# Framework, Approach and System of Intelligent Fault Tree Analysis for Nuclear Safety Assessment

A Thesis Submitted for the Degree of
Doctor of Philosophy
By
**Julwan Hendry PURBA**

University of Technology, Sydney
July, 2013

# TABLE OF CONTENTS

*CHAPTER 4 An Area Defuzzification Technique to Generate Nuclear Event Fuzzy Failure Rates*

*CHAPTER 5 A Fuzzy Reliability Approach to Assess Basic Events of Fault Trees Through Qualitative Data Processing*

# CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literatures used are indicated in the thesis.

Sydney, 1 July 2013

Production Note:
Signature removed prior to publication.

Julwan Hendry PURBA

# DEDICATION

*To my amazing wife, Rita, for sharing the pain, sorrow and depression during the hard time and above all for her unconditional love, patience and encouragement.*

*To my wonderful sons, Carlo & Nathan, for being the nicest friends through this challenging and exciting journey.*

“My help comes from the LORD, the Maker of heaven and earth.” Psalm 121:2.

# ACKNOWLEDGEMENTS

One of the great pleasures of writing this thesis is acknowledging the efforts of many peoples who were involved in and crucial to the process of my PhD study.

I would like to express my sincere gratitude to my principal supervisor, Prof. Jie Lu, for accepting me as one of her PhD students and guiding me to complete my study. Thank you for your continuous accurate critical comments and suggestions, patience, and encouragement, which have influenced my critical thinking and strengthened this study significantly. Your strict academic attitude, generous personality and conscientious working style have shaped me into a good researcher and will be of great benefit to me in my future research work and life. I also would like to address my sincere thanks to my co-supervisor, Prof. Guangquan Zhang for his knowledgeable suggestions and invaluable advice, which have greatly improved the quality of my research. I also would like to address my sincere thanks to my external-supervisor, the late Prof. Da Ruan, for his great ideas and invaluable comments to strengthen my research in the first half of my study. To me, you are not only an outstanding researcher and a great supervisor, but also a warm-hearted friend. I am really honoured to have had you as one of my PhD supervisors. Rest in peace Prof.

I also wish to express my appreciation to all my friends and the members of the Decision Systems & e-Service Intelligence (DeSI) Lab for their help, participation and invaluable comments in every presentation I made during my study. Friendships and encouragements that we have developed during this journey will be good memories in my future research life. I wish you all the very best in your future research works and life.

I also appreciate the travel funding that I have received from the FEIT and the UTS Vice-Chancellor conference fund for attending an international conference.

I also would like to thank Barbara Munday and Sue Felix from the Centre for Quantum Computation & Intelligent Systems (QCIS) for being proofreaders of my published papers and thesis. I sincerely appreciate the efforts you have given to proofread the papers and the thesis.

Finally, I would like to thank AusAID for funding and providing support during my PhD study. I am very grateful to have been able to study and have experiences in a very beautiful country like Australia. This dream would not have come true without the support from AusAID.

# LIST OF FIGURES

# LIST OF TABLES

# ABSTRACT

Probabilistic safety assessment by fault tree analysis has been considered as an important tool to evaluate safety systems of nuclear power plants in the last two decades. However, since the estimation of failure probabilities of rare events with high consequences is the focus of this assessment, it is often very difficult to obtain component failure rates, which are specific to the nuclear power plant under evaluation. The motivation of this study is how to obtain basic event failure rates when basic events do not have historical failure data and expert subjective justifications, which are expressed in qualitative failure possibilities, are the only means to evaluate basic event failures.

This thesis describes a new intelligent hybrid fault tree analysis framework to overcome the weaknesses of conventional fault tree analysis, qualitative failure possibilities and their corresponding mathematical representations to articulate nuclear event failure likelihoods, an area defuzzification technique to decode the membership functions of fuzzy sets representing nuclear event failure possibilities into nuclear event reliability scores, and a fuzzy reliability approach to generate nuclear event quantitative fuzzy failure rates from the corresponding qualitative failure possibilities subjectively evaluated by experts. Seven qualitative linguistic terms have been defined to represent nuclear event failure possibilities, i.e. *very low*, *low*, *reasonably low*, *moderate*, *reasonably high*, *high*, and *very high* and the corresponding mathematical forms are represented by triangular fuzzy numbers, which are defined in the [0, 1] universe of discourse based on nuclear event failure data documented in literatures using inductive reasoning. Finally, an intelligent software system called InFaTAS-NuSA, which has been developed to realize the new intelligence hybrid fault tree analysis framework to overcome the limitations of the existing fault tree analysis software systems by accepting both quantitative failure probabilities and qualitative failure possibilities, is also described in this thesis.

The results of the InFaTAS-NuSA evaluation using a real world application confirm that InFaTAS-NuSA has yielded similar outputs as the outputs generated by a well-known fault tree analysis software system, i.e. SAPHIRE, and therefore it can overcome the limitation of the existing fault tree analysis software system, which can accept only quantitative failure probabilities. The experiment results also show that the fuzzy reliability approach seems to be a sound alternative for conventional reliability approach to deal with basic events which do not have historical failure data and expert subjective opinions are the only means to obtain their failure information.

# Chapter 1

# INTRODUCTION

## 1.1 BACKGROUND

System safety is a major requirement for complex systems such as nuclear power plants. The functions of the nuclear safety system are to ensure that nuclear facilities can normally operate without an excessive risk exposure to staffs and environment, to prevent accidents, and to mitigate the consequences of accidents if they occur. In 1957, the United Nations set up the International Atomic Energy Agency to act as an auditor of world nuclear safety and work together with nuclear safety inspectorates in member countries, which operates nuclear power plants.

Even though nuclear power plants have been designed to be safe in their operation and safe in the event of any malfunction or accident, incidents and accidents still may happen as in other industries. The most recent nuclear disaster to date is Fukushima Daiichi nuclear power plants, which happen in March 2011. The disaster was affected seriously by a huge tsunami following the Great East Japan Earthquake. Three of six reactors, which were operating at that time, shut down automatically due to this earthquake to prevent potential accidents to the reactors. The control rods had been inserted into the core to stop chain reaction. However, at this point, decay heat at about 7% of the full power heat load under normal operating conditions has to be carried out by the cooling system from the core to avoid fuel meltdown. Unfortunately, the earthquake also destroyed external power supply and hence, backup power system had to work to keep the coolant pumps working. Later, the tsunami induced by the earthquake swamped and flooded the diesel generators to cause pump failure. This situation led to weeks of drama and loss of the reactors. However, Fukushima accidents will have significant implications and provide valuable knowledge to enhance the nuclear power plant safety systems.

Over the past two decades, a probabilistic safety assessment has been considered to be an important analysis tool to ensure the safety of a nuclear power plant in relation to potential initiating events that can be caused by random component failures, human errors, internal and external hazards. The probabilistic safety assessment provides a comprehensive and structured approach to identify and understand key plant vulnerabilities, to develop accident scenarios, to assess the level of the plant safety, and to derive numerical estimates of potential risks. Designers, utility and regulatory personnel use the probabilistic safety assessment results to verify the nuclear power plant design, to assess the possible changes to the plant design or operation, and to assess the potential changes to the plant licensing basis (Delaney, Apostolakis & Driscoll 2005; Kishi et al. 2004; Liu, Tong & Zhao 2008). Based on the probabilistic safety assessment results, nuclear power plants are subject to change to enhance their safety level. Where the results of the probabilistic safety assessment indicate that changes could be made to the design or operation of the plant to reduce risk, the changes should be incorporated where reasonably achievable.

A fault tree analysis has been widely used as a tool for the nuclear power plant probabilistic safety assessment. To perform this analysis, safety analysts have to provide failure rates of all basic events in the system fault tree. Since the estimation of failure probabilities of rare events with high consequences is the focus of the nuclear power plant probabilistic safety assessment, it is often very difficult to obtain component failure data, which are specific to the nuclear power plant being evaluated. It is inevitable to obtain component failure data from other sources. Generic data can be taken from other nuclear power plants or nuclear industries other than nuclear power plants to be used in the nuclear power plant probabilistic safety assessment as secondary sources. Component failure data can also be taken from non-nuclear experiences such as military data sources of electronic equipment and component testing if both primary and secondary sources are not enough (Hsu & Musicki 2005). Since the used data are not comprehensive into the area under investigation, nuclear safety analysts have to deal with imprecision and uncertainties (Shu, Li & Qiu 2008; Song, Zhang & Chan 2009). Moreover, the results also will not show the real situation of the system function to be used for future recommendations on the safety improvement (NEA 2005).

The limitation of the conventional fault tree analysis arises from the insufficient reliable statistical data to probabilistically estimate basic event failures. The concept of the fuzzy set theory has been proposed and implemented for the nuclear safety assessment to overcome the limitation of the conventional fault tree analysis. Fuzzy probabilities have been used to represent basic event failure probabilities to calculate the failure probability of a typical emergency core cooling system (Misra & Weber 1990). In this approach, the failure rates of the all basic events were represented by fuzzy numbers and the calculation of the failure probability of the top event was in the fuzzy framework by using fuzzy combination rules. Boolean "AND" and "OR" gates were represented by a fuzzy multiplication rule and a fuzzy complementation rule, respectively. However, in complex systems, the fault tree might have other Boolean gates such as "PRIORITY AND" gate, "EXCLUSIVE OR" gate, and "INHIBIT" gate (Ericson 2005).

Moreover, an $\alpha$–cut method in justify membership functions has been introduced to calculate failure probability of the reactor protective system (WASH-1400) (Suresh, Babar & Venkat Raj 1996). In this approach, all basic events were still assumed to have at least a small number of recorded failures to model their failures using triangular fuzzy numbers. A point median value and an error factor of component failure probability distributions were used to calculate the left and the right supports of the triangular fuzzy numbers. Meanwhile, the core of the triangular fuzzy numbers is represented by the point median value. They also introduced a fuzzy importance measure and a fuzzy uncertainty importance measure to evaluate critical components. This approach has also been implemented to estimate the failure probabilities of the auxiliary feed water system

(AFWS) of the Angra-I Westinghouse nuclear power plant (Guimaraes & Ebecken 1999) and of the containment cooling system (CCS) of a typical four-loops pressurized water reactor (Guimaraes & Lapa 2008). However, it is not possible to obtain probability distributions for the all basic event of a fault tree (Haimes 2004).

In the situation when little quantitative information is available, qualitative data expressed in linguistic terms can be used to justify system reliability (Coletti & Scozzafava 2004; Lu et al. 2007; Suresh, Babar & Venkat Raj 1996). Experts are also more comfortable to justify event failures using qualitative words rather than quantitative judgment when quantitative historical failure data are unavailable or insufficient (Ferdous et al. 2011; Mentes & Helvacioglu 2011). For example, it is common to say that 'there is a *low possibility* that the basic event *A* is *fail*' rather than the *failure probability* of basic event *A* is *'1.5E-3'*. In this assessment, the '*low failure possibility*' is a qualitative word. Therefore, when the corresponding statistic information for basic events is inadequate, it is more relevant to use *failure possibility* rather than *failure probability*. To deal with imprecision and uncertainties coming with the event failure possibility justifications, failure possibilities can be treated as fuzzy numbers (Dumitrescu et al. 2006; Sharma & Sudhakar 1993; Wolkenhauer 2001). This study explores and applies both fuzzy set theory and failure possibility theory to evaluate basic events of the fault tree analysis, which do not have historical failure data, and expert subjective justifications are the only method to obtain their failure possibilities. To observe the effects of the variations of the basic event failure possibilities to the top event failure probability, sensitivity analysis is also investigated.

## 1.2 RESEARCH CHALLENGES

To overcome the limitation of the existing fault tree analysis for nuclear power plant probabilistic safety assessment as described above, this study aims to answer the following specific research questions.

**Question 1: How to deal with basic events of fault trees that do not have historical failure data using qualitative failure possibilities**

In the absence of historical basic event failure data for assessing their quantitative failure probabilities, qualitative failure possibilities, which are expressed in linguistic values, can be used to evaluate basic event reliability. Therefore, the concepts and the current applications of failure possibilities will be investigated. The existing fault tree analysis framework for nuclear power plant probabilistic safety assessment will also be investigated. Based on the results of the investigations, an intelligent hybrid fuzzy fault tree analysis framework will be developed by introducing a failure possibility-based approach into the quantitative phase of conventional fault tree analysis for dealing with basic events that do not have quantitative failure data.

**Question 2: How to develop nuclear event qualitative failure possibilities and their corresponding mathematical representations**

Since qualitative failure possibilities are expressed in linguistic terms, qualitative words used to grade nuclear event failure possibilities will be investigated and developed. This failure possibility distribution will represent a range of nuclear event failures from the lowest failure possibility to the highest failure possibility and enable experts to subjectively assess basic event failures using qualitative words. To be able to mathematically estimate the failure probability of the top event, those nuclear event failure possibilities need to have their corresponding mathematical representations. Since fuzzy sets can mathematically represent qualitative linguistic values, the concepts and the current related applications of fuzzy sets will also be investigated. Based on the results of the investigation, membership functions of fuzzy sets to mathematically represent those nuclear event failure possibilities will be developed to enable safety analysts to mathematically assess the failure probability of the top event of a fault tree.

**Question 3: How to decode fuzzy values into their corresponding single numerical values**

Since nuclear event qualitative failure possibilities are mathematically represented by the membership functions of fuzzy numbers, a single numerical value for each membership functions need to be generated to score how possible that a nuclear event will become fail. This goal can be achieved using a defuzzification technique. Therefore, existing defuzzification techniques will deeply be investigated. Based on the results of the investigation, essential fuzzy rules for evaluating nuclear events will be defined and a suitable defuzzification technique for assessing nuclear event failures using qualitative failure possibilities will be developed.

**Question 4: How to generate nuclear event quantitative fuzzy failure rates from their corresponding qualitative failure possibilities**

In conventional reliability theory, basic event failure rates are expressed in quantitative values, which are probabilistically calculated from their historical failure data. In this study, nuclear event failures are expressed in qualitative failure possibilities. Therefore, existing research on the application of qualitative linguistic terms for assessing the reliabilities of engineering systems will be investigated. Based on the results of the investigation, a fuzzy reliability approach will be developed to generate nuclear event quantitative fuzzy failure rates from their corresponding qualitative failure possibilities.

**Question 5: How to support safety analysts to assess the safety systems of nuclear power plants involving both qualitative failure possibilities and quantitative failure probabilities**

Based on the intelligent hybrid fault tree analysis framework, the nuclear event qualitative failure possibilities and their corresponding mathematical representations, the suitable defuzzification technique, and the fuzzy reliability approach, which have been developed at the previous stages, an intelligent fault tree analysis software system will be developed to overcome the limitations of the existing fault tree analysis for nuclear power plant probabilistic safety assessment. Since same nuclear events may be subjectively evaluated by experts of having different failure possibilities, imprecision and uncertainties in this assessment need to be measured. Therefore sensitivity of the top event failure probability to the variation of the nuclear event failure possibilities will also be evaluated in the new developed intelligent system.

These five research questions have been addressed in this thesis to overcome the limitations of the nuclear power plant probabilistic safety assessment by fault tree analysis.

## 1.3 RESEARCH OBJECTIVES

In relation to the research questions described in Section 1.2, the objectives of this study, which will be achieved, are as follows.

**Objective 1: To develop a new intelligent hybrid fuzzy fault tree analysis framework to deal with basic events whose failures are expressed in qualitative failure possibilities**

A new intelligent hybrid fault tree analysis framework, which implements two types of approaches in the quantitative phase to deal with two different types of basic events, will be developed. The first approach is a failure possibility-based approach to deal with basic events whose failures are subjectively justified by experts using qualitative failure possibilities. The second approach is a failure probability-based approach to deal with basic events that have historical failure data for estimating their quantitative failure probability. Therefore, the new intelligent hybrid fault tree analysis framework will be able to deal with not only basic event quantitative failure probabilities but also qualitative failure possibilities. This framework will be described by a diagram to show its new features and its applicability will be mathematically validated using a simplified safety system of a typical nuclear power plant.

**Objective 2: To develop nuclear event qualitative failure possibilities and their corresponding mathematical representations**

A number of failure possibility terms will be developed to grade nuclear event failures from the lowest failure possibility to the highest failure possibility. Experts will use these terms to subjectively and qualitatively evaluate the failures of the basic events of fault trees. In addition, membership functions of fuzzy numbers will also be developed to mathematically represent those nuclear event qualitative failure possibilities. Safety analysts will use these membership functions to assess the failure probability of the top event of fault trees.

**Objective 3: To develop a defuzzification technique that is suitable for nuclear safety assessment by fault tree analysis involving qualitative failure possibilities**

Essential fuzzy rules for evaluating nuclear events will be defined and a suitable defuzzification technique will be developed to decode membership functions of fuzzy numbers into a single numerical value to represent how possible a nuclear event to become fail. These predefined fuzzy rules will be used to validate the performance and the effectiveness of the developed defuzzification technique for nuclear safety assessment involving qualitative failure possibilities.

**Objective 4: To develop a fuzzy reliability approach for generating nuclear event quantitative fuzzy failure rates from their corresponding qualitative failure possibilities**

A fuzzy reliability approach will be developed to complement conventional reliability approach. The fuzzy reliability approach will only deal with basic events whose failures are qualitatively expressed by the failure possibilities and mathematically represented by the membership functions of fuzzy numbers. The applicability and the effectiveness of the quantification process of the developed fuzzy reliability approach will be validated by comparing the fuzzy failure rates generated by the approach with the real nuclear event failure probabilities collected from nuclear power plant operating experiences.

**Objective 5: To develop an intelligent fault tree analysis software system to support safety analysts to evaluate nuclear power plant safety**

An intelligent fault tree analysis software system will be developed by implementing the previous four research objectives to overcome the limitations of the current nuclear power plant probabilistic safety assessment by fault tree analysis. To verify its accuracy and effectiveness for assessing the safety systems of nuclear power plants, this intelligent software system will be mathematically validated using a real nuclear power plant safety system, which has been evaluated using an existing well-known fault tree analysis software system.

This study has achieved all these research objectives, which are described in details in the following chapters.

## 1.4 Research Contributions

This study contributes both theory and practice of the nuclear power plant probabilistic safety assessment and the basic event fault tree evaluation.

