08
BE4 BE13 BE14	1.001E-08	3.379E-08	1.564E-07	2.703E-07
BE5 BE13 BE14	1.344E-10	4.536E-10	2.100E-09	3.628E-09

Table C1.2.5: Top event probability with 5 % error in basic events

Fuzzy probability analysis	$P_{A(T)}$	$P_{B(T)}$	$P_{C(T)}$	$P_{D(T)}$
Top event fuzzy set (5.0% error)	1.027E-04	1.922E-04	4.493E-04	6.179E-04
Top event fuzzy set (-5.0% error)	8.858E-05	1.640E-04	3.785E-04	5.182E-04
Most likely Top Event	2.959E-04			
Exact top event probability	2.892 E-04			
Percentage of error on top-event	~2.3% (approximately)			

Table C1.2.6: Fuzzy top event probability calculated by the random samples (5 % error in basic events)

Number of random samples: 8000

Fuzzy probability analysis	$P_{A(T)}$	$P_{B(T)}$	$P_{C(T)}$	$P_{D(T)}$
Top event fuzzy set (5.0% error)	1.199E-04	2.021E-04	4.568E-04	5.769E-04
Top event fuzzy set (-5.0% error)	9.393E-05	1.592E-04	3.627E-04	4.566E-04
Most likely Top Event	2.952E-04			
Exact top event probability	2.892 E-04			
Percentage of error on top-event	~2.3% (approximately)			

C2: 10% ERROR IN BASIC EVENTS

C2.1 Uncertainty analysis for conventional probability approach

Table C2.1: MiniTab output

Variable	N	Mean	SE Mean	StDev	Median
Top event	8000	0.000324	0.00000104	0.000104	0.000308

C2.2 Uncertainty analysis for fuzzy probability approach

Table C2.2.1: Fuzzy probability with -10.0 % error in basic events data

Fuzzy Probability	Fuzzy Number with -10% error ("around")	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	9.000E-05	4.500E-05	6.750E-05	1.125E-04	1.350E-04
P_{BE2}	9.000E-08	4.500E-08	6.750E-08	1.125E-07	1.350E-07
P_{BE3}	5.976E-04	2.988E-04	4.482E-04	7.470E-04	8.964E-04
P_{BE4}	6.705E-03	3.353E-03	5.029E-03	8.381E-03	1.006E-02
P_{BE5}	9.000E-05	4.500E-05	6.750E-05	1.125E-04	1.350E-04
P_{BE6}	1.980E-02	9.900E-03	1.485E-02	2.475E-02	2.970E-02
P_{BE7}	7.497E-02	3.749E-02	5.623E-02	9.371E-02	1.125E-01
P_{BE8}	9.000E-03	4.500E-03	6.750E-03	1.125E-02	1.350E-02
P_{BE9}	3.330E-05	1.665E-05	2.498E-05	4.163E-05	4.995E-05
P_{BE10}	1.800E-02	9.000E-03	1.350E-02	2.250E-02	2.700E-02
P_{BE11}	6.219E-02	3.110E-02	4.664E-02	7.774E-02	9.329E-02
P_{BE12}	9.000E-04	4.500E-04	6.750E-04	1.125E-03	1.350E-03
P_{BE13}	3.330E-05	1.665E-05	2.498E-05	4.163E-05	4.995E-05
P_{BE14}	2.259E-01	1.130E-01	1.694E-01	2.824E-01	3.389E-01

Table C2.2.2: Fuzzy probability of MCSs (-10% error in basic events)

MCSs	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
BE1	4.500E-05	6.750E-05	1.125E-04	1.350E-04
BE2	4.500E-08	6.750E-08	1.125E-07	1.350E-07
BE3 BE6	2.958E-06	6.656E-06	1.849E-05	2.662E-05
BE4 BE6	3.319E-05	7.468E-05	2.074E-04	2.987E-04
BE5 BE6	4.455E-07	1.002E-06	2.784E-06	4.010E-06
BE3 BE7 BE8 BE9	8.392E-13	4.248E-12	3.278E-11	6.798E-11
BE4 BE7 BE8 BE9	9.416E-12	4.767E-11	3.678E-10	7.627E-10
BE5 BE7 BE8 BE9	1.264E-13	6.398E-13	4.937E-12	1.024E-11
BE3 BE12 BE14	1.519E-08	5.126E-08	2.373E-07	4.101E-07
BE4 BE12 BE14	1.704E-07	5.751E-07	2.662E-06	4.601E-06
BE5 BE12 BE14	2.287E-09	7.719E-09	3.574E-08	6.176E-08
BE3 BE7 BE8 BE10	4.536E-10	2.296E-09	1.772E-08	3.674E-08
BE4 BE7 BE8 BE10	5.090E-09	2.577E-08	1.988E-07	4.123E-07
BE5 BE7 BE8 BE10	6.832E-11	3.459E-10	2.669E-09	5.534E-09
BE3 BE7 BE8 BE11	1.567E-09	7.934E-09	6.122E-08	1.269E-07
BE4 BE7 BE8 BE11	1.758E-08	8.902E-08	6.869E-07	1.424E-06
BE5 BE7 BE8 BE11	2.360E-10	1.195E-09	9.220E-09	1.912E-08
BE3 BE13 BE14	5.619E-10	1.897E-09	8.780E-09	1.517E-08
BE4 BE13 BE14	6.305E-09	2.128E-08	9.851E-08	1.702E-07
BE5 BE13 BE14	8.463E-11	2.856E-10	1.322E-09	2.285E-09

Table C2.2.3: Fuzzy probability with 10.0 % error in basic events data

Fuzzy Probability	Fuzzy Number with 10% error (“around”)	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	1.100E-04	5.500E-05	8.250E-05	1.375E-04	1.650E-04
P_{BE2}	1.100E-07	5.500E-08	8.250E-08	1.375E-07	1.650E-07
P_{BE3}	7.304E-04	3.652E-04	5.478E-04	9.130E-04	1.096E-03
P_{BE4}	8.195E-03	4.098E-03	6.146E-03	1.024E-02	1.229E-02
P_{BE5}	1.100E-04	5.500E-05	8.250E-05	1.375E-04	1.650E-04
P_{BE6}	2.420E-02	1.210E-02	1.815E-02	3.025E-02	3.630E-02
P_{BE7}	9.163E-02	4.582E-02	6.872E-02	1.145E-01	1.374E-01
P_{BE8}	1.100E-02	5.500E-03	8.250E-03	1.375E-02	1.650E-02
P_{BE9}	4.070E-05	2.035E-05	3.053E-05	5.088E-05	6.105E-05
P_{BE10}	2.200E-02	1.100E-02	1.650E-02	2.750E-02	3.300E-02
P_{BE11}	7.601E-02	3.801E-02	5.701E-02	9.501E-02	1.140E-01
P_{BE12}	1.100E-03	5.500E-04	8.250E-04	1.375E-03	1.650E-03
P_{BE13}	4.070E-05	2.035E-05	3.053E-05	5.088E-05	6.105E-05
P_{BE14}	2.761E-01	1.381E-01	2.071E-01	3.451E-01	4.142E-01

Table C2.2.4: Fuzzy probability of MCSs (10% error in basic events)