(1) Our intelligent hybrid fault tree analysis framework overcomes the weaknesses of existing fault tree analyses, which cannot deal with basic events whose failures expressed in qualitative failure possibilities. The framework enables experts to subjectively evaluate nuclear event failures using qualitative failure possibilities by saying, for example, that the *possibility* of basic event *X* to become *fail* is *low* rather than using quantitative failure probability by saying, for example, that the *failure probability* of nuclear event *X* is 1.6E-5.

(2) Our fuzzy reliability approach brings a new way to evaluate basic events of fault trees. The approach can be a complement for the conventional reliability approach to deal with basic events, which do not have historical failure data for calculating their failure probabilities. The approach generates quantitative failure rates; say

*1.6E-5* for example, from qualitative failure information; say *a low failure possibility* for example.

(3) Our intelligent fault tree analysis software system can directly be applied into three different types of fault tree analysis. The first application is for analysing existing nuclear power plants, which have complete plant specific data, through the use of the failure probability-based approach. The second application is to analyse new nuclear power plants, which do not have operating history yet, or new projects, which only exist on paper, through the use of the failure possibility-based approach. The last application is for analysing nuclear power plants, which partially have plant specific data through the combination of the two approaches.

Two main innovations, which can be achieved from this study, are as follows.

(1) The developed nuclear event failure possibilities and their corresponding mathematical representations enable experts to subjectively evaluate basic event failures using their expertise, experiences and intuition.

(2) The new developed area defuzzification technique offers a new way to decode fuzzy values into single numerical values for ranking fuzzy sub-sets and/or for helping decision makers to prioritize decisions involving two or more alternatives represented by fuzzy numbers.

## 1.5 RESEARCH METHODOLOGY

This Section describes how the research objectives given in Section 1.3 have been achieved in this study.

### 1.5.1 PROBLEM DEFINITION

At this stage, thorough and in-depth analysis of relative old and new literatures is accomplished to identify the original problems of the current nuclear power plant probabilistic safety assessment by fault tree analysis. In line with this identification, existing methods and approaches to improve conventional fault tree analysis are compared to uncover their common disadvantages and finally to reveal possible research gaps. Possible research gaps found are then structured to be further investigated and studied in the future research project. Big problems are divided into several sub problems to define specific research questions. Having decided upon the research questions, research objectives and outcomes are then defined. Based on the research objectives, significances and innovations of this study are revealed.

### 1.5.2 PLANNING

This stage involves several decisions and assessment. Corresponding researches and technologies are deeply studied to fill the research gaps accordingly. Key difficulties and challenges in the available technologies will be identified for further more in-depth investigation. New framework, model, technique, approach, and software system needed to overcome the weaknesses of existing nuclear power plant probabilistic safety assessment by fault tree analysis found in the previous stage are set. Resources and strategies needed for analysis and validation to see the feasibility of the proposed solution are also determined at this stage. Finally, a comprehensive road map to achieve the research objectives is then defined in a project management plan and ready for full-scale implementation.

### 1.5.3 Development

At this stage, the new framework, model, technique, approach, and software system that have been defined in the previous stage are realized to gain the research objectives. A new intelligent hybrid fault tree analysis framework, which integrates failure probability-based approach with failure possibility-based approach in the quantitative phase of fault tree analysis, is developed. Models of nuclear event qualitative failure possibilities and their corresponding mathematical representation are then developed to be realized in the new intelligent hybrid framework. Next, an area defuzzification technique is developed to decode fuzzy values into single numerical values to represent how possible a nuclear event will become fail. Then, a fuzzy reliability approach to generate quantitative fuzzy failure rates from qualitative failure possibilities is formulated to also be realized in the intelligent hybrid framework to deal with basic events whose failures are subjectively evaluated by experts using qualitative failure possibilities. Finally, the intelligent hybrid fault tree analysis framework is realized by developing an intelligent fault tree analysis software system to deal not only with quantitative failure probabilities but also with qualitative failure possibilities. This new software system overcomes the limitations of the existing fault tree analysis software systems for evaluating nuclear power plant safety.

### 1.5.4 Analysis And Validation

At this stage, illustrative case studies as well as real-world applications are conducted to analyse and validate the performance and the effectiveness of the developed intelligent hybrid framework, the nuclear event qualitative failure possibilities and their corresponding mathematical representations, the area defuzzification technique, the fuzzy reliability approach, and the intelligent fault tree analysis software system. These analysis and validation explore their applicability and feasibility for assessing nuclear event failures without the need for historical failure data as well as nuclear power plant safety system. Moreover, the results of the analysis and evaluation are used for further improvements and/or find new directions for development.

### 1.5.5 EVALUATION AND REVISION

At this stage, a real-world application, which is the first model of the reactor protection system of the U.S. combustion engineering pressurized water reactor, is used to evaluate the feasibility of the developed intelligent fault tree analysis software system to conclude this study. The outputs of this software system are compared with those of the same system generated by an existing fault tree analysis software system for nuclear power plant safety assessment, i.e. SAPHIRE. The results of this comparison are then used to revise the software system as needed. Based on the results of this evaluation and revision, all research objectives have been achieved and the limitations of the existing fault tree analysis software system have been overcome.

## 1.6 THESIS STRUCTURE

This thesis is structured as follows.

Chapter 2 reviews six main topics related to this project, namely: (1) nuclear safety assessment; (2) fault tree analysis; (3) fuzzy sets; (4) failure possibility; (5) importance measure; and (6) sensitivity analysis.

Chapter 3 describes a new intelligent hybrid fault tree analysis framework and proposes the framework to solve the current problems of the nuclear power plant probabilistic safety assessment by fault tree analysis. A case study using a simple safety system of a typical nuclear power plant is also given in this chapter to explain and validate the quantification process of the framework.

Chapter 4 introduces essential fuzzy rules, which needs to be met by a technique to defuzzify the membership functions of fuzzy numbers into a nuclear event failure possibility score representing the most value that experts believe a nuclear event will occur. Then it presents an area defuzzification technique and validates the technique against the predefined fuzzy rules and the real reliability data taken from the nuclear power plants to see its suitability for the nuclear safety assessment by the fault tree analysis involving qualitative failure possibilities.

Chapter 5 explains a fuzzy reliability approach to generate nuclear event quantitative failure rates from the corresponding qualitative failure possibilities. A case study to validate the quantification process of the approach is also given in this chapter.

Chapter 6 describes an intelligent fault tree analysis software system to realize the intelligent hybrid framework. A real-world application to validate the developed intelligent system is also given in this chapter.

Chapter 7 summarizes the study and provides new research directions that could be pursued in the future.

References list all sources that have been used to complete the study and to write this thesis.

Appendix provides the fault trees of the first model of the reactor protection system of the U.S. combustion engineering pressurized water reactor, which are used to validate the developed intelligent system.

The relationships amongst chapters of this thesis are graphically described in Figure 1.1.

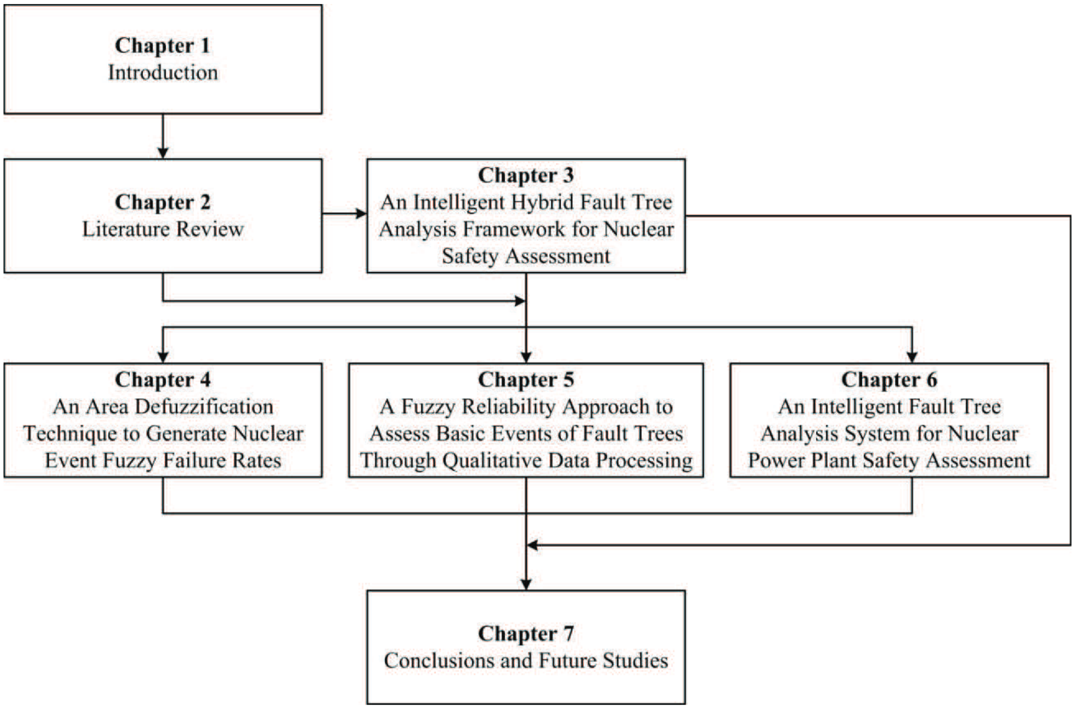

Chapter 1
Introduction
Chapter 2
Literature Review
Chapter 3
An Intelligent Hybrid Fault Tree Analysis Framework for Nuclear Safety Assessment
Chapter 4
An Area Defuzzification Technique to Generate Nuclear Event Fuzzy Failure Rates
Chapter 5
A Fuzzy Reliability Approach to Assess Basic Events of Fault Trees Through Qualitative Data Processing
Chapter 6
An Intelligent Fault Tree Analysis System for Nuclear Power Plant Safety Assessment
Chapter 7
Conclusions and Future Studies

**Figure 1.1 Relationships amongst thesis chapters.**

## 1.7 PUBLICATIONS RELATED TO THIS THESIS

Below is the list of publications relating to this thesis from the beginning of the study to present.

**Book Chapters**

1. Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2010, 'A hybrid approach for fault tree analysis combining probabilistic method with fuzzy numbers', in L. Rutkowski, R. Scherer, R. Tadeusiewicz, L.A. Zadeh & J.M. Zurada (eds), *Artificial Intelligence and Soft Computing*, vol. 1, Springer, Berlin / Heidelberg, pp. 194-201.

2. Purba, J.H., Lu, J. & Zhang, G. 2012, 'Fuzzy failure rate for nuclear power plant probabilistic safety assessment by fault tree analysis', in C. Kahraman (ed.),

*Computational Intelligence Systems in Industrial Engineering*, Atlantis Press, pp. 133-157.

**International Journals**

3. Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2011, 'Failure possibilities for nuclear safety assessment by fault tree analysis', *International Journal of Nuclear Knowledge Management*, vol. 5, no. 2, pp. 162-177.

4. Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2012, 'An area defuzzification technique to assess nuclear event reliability data from failure possibilities', *International Journal of Computational Intelligence and Applications*, vol. 11, no. 4, 1250022 (16 pp).

5. Purba, J.H., Lu, J., Zhang, G. & Pedrycz, W., 'A fuzzy reliability algorithm to assess basic events of fault trees through qualitative data processing', *Fuzzy Sets and Systems (Available online 18 June 2013)*.

6. Purba, J.H., Lu, J. & Zhang, G., 'Intelligent fault tree analysis software system to assess nuclear power plant safety', *Risk Analysis (under review)*.

**International Conferences**

7. Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2010, 'Probabilistic safety assessment in nuclear power plants by fuzzy numbers', in: *Proceedings of 9th International FLINS Conference,* August 2-4, 2010, Chengdu – China, pp. 256-262.

8. Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2012, 'A failure possibility-based reliability algorithm for nuclear safety assessment by fault tree analysis', in: *Proceedings of 1st International Workshop on Safety & Security Risk Assessment and Organizational Cultures (SSRAOC2012)*, January 29-31, 2012, SCK•CEN, Antwerp – Belgium, pp. 29-36.

9. Purba, J.H., Lu, J. & Zhang, G. 2012, 'An area defuzzification technique and essential fuzzy rules for defuzzifying nuclear event failure possibilities into reliability data', in: *Proceedings of 10th International FLINS Conference*, August 26-29, 2012, Istanbul – Turkey, pp. 1208-1213.

Chapter 2

# LITERATURE REVIEW

Since this study involves nuclear safety assessment, fault tree analysis, fuzzy sets, failure possibility, importance measure, and sensitivity analysis, we review literatures in these topics below.

## 2.1 NUCLEAR SAFETY ASSESSMENT

In constructing a nuclear power plant, engineers must comply with a number of strict regulations to limit the possible radioactive releases. These regulations are applied throughout the lifetime of the plant, i.e. from the design and construction stages to the operating phases and final decommissioning. There are three main goals of the nuclear power plant safety, namely: 1) to ensure that the plant will operate normally and without an excessive risk of radioactive materials to the operating staffs and environment; 2) to prevent incidents; and 3) to limit the consequences of any incident that might happen.

Nuclear safety assessment is currently achieved by the so-called probabilistic safety analysis (Garrick & Christie 2002). The probabilistic safety assessment is an analysis, which is used during both design and operating stages of nuclear power plants, to identify and to analyze every possible condition and event sequences that might cause reactor core damage (Kishi et al. 2004). Safety functions and their associated systems, which are necessary to carry out the safety functions, are evaluated by this assessment. Designers, utility and regulatory personnel can use the probabilistic safety assessment results to verify the nuclear power plant design, to assess the possible changes to the plant design or operation, and to assess the potential changes to the plant licensing basis (Delaney, Apostolakis & Driscoll 2005; Lederman, Niehaus & Tomic 1996; Liu, Tong & Zhao 2008).

In the nuclear power plant probabilistic safety assessment, nuclear safety analysts must have confidence in the input data to gain confidence in the results. On the basis of this consideration, it is recommended to use plant specific data, which can be taken from operator logs and maintenance logs. The data will represent the actual failure of a specific component in the specific operating and maintenance environment. In line with this, the International Atomic Energy Agency has introduced and defined the concept of living probabilistic safety assessment in TECDOC-1106 to encourage all nuclear power plant owners to collect and store precise failure data of their plants as far as possible (IAEA 1999) and redefined by Nuclear Energy Agency in a report by a group of experts (NEA 2005). If the failure probabilities of plant events and components are well known in advance, the failure probability of the nuclear safety system can be estimated and the relative importance of any individual event and component to the system failure probability can be calculated (Huang, Tonga & Zuo 2004; Wall, Haugh & Worlege 2001). In case of unavailable plant precise failure data, it is common to use a generic database that can be taken from various sources such as other nuclear power plants, nuclear industries other than nuclear power plants, and non-nuclear industries (Hsu & Musicki 2005).

Fault tree analysis has been widely used as a deductive tool for nuclear power plant probabilistic safety assessment to assess the failure probabilities of particular safety functions or safety systems (Bodansky 2004; Dhillon 2005; Ericson 2005; Guimaraes & Lapa 2008; Hadavi 2008; Stacey 2007; Yuhua & Datao 2005). It provides a comprehensive and structured approach to identify and understand key plant vulnerabilities, to develop accident scenarios, to assess the level of plant safety, and to derive numerical estimates of potential risks (Delaney, Apostolakis & Driscoll 2005; Kishi et al. 2004; Liu, Tong & Zhao 2008; Niehaus 1989).

## 2.2 FAULT TREE ANALYSIS

A fault tree is a graphical model representing the combinations of parallel and/or sequential fault events that can lead to the occurrence of the predefined undesired top event (Ericson 2005). It depicts logical interrelationships amongst basic events to the top event. Boolean gates denote the relationship between inputs and an output. The higher event is the output of the gate and the lower events are the inputs to the gate. In drawing a fault tree, the process starts from the higher faults to the more basic faults. In this analysis, Boolean algebras are used to mathematically represent the tree diagram and calculate the output of every logic gate (Epstein & Rauzy 2005; Ericson 2005; Huang, Tonga & Zuo 2004). The occurrence probability of the undesired top event is a function of the reliability data of primary events, which are also known as basic events (IAEA 2007; Verma, Srividya & Karanki 2010; Yang 2007).

In general, the existing nuclear power plant probabilistic safety assessment by fault tree analysis consists of three major analysis types, i.e. (1) qualitative analysis to evaluate minimal cut sets in the fault tree; (2) quantitative analysis to calculate cut set failure probabilities and the top event failure probability; and (3) importance measure evaluation to see how far a basic event and a cut set contribute to the top event failure probability (Borgonovo 2007a; Ferdous et al. 2007; Lin & Wang 1997; Song, Zhang & Chan 2009; Vesely et al. 1981). The typical framework of the nuclear power plant probabilistic safety assessment by the conventional fault tree analysis is depicted in Figure 2.1.

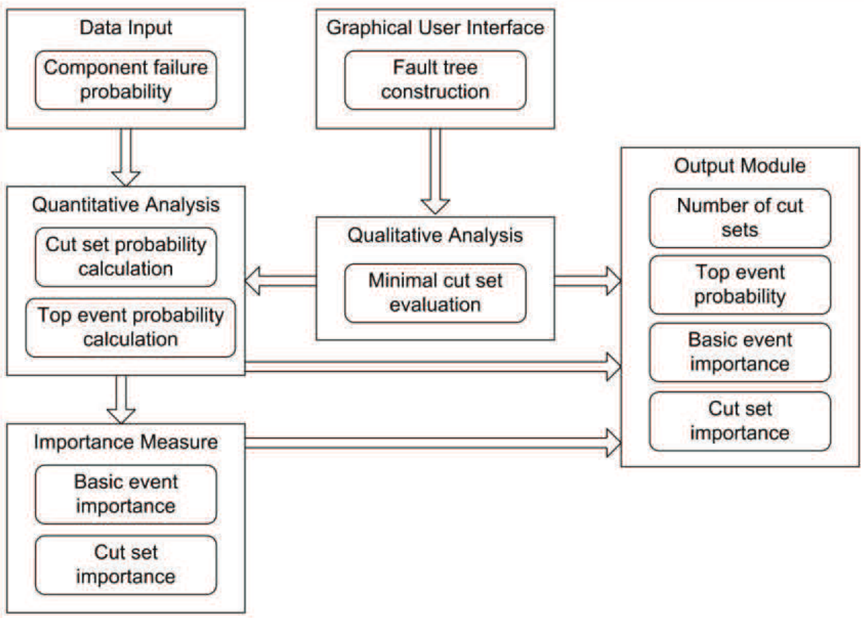


**Figure 2.1 Typical framework of the nuclear power plant probabilistic safety assessment by fault tree analysis.**

Two types of results can be obtained from fault tree analysis, i.e. qualitative and quantitative results (Lin & Wang 1997; Song, Zhang & Chan 2009; Vesely et al. 1981). The qualitative results include minimal cut sets and qualitative component importance. Meanwhile, the quantitative results include absolute probabilities and quantitative component and/or minimal cut set importance.