MCSs	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
BE1	5.500E-05	8.250E-05	1.375E-04	1.650E-04
BE2	5.500E-08	8.250E-08	1.375E-07	1.650E-07
BE3 BE6	4.419E-06	9.943E-06	2.762E-05	3.977E-05
BE4 BE6	4.958E-05	1.116E-04	3.099E-04	4.462E-04
BE5 BE6	6.655E-07	1.497E-06	4.159E-06	5.990E-06
BE3 BE7 BE8 BE9	1.873E-12	9.480E-12	7.315E-11	1.517E-10
BE4 BE7 BE8 BE9	2.101E-11	1.064E-10	8.208E-10	1.702E-09
BE5 BE7 BE8 BE9	2.820E-13	1.428E-12	1.102E-11	2.284E-11
BE3 BE12 BE14	2.773E-08	9.358E-08	4.333E-07	7.487E-07
BE4 BE12 BE14	3.111E-07	1.050E-06	4.861E-06	8.400E-06
BE5 BE12 BE14	4.176E-09	1.409E-08	6.525E-08	1.128E-07
BE3 BE7 BE8 BE10	1.012E-09	5.125E-09	3.954E-08	8.199E-08
BE4 BE7 BE8 BE10	1.136E-08	5.750E-08	4.437E-07	9.200E-07
BE5 BE7 BE8 BE10	1.524E-10	7.718E-10	5.955E-09	1.235E-08
BE3 BE7 BE8 BE11	3.497E-09	1.771E-08	1.366E-07	2.833E-07
BE4 BE7 BE8 BE11	3.924E-08	1.987E-07	1.533E-06	3.178E-06
BE5 BE7 BE8 BE11	5.267E-10	2.666E-09	2.057E-08	4.266E-08
BE3 BE13 BE14	1.026E-09	3.463E-09	1.603E-08	2.770E-08
BE4 BE13 BE14	1.151E-08	3.885E-08	1.799E-07	3.108E-07
BE5 BE13 BE14	1.545E-10	5.215E-10	2.414E-09	4.172E-09

Table C2.2.5: Top event probability with 10 % error in basic events

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (10.0% error)	1.101E-04	2.070E-04	4.870E-04	6.712E-04
Top event fuzzy set (-10.0% error)	8.186E-05	1.507E-04	3.453E-04	4.717E-04
Most likely top event	2.975E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~2.87% (approximately)			

Table C2.2.6: Fuzzy top event probability calculated by the random samples (10 % error in basic events)

Number of random samples: 8000

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (10.0% error)	1.255E-04	2.270E-04	4.940E-04	6.382E-04
Top event fuzzy set (-10.0% error)	7.878E-05	1.460E-04	3.174E-04	4.101E-04
Most likely top event	2.961E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~3.13% (approximately)			

C3: 15% ERROR IN BASIC EVENTS

C3.1 Uncertainty analysis for conventional probability approach

Table C3.1: MiniTab output

Variable	N	Mean	SE Mean	StDev	Median
Top event	8000	0.000348	0.00000135	0.000121	0.0003001

C3.2. Uncertainty analysis for fuzzy probability approach

Table C3.2.1: Fuzzy probability with -15% error in basic events data

Fuzzy Probability	Fuzzy Number with -15% error ("around")	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	8.500E-05	4.250E-05	6.375E-05	1.063E-04	1.275E-04
P_{BE2}	8.500E-08	4.250E-08	6.375E-08	1.063E-07	1.275E-07
P_{BE3}	5.644E-04	2.822E-04	4.233E-04	7.055E-04	8.466E-04
P_{BE4}	6.333E-03	3.166E-03	4.749E-03	7.916E-03	9.499E-03
P_{BE5}	8.500E-05	4.250E-05	6.375E-05	1.063E-04	1.275E-04
P_{BE6}	1.870E-02	9.350E-03	1.403E-02	2.338E-02	2.805E-02
P_{BE7}	7.081E-02	3.540E-02	5.310E-02	8.851E-02	1.062E-01
P_{BE8}	8.500E-03	4.250E-03	6.375E-03	1.063E-02	1.275E-02
P_{BE9}	3.145E-05	1.573E-05	2.359E-05	3.931E-05	4.718E-05
P_{BE10}	1.700E-02	8.500E-03	1.275E-02	2.125E-02	2.550E-02
P_{BE11}	5.874E-02	2.937E-02	4.405E-02	7.342E-02	8.810E-02
P_{BE12}	8.500E-04	4.250E-04	6.375E-04	1.063E-03	1.275E-03
P_{BE13}	3.145E-05	1.573E-05	2.359E-05	3.931E-05	4.718E-05
P_{BE14}	2.134E-01	1.067E-01	1.600E-01	2.667E-01	3.200E-01

Table C3.2.2: Fuzzy probability of MCSs (-15% error in basic events)

MCSs	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
BE1	4.250E-05	6.375E-05	1.063E-04	1.275E-04
BE2	4.250E-08	6.375E-08	1.063E-07	1.275E-07
BE3 BE6	2.639E-06	5.937E-06	1.649E-05	2.375E-05
BE4 BE6	2.960E-05	6.661E-05	1.850E-04	2.664E-04
BE5 BE6	3.974E-07	8.941E-07	2.484E-06	3.576E-06
BE3 BE7 BE8 BE9	6.677E-13	3.380E-12	2.608E-11	5.408E-11
BE4 BE7 BE8 BE9	7.491E-12	3.792E-11	2.926E-10	6.068E-10
BE5 BE7 BE8 BE9	1.006E-13	5.091E-13	3.928E-12	8.145E-12
BE3 BE12 BE14	1.279E-08	4.318E-08	1.999E-07	3.454E-07
BE4 BE12 BE14	1.435E-07	4.845E-07	2.243E-06	3.876E-06
BE5 BE12 BE14	1.927E-09	6.503E-09	3.011E-08	5.202E-08
BE3 BE7 BE8 BE10	3.609E-10	1.827E-09	1.410E-08	2.923E-08
BE4 BE7 BE8 BE10	4.049E-09	2.050E-08	1.582E-07	3.280E-07
BE5 BE7 BE8 BE10	5.435E-11	2.752E-10	2.123E-09	4.403E-09
BE3 BE7 BE8 BE11	1.247E-09	6.313E-09	4.871E-08	1.010E-07
BE4 BE7 BE8 BE11	1.399E-08	7.083E-08	5.465E-07	1.133E-06
BE5 BE7 BE8 BE11	1.878E-10	9.507E-10	7.336E-09	1.521E-08
BE3 BE13 BE14	4.734E-10	1.598E-09	7.397E-09	1.278E-08
BE4 BE13 BE14	5.311E-09	1.793E-08	8.299E-08	1.434E-07
BE5 BE13 BE14	7.129E-11	2.406E-10	1.114E-09	1.925E-09

Table C3.2.3: Fuzzy probability with 15 % error in basic events data

Fuzzy Probability	Fuzzy Number with 15% error (“around”)	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	1.150E-04	5.750E-05	8.625E-05	1.438E-04	1.725E-04
P_{BE2}	1.150E-07	5.750E-08	8.625E-08	1.438E-07	1.725E-07
P_{BE3}	7.636E-04	3.818E-04	5.727E-04	9.545E-04	1.145E-03
P_{BE4}	8.568E-03	4.284E-03	6.426E-03	1.071E-02	1.285E-02
P_{BE5}	1.150E-04	5.750E-05	8.625E-05	1.438E-04	1.725E-04
P_{BE6}	2.530E-02	1.265E-02	1.898E-02	3.163E-02	3.795E-02
P_{BE7}	9.580E-02	4.790E-02	7.185E-02	1.197E-01	1.437E-01
P_{BE8}	1.150E-02	5.750E-03	8.625E-03	1.438E-02	1.725E-02
P_{BE9}	4.255E-05	2.128E-05	3.191E-05	5.319E-05	6.383E-05
P_{BE10}	2.300E-02	1.150E-02	1.725E-02	2.875E-02	3.450E-02
P_{BE11}	7.947E-02	3.973E-02	5.960E-02	9.933E-02	1.192E-01
P_{BE12}	1.150E-03	5.750E-04	8.625E-04	1.438E-03	1.725E-03
P_{BE13}	4.255E-05	2.128E-05	3.191E-05	5.319E-05	6.383E-05
P_{BE14}	2.887E-01	1.443E-01	2.165E-01	3.608E-01	4.330E-01