### 2.2.1 FAULT TREE MODEL

A typical fault tree model is composed of a number of symbols to describe events, Boolean gates, and page transfers. Event symbols represent nuclear events, i.e. intermediate events and basic events, which may fail in the system to cause the undesired top event to occur. Boolean gate symbols represent relationships between input events and an output event in graphical form. Some Boolean gates will occur if a condition attached to the gates is satisfied. Transfer event symbols are pointers to indicate sub-tree branches that are used elsewhere in the tree. All those symbols, together with their name and description, are shown in Tables 2.1, 2.2 and 2.3 (Dhillon 1999; Ericson 2005; Vesely et al. 1981).

**Table 2.1 Event symbols.**

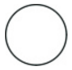
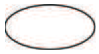
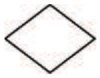
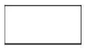
| Symbol | Name | Description |
|---|---|---|
|  | Basic event | A basic event, which do not need further development |
|  | Conditional event | A specific condition is applied PRIORITY AND and INHIBIT logic gates |
|  | Undeveloped event | A fault event, which cannot be further developed due to lack of information |
|  | Intermediate event | A fault event, which is resulted from an operation of a Boolean gate |

**Table 2.2 Boolean gate symbols.**

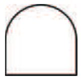
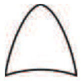
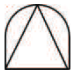
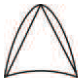
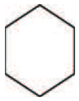
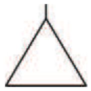
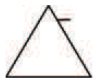
| Symbol | Name | Description |
|---|---|---|
|  | AND | The output event occurs when all input events occur |
|  | OR | The output event occurs when at least one of input events occur |
|  | PRIORITY AND | The output event occurs when all input events occur in a specific condition |
|  | EXCLUSIVE OR | The output event occur when exactly only one of input events occurs |
|  | INHIBIT | The output event occur when a single input event occurs within an enabling condition |

**Table 2.3 Page transfer symbols.**

| Symbol | Name | Description |
|---|---|---|
|  | TRANSFER IN | The fault tree is further developed at the corresponding TRANSFER OUT |
|  | TRANSFER OUT | The fault tree is the attachment of the corresponding TRANSFER IN |

### 2.2.2 Boolean Algebra

Boolean algebra is the algebra of fault events used in a fault tree to mathematically represent the relationship between input fault events and an output fault event of a Boolean gate in the tree. This relationship describes a situation where an output of the gate either fails or not. This Boolean algebra is very useful for constructing and simplifying a complicated fault tree by eliminating repeating events and/or non minimal cut sets. Some important Boolean algebra is given in Table 2.4 (Haimes 2004; Vesely et al. 1981).

**Table 2.4 Boolean algebras.**

| Rules | Engineering Symbolism | Mathematical Symbolism |
|---|---|---|
| Idempotent law | X . X = X<br>X + X = X | X ∩ X = X<br>X ∪ X = X |
| Distributive law | X . (Y + Z) = X . Y + X . Z | X ∩ (Y ∪ Z) = (X ∩ Y) ∪ (X ∩ Z) |
| Commutative law | X . Y = Y . X<br>X + Y = Y + X | X ∩ Y = Y ∩ X<br>X ∪ Y = Y ∪ X |
| Absorption law | X . (X + Y) = X<br>X + (X . Y) = X | X ∩ (X ∪ Y) = X<br>X ∪ (X ∩ Y) = X |

### 2.2.3 Failure Probability Calculation

The failure probability of an output event from two or more independent input events combined by a Boolean OR gate as shown in Figure 2.2 is calculated using Eq. (2.1) and by a Boolean AND gate as shown in Figure 2.3 is calculated using Eq. (2.2).

$$P(A_0) = 1 - \prod_{i=1}^{n}\{1 - P(A_i)\} \tag{2.1}$$

$$P(A_0) = \prod_{i=1}^{n} P(A_i) \tag{2.2}$$

where $P(A_i)$ is the failure probability of the input event $A_i$ and $n$ is the number of input events to the Boolean gate.

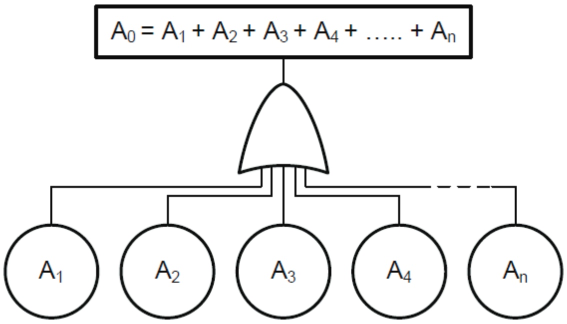


**Figure 2.2 Boolean OR gate with *n* input events.**

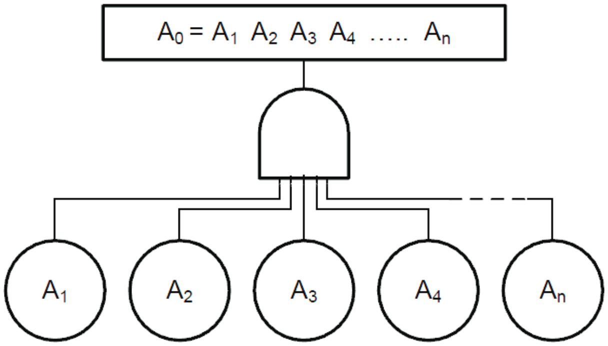
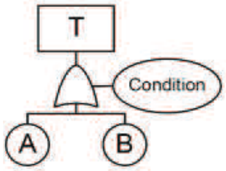
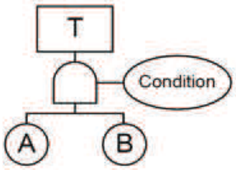
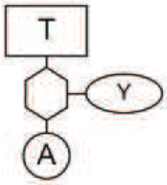


**Figure 2.3 Boolean AND gate with *n* input events.**

The top event $A_0$ in Figure 2.2 will fail if all input events $A_i$ fail together at the same time. On the other hand, the top event $A_0$ in Figure 2.3 will fail if one of input events $A_i$ fails.

The fault tree representations and the corresponding failure probability calculation formulas for other three Boolean gates that are attached by a condition are shown in Table 2.5 (Ericson 2005).

**Table 2.5 Probability calculation formulas for other Boolean gates.**

| Boolean gates | Fault tree representations | Probability calculation formulas |
|---|---|---|
| Exclusive OR Gate |  | $P(T) = P(A) + P(B) - 2 \times P(A) \times P(B)$ |
| Priority AND Gate |  | $P(T) = \frac{P(A) \times P(B)}{N!}$<br>where $N$ is the number of inputs |
| Inhibit Gate |  | $P(T) = P(A) \times P(Y)$ |

## 2.2.4 Repeated Fault Events, Cut Sets and Minimal Cut Sets

To obtain reliable results in the fault tree analysis, repeating events and non minimal cut sets must be eliminated prior to calculating the occurrence probability of the undesired top event (Dhillon 1999). Both top-down and bottom-up algorithms are the two most common approaches for generating cut sets for fault trees and the laws of Boolean algebras can be used to remove all non minimal cut sets and duplicate cut sets to obtain minimal cut sets (Ericson 2005; Haimes 2004; Vesely et al. 1981).

### (1) Repeated Fault Events

Repeated fault events are events, which appear in system fault tree more than once. For example, in the fault tree shown in Figure 2.4, all basic events, i.e. $A$, $B$ and $C$ are repeating events. These three repeating events have to be eliminated before the failure probability of the top event, i.e. $T$, is calculated.

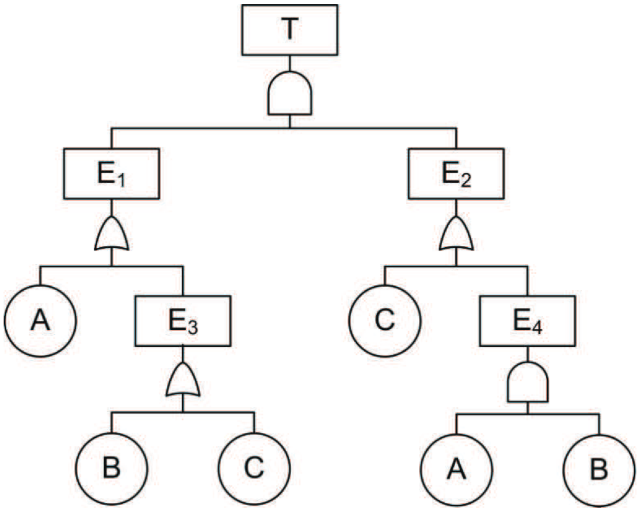


**Figure 2.4 Fault tree with repeating events.**

(2) CUT SETS

A cut set is a set of fault events if they occur together can cause the top undesired event to occur. The corresponding mathematical representation of the system fault tree in Figure 2.4 can be written as follows.

$T = E_1 \,.\, E_2$

$E_1 = A + E_3$

$E_2 = C + E_4$

$E_3 = B + C$

$E_4 = A \,.\, B$

By substitution and implementation of the four laws of the Boolean algebras in Table 2.4, we can obtain cut sets for the fault tree in Figure 2.4 as follows.

$T = (A + E_3) \,.\, (C + E_4) = A \,.\, C + A \,.\, E_4 + C \,.\, E_3 + E_3 \,.\, E_4$

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

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

$$T = A \,.\, C + A \,.\, B + B \,.\, C + C + A \,.\, B \,.\, C \tag{2.3}$$

From Eq. (2.3), we can see that the fault tree in Figure 2.4 has five cut sets, namely: *AC*, *AB*, *BC*, *C*, and *ABC*.

### (3) MINIMAL CUT SETS

A minimal cut set is a cut set that has been reduced into the minimum number of fault events to cause the top undesired event to occur (Dhillon 1999; Ericson 2005; Haimes 2004; Vesely et al. 1981). The number of different basic events in a minimal cut set is called the order of the cut set. When we have a cut set with only one basic event, the top event will occur as soon as this basic event occurs. When a cut set has two basic events, both of these have to occur at the same time to cause the top event to occur (Vesely et al. 1981). A cut set of order one is usually more critical than a cut set of order two or higher.

In Eq. (2.3), we can see that three cut sets, i.e. *A.C, B.C* and *A.B.C*, are not minimal cut sets because if the cut set *C* fail then basic events *A* and/or *B* do not need to fail to cause the top event *T* to fail. Hence, the minimal cut sets of the fault tree in Figure 2.4 are *C* and *A.B*. Using these two minimal cut sets, the fault tree in Figure 2.4 can be simplified as shown in Figure 2.5. This simplified fault tree has been free of repeating events and non minimal cut sets.

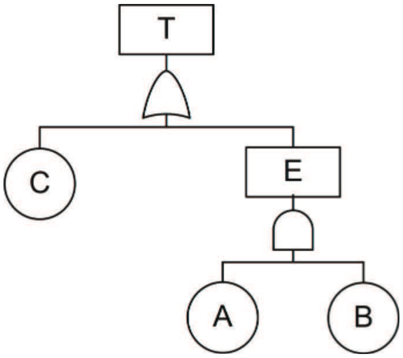


**Figure 2.5 Simplified fault tree of the fault tree in Figure 2.4.**

## 2.2.5 SOFTWARE SYSTEMS FOR FAULT TREE ANALYSIS

Due to the complexity of fault tree analysis, a number of personal computer-based software systems have been developed. The Probabilistic Safety Analysis PACKage (PSAPACK) and the Systems Analysis Programs for Hands-On Integrated Reliability

Evaluations (SAPHIRE) are two well-known fault tree analysis software packages for nuclear power plant probabilistic safety assessment.

PSAPACK was developed by the International Atomic Energy Agency in cooperation with its Member States, and at the beginning of the development process, this package was intended to be used for training purposes (Lederman, Vallerga & Bojadjiev 1990). PSAPACK has been used to evaluate the safety systems of various nuclear power plants (Arul et al. 2006; Suresh, Babar & Venkat Raj 1996; Uryas'ev & Vallerga 1993; Vinod et al. 2003). Meanwhile, SAPHIRE was developed by the United State Nuclear Regulatory Commission (US-NRC) at the Idaho National Laboratory (INL) (Smith et al. 2008). This fault tree analysis software package was developed primarily for assessing nuclear power plant safety systems (Harvego et al. 2006). SAPHIRE has been used to evaluate the Iranian heavy water research reactor (IHWRR) (Faghihi et al. 2008), the Combustion Engineering reactor protection system (Bickel 2008; Wierman et al. 2001b), the typical TRIGA research reactor (Arshi, Nematollahi & Sepanloo 2010), and the Babcock and Wilcox Reactor Protection System (Wierman et al. 2001a).

### 2.2.6 Fault Tree Analysis Of The U.S. Combustion Engineering Reactor Protection System

The U.S. Combustion Engineering Reactor Protection System (CERPS) comprises numerous electronic and mechanical components to produce an automatic or manual rapid shutdown when the reactor experiences disturbed conditions and requires a trip to stop the nuclear reaction. Nuclear event data for this CERPS during the period 1984 through 1998 operating experience are well documented in Wierman et al. (2001b) to be used for validation and evaluation of the research outputs.

Many researchers have also used this data source to validate their proposed new approach. Bondavalli & Filippini (2004) used this data source to validate their proposed deterministic stochastic petri net to assess the availability and performability of the safety function of the reactor protection system. In the study by Bartha et al. (2005), this data source was used to validate their proposed periodic and outage testing methodology of the reactor protection systems in the Paks Nuclear Power Plant. Meanwhile, Kang & Han (2006) used this data source to calculate alpha parameters to make the common cause failure event failure rates suitable for the emergency diesel generator for Ulchin Unit 3. Bickel (2008) used this data set to evaluate the risk implications of the core protection calculator system failure in the reactor protection system.

## 2.3 Fuzzy Set Theory

Zadeh (1965) introduced fuzzy set theory to deal with and mathematically model information uncertainties and since then this theory has been developed and applied in a number of real world applications. This section briefly reviews the concepts of fuzzy sets, fuzzy numbers, fuzzy aggregation, fuzzy reliability, and defuzzification technique.

### 2.3.1 Fuzzy Sets

Let $X$ be a collection of object universe whose elements are denoted by $x$. A fuzzy subset $A$ in $X$ is characterized by its membership function $\mu_A(X)$. This function associates with every single element $x$ in $X$ in the interval [0,1] (Zadeh 1965).

$$\mu_A: X \to [0,1],\ x \mapsto \mu_A(x) \epsilon [0,1] \tag{2.4}$$

The value of the membership function $\mu_A(X)$ represents the membership grade of $x$ in $X$. The closer the value to 1 is, the stronger the degree of membership of $x$ in $A$ *is*. Some basic notions that are defined for fuzzy sets are union, intersection, and complementation as shown in Eqs. (2.5-2.7), respectively (Bector & Chandra 2005; Lu et al. 2007).

$$\mu_{A\cup B}(x) = max(\mu_A(x), \mu_B(x)) = \mu_A(x) \vee \mu_B(x) \tag{2.5}$$

$$\mu_{A\cap B}(x) = min(\mu_A(x), \mu_B(x)) = \mu_A(x) \wedge \mu_B(x) \tag{2.6}$$

$$\mu_{A^c}(x) = 1 - \mu_A(x) \tag{2.7}$$

### 2.3.2 FUZZY NUMBERS

A fuzzy number is one type of fuzzy sets with normalized membership function. A fuzzy number $\tilde{A}$ is a subset of real line $R$ whose membership function $\mu_{\tilde{A}}(x)$ can be a continuously mapping from $R$ into a closed interval [*0,1*]. The membership function $\mu_{\tilde{A}}(x)$ has the following characteristics (Dubois & Prade 1978).

(a) $\mu_{\tilde{A}}(x) = 0$, for all $x \in (-\infty, a]$;

(b) $\mu_{\tilde{A}}(x)$ is strictly increasing on $[a,b]$;

(c) $\mu_{\tilde{A}}(x) = 1$, for all $x \in [b,c]$;

(d) $\mu_{\tilde{A}}(x)$ is strictly decreasing on $[c,d]$;

(e) $\mu_{\tilde{A}}(x) = 0$, for all $x \in [\mathrm{d}, \infty)$,

where *a, b, c,* and *d* are real numbers and $a \leq b \leq c \leq d$.

It is assumed that the fuzzy number $\tilde{A}$ is convex and bounded, unless it is specifically specified in a certain condition and application (Wang et al. 2006). The membership function of the fuzzy number $\tilde{A}$ can be expressed as follows.

$$\mu_{\tilde{A}}(x) = \begin{cases} \mu_{\tilde{A}}^{L}(x), & a \leq x \leq b \\ 1, & b \leq x \leq c \\ \mu_{\tilde{A}}^{R}(x), & c \leq x \leq d \\ 0, & \text{otherwise} \end{cases} \tag{2.8}$$

where $\mu_{\tilde{A}}^{L}(x): [a,b] \rightarrow [0,1]$ and $\mu_{\tilde{A}}^{R}(x): [c,d] \rightarrow [0,1]$. The former is called the left membership function and the latter is the right membership function (Abbasbandy & Hajjari 2009; Wang et al. 2006). If both $\mu_{\tilde{A}}^{L}(x)$ given in Eq. (2.9) and $\mu_{\tilde{A}}^{R}(x)$ given in Eq. (2.10) are linear as shown in Figure 2.6, then the fuzzy number $\tilde{A}$ is a trapezoidal fuzzy number and usually denoted by $\tilde{A}$ = (*a,b,c,d*). In a special case when $b = c$, the trapezoidal fuzzy number is transformed into a triangular fuzzy number.