Table C3.2.4: Fuzzy probability of MCSs (15% error in basic events)

MCSs	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
BE1	5.750E-05	8.625E-05	1.438E-04	1.725E-04
BE2	5.750E-08	8.625E-08	1.438E-07	1.725E-07
BE3 BE6	4.830E-06	1.087E-05	3.019E-05	4.347E-05
BE4 BE6	5.419E-05	1.219E-04	3.387E-04	4.877E-04
BE5 BE6	7.274E-07	1.637E-06	4.546E-06	6.546E-06
BE3 BE7 BE8 BE9	2.237E-12	1.133E-11	8.739E-11	1.812E-10
BE4 BE7 BE8 BE9	2.510E-11	1.271E-10	9.805E-10	2.033E-09
BE5 BE7 BE8 BE9	3.369E-13	1.706E-12	1.316E-11	2.729E-11
BE3 BE12 BE14	3.168E-08	1.069E-07	4.951E-07	8.555E-07
BE4 BE12 BE14	3.555E-07	1.200E-06	5.555E-06	9.598E-06
BE5 BE12 BE14	4.772E-09	1.610E-08	7.456E-08	1.288E-07
BE3 BE7 BE8 BE10	1.209E-09	6.122E-09	4.724E-08	9.795E-08
BE4 BE7 BE8 BE10	1.357E-08	6.869E-08	5.300E-07	1.099E-06
BE5 BE7 BE8 BE10	1.821E-10	9.220E-10	7.114E-09	1.475E-08
BE3 BE7 BE8 BE11	4.178E-09	2.115E-08	1.632E-07	3.384E-07
BE4 BE7 BE8 BE11	4.688E-08	2.373E-07	1.831E-06	3.797E-06
BE5 BE7 BE8 BE11	6.292E-10	3.185E-09	2.458E-08	5.097E-08
BE3 BE13 BE14	1.172E-09	3.957E-09	1.832E-08	3.165E-08
BE4 BE13 BE14	1.315E-08	4.439E-08	2.055E-07	3.551E-07
BE5 BE13 BE14	1.766E-10	5.959E-10	2.759E-09	4.767E-09

Table C3.2.5: Top event probability with 15 % error in basic events

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (15.0% error)	1.178E-04	2.225E-04	5.262E-04	7.266E-04
Top event fuzzy set (-15.0% error)	7.537E-05	1.379E-04	3.137E-04	4.274E-04
Most likely top event	2.985E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~3.22% (approximately)			

Table C3.2.6: Fuzzy top event probability calculated by the random samples (15 % error in basic events)

Number of random samples: 8000

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (15.0% error)	1.255E-04	2.365E-04	4.961E-04	6.382E-04
Top event fuzzy set (-15.0% error)	8.474E-05	1.414E-04	3.273E-04	4.009E-04
Most likely top event	3.001E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~3.77% (approximately)			

C4: 20% ERROR IN BASIC EVENTS

C4.1 Uncertainty analysis for conventional probability approach

Table C4.1: MiniTab output

Variable	N	Mean	SE Mean	StDev	Median
Top event	8000	0.000463	0.00000315	0.000282	0.000528

C4.2 Uncertainty analysis for fuzzy probability approach

Table C4.2.1: Fuzzy probability with -20% error in basic events data

Fuzzy Probability	Fuzzy Number with -20% error ("around")	Trapezoidal representations ($P_{IA}, P_{IB}, P_{IC}, P_{ID}$)			
P_{BE1}	8.000E-05	4.000E-05	6.000E-05	1.000E-04	1.200E-04
P_{BE2}	8.000E-08	4.000E-08	6.000E-08	1.000E-07	1.200E-07
P_{BE3}	5.312E-04	2.656E-04	3.984E-04	6.640E-04	7.968E-04
P_{BE4}	5.960E-03	2.980E-03	4.470E-03	7.450E-03	8.940E-03
P_{BE5}	8.000E-05	4.000E-05	6.000E-05	1.000E-04	1.200E-04
P_{BE6}	1.760E-02	8.800E-03	1.320E-02	2.200E-02	2.640E-02
P_{BE7}	6.664E-02	3.332E-02	4.998E-02	8.330E-02	9.996E-02
P_{BE8}	8.000E-03	4.000E-03	6.000E-03	1.000E-02	1.200E-02
P_{BE9}	2.960E-05	1.480E-05	2.220E-05	3.700E-05	4.440E-05
P_{BE10}	1.600E-02	8.000E-03	1.200E-02	2.000E-02	2.400E-02
P_{BE11}	5.528E-02	2.764E-02	4.146E-02	6.910E-02	8.292E-02
P_{BE12}	8.000E-04	4.000E-04	6.000E-04	1.000E-03	1.200E-03
P_{BE13}	2.960E-05	1.480E-05	2.220E-05	3.700E-05	4.440E-05
P_{BE14}	2.008E-01	1.004E-01	1.506E-01	2.510E-01	3.012E-01

Table C4.2.2: Fuzzy probability of MCSs (-20% error in basic events)

MCSs	Trapezoidal representations $P_{IA}, P_{IB}, P_{IC}, P_{ID}$			
BE1	4.000E-05	6.000E-05	1.000E-04	1.200E-04
BE2	4.000E-08	6.000E-08	1.000E-07	1.200E-07
BE3 BE6	2.337E-06	5.259E-06	1.461E-05	2.104E-05
BE4 BE6	2.622E-05	5.900E-05	1.639E-04	2.360E-04
BE5 BE6	3.520E-07	7.920E-07	2.200E-06	3.168E-06
BE3 BE7 BE8 BE9	5.239E-13	2.652E-12	2.047E-11	4.244E-11
BE4 BE7 BE8 BE9	5.878E-12	2.976E-11	2.296E-10	4.761E-10
BE5 BE7 BE8 BE9	7.890E-14	3.994E-13	3.082E-12	6.391E-12
BE3 BE12 BE14	1.067E-08	3.600E-08	1.667E-07	2.880E-07
BE4 BE12 BE14	1.197E-07	4.039E-07	1.870E-06	3.231E-06
BE5 BE12 BE14	1.606E-09	5.422E-09	2.510E-08	4.337E-08
BE3 BE7 BE8 BE10	2.832E-10	1.434E-09	1.106E-08	2.294E-08
BE4 BE7 BE8 BE10	3.177E-09	1.609E-08	1.241E-07	2.574E-07
BE5 BE7 BE8 BE10	4.265E-11	2.159E-10	1.666E-09	3.455E-09
BE3 BE7 BE8 BE11	9.784E-10	4.953E-09	3.822E-08	7.925E-08
BE4 BE7 BE8 BE11	1.098E-08	5.558E-08	4.288E-07	8.892E-07
BE5 BE7 BE8 BE11	1.474E-10	7.460E-10	5.756E-09	1.194E-08
BE3 BE13 BE14	3.947E-10	1.332E-09	6.167E-09	1.066E-08
BE4 BE13 BE14	4.428E-09	1.494E-08	6.919E-08	1.196E-07
BE5 BE13 BE14	5.944E-11	2.006E-10	9.287E-10	1.605E-09