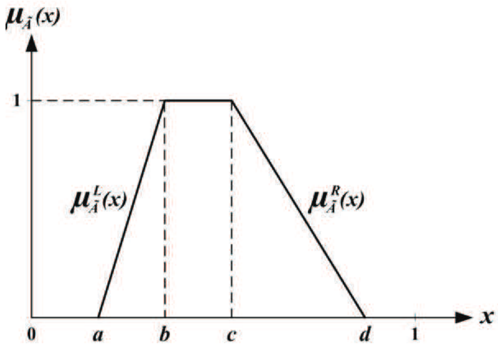


**Figure 2.6 Trapezoidal and triangular fuzzy numbers.**

$$\mu_{\tilde{A}}^{L}(x) = \frac{x-a}{b-a} \tag{2.9}$$

$$\mu_{\tilde{A}}^{R}(x) = \frac{d-x}{d-c} \tag{2.10}$$

Since the left membership function is continuous and strictly increasing, it has an inverse function, i.e. $\mu_{\tilde{A}}^{L}(y)$, as given in Eq. (2.11). Meanwhile, since the right membership function is also continuous and strictly decreasing, it also has an inverse function, i.e. $\mu_{\tilde{A}}^{R}(y)$, as given in Eq. (2.12) (Cheng 1998; Chu & Tsao 2002).

$$\mu_{\tilde{A}}^{L}(y) = \left(\mu_{\tilde{A}}^{L}(x)\right)^{-1} = a + (b-a)y \tag{2.11}$$

$$\mu_{\tilde{A}}^{R}(y) = \left(\mu_{\tilde{A}}^{R}(x)\right)^{-1} = d + (c-d)y \tag{2.12}$$

where y ∈ [0,1]. These inverse functions are graphically shown in Figure 2.7.

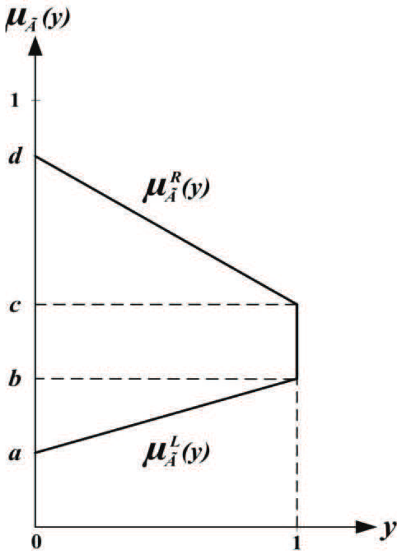


**Figure 2.7 Inverse of the trapezoidal fuzzy numbers.**

Some basic notions that are defined for fuzzy numbers are fuzzy addition, subtraction, and multiplication. The fuzzy addition, subtraction, and multiplication of two fuzzy numbers $A$ and $B$ at α-cut, $A_{\alpha} = \left[a_1^{(\alpha)},\ a_2^{(\alpha)}\right]$ and $B_{\alpha} = \left[b_1^{(\alpha)},\ b_2^{(\alpha)}\right]$ respectively, are shown in Eqs. (2.13-2.16) (Bector & Chandra 2005; Gupta & Bhattacharya 2007).

$$A + B = \left[a_1^{(\alpha)} + b_1^{(\alpha)}, a_2^{(\alpha)} + b_2^{(\alpha)}\right] \tag{2.13}$$

$$A - B = \left[a_1^{(\alpha)} - b_2^{(\alpha)}, a_2^{(\alpha)} - b_1^{(\alpha)}\right] \tag{2.14}$$

$$\begin{aligned} A\ .\ B = \Big[&min\left(a_1^{(\alpha)}.\ b_1^{(\alpha)}, a_1^{(\alpha)}.\ b_2^{(\alpha)}, a_2^{(\alpha)}.\ b_1^{(\alpha)}, a_2^{(\alpha)}.\ b_2^{(\alpha)}\right), \\ &max\left(a_1^{(\alpha)}.\ b_1^{(\alpha)}, a_1^{(\alpha)}.\ b_2^{(\alpha)}, a_2^{(\alpha)}.\ b_1^{(\alpha)}, a_2^{(\alpha)}.\ b_2^{(\alpha)}\right)\Big] \end{aligned} \tag{2.15}$$

$$\text{If } a_1^{(\alpha)} \geq 0 \text{ and } b_1^{(\alpha)} \geq 0 \text{ then } A\ .\ B = \left[a_1^{(\alpha)}.\ b_1^{(\alpha)}, a_2^{(\alpha)}.\ b_2^{(\alpha)}\right] \tag{2.16}$$

Fuzzy numbers can have different form for different application or different engineering systems. The selection of a certain fuzzy numbers depends on the nature of the problem at hand (Markowski & Mannan 2008). Trapezoidal and triangular fuzzy numbers form a sound practical alternative (Ferdous et al. 2011; Wolkenhauer 2001) to reflect uncertainties, inaccuracy and fuzziness of human justifications involving in linguistic values (Hryniewicz 2007; Ross 2004b; Zhang, Ma & Lu 2009). They have been implemented in offshore engineering systems (Liu et al. 2008a; Liu, Martinez & Wang 2008; Liu et al. 2008b; Ren et al. 2005; Yang, Bonsall & Wang 2008), a power transformer (Wu et al. 2007), a robot drilling system (Lin & Wang 1997), nuclear power plants (Gentile, Rogers & Mannan 2003; Guimaraes & Lapa 2004, 2007, 2008; Huang, Chen & Wang 2001b; Suresh, Babar & Venkat Raj 1996), and a conveyor system (Gupta & Bhattacharya 2007).

### 2.3.3 Fuzzy Aggregations

A fuzzy aggregation technique is used to aggregate two or more fuzzy numbers. There are many aggregation techniques, which have been developed and implemented in engineering system application. We can classify existing fuzzy aggregation techniques into two groups; (1) fuzzy aggregation of same types of fuzzy numbers, i.e. arithmetic averaging and weighted averaging operations; and (2) fuzzy aggregation of different types of fuzzy numbers, i.e. "mean operator".

#### (1) Arithmetic Averaging

An arithmetic averaging operation can be used to aggregate $n$ membership functions of fuzzy numbers of the same types as given in Eq. (2.17) (Huang, Chen & Wang 2001b).

$$\mu(x) = \frac{1}{n} \otimes [\mu_1(x) \oplus \mu_2(x) \oplus \mu_3(x) \oplus \cdots \oplus \mu_n(x)] \qquad (2.17)$$

where $\mu_i(x)$ is a membership function of a fuzzy number and $n$ is the number of fuzzy numbers to be aggregated.

The arithmetic averaging operation is good for aggregating expert opinions because it can satisfy two characteristics of rational combination (Huang, Chen & Wang 2001b). The first characteristic is if the variation in the possibility distribution is small, it cannot produce a noticeable change. The second characteristic is if the weight of the experts is equal, it can also include relative importance weight among experts.

### (2) WEIGHTED AVERAGING

A weighted averaging is the extension of the arithmetic averaging operation by considering expert credibility level. This technique gives a weight of judgment to every expert representing their credibility level and the correlation between their judgments as given in Eq. (2.18) (Canos & Liern 2008; Guh, Po & Lee 2008; Gupta & Bhattacharya 2007; Lu, Zhang & Ruan 2008; Tsiporkova & Boeva 2006).

$$\mu(x) = \frac{w_1.\mu_1(x) \oplus w_2.\mu_2(x) \oplus w_3.\mu_3(x) \oplus \ldots \oplus w_n.\mu_n(x)}{w_1 \oplus w_2 \oplus w_3 \oplus \ldots \oplus w_n} \tag{2.18}$$

where *n* is the number of experts, $\mu_i(x)$ is the membership function of the fuzzy number given by the $i^{th}$ expert and $w_i$ is the weight of judgment given to the $i^{th}$ expert.

### (3) MEAN OPERATOR

A mean operator can be used to aggregate *n* membership functions of fuzzy numbers of the different types as given in Eqs. (2.22-2.23). The mean operator involves two consecutive operations: an $\alpha$-cut addition followed by an arithmetic averaging operation as described below (Ben-Arieh 2005; Chin et al. 2009; Lin & Wang 1997; Wu, Apostolakis & Okrent 1990).

The addition of fuzzy numbers *M* and *N* at the $\alpha$-level can be computed as follows.

$$f_{M \oplus N}(z) = \max_{z=x+y}\left(f_M(x) \wedge f_N(y)\right) \tag{2.19}$$

where $f_M(x)$ is the membership function of a trapezoidal fuzzy number $M(a_m,b_m,c_m,d_m)$ and $f_N(y)$ is the membership function of a triangular fuzzy number $N(a_n,b_n,c_n)$. If the α-cut of the fuzzy number *M* is $M_\alpha = [M_\alpha{}^L, M_\alpha{}^R]$ and the α-cut of the fuzzy number *N* is $N_\alpha = [N_\alpha{}^L, N_\alpha{}^R]$ then the aggregation of fuzzy numbers *M* and *N* at the α-level is computed as in Eq. (2.20).

$$f_{M \oplus N}(z) = [M_\alpha^L + N_\alpha^L, M_\alpha^R + N_\alpha^R] \tag{2.20}$$

Then, the averaging of the $\alpha$-cut addition in Eq. (2.20) is calculated as follows.

$$Z = \frac{f_{M\oplus N}(z)}{2} = \left[\frac{[(b_m-a_m)+(b_n-a_n)]\alpha+(a_m+a_n)}{2}, \frac{(d_m+c_n)-[(d_m-c_n)+(c_n-b_n)]\alpha}{2}\right] \quad (2.21)$$

Therefore, the α-cut of the final fuzzy number $Z$ is $Z_\alpha = [Z_\alpha{}^L, Z_\alpha{}^R]$, which is calculated as follows.

$$Z_\alpha^L = \frac{[(b_m-a_m)+(b_n-a_n)]\alpha+(a_m+a_n)}{2} \quad (2.22)$$

$$Z_\alpha^R = \frac{(d_m+c_n)-[(d_m-c_n)+(c_n-b_n)]\alpha}{2} \quad (2.23)$$

### 2.3.4 Fuzzy Reliability

A fuzzy reliability approach is an approach to estimate system reliability by utilizing the concept of failure possibility and fuzzy sets to overcome the limitation of the probabilistic reliability approach. Fuzzy set theory was first introduced as useful tools to complement conventional reliability theories in 1989 (Onisawa). Since then, several authors have attempted to develop techniques involving fuzzy set theory to evaluate system reliabilities. Bing et al. (2000) combined a fuzzy linear regression method with a finite element method to evaluate the reliability of mechanical structures. In this approach, a membership function of a triangular fuzzy number is used to express the structure stress. To overcome the limitation of the traditional Failure Mode, Effects and Criticality Analysis (FMECA), a fuzzy rule-based approach has been implemented to prioritize failure modes in (Bowles & Pelaez 1995; Gargama & Chaturvedi 2011; Xu et al. 2002). Furthermore, Zio et al. (2009) developed a fuzzy expert system for human reliability analysis to elicitate factors influencing conditional human error for two dependence successive operator actions in a nuclear power plant accident. Meanwhile, Deshpande and Khanna (1995) proposed fuzzy probabilities for fault tree analysis to estimate the failure probabilities of a storage tank of an ammonia plant and an nitric acid reactor. In this approach, trapezoidal fuzzy numbers are used to represent the failure of basic events and the fuzzy rules of multiplication and complementation are used to represent the “AND” and “OR” Boolean gates, respectively.

In Karimi & Hüllermeier (2007), fuzzy set theory has been used to complement probability theory to assess the risk of natural disaster when statistical data and/or physical knowledge are insufficient for probabilistic analysis. Ding & Lisnianski (2008) developed a fuzzy universal generating function in which fuzzy numbers used to represent the state probability and fuzzy composition operators introduced to assess the reliability of a multi state system. In Wang et al. (2011), a fuzzy reliability model is developed to deal with the drawbacks of the rule-based quantified cognitive reliability and error analysis method for power system safety assessment. Moreover, Pandey & Tyagi (2007) proposed a profust reliability to evaluate degradable systems and a fuzzy numbers-based method to assess system failure rate parameters. Meanwhile, Ding et al. (2010; 2008) proposed the membership function of fuzzy numbers to represent a sub system state in the reliability assessment of multi-state weighted *k*-out-of-*n* systems.

### 2.3.5 DEFUZZIFICATION TECHNIQUES

Defuzzification is a process of synthesis the output of fuzzy systems, which incorporates the representations of imprecision and/or uncertainties, to be a single scalar quantity as opposed to fuzzy sets (Klir & Yuan 2001). There are many defuzzification techniques, which have been developed and implemented in engineering system safety analysis involving fuzzy concepts. Huang, Chen & Wang (2001b) identified that there is no one single defuzzification technique, which is best for all applications. In addition, Bowles & Pelaez (1995) stated that the selection of the defuzzification technique is based on the requirements of the real situation and the point of view.

Van Leekwijck & Kerre (1999) have formulated criteria to develop defuzzification techniques. Then, they used those predefined criteria to evaluate and classify existing defuzzification techniques. Furthermore, a number of authors have also compared existing defuzzification techniques for ranking *n* fuzzy subsets (Abbasbandy & Asady 2006; Abbasbandy & Hajjari 2009; Asady & Zendehnam 2007; Bortolan & Degani 1985; Chen & Tang 2008; Cheng 1998; Kim & Park 1990; Liou & Wang 1992).

Four well-known defuzzification techniques, which have been widely implemented in engineering systems, are the left and the right, the centroid, the area between the centroid and the original points, and the centroid-based Euclidean distance defuzzification techniques.

### (1) Left And Right Fuzzy Ranking Defuzzification Technique

Left and right fuzzy ranking defuzzification technique applies the concept of the maximizing set and the minimizing set of a normal fuzzy number to calculate the total utility score of a fuzzy number. If $\tilde{A}$ is a trapezoidal fuzzy number then its crisp value ($cv$) is defuzzified from its membership functions using Eq. (2.24) (Chen 1985; Lin & Wang 1997; Wang 2009; Yuhua & Datao 2005).

$$cv = d\left(\mu_{\tilde{A}}(x)\right) = \frac{U_{\tilde{A}}^{R}(x)+1-U_{\tilde{A}}^{L}(x)}{2} \tag{2.24}$$

where $U_{\tilde{A}}^{L}(x)$ and $U_{\tilde{A}}^{R}(x)$ are the left and the right utility values of the fuzzy number $\tilde{A}$, which can be calculated using Eqs. (2.25-2.26), respectively.

$$U_{\tilde{A}}^{L}(x) = sup[\mu_{\tilde{A}}(x) \wedge f_{min}(x)] \tag{2.25}$$

$$U_{\tilde{A}}^{R}(x) = sup[\mu_{\tilde{A}}(x) \wedge f_{max}(x)] \tag{2.26}$$

Meanwhile, $f_{max}(x)$ and $f_{min}(x)$ are the maximizing set and the minimizing set of a normal fuzzy number, which can be obtained using Eqs. (2.27-2.28), respectively.

$$f_{max}(x) = \begin{cases} x & 0 \leq x \leq 1 \\ 0 & otherwise \end{cases} \tag{2.27}$$

$$f_{min}(x) = \begin{cases} 1-x & 0 \leq x \leq 1 \\ 0 & otherwise \end{cases} \tag{2.28}$$

In graphical representation as shown in Figure 2.8, the right utility value of the fuzzy number $\tilde{A}$ is the $y$-value of the coordinate of the intersection point between the maximizing set and the right side of the fuzzy number $\tilde{A}$. On the other hand, the left utility value of a fuzzy number $\tilde{A}$ is the $y$-value of the coordinate of the intersection point between the minimizing set with the left side of the fuzzy number $\tilde{A}$ (Chen 1985; Dubois & Prade 1978).

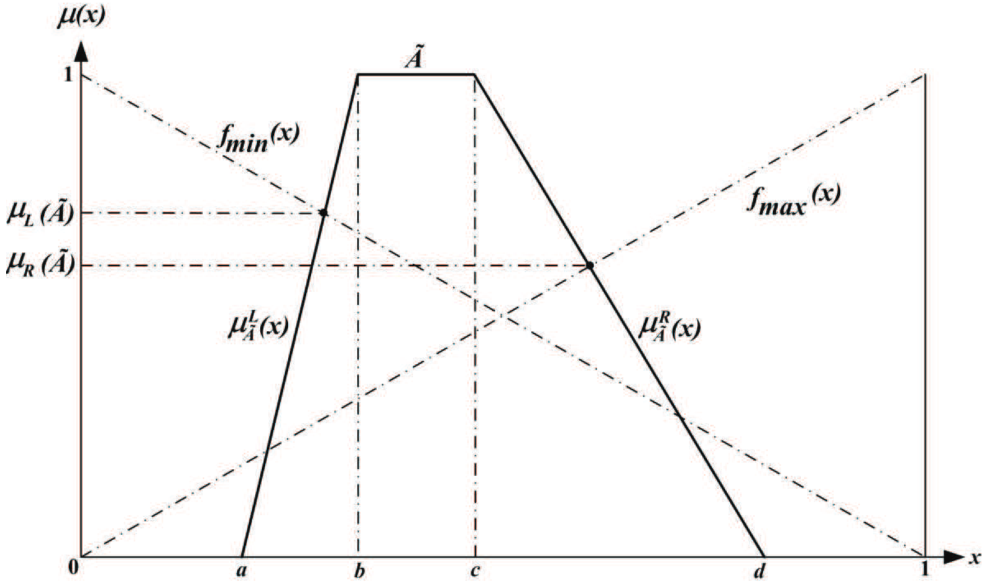


**Figure 2.8 Graphical representation of the utility value the trapezoidal fuzzy number.**

### (2) CENTROID DEFUZZIFICATION TECHNIQUE

Centroid defuzzification technique calculates the crisp value of a fuzzy number based on its center of gravity of the area under its membership function in the horizontal axis. If $\tilde{A}$ is a trapezoidal fuzzy number then its crisp value ($cv$) is defuzzified from its membership functions using Eq. (2.29) (Gupta & Bhattacharya 2007; Opricovic & Tzeng 2003; Pan 2006; Pan & Wang 2007; Wang 2009).

$$cv = d\big(\mu(A)\big) = \frac{\int_a^b x.\mu^L_{\tilde{A}}(x)dx + \int_b^c xdx + \int_c^d x.\mu^R_{\tilde{A}}(x)dx}{\int_a^b \mu^L_{\tilde{A}}(x)dx + \int_b^c dx + \int_c^d \mu^R_{\tilde{A}}(x)dx} \tag{2.29}$$

where $\mu^L_{\tilde{A}}(x)$ and $\mu^R_{\tilde{A}}(x)$ are the left and the right membership functions as given in Eqs. (2.9-2.10), respectively.