Table C4.2.3: Fuzzy probability with 20 % error in basic events data

Fuzzy Probability	Fuzzy Number with 20% error ("around")	Trapezoidal representations ($P_{iA}, P_{iB}, P_{iC}, P_{iD}$)			
P_{BE1}	1.200E-04	6.000E-05	9.000E-05	1.500E-04	1.800E-04
P_{BE2}	1.200E-07	6.000E-08	9.000E-08	1.500E-07	1.800E-07
P_{BE3}	7.968E-04	3.984E-04	5.976E-04	9.960E-04	1.195E-03
P_{BE4}	8.940E-03	4.470E-03	6.705E-03	1.118E-02	1.341E-02
P_{BE5}	1.200E-04	6.000E-05	9.000E-05	1.500E-04	1.800E-04
P_{BE6}	2.640E-02	1.320E-02	1.980E-02	3.300E-02	3.960E-02
P_{BE7}	9.996E-02	4.998E-02	7.497E-02	1.250E-01	1.499E-01
P_{BE8}	1.200E-02	6.000E-03	9.000E-03	1.500E-02	1.800E-02
P_{BE9}	4.440E-05	2.220E-05	3.330E-05	5.550E-05	6.660E-05
P_{BE10}	2.400E-02	1.200E-02	1.800E-02	3.000E-02	3.600E-02
P_{BE11}	8.292E-02	4.146E-02	6.219E-02	1.037E-01	1.244E-01
P_{BE12}	1.200E-03	6.000E-04	9.000E-04	1.500E-03	1.800E-03
P_{BE13}	4.440E-05	2.220E-05	3.330E-05	5.550E-05	6.660E-05
P_{BE14}	3.012E-01	1.506E-01	2.259E-01	3.765E-01	4.518E-01

Table C4.2.1.4: Fuzzy probability of MCSs (20% error in basic events)

MCSs	Trapezoidal representations ($P_{iA}, P_{iB}, P_{iC}, P_{iD}$)			
BE1	6.000E-05	9.000E-05	1.500E-04	1.800E-04
BE2	6.000E-08	9.000E-08	1.500E-07	1.800E-07
BE3 BE6	5.259E-06	1.183E-05	3.287E-05	4.733E-05
BE4 BE6	5.900E-05	1.328E-04	3.688E-04	5.310E-04
BE5 BE6	7.920E-07	1.782E-06	4.950E-06	7.128E-06
BE3 BE7 BE8 BE9	2.652E-12	1.343E-11	1.036E-10	2.148E-10
BE4 BE7 BE8 BE9	2.976E-11	1.507E-10	1.162E-09	2.410E-09
BE5 BE7 BE8 BE9	3.994E-13	2.022E-12	1.560E-11	3.235E-11
BE3 BE12 BE14	3.600E-08	1.215E-07	5.625E-07	9.720E-07
BE4 BE12 BE14	4.039E-07	1.363E-06	6.311E-06	1.091E-05
BE5 BE12 BE14	5.422E-09	1.830E-08	8.471E-08	1.464E-07
BE3 BE7 BE8 BE10	1.434E-09	7.258E-09	5.600E-08	1.161E-07
BE4 BE7 BE8 BE10	1.609E-08	8.143E-08	6.283E-07	1.303E-06
BE5 BE7 BE8 BE10	2.159E-10	1.093E-09	8.434E-09	1.749E-08
BE3 BE7 BE8 BE11	4.953E-09	2.508E-08	1.935E-07	4.012E-07
BE4 BE7 BE8 BE11	5.558E-08	2.814E-07	2.171E-06	4.502E-06
BE5 BE7 BE8 BE11	7.460E-10	3.777E-09	2.914E-08	6.042E-08
BE3 BE13 BE14	1.332E-09	4.495E-09	2.081E-08	3.596E-08
BE4 BE13 BE14	1.494E-08	5.044E-08	2.335E-07	4.035E-07
BE5 BE13 BE14	2.006E-10	6.770E-10	3.134E-09	5.416E-09

Table C4.2.5: Top event probability with 20 % error in basic events

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (20.0% error)	1.257E-04	2.384E-04	5.670E-04	7.844E-04
Top event fuzzy set (-20.0% error)	6.910E-05	1.257E-04	2.835E-04	3.853E-04
Most likely top event	3.036E-04			
Exact top event probability	2.892 E-04			
Percentage of error on top-event	~5% (approximately)			

Table C4.2.6: Fuzzy top event probability calculated by the random samples (20% error in basic events)

Number of random samples: 8000

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (20.0% error)	1.255E-04	2.270E-04	4.940E-04	6.382E-04
Top event fuzzy set (-20.0% error)	8.327E-05	1.543E-04	3.355E-04	4.335E-04
Most likely top event	3.027E-04			
Exact top event probability	2.892 E-04			
Percentage of error on top-event	~4.75% (approximately)			

C5: α -CUT METHOD FOR UNCERTAINTY ANALYSIS

The concept of α -cuts can also be another approach for checking the cumulating error on top-event of a fault tree besides the two approaches used in this study. The following example for specific α -level is also proving that this approach gives the same results as the fuzzy uncertainty analysis approach developed in the study.

Example:

For implementing α -cut concept in uncertainty analyses at first consider a specific membership grade or α value, which is 0.75 for all basic events trapezoidal membership function. The corresponding four-tuple (P_{iA} , P_{iB} , P_{iC} , P_{iD}) values for basic events data are calculated by using equation 4.3. Usually α grade value can be any value between 0 to 1. As for example here the concept is applied for estimating cumulating error on top-event if the basic events have 15% error.

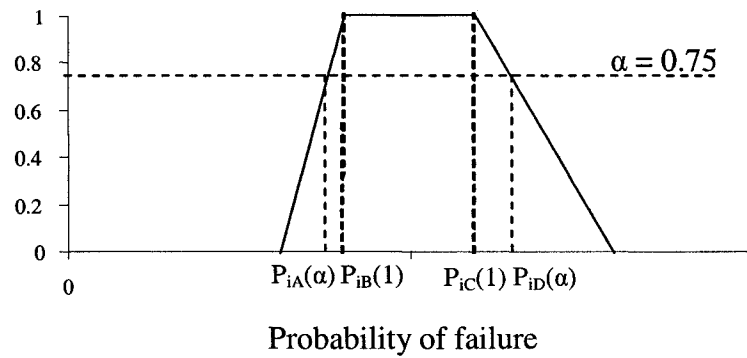


Figure: Trapezoidal representation of basic event probability with α -cut

Procedure of uncertainty analysis with α -cuts

1. Consider $\pm 15\%$ error in basic events data.
2. Fuzzyfying the basic events data and calculating the corresponding α -cut values [$P_{iA}(\alpha)$, $P_{iB}(1)$, $P_{iC}(1)$, $P_{iD}(\alpha)$] using the membership equation. [Using equation 4.3]
3. Calculating the all cutsets probability and Fuzzy top-event probability of the fault tree using fuzzy arithmetic rules. [Using equation 4.6, 4.7 and 4.8]
4. Calculating most likely top event probability using weighted average defuzzification method. [Using equation 4.9]
5. Calculating the cumulative error in the top event.

The summary table for the calculation of implementation of α -cut in uncertainty analysis has shown in Table C5.1. Table C5.2 shows the results obtained by using fuzzy uncertainty model developed in the study. These two tables actually show that the cumulating error on top event is nearly same for both approaches (α -cut concept and fuzzy uncertainty approach) if the basic events data has $\pm 15\%$ error.

Table C 5.1: Top event probability with 15 % error in basic events (using α -cut concept)

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (15.0% error)	1.933E-04	2.224E-04	5.261E-04	5.732E-04
Top event fuzzy set (-15.0% error)	1.207E-04	1.379E-04	3.136E-04	3.404E-04
Most likely top event	2.993E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~3.49% (approximately)			

Table C 5.2: Top event probability with 15 % error in basic events (traditional approach)

Fuzzy probability analysis	P_{A(T)}	P_{B(T)}	P_{C(T)}	P_{D(T)}
Top event fuzzy set (15.0% error)	1.178E-04	2.225E-04	5.262E-04	7.266E-04
Top event fuzzy set (-15.0% error)	7.537E-05	1.379E-04	3.137E-04	4.274E-04
Most likely top event	2.985E-04			
Exact top event probability	2.892E-04			
Percentage of error on top-event	~3.22% (approximately)			