This technique is also well-known as the center of gravity or the center of area (Opricovic & Tzeng 2003; Ross 2004b; Wang et al. 2009).

### (3) Area Between The Centroid And Original Points Defuzzification Technique

Area between centroid point and original point defuzzification technique calculates the crisp value of a fuzzy number based on its centroid point and original point. If $\tilde{A}$ is a trapezoidal fuzzy number then its crisp value ($cv$) is defuzzified from its membership functions using Eq. (2.30) (Chu & Tsao 2002; Wang & Lee 2008; Wang et al. 2006).

$$cv = d\left(\mu_{\tilde{A}}(x)\right) = x_0\left(\tilde{A}\right).y_0(\tilde{A}) \tag{2.30}$$

where $x_0\left(\tilde{A}\right)$ is the horizontal axis and $y_0(\tilde{A})$ is the vertical axis of the centroid coordinate of the fuzzy number $\tilde{A}$.

The centroid coordinate of the trapezoidal fuzzy number in Eq. (2.30) can be calculated using Eqs. (2.31-2.32) (Wang et al. 2006).

$$x_0\left(\tilde{A}\right) = \frac{\int_a^b x.\mu_{\tilde{A}}^L(x)dx + \int_b^c xdx + \int_c^d x.\mu_{\tilde{A}}^R(x)dx}{\int_a^b \mu_{\tilde{A}}^L(x)dx + \int_b^c dx + \int_c^d \mu_{\tilde{A}}^R(x)dx} \tag{2.31}$$

$$y_0\left(\tilde{A}\right) = \frac{\int_0^1 y.\mu_{\tilde{A}}^R(y)dy - \int_0^1 y.\mu_{\tilde{A}}^L(y)dy}{\int_0^1 \mu_{\tilde{A}}^R(y)dy - \int_0^1 \mu_{\tilde{A}}^L(y)dy} \tag{2.32}$$

where $\mu_{\tilde{A}}^L(x)$ and $\mu_{\tilde{A}}^R(x)$ are the left and the right membership functions as given in Eqs. (2.9-2.10). Meanwhile, $\mu_{\tilde{A}}^L(y)$ and $\mu_{\tilde{A}}^R(y)$ are the inverse of the left and the right membership functions, respectively, as given in Eqs. (2.11-2.12).

### (4) Centroid-Based Euclidean Distance Defuzzification Technique

Centroid based Euclidean distance defuzzification technique calculates the crisp value of a fuzzy number based on its Euclidean distance. If $\tilde{A}$ is a trapezoidal fuzzy number then its crisp value ($cv$) is defuzzified from its membership functions using Eq. (2.33) (Cheng 1998; Chu & Tsao 2002; Pan & Yeh 2003a, 2003b; Wang et al. 2006).

$$cv = d\left(\mu_{\tilde{A}}(x)\right) = \sqrt{\left[x_0\left(\tilde{A}\right)\right]^2 + \left[y_0\left(\tilde{A}\right)\right]^2} \tag{2.33}$$

where $x_0(\tilde{A})$ is the horizontal axis and $y_0(\tilde{A})$ is the vertical axis of the centroid coordinate of the fuzzy number $\tilde{A}$ as given in Eqs. (2.31-2.32).

## 2.4 Failure Possibility And Membership Function Development

A theory of possibility, which is proposed by Zadeh (1978) as a further development of fuzzy set theory (Zadeh 1965), pointed out that a possibility distribution can be viewed as fuzzy sets. Wolkenhauer technically defined that a possibility distribution is fuzzy sets and all fuzzy sets are possibility distributions (2001). The possibility distribution numerically corresponds to the membership functions of fuzzy sets, i.e., $\pi_x(x) = \mu_A(x)$, where $x$ is a fuzzy variable and $A$ is the fuzzy set induced by $X$ (Dubois & Prade 1994). A failure possibility is a measure to what extent a value $x$ in the set $X$ to be a member of the subset $A_i \subseteq X$, which can be described by a membership function $\mu_{Ai}(x)$. This membership function is a mathematical representation of a subjective assessment of the failure possibility of an event (Moller et al. 1999). Safety evaluators can specify a range of values in the failure possibility distribution to qualitatively evaluate event failures (Dumitrescu et al. 2006). It can be used to estimate human error effects under ambiguous interacting environment (Kim & Bishu 2006 ).

### 2.4.1 Failure Possibility Development

This section describes the concepts of linguistic variable, data granularity and error possibility, which are commonly used in the failure possibility development.

### (1) Linguistic Variable

A linguistic variable is a variable which stores words or sentences as its values. Like in math, numerical variables take numerical values, in fuzzy set theory; linguistic variables take on linguistic values which are human words. It is used in the situation where information cannot be described and assessed quantitatively but qualitatively (Lu, Zhang & Ruan 2008; Lu et al. 2007; Martinez et al. 2007).

Linguistic values present in human reasoning and can be formalized as membership functions of fuzzy sets (Hryniewicz 2007; Zhang, Ma & Lu 2009). When the event is absent (not recorded) or, we are provided with inadequate (too few data to draw sound statistical inference), improper (poor record keeping), and inaccurate data, in the modeling of system reliability we resort ourselves to expert opinions (Celik, Lavasani & Wang 2010; Cho, Choi & Kim 2002; Ferdous et al. 2011; Hryniewicz 2007). Expert opinions, which are commonly given in linguistic values (Ferdous et al. 2011; Mentes & Helvacioglu 2011), have been successfully implemented in risk analysis (Lin & Bier 2008; Mazzuchi, Linzey & Bruning 2008). Expert opinions have also been implemented in nuclear engineering for making engineering decision (Moon & Kang 1999) and were in very good agreements with data from actual operating experiences (IAEA 1988). The advantage of using linguistic variables in engineering system safety analysis is that it can intuitively and easily express expert opinions which cannot be represented by numerical values (Huang, Chen & Wang 2001a; Lin & Wang 1997).

Cooke et al. (2008) recommended three indicators to choose experts, i.e. the number of scientific publications, recommendations from a wide range of experts, and experiences with previous similar studies. In real applications, the experts may have different levels of expertise, background and working experience. Hence, they may demonstrate different perceptions about the same events and subjectively provide different assessment. To reflect their differences of assessment, different justification weights may be assigned to every expert. Cooke and Goossens (2008) have formulated two key performance-based indicators to weight experts, i.e. calibration and informativeness. This technique needs ‘seed variables’ whose values have been known but at the time of assessment, the experts do not know those values. Using calibration questions, the probabilities of experts to correctly answer the questions can be drawn. The seed variables and the calibration questions must be as closely as possible to the problems that the study was intended to solve (Lin & Bier 2008). This technique has also been implemented in Tuomisto et al. (2008) to weight experts on air pollution epidemiology.

### (2) DATA GRANULARITY

Data granularity is the number of linguistic terms used to characterize phenomenon that cannot be represented by numerical values. The granularity of the linguistic terms that are commonly used in engineering system safety is from four to seven terms (Gentile, Rogers & Mannan 2003; Guimaraes & Lapa 2007; Gupta & Bhattacharya 2007; Liu et al. 2008b; Liu et al. 2005; Liu et al. 2004; Markowski, Mannan & Bigoszewska 2009; Pillay & Wang 2003; Ren et al. 2005; Yang et al. 2006; Yang, Bonsall & Wang 2008). This granularity is decided by experts in the field of the system being analyzed and in line with the situation of the case of the interest. For example, in offshore engineering systems, five to seven linguistic terms are used for antecedents and four linguistic terms are used for consequences in the fuzzy rules (Liu et al. 2008b; Ren et al. 2005; Yang, Bonsall & Wang 2008). Meanwhile, Guimaraes and Lapa use the granularity of five linguistic terms to estimate the safety level of the containment cooling system of a nuclear power plant (2007).

### (3) ERROR POSSIBILITY

Onisawa (1988) proposed a logarithmic function to fit the very small error possibility, which is expressed by a fuzzy subset of the unit interval [0, 1], to the nature of human judgment. This function considers the proportionality of human sensation to the logarithmic value of a physical quantity, as shown in Eq. (2.34).

$$e = \frac{1}{1+\left[K \times log\left(\frac{1}{E_m}\right)\right]^3} \tag{2.34}$$

where $e$ is error likelihood and $E_m$ is error possibility. Meanwhile, $K$ is a constant representing the safety criterion, which can be calculated using Eq. (2.35).

$$K = \frac{1}{log\left[\frac{1}{e_r}\right]} \tag{2.35}$$

where $e_r$ is the error rate of human justifications, which is calculated as follows.

$$e_r = \frac{\text{the lowest lower bound of the error rate}}{\text{the error rate of a routine}} \tag{2.36}$$

Furthermore, the lowest lower bound of the error rate is $5 \times 10^{-5}$ and the error rate of a routine is $10^{-2} - 10^{-3}$. Therefore $e_r = 5 \times 10^{-3}$ and $K = 0.435$ (Mentes & Helvacioglu 2011; Onisawa 1988; Pan & Wang 2007; Swain & Guttmann 1983).

### 2.4.2 MEMBERSHIP FUNCTION DEVELOPMENT

This section describes procedures, which have been widely used to develop membership functions. There are six straightforward techniques to assign membership functions to fuzzy variables, namely: intuition, inference, rank ordering, neural network, genetic algorithm, and inductive reasoning (Ross 2004a).

#### (1) INTUITION

An intuition technique is simply based on human innate intelligence and understanding of an issue. Using contextual and semantic knowledge, analysts can develop membership functions for fuzzy variables “temperature” differently for different context. For example, membership functions for fuzzy variables, as shown in Figure 2.9, i.e. cold, cool, warm, and hot, are used to describe temperature.

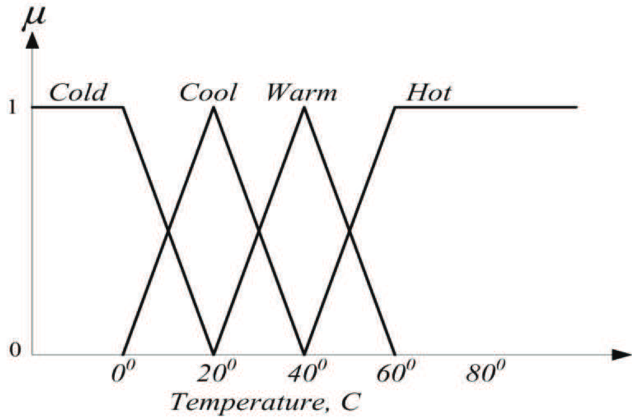


**Figure 2.9 Membership functions to describe temperature using fuzzy variables.**

The temperatures in Figure 2.9 are referred to, for example, the range of the safe operating temperatures of a steam turbine. If we want to refer the temperature to the human comfort, we will obtain another set of membership functions.

### (2) INFERENCE

An inference technique uses facts and knowledge to infer a conclusion. For example, if a triangle has $A$, $B$ and $C$ to be its inner angles in which $A \geq B \geq C \geq 0$, then the universe of triangles will be

$$U = \{(A, B, C) \mid A \geq B \geq C \geq 0\, ;\ A + B + C = 180^0\}$$

Let us say that we want to identify the membership function of a triangle by grouping triangles into five types, i.e. isosceles triangle, right triangle, isosceles and right triangle, equilateral triangle, and other triangles. Based on the facts and knowledge that we already know about those five types of shapes, an isosceles triangle has the following algorithm to develop its membership functions

$$\mu(A, B, C) = 1 - \frac{1}{60^0}\min(A - B, B - C)$$

If we know the algorithm for the other four types, we will be able to identify the membership functions for a triangle for the five types of triangles.

### (3) RANK ORDERING

A rank ordering technique assigns preferences to develop membership values for a fuzzy variable. These preferences can be collected from an individual, a group of people, a poll or other opinion collecting methods. By doing pair wise comparisons to the obtained preferences, the order of the membership functions can be defined. This technique is very good for fuzzy decision making to order possible decisions to be made.

### (4) NEURAL NETWORK

A neural network technique uses the concepts of the working network of the human neurons to determine the membership functions. This technique needs a number of input data, which are grouped into two data sets, i.e. a training data set and a checking data set.

The training data set are used to train the neural network, which has been created, in a repetitive process until all data within the training data set have their corresponding membership values. Then, the checking data set are used to check the performance of the neural network, which has been trained using the training data set. When the analysts satisfied with the performance of the neural network, the neural network is ready to determine the membership values for any given input data.

### (5) GENETIC ALGORITHM

A genetic algorithm technique is based on the concepts of Darwin's theory saying that the fittest living thing will survive. This algorithm involves several steps. Firstly, some possible functional mapping, membership functions and their corresponding shapes, are defined for a problem to be solved. Then, a fitness function is used to evaluate the fitness of each membership function. A set of good membership functions are then selected to create a new generation of membership functions. The process of the generation and evaluation will continue until the solution within a generation is convergence.

### (6) Inductive Reasoning

An inductive reasoning develops membership functions based on an ideal scheme. This scheme describes the relationships between input and output for a well-established database. The purpose of the induction in this technique is to find a rule to match the established input-output relationships.

## 2.5 Importance Measures

An importance measure is a measure used to assess how far an event or a component contributes to the system failure in the fault tree analysis (Borgonovo 2007a; Cheok, Parry & Sherry 1998; Ericson 2005). This measure is very useful in engineering system to identify the potential causes of the failure or to identify weak paths in the system designs and components. Risk managers can apply information obtained from this assessment to improve the safety level of the system by implementing risk reduction measure into the new design or build a more innovative design.

Minimal cut set and Fussell–Vesely importance measures are two most common methods used in fault tree analysis (Ericson 2005; van der Borst & Schoonakker 2001; Vinod et al. 2003). The minimal cut set importance measure can be used to rank the impact of every single minimal cut set to the occurrence of the top event failure (Ericson 2005). Meanwhile, the FV importance measure is the most common measure used evaluate the contribution of basic events to the occurrence of the top event failure for risk reduction indicator (van der Borst & Schoonakker 2001).

## 2.6 Sensitivity Analysis

Sensitivity analysis is defined as the study to understand uncertainty in the output of a model due to different sources of uncertainty in the input model (Apostolakis 1995;

Borgonovo 2007b; Saltelli 2002). It is used to evaluate system quantitative parameters after modifying the failure frequencies and can determine how sensitive system parameters to the change of the failure frequencies (Ferdous et al. 2007). The result of the sensitivity analysis can be used to support decision making, to ease communication between modellers and decision makers, and to increase understanding or quantification of the system (Pannell 1997). This is the most useful and most widely analysis technique used by modellers to support decision makers (Huang & Chang 2007).

In general, sensitivity analysis is a very simple idea, which incorporates two simple tasks i.e. changes the input parameters and observes the impacts to the model. In sensitivity analysis, three important things need to be clearly understood prior to analyse the system sensitivity, i.e. 1) what to be varied in the system; 2) what to be observed in the system; and 3) what experimental design to be performed for sensitivity analysis. Pannell (1997) suggest three different strategies for sensitivity analysis starting from the most comprehensive strategy to the simplest strategy.

The results of sensitivity analysis can be plotted as output versus the input parameters. The shape of the curve can determine the sensitivity of the output to the input parameters. A steeply changing curve indicates that the output is sensitive to the value of the input parameters. A relative flat curve indicates that the output is not sensitive to the value of the input parameters.

System sensitivity can be calculated using the partial derivative of the top event probability to the probability of a particular basic event (Ou & Dugan 2003). Sensitive index has been proposed to rank the sensitiveness of each basic event for fuzzy fault tree. It calculates the change percentage of the top event fuzzy probability due to the change of the fuzzy failure probability in the leave nodes (Chanda & Bhattacharjee 1998). Huang & Chang propose an improved decomposition scheme to analyse the sensitivity of dynamic tree and gate (2007). They use a linear-time algorithm proposed in (Dutuit & Rauzy 1996) to detect modules of fault tree. Ferdous et al. categorize two different basic steps for sensitivity analysis, i.e. cut set importance determination and improvement index estimation (2007).

This chapter has reviewed the concepts of the nuclear safety assessment, the fault tree analysis, the fuzzy sets, the failure possibility, the importance measures, and the sensitivity analysis. These concepts are used in Chapters 3, 4, 5 and 6 of this thesis.

# Chapter 3

# An Intelligent Hybrid Fault Tree Analysis Framework For Nuclear Safety Assessment

## 3.1 Introduction

The limitation of conventional fault tree analysis arises from the lack of sufficient historical failure data to estimate basic event failure probability. This chapter presents an intelligent hybrid fuzzy fault tree analysis framework to overcome this limitation. The intelligent hybrid framework introduces a failure possibility-based approach, which is integrated into the quantitative phase of the conventional fault tree analysis, to deal with basic events that do not have quantitative historical failure data for calculating their failure probabilities. The introduction of this failure possibility-based approach will overcome the limitation of the nuclear power plant probabilistic safety assessment by fault tree analysis by taking expert subjective opinions, which are expressed in qualitative failure possibilities, to evaluate nuclear event failures.

The remainder of this chapter is structured as follows. The framework of the intelligent hybrid fault tree analysis is described in Section 3.2. In Section 3.3, the failure possibility-based approach is explained in detail and an illustrative case study to demonstrate how the intelligent hybrid fault tree analysis can solve the current problems of conventional fault tree analysis is given in Section 3.4. Finally, this chapter is summarized in Section 3.5. The work presented in this chapter has been reported in three of our publications listed in Section 1.7, i.e. publication numbers 1, 3 and 7.

## 3.2 AN INTELLIGENT HYBRID FAULT TREE ANALYSIS FRAMEWORK

In general, the typical conventional fault tree analysis consists of four analysis phases, namely: system analysis, qualitative analysis, quantitative analysis, and criticality analysis. The proposed intelligent hybrid fault tree analysis framework introduces fuzzy failure rates, which are generated using a failure possibility-based approach, into the quantitative analysis phase as depicted in Figure 3.1 to overcome the limitations of conventional fault tree analysis.

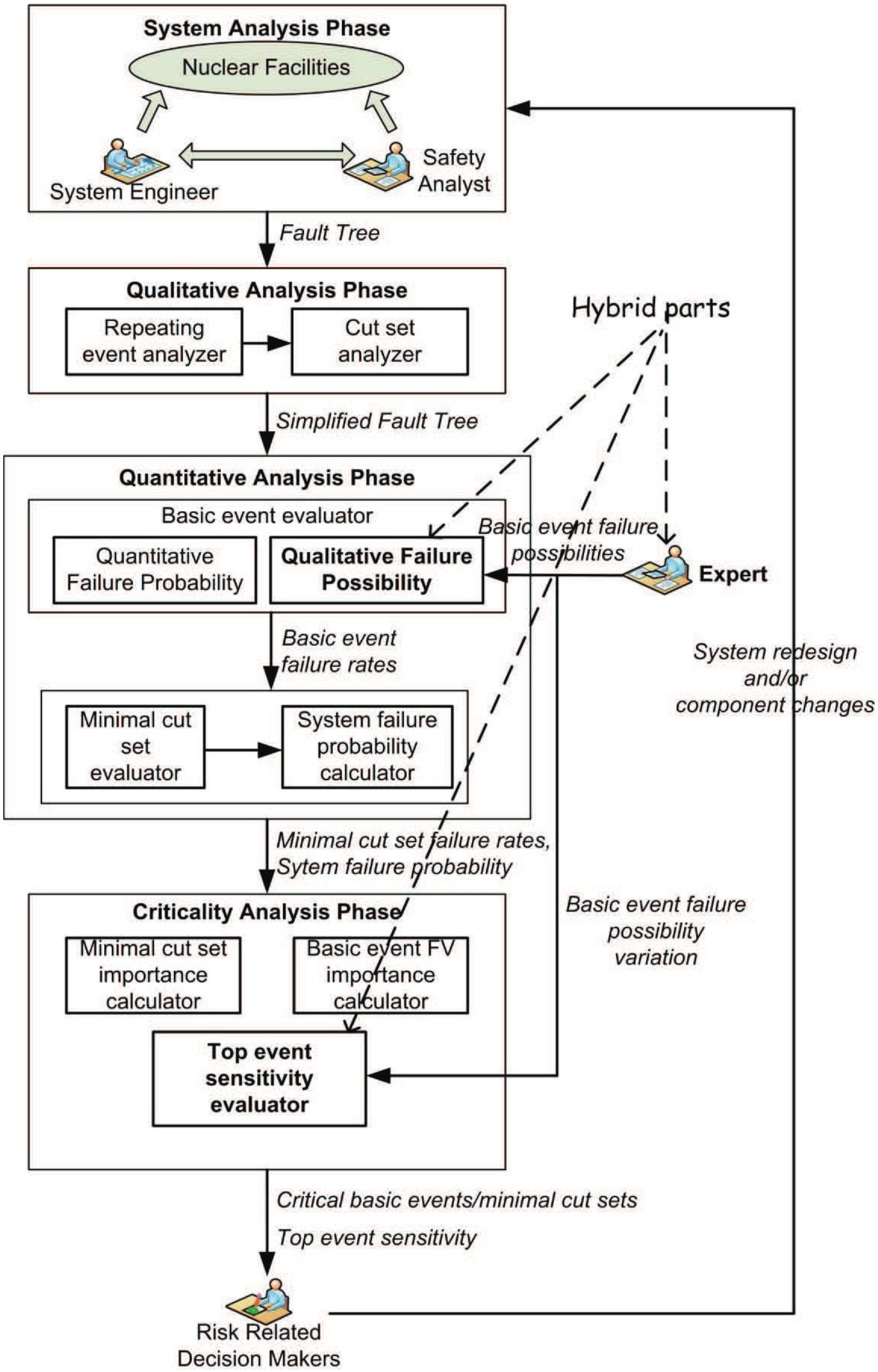

System Analysis Phase
Nuclear Facilities
System Engineer
Safety Analyst
Fault Tree
Qualitative Analysis Phase
Repeating event analyzer
Cut set analyzer
Hybrid parts
Simplified Fault Tree
Quantitative Analysis Phase
Basic event evaluator
Quantitative Failure Probability
Qualitative Failure Possibility
Basic event failure possibilities
Expert
Basic event failure rates
Minimal cut set evaluator
System failure probability calculator
System redesign and/or component changes
Minimal cut set failure rates, Sytem failure probability
Basic event failure possibility variation
Criticality Analysis Phase
Minimal cut set importance calculator
Basic event FV importance calculator
Top event sensitivity evaluator
Critical basic events/minimal cut sets
Top event sensitivity
Risk Related Decision Makers

**Figure 3.1 Intelligent hybrid fault tree analysis framework.**

In the following sub-sections, each phase in Figure 3.1 will be discussed in detail to show the quantification process of the framework.

### 3.2.1 System Analysis Phase

In this phase, safety analysts choose a safety system to be evaluated. With the help of system engineers, the performance of this system is investigated to discover possible scenarios leading to the failure of this system that may occur during its lifetime. This phase generates a fault tree of the system failure. Event symbols, Boolean gate symbols and transfer event symbols as described in Chapter 2 are used to graphically represent system fault trees.

In drawing a fault tree, the process starts with the higher faults and leads to the more basic faults. Hence, a complete fault tree is actually a combination of two or more sub-trees. A sub-tree consists of one top event, two or more bottom events and a Boolean gate to denote a relationship between inputs, which are the bottom events, and an output, which is the top event of the sub-tree. By seeing this relationship, we will be able to understand whether only one bottom event or all bottom events need to fail to cause the top event to fail.

### 3.2.2 Qualitative Analysis Phase

Since a defence-in-depth principle is the concept for designing nuclear power plant safety system, we need to evaluate any possible combination of basic events to that will cause the top event to fail. Hence in this phase, minimal cut sets of the fault tree developed in the analysis phase are evaluated by eliminating repeating events and non minimal cut sets from the fault tree. Boolean algebra properties as described in Chapter 2 are used to eliminate all repeating events and non-minimal cut sets.

This phase has two analyzers, i.e. a “repeating event analyzer” to find and eliminate repeating basic events and a “cut set analyzer” to find and eliminate non-minimal cut sets from the fault tree, which have been developed in the previous system analysis phase. The outputs of the "repeating event analyzer" are used by the "cut set analyzer" to develop minimal cut sets of the system fault tree. This phase, then, generates a simplified fault tree, which is equivalent to the previous fault tree but is free from repeating events and non-minimal cut sets.

### 3.2.3 Quantitative Analysis Phase

In this phase, all basic events and minimal cut sets of the simplified fault tree generated in the qualitative analysis phase are evaluated and their individual failure probability is calculated. The function of the "basic event evaluator" in Figure 3.1 is to enable safety analysts to assess two types of basic event failure, i.e. quantitative failure probability and qualitative failure possibility.

The quantitative failure probability is provided for basic events which have historical failure data for calculating their quantitative failure probability. Meanwhile, the qualitative failure possibility is provided for other basic events, which do not have quantitative historical data but only expert subjective evaluations, expressed in natural linguistic terms (qualitative words) and which, in the context of failure possibilities, are the only method of obtaining failure information. The details of how to convert qualitative failure possibilities into quantitative failure probabilities is described in Section 3.3.

Based on the probability calculation formulas for Boolean gates given in Chapter 2, the failure probability of a minimal cut set is calculated by the "minimal cut set evaluator" using Eq. (3.1). Meanwhile, Eq. (3.2) is used by the "system failure probability calculator" to calculate the failure probability of the top event.

$$P_{mcs_i} = \prod_{j=1}^{n} P_{b_j} \tag{3.1}$$

$$P_T = 1 - \prod_{i=1}^{m} \{1 - P_{mcs_i}\} \tag{3.2}$$

where $P_{mcs_i}$ is the failure probability of the $i^{th}$ minimal cut set, $P_{b_j}$ is the failure probability of the $j^{th}$ basic event, $n$ is the number of basic events in the $i^{th}$ minimal cut set, $P_T$ is the overall probability of the top event, and *m* is the number of minimal cut sets in the system fault tree.

### 3.2.4 CRITICALITY ANALYSIS PHASE

In this phase, the “minimal cut set importance calculator” and the “basic event FV importance calculator” calculate the contribution of every minimal cut set and basic event to the failure occurrence of the safety system and then generate their criticality rank based on their contribution weights. The basic event or minimal cut set with the most contributors is the most critical to the system. The basic event or minimal cut set with the least contributor is the least critical in the system. Meanwhile, the “top event sensitivity evaluator” evaluates how sensitive the system is to the variations of the basic event failure possibilities given by experts.

The Fussell-Vesely (FV) importance is used to order the contribution of a basic event to the top event probability as in Eq. (3.3).

$$FV_b = \frac{\sum_{i=1}^{n} P_{mcs_i(b)}}{P_T} \tag{3.3}$$

where *b* is the basic event to be evaluated, $P_T$ is the overall probability of the top event as in Eq. (3.2), $P_{mcs_i(b)}$ is the probability of the $i^{th}$ minimal cut set containing the basic event *b* as in Eq. (3.1) and *n* is the number of minimal cut sets containing the basic event *b*.

Meanwhile, the contribution of a minimal cut set to the failure occurrence of the top event is calculated using minimal cut set (*mcs*) importance as in Eq. (3.4).

$$\%mcs_i = \frac{P_{mcs_i}}{P_T} \times 100\% \tag{3.4}$$

where $\%mcs_i$ is the contribution percentage of the $i^{th}$ minimal cut set, $P_{mcs_i}$ is the failure probability of the $i^{th}$ minimal cut set as in Eq. (3.1), and $P_T$ is the overall probability of the top event, as in Eq. (3.2).

An illustrative case study to mathematically validate the performance of the intelligent hybrid fault tree analysis framework in Figure 3.1 is given in Section 3.5.

## 3.3 A FAILURE POSSIBILITY-BASED APPROACH

A failure possibility-based approach is introduced into the quantitative phase of the conventional fault tree analysis to estimate failure rates of basic events, which do not have historical failure data to calculate their quantitative failure probabilities. Hence, in this case, expert subjective assessments are the only alternative method for obtaining their failures. This approach utilizes qualitative linguistic values in the context of failure possibilities to evaluate basic event failure, membership functions of fuzzy numbers to mathematically represent those qualitative linguistic values, a defuzzification technique to defuzzify a membership function to a crisp score, and a logarithmic function to generate a fuzzy failure rate from a crisp score. The failure possibility-based approach is described as follows.

### 3.3.1 FAILURE POSSIBILITY DEVELOPMENT

A failure possibility distribution (*fpd*) is a range of qualitative linguistic values used to represent basic event failure possibilities. This distribution scales-up basic event failures from the lowest possibility to the highest possibility, for example from '*very low failure possibility*' to '*very high failure possibility*', which can be expressed as follows.

$$fpd = \{\textit{very low, low, medium, high, very high}\} \tag{3.5}$$

Basic event failure possibilities can be graded on the basis of the type of components or the likely failure occurrences. Based on the component types, for example, *very low failure possibility* can be used to represent components, which are rigid and very unlikely to fail even once. Meanwhile, *very high failure possibility* can be used to represent components which have many moving parts and are near certain to fail several times. Based on the likely failure occurrences, for example, *very low failure possibility* could be used to represent components whose failure rates are less than $10^{-8}$. Meanwhile, *very high failure possibility* could be used to represent components whose failure rates are greater than $10^{-3}$. This grading will, of course, be different on different applications. For instance, $10^{-3}$ could be defined as *high failure possibility* for nuclear accidents but as *low failure possibility* for motor cycle accidents. Therefore, safety analysts have to define this failure possibility grading based on the system problems on hand.

The output of this development is a failure possibility distribution to be used by experts to subjectively and qualitatively evaluate basic event failures.

### 3.3.2 MEMBERSHIP FUNCTION DEVELOPMENT

The membership functions of the fuzzy numbers to mathematically represent those qualitative linguistic values in the basic event failure possibility distribution in Eq. (3.5) may be developed in the [0, 1] universe of discourse. This means that the closer the fuzzy probabilities are to 0, the less likely the basic events are to fail. On the other hand, the closer the fuzzy probabilities are to 1, the more likely the basic events are to fail. Meanwhile, the horizontal axis represents the fuzzy failure rates of basic events, which is also defined between 0 and 1. This means that the closer the fuzzy numbers are to the point of origin, the lower the basic event fuzzy failure rates are. On the other hand, the farther the fuzzy numbers are from the point of origin, the higher the basic event fuzzy failure rates are. The membership function of the trapezoidal fuzzy numbers and/or triangular fuzzy numbers may be used to mathematically represent nuclear event failure possibilities. However, it is also important to note that membership function used in this approach can take a different form for different engineering systems. Furthermore, intuition, inference, rank ordering, neural networks, genetic algorithms, and/or inductive reasoning as described in Chapter 2 can be used to assign membership values of the chosen membership functions.

The outputs of this development are the membership functions of the fuzzy numbers to mathematically represent each qualitative value in the failure possibility distribution in Eq. (3.5).

### 3.3.3 BASIC EVENT EVALUATION

The expert-opinion elicitation process is a formal process of obtaining information or answers to specific questions about basic event failure possibilities. The purpose of this evaluation is to collect the failure possibility of an event from a group of experts. The number of scientific publications, recommendations from a wide range of experts, and experiences with previous similar studies as described in Chapter 2 can be used as indicators to select experts for this elicitation process. An expert is a very skilful person, who is familiar with the system, understands the system's working environment, and has considerable training in and knowledge of the nuclear field. For example, we can ask every expert in the group to justify the failure likelihood of the event *A* using the predefined failure possibility in Eq. (3.5) as follows.

*How likely is the basic event A to fail? Is it very low, low, medium, high, or very high?*

Since each expert involved in the evaluation process may have different expertise, working experience and justification confidence level, they may evaluate the same events with different failure possibilities. Hence, fuzzy aggregation methods are used to aggregate different evaluator opinions to reach a consensus. The arithmetic averaging operation described in Chapter 2 can be used to aggregate *n* membership functions of fuzzy numbers of the same type. Meanwhile, if the membership functions used to represent failure possibilities are of different types, then the mean operator described in Chapter 2 can be used for aggregation.

The output of this evaluation is the final membership function representing the failure possibility of every individual basic event in the fault tree of the system under investigation.

### 3.3.4 FAILURE POSSIBILITY SCORE GENERATION

A failure possibility score (*FPS*) is a crisp score which is defuzzified from a membership function to represent the expert belief of the most likely score indicating that an event may occur. A defuzzification technique as described in Chapter 2 may be used to generate a failure possibility score from a membership function of fuzzy number. However, safety analysts have to choose the most suitable technique for a specific application.

The output of this generator is a fuzzy possibility score for every individual basic event in the fault tree of the system under investigation.

### 3.3.5 Fuzzy Failure Rate Generation

A fuzzy failure rate (*FFR*) is an error rate which is obtained by dividing the frequency of an error with the total chance that an event may have error. Based on Onisawa's logarithmic function described in Chapter 2, an *FFR* for a basic event is generated as follows.

$$FFR = \begin{cases} \frac{1}{10^m}, & FPS \neq 0 \\ 0, & FPS = 0 \end{cases} \tag{3.6}$$

where $m = \left[\frac{1-FPS}{FPS}\right]^{1/3} \times 2.301$.

The outputs of this generator are fuzzy failure rates for basic events in the fault tree of the system under investigation.

## 3.4 An Illustrative Case Study

This section demonstrates the applicability and effectiveness of the intelligent hybrid fault tree analysis framework to assess nuclear power plant safety using a case-based illustration. First, it describes the safety system used for the validation and then illustrates the quantification process of the intelligent hybrid fault tree analysis framework.

### 3.4.1 SAFETY SYSTEM DESCRIPTION

The main objectives of the safety systems of nuclear power plants are to safely shutdown reactors, to maintain reactors in safe shutdown conditions, and to prevent radioactive material releases during normal operations and accidents. A high pressure core spray system (HPCSS) is an integral part of an emergency core cooling system (ECCS) in boiling water reactors (BWRs). The function of this HPCSS is to depressurize and supply water to the primary system in the event of loss of reactor coolant inventory. If this safety system works well, fuel cladding damage can be avoided. A simplified model of HPCSS by Paredes et al. (2009) in Figure 3.2 is used to illustrate the feasibility and effectiveness of the intelligent hybrid fault tree analysis framework to overcome the limitation of the conventional fault tree analysis for nuclear safety assessment.

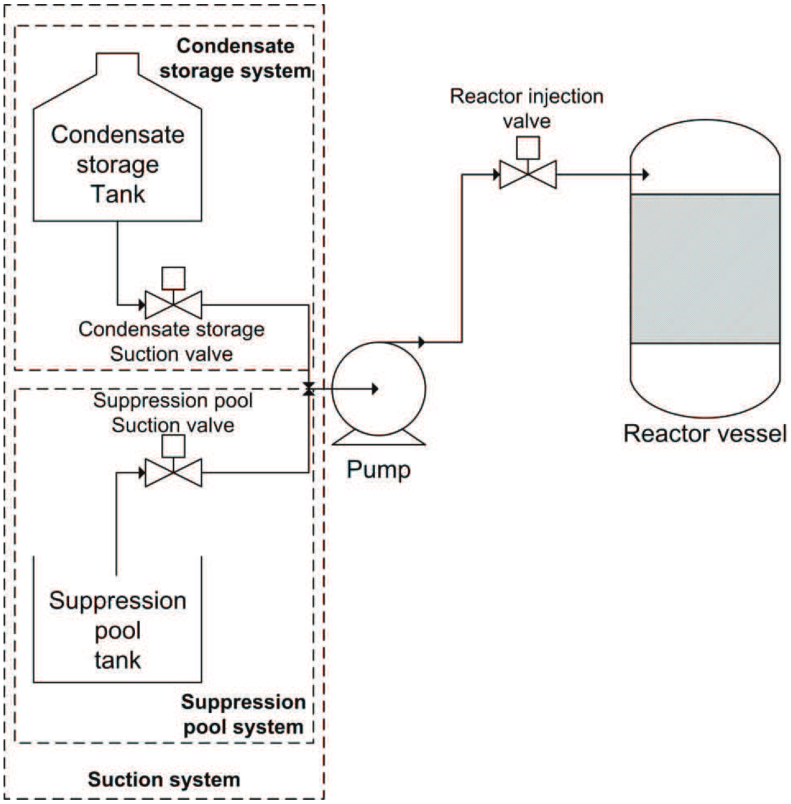


**Figure 3.2 Simplified HPCSS diagram.**

### 3.4.2 Quantification Process Of The Intelligent Hybrid Fault Tree Analysis Framework

This section mathematically illustrates the quantification process of the intelligent hybrid fault tree analysis framework to assess the failure probability of the simplified HPCSS diagram in Figure 3.2.

#### (1) System Analysis Phase

The HPCSS fails if there is no water flowing into the reactor vessel in the event of a loss of coolant accident (LOCA). By investigating the system in Figure 3.2, it can be seen that there are three possibilities causing the HPCSS to fail. The first possible cause is that the reactor injection valve fails to open. If we assume that this valve works well, then the second possible cause is that the pump cannot pump water from the suction system into the reactor injection valve. If we also assume that the pump works well, the third possible cause is that the suction system cannot supply water to the pump. These three possible causes are represented by an "OR" gate in the fault tree in Figure 3.3.

The failure of the suction system to supply water from the tank to the pump can be further investigated. The suction system fails if both the condensate storage system and the suppression pool system fail at the same time. This scenario is then represented by an "AND" gate in the fault tree in Figure 3.3.

The failure of the condensate storage system and the suppression pool system to supply water to the pump can still be further investigated. The condensate storage system fails if the condensate storage suction valve fails to open or the condensate storage tank level is low. This failure scenario is then represented by an "OR" gate in the fault tree in Figure 3.3. The same failure scenario occurs to the suppression pool system as well. The complete fault tree to graphically represent the failure scenario of the simplified HPCSS in Figure 3.2 is shown in Figure 3.3, and Table 3.1 lists the meanings of the symbols used in the fault tree.

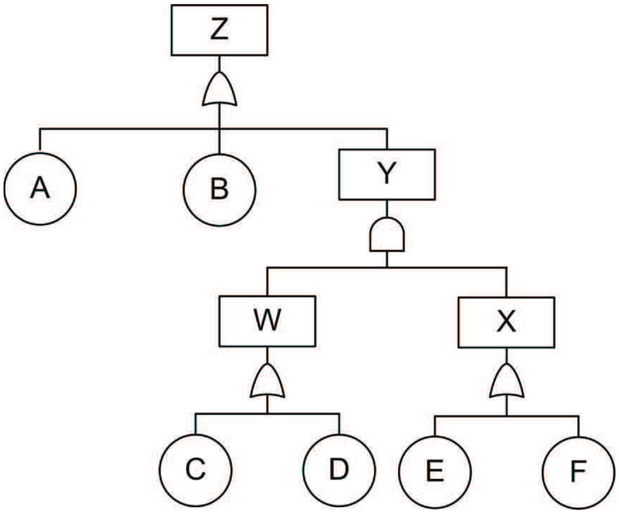


**Figure 3.3 Simplified HPCSS fault tree.**

**Table 3.1 Meanings of the symbols in the fault tree Figure 3.3.**

| Events | Legends |
|---|---|
| *A* | The pump has failed |
| *B* | The reactor injection valve has failed |
| *C* | The condensate storage water level is low |
| *D* | The condensate storage suction valve has failed |
| *E* | The suppression pool water level is low |
| *F* | The suppression pool suction valve has failed |
| *W* | The condensate storage system has failed |
| *X* | The suppression pool system has failed |
| *Y* | The water suction system has failed |
| *Z* | The HPCSS has failed |

### (2) QUALITATIVE ANALYSIS PHASE

In the simplified HPCSS fault tree in Figure 3.3, it can be seen that there are six basic events, i.e. *A*, *B*, *C*, *D*, *E*, and *F*, and three intermediate events, i.e. *W*, *X* and *Y*. We can also see that the fault tree has been free of repeating events.

Each sub-system in Figure 3.3 can be represented by Boolean algebra as shown in Eqs. (3.7-3.10).

$$Z = A + B + Y \tag{3.7}$$

$$Y = W \, . \, X \tag{3.8}$$

$$W = C + D \tag{3.9}$$

$$X = E + F \tag{3.10}$$

By substitution, the cut sets for the top event of the fault tree in Figure 3.3 are generated as follows.

$$Z = A + B + (C + D) \, . \, (E + F) = A + B + C \, . \, E + C \, . \, F + D \, . \, E + D \, . \, F \tag{3.11}$$

From Eq. (3.11), it can be seen that the fault tree has six cut sets, i.e. *A*, *B*, *CE*, *CF*, *DE*, and *DF*. All six cut sets have been minimal. Hence, the fault tree in Figure 3.3 has two simple-component minimal cut sets, i.e. *A* and *B*, and four double-component minimal cut sets, i.e. *CE*, *CF*, *DE*, and *DF*.

### (3) QUANTITATIVE ANALYSIS PHASE

To show how the intelligent hybrid fault tree analysis can integrate quantitative failure probabilities with qualitative failure possibilities, let us simply assume that the basic event *A* has historical failure data and hence its quantitative failure probability can be calculated. This failure probability is then directly provided to the proposed intelligent hybrid framework as described in (a). Meanwhile, we assume that basic events *B*, *C*, *D*, *E*, and *F* do not have historical failure data and hence, expert subjective evaluations, which are expressed in qualitative failure possibilities, are the only method for collecting their failures as described in (b).

### (a) QUANTITATIVE FAILURE PROBABILITY

For illustration purposes only, let us assume that the basic event *A* has historical failure data, which are recorded in reliable sources such as log or maintenance books. These recorded data are then used to calculate its failure probability. For the sake of simplicity, we assume that the failure probability of the basic event *A* is 1.53E-2. We need to note that this failure probability does not represent the real failure of the pump used by the simplified HPCSS in Figure 3.3, but only illustrates the quantification process of the proposed intelligent hybrid fault tree analysis framework.

### (b) QUALITATIVE FAILURE POSSIBILITY

The failure possibility-based approach described in Section 3.4 is used to generate the fuzzy failure rates of basic events *B*, *C*, *D*, *E*, and *F* from their failure possibilities evaluated by experts.

#### *Step 1: Define basic event failure possibility distribution*

The failure possibility distribution (*fpd*) to evaluate basic events *B*, *C*, *D*, *E*, and *F* in this case study is defined on the basis of the type of components, for example, by five qualitative linguistic values, i.e., "*very low*", "*low*", "*medium*", "*high*", and "*very high*" failure possibilities.

$$fpd = \{very\ low, low, medium, high, very\ high\} \tag{3.12}$$

The failure possibility distribution in Eq. (3.12) is not for the real failure possibilities to qualitatively express nuclear event failures but for mathematical illustration purposes only. The real qualitative nuclear event failure possibilities are developed and described in Chapter 4.

#### *Step 2: Mathematically represent failure possibilities*

Those failure possibilities defined in Eq. (3.12) are mathematically represented by, for example, the membership function of the trapezoidal fuzzy numbers and triangular fuzzy numbers, as shown in Table 3.2.

**Table 3.2 Failure possibilities and their corresponding membership functions.**

| Failure possibilities | Membership functions |
|---|---|
| *Very low* | $\mu_{VL}(x) = (0.0,0.1,0.2)$ |
| *Low* | $\mu_{L}(x) = (0.1,0.25,0.4)$ |
| *Medium* | $\mu_{M}(x) = (0.34,0.4,0.58,0.64)$ |
| *High* | $\mu_{H}(x) = (0.58,0.72,0.86)$ |
| *Very High* | $\mu_{VH}(x) = (0.8,0.9,1.0)$ |

The membership values in Table 3.2 are not for the real application but for mathematical illustration purposes only. The real membership functions of the fuzzy numbers to mathematically represent the real nuclear event failure possibilities are developed and described in Chapter 4.

### *Step 3: Evaluate basic event failure possibilities*

In this illustrative example, three different experts are assumed to be asked to subjectively evaluate the failure possibilities of basic events *B*, *C*, *D*, *E*, and *F* in Figure 3.3 using those failure possibilities in Eq. (3.12). Their subjective justification results are given in Table 3.3.

**Table 3.3 Questionnaires and expert subjective evaluation results.**

| Basic Event | Questions | Expert 1 | Expert 2 | Expert 3 |
|---|---|---|---|---|
| *B* | How likely is the reactor injection valve to fail? | *Low* | *Low* | *Medium* |
| *C* | How likely is the water level of the condensate storage to be low? | *Very Low* | *Very Low* | *Low* |
| *D* | How likely is the suction valve of the condensate storage to fail? | *Low* | *Very Low* | *Low* |
| *E* | How likely is the water level of the suppression pool to be low? | *Very Low* | *Very Low* | *Low* |
| *F* | How likely is the suction valve of the suppression pool to fail? | *Low* | *Very Low* | *Low* |

The justification results in Table 3.3 are illustrative character of experts to show how the failure possibility-based approach can be used to assess basic event failure rates without the need for historical failure data.

Since the failure possibilities of the basic event $B$ ($\mu_B(x)$) evaluated by experts are mathematically represented by different types of membership function, the final membership function is calculated using the mean operator in Eqs. (2.17-2.18), as shown below.

$$Z_\alpha^L = \frac{[(0.4-0.34)+(0.25-0.1)]\alpha+(0.34+0.1)}{2} = 0.105\alpha + 0.22,$$

$$Z_\alpha^R = \frac{(0.64+0.4)-[(0.64-0.58)+(0.4-0.25)]\alpha}{2} = 0.52 - 0.105\alpha.$$

By mapping both $Z_\alpha^L$ and $Z_\alpha^R$ back into a fuzzy membership function, the final membership function for the basic event *B* is $\mu_B(x) = (0.22{,}0.33{,}0.42{,}0.52)$.

Since the failure possibilities of the basic event *C* ($\mu_C(x)$) evaluated by experts are mathematically represented by the same types of membership function, the final membership function is calculated using the arithmetic averaging in Eq. (2.12), as shown below.

$$\mu_C(x) = \frac{1}{3}[(0.0{,}0.1{,}0.2) \oplus (0.0{,}0.1{,}0.2) \oplus (0.1{,}0.25{,}0.4)] = (0.03{,}0.15{,}0.27)$$

The same procedures as those used to calculate the final membership function of basic event *C* ($\mu_C(x)$) are also applied to the basic events *D*, *E* and *F* in Table 3.4.

**Table 3.4 Basic event final membership functions.**

| Basic events | Final membership functions |
|---|---|
| *B* | $\mu_B(x) = (0.22, 0.33, 0.42, 0.52)$ |
| *C* | $\mu_C(x) = (0.03, 0.15, 0.27)$ |
| *D* | $\mu_D(x) = (0.07, 0.20, 0.33)$ |
| *E* | $\mu_E(x) = (0.03, 0.15, 0.27)$ |
| *F* | $\mu_F(x) = (0.07, 0.20, 0.33)$ |

### *Step 4: Defuzzify membership functions into basic event failure possibility scores*

The failure possibility scores (*FPS*) for all basic events in Table 3.1 are defuzzified from their corresponding final membership functions in Table 3.4 using, for example, the centroid-based Euclidean distance in Eq. (2.28). The results of this calculation are given in Table 3.5.

### *Step 5: Generate basic event fuzzy failure rates*

The fuzzy failure rates (*FFR*) for all basic events in Table 3.1 are generated from their corresponding failure possibility scores in Table 3.5 using Eq. (3.6). The results of this calculation are also given in Table 3.5.

**Table 3.5 Pairs of basic event *FPSs* and *FFRs*.**

| Basic Event | *FPS* | *FFR* |
|---|---|---|
| *B* | 0.552458 | 7.16E-3 |
| *C* | 0.365529 | 1.72E-3 |
| *D* | 0.388730 | 2.11E-3 |
| *E* | 0.365529 | 1.72E-3 |
| *F* | 0.388730 | 2.11E-3 |

The failure probabilities for those minimal cut sets evaluated in Eq. (3.11) are calculated using Eq. (3.1) and the results are shown Table 3.6.

**Table 3.6 Minimal cut set failure probabilities.**

| Minimal cut sets | Failure probabilities |
|---|---|
| *A* | 1.53E-2 |
| *B* | 7.16E-3 |
| *CE* | 2.95E-6 |
| *CF* | 3.62E-6 |
| *DE* | 3.62E-6 |
| *DF* | 4.45E-6 |

Meanwhile, the failure probability of the top event, which is the failure of the simplified HPCSS to depressurize and supply water to the primary system in case of loss of reactor coolant inventory shown in Figure 3.2, is 2.24E-2, which is calculated using Eq. (3.2).

(4) Criticality Analysis Phase

Using Eq. (3.3), the *FV* importance of basic event *C,* for example, is calculated as follows.

$$FV_C = \frac{2.95\text{E-}6+3.62\text{E-}6}{2.24\text{E-}2} = 2.94\text{E-}4$$

The FV importance for other basic events in Table 3.7 is calculated using the same procedures.

**Table 3.7 Basic event $FV$ importances.**

| Basic events | $FV$ importance | Critical order |
|---|---|---|
| $A$ | 6.84E-1 | 1 |
| $B$ | 3.20E-1 | 2 |
| $C$ | 2.94E-4 | 4 |
| $D$ | 3.61E-4 | 3 |
| $E$ | 2.94E-4 | 4 |
| $F$ | 3.61E-4 | 3 |

Using Eq. (3.4), the *MCS* importance for the minimal cut set *DF,* for example, is calculated as follows.

$$\%MCS_{DF} = \frac{4.45\text{E-}6}{2.24\text{E-}2} \times 100\% = 0.02\%$$

The *MCS* importance for other minimal cut sets in Table 3.8 is calculated using the same procedures.

**Table 3.8 Minimal cut set importances.**

| Basic events | *%MCS* | Critical order |
|---|---|---|
| *A* | 68.40% | 1 |
| *B* | 32.02% | 2 |
| *CE* | 0.01% | 4 |
| *CF* | 0.02% | 3 |
| *DE* | 0.02% | 3 |
| *DF* | 0.02% | 3 |

### 3.4.3 Result Analysis

From Table 3.5, it can be seen that those fuzzy failure rates generated by the proposed failure possibility-based approach have similar representations to the quantitative failure probabilities calculated from the historical failure data. These results confirm that the failure possibility-based approach is a sound alternative approach to evaluate basic events which do not have historical failure data for calculating their quantitative failure probabilities, and for which expert subjective evaluations are the only means to obtain basic event failures. Moreover, the failure possibility-based approach is more intuitive and easy for experts to use to evaluate basic events where quantitative historical failure data are insufficient or unavailable for numerical estimation.

The results of the quantitative analysis phase shown in Table 3.6 and the results of the criticality analysis shown in Table 3.7 and Table 3.8 confirm that the intelligent hybrid fault tree analysis framework, which integrates the quantitative failure probabilities and qualitative failure possibilities into the quantitative analysis phase to evaluate basic events, is applicable for analyzing nuclear power plant safety systems.

We also note that the fuzzy failure rates generated from qualitative failure possibilities by the failure possibility-based approach, and the quantitative failure probability, which is directly given to the framework, are not real values. Moreover, the nuclear event failure possibilities and their mathematical representation in this chapter are used only to illustrate the working and quantification process of the proposed intelligent hybrid fault tree analysis framework. Therefore, the failure probability calculated for the undesired top event in Figure 3.3 does not represent the real HPCSS.

## 3.5 SUMMARY

This chapter describes an intelligent hybrid fault tree analysis framework to overcome the limitation of conventional fault tree analysis for nuclear power plant probabilistic safety assessment. The intelligent hybrid framework introduces a failure possibility-based approach into the quantitative analysis phase of the conventional fault tree analysis to evaluate basic events which do not have quantitative historical failure data, and for which subjective assessment is the only alternative for obtaining basic event failures. In the failure possibility-based approach, experts are asked to subjectively evaluate basic event failures using qualitative linguistic values to describe basic event failure possibilities. The failure possibilities are intuitive and make it easy for experts to evaluate basic events when there are no historical data for numerical estimation. The membership functions of trapezoidal and triangular fuzzy numbers are then used to mathematically represent those failure possibilities. To avoid bias in the basic event evaluation, a group of experts subjectively assesses basic event failure possibilities and a fuzzy number aggregation technique is used to generate a final membership function. A defuzzification technique is then used to defuzzify membership functions into component failure possibility scores and a logarithmic function is used to generate basic event fuzzy failure rates which are suitable for the intelligent hybrid framework. The mathematical illustration shows that the proposed intelligent hybrid fault tree analysis framework can be applied for nuclear power plant probabilistic safety assessment.

An area defuzzification technique, nuclear event failure possibilities and their mathematical representation to be implemented in the proposed intelligent hybrid fault tree analysis framework are described in detail in Chapter 4. Meanwhile, a fuzzy reliability approach to generate nuclear event quantitative failure rates from the corresponding qualitative failure possibilities to be also implemented in this proposed intelligent hybrid framework is described in detail in Chapter 5. Furthermore, an Intelligent Fault Tree Analysis System for Nuclear Safety Assessment (InFaTAS-NuSA) to realize the proposed intelligent hybrid fault tree analysis framework for nuclear power plant safety assessment is described in detail in Chapter 6.

Chapter 4

# AN AREA DEFUZZIFICATION TECHNIQUE TO GENERATE NUCLEAR EVENT FUZZY FAILURE RATES

## 4.1 INTRODUCTION

The intelligent hybrid fault tree analysis framework described in Chapter 3 integrates the failure possibility-based approach into the quantitative analysis phase of the conventional fault tree analysis to overcome the limitation of the conventional fault tree analysis. The objective of this failure possibility-based approach is to deal with nuclear events, which do not have historical failure data for calculating their quantitative failure probabilities. In this intelligent hybrid framework, a defuzzification technique is essential to defuzzify (decode) the membership function of the fuzzy numbers into a failure possibility score that represents whether a nuclear event might occur.

Since different defuzzification techniques will result in different scores, it is very important to use an appropriate defuzzification technique for a specific application. This chapter presents an area defuzzification technique to realize this requirement and introduces five essential fuzzy rules which need to be satisfied by any defuzzification technique in nuclear application. The remainder of this chapter is structured as follows. Section 4.2 briefly describes the definitions of nuclear event failure possibility scores and nuclear event fuzzy failure rates. Five essential fuzzy rules to be met by any defuzzification technique in nuclear application are presented in Section 4.3. Section 4.4 describes the area defuzzification technique in detail. Nuclear event failure possibilities and their corresponding mathematical representation are developed and described in Section 4.5. Two types of validation of the area defuzzification technique are also given in Section 4.5. The purpose of these two types of validation is to mathematically confirm the applicability and effectiveness of the area defuzzification technique to assess nuclear event failures from qualitative failure possibilities. Finally, this chapter is summarized in Section 4.6. The work presented in this chapter has been reported in three of our publications listed in Section 1.7, i.e. publication numbers 2, 4, and 9.

## 4.2 Definitions Of Nuclear Event Reliability Score And Fuzzy Failure Rate

This section gives two important definitions used to generate quantitative nuclear event reliability data from their corresponding qualitative failure possibilities which are mathematically represented by membership functions of fuzzy numbers.

**Definition 4.1 (Nuclear Event Reliability Score).** A nuclear event reliability score (*Rs*) is a crisp score representing the value that experts believe most likely indicate that a nuclear event might occur. This score is generated from a membership function of fuzzy number ($\mu_{\tilde{A}}(x)$) using a defuzzification technique as formulated in Eq. (4.1).

$$R_s = d\big(\mu_{\tilde{A}}(x)\big) \tag{4.1}$$

**Definition 4.2 (Nuclear Event Fuzzy Failure Rate).** A nuclear event fuzzy failure rate (*R*) is nuclear event reliability data generated from the corresponding reliability score using Onisawa’s logarithmic function described in Chapter 2, as shown in Eq. (4.2).

$$R = \begin{cases} \frac{1}{10^m}, & R_s \neq 0 \\ 0, & R_s = 0 \end{cases} \tag{4.2}$$

where $m = \left[\frac{1-R_S}{R_S}\right]^{1/3} \times 2.301$ and $R_s$ is the corresponding nuclear event reliability score defuzzified from the nuclear event membership function of fuzzy numbers as in Eq. (4.1).

## 4.3 Essential Fuzzy Rules

A nuclear event failure possibility distribution is designed within interval [0,1] in the Cartesian plane. This means that the lowest failure possibility is set closer to zero (0) and the highest failure possibility is set closer to one (1). Intuitively, nuclear event fuzzy failure rates generated from the corresponding failure possibilities have to increase when the membership functions of the fuzzy numbers are shifted from the left to the right in the Cartesian plane. The closer the membership function is to the point of origin, the smaller the fuzzy failure rate is. On the other hand, the further the membership function is from the point of origin, the higher the fuzzy failure rate is. Consequently, there will be no two different membership functions in the Cartesian plane that result in the same fuzzy failure rates. Based on this shifting analysis, we define four fuzzy rules to be satisfied by the chosen defuzzification technique, i.e. membership function shifting rule, left membership function shifting rule, core membership function shifting rule, and right membership function shifting rule.

It is very important to note that the generated nuclear event fuzzy failure rates should be closely similar to the real data collected from operating experiences and/or experiments. This implies that the chosen defuzzification technique should be able to generate fuzzy failure rates within the real nuclear event reliability data range. In general, nuclear event reliability data, which are directly collected from nuclear power plant operating experiences, are mostly less than $10^{-2}$ and could be of order $10^{-5}$ to $10^{-11}$ (IAEA 1997; Papazoglou et al. 1984; Wierman et al. 2001a, 2001b). Based on this reliability data range analysis, we define one fuzzy rule to be satisfied by the chosen defuzzification technique, i.e. the reliability data range rule.

The chosen defuzzification technique to decode the membership functions of the fuzzy numbers representing nuclear event failure possibilities into their corresponding fuzzy failure rates has to satisfy those five essential fuzzy rules mentioned above.

Let $\tilde{A}$ be a normal trapezoidal fuzzy number representing a nuclear event failure possibility. Let $a$ be the left support, $b$ be the left core, $c$ be the right core, and $d$ be the right support of the fuzzy number $\tilde{A}$. Let $\Delta x$ be the translation range of the fuzzy number $\tilde{A}$ in the horizontal axis. Let $R(\tilde{A})$ be the nuclear event reliability data generated from the corresponding fuzzy number $\tilde{A}$. The chosen defuzzification technique for assessing nuclear event reliability data from the corresponding failure possibilities than has to satisfy the five fuzzy rules below.

### 4.3.1 MEMBERSHIP FUNCTION SHIFTING RULE

If the trapezoidal fuzzy number $\tilde{A}(a,b,c,d)$ is horizontally shifted to the right, i.e. $\tilde{A}_1(a_1,b_1,c_1,d_1)$, in the Cartesian plane in which $a_1 = a+\Delta x$, $b_1 = b+\Delta x$, $c_1 = c+\Delta x$, and $d_1 = d+\Delta x$, then the nuclear event reliability data generated from $\tilde{A}_1$, i.e. $R(\tilde{A}_1)$ has to be greater than the reliability data generated from $\tilde{A}$, i.e. $R(\tilde{A})$.

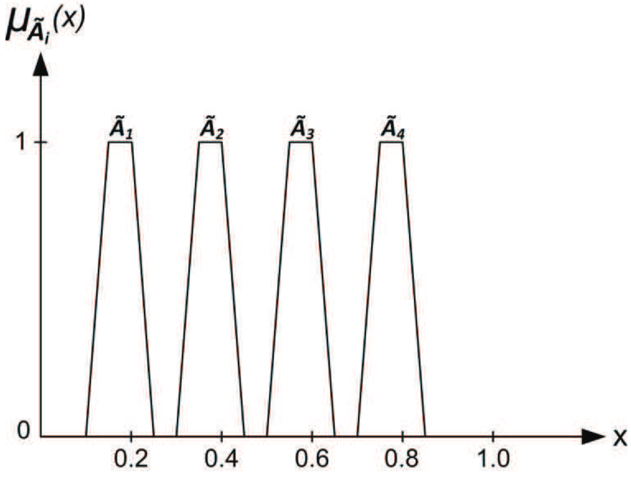


**Figure 4.1 Membership function shifting.**

Using Figure 4.1 as an example, the reliability data generated from $\tilde{A}_4$(0.70,0.75,0.80,0.85) must be greater than the reliability data generated from

$\tilde{A}_3$(0.50,0.55,0.60,0.65). The reliability data generated from $\tilde{A}_3$ must be greater than the reliability data generated from $\tilde{A}_2$(0.30,0.35,0.40,0.45). The reliability data generated from $\tilde{A}_2$ must be greater than the reliability data generated from $\tilde{A}_1$(0.10,0.15,0.2,0.25).

### 4.3.2 LEFT MEMBERSHIP FUNCTION SHIFTING RULE

If the left membership function of the trapezoidal fuzzy number $\tilde{A}(a,b,c,d)$ is horizontally shifted to the right, i.e. $\tilde{A}_1(a_1,b_1,c,d)$, in the Cartesian plane in which $a_1 = a+\Delta x$ and $b_1 = b+\Delta x$, the reliability data generated from $\tilde{A}_1$, i.e. $R(\tilde{A}_1)$ has to be greater than the reliability data generated from $\tilde{A}$, i.e. $R(\tilde{A})$.

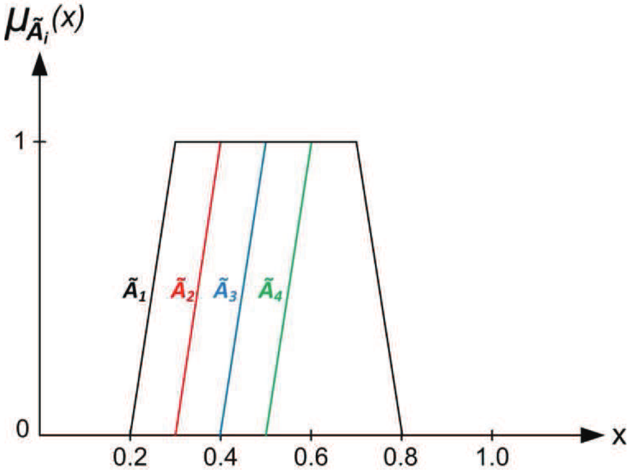


**Figure 4.2 Left membership function shifting.**

Using Figure 4.2 as an example, the reliability data generated from $\tilde{A}_4$(0.5,0.6,0.7,0.8) must be greater than the reliability data generated from $\tilde{A}_3$(0.4,0.5,0.7,0.8). The reliability data generated from $\tilde{A}_3$ must be greater than the reliability data generated from $\tilde{A}_2$(0.3,0.4,0.7,0.8). The reliability data generated from $\tilde{A}_2$ must be greater than the reliability data generated from $\tilde{A}_1$(0.2,0.3,0.7.0.8).

### 4.3.3 Core Membership Function Shifting Rule

If the core of the trapezoidal fuzzy number $\tilde{A}(a,b,c,d)$ is horizontally shifted to the right, i.e. $\tilde{A}_1(a,b_1,c_1,d)$, in the Cartesian plane in which $b_1 = b+\Delta x$ and $c_1 = c+\Delta x$, the reliability data generated from $\tilde{A}_1$, i.e. $R(\tilde{A}_1)$ has to be greater than the reliability data generated from $\tilde{A}$, i.e. $R(\tilde{A})$.

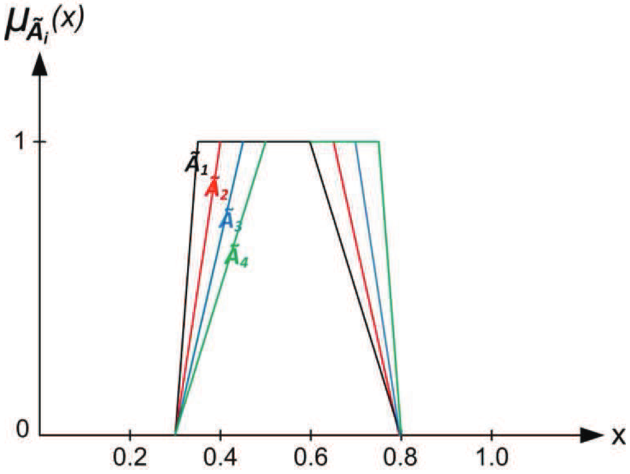


**Figure 4.3 Core membership function shifting.**

Using Figure 4.3 as an example, the reliability data generated from $\tilde{A}_4$(0.3,0.7,0.8,0.9) must be greater than the reliability data generated from $\tilde{A}_3$(0.3,0.6,0.7,0.9). The reliability data generated from $\tilde{A}_3$ must be greater than the reliability data generated from $\tilde{A}_2$(0.3,0.5,0.6,0.9). The reliability data generated from $\tilde{A}_2$ must be greater than the reliability data generated from $\tilde{A}_1$(0.3,0.4,0.5,0.9).

### 4.3.4 Right Membership Function Shifting Rule

If the right membership function of the trapezoidal fuzzy number of $\tilde{A}(a,b,c,d)$ is horizontally shifted to the right, i.e. $\tilde{A}_1(a,b,c_1,d_1)$, in the Cartesian plane in which $c_1 = c+\Delta x$, and $d_1 = d+\Delta x$, the reliability data generated from $\tilde{A}_1$, i.e. $R(\tilde{A}_1)$, has to be greater than the reliability data generated from $\tilde{A}$, i.e. $R(\tilde{A})$.

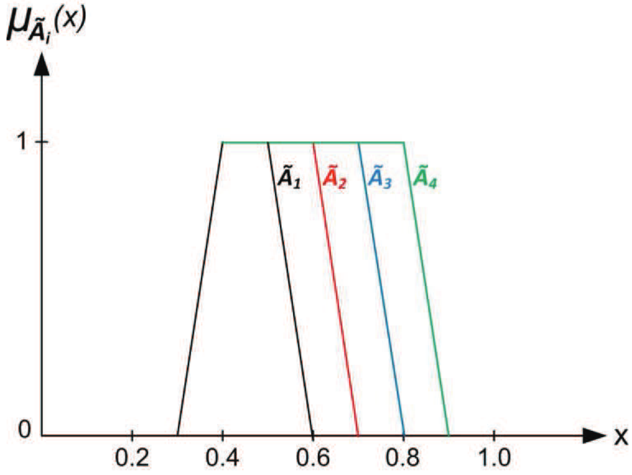


**Figure 4.4 Right membership function shifting.**

Using Figure 4.4 as an example, the reliability data generated from $\tilde{A}_4$(0.3,0.4,0.8,0.9) must be greater than the reliability data generated from $\tilde{A}_3$(0.3,0.4,0.7,0.8). The reliability data generated from $\tilde{A}_3$ must be greater than the reliability data generated from $\tilde{A}_2$(0.3,0.4,0.6,0.7). The reliability data generated from $\tilde{A}_2$ must be greater than the reliability data generated from $\tilde{A}_1$(0.3,0.4,0.5,0.6).

### 4.3.5 Reliability Data Range Rule

If $\tilde{A}$ is a set of fuzzy numbers in the Cartesian plane and $R$ is a set of reliability data generated from each member of the set $\tilde{A}$, then each member in $R$ must be less than 1.0E-2 and greater than 1.0E-12 as defined below.

If $\tilde{A} = \{\tilde{A}_i \,/\, i = 1, 2, \ldots, n\}$ and $R = \{R_i \mid i = 1, 2, \ldots, n\}$ then 1.0E-2 $\leq R_i \leq$ 1.0E-12

where $n$ is the number of fuzzy number in the set.

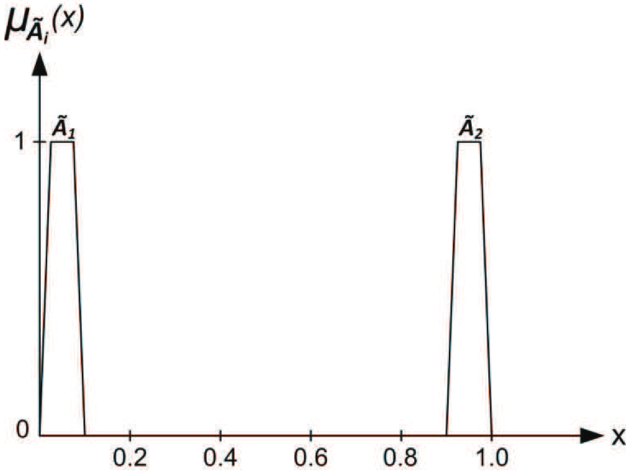


**Figure 4.5 Membership function range.**

Using Figure 4.5 as an example, the reliability data generated from $\tilde{A}_1$(0.00,0.03,0.05,0.08) and $\tilde{A}_2$(0.92,0.97,0.98,1.00) must be between 1.0E-2 and 1.0E-12.

## 4.4 AREA DEFUZZIFICATION TECHNIQUE

Area defuzzification technique (*ADT*) utilizes the centroid point of the membership functions on the vertical axis and its intersection with the left and the right membership functions, as represented by the grayed area in Figure 4.6 and formulated in Eq. (4.3).

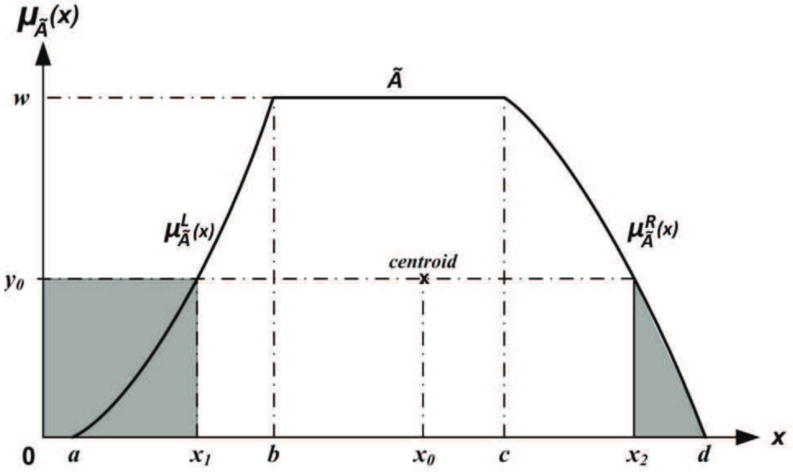


**Figure 4.6 Area defuzzification technique.**

$$ADT = d\left(\mu_{\tilde{A}}(x)\right) = x_1 y_0 + \int_{x_2}^{d} \mu^R_{\tilde{A}}(x)dx \tag{4.3}$$

where $y_0$ is the centroid point of the real fuzzy number $\tilde{A}$ on the vertical axis, $x_1$ is the intersection point between the line $y_0$ and the left membership function $\mu^L_{\tilde{A}}(x)$ on the horizontal axis, and $x_2$ is the intersection point between the line $y_0$ and the right membership function $\mu^R_{\tilde{A}}(x)$ on the horizontal axis. $y_0$, $x_1$ and $x_2$ are calculated using Eqs. (4.4-4.6).

$$y_0 = \frac{\int_0^w y.\mu^R_{\tilde{A}}(y)dy - \int_0^w y.\mu^L_{\tilde{A}}(y)dy}{\int_0^w \mu^R_{\tilde{A}}(y)dy - \int_0^w \mu^L_{\tilde{A}}(y)dy} \tag{4.4}$$

$$x_1 = \mu^L_{\tilde{A}}(y_0) \tag{4.5}$$

$$x_2 = \mu^R_{\tilde{A}}(y_0) \tag{4.6}$$

where $\mu^L_{\tilde{A}}(x)$, $\mu^R_{\tilde{A}}(x)$, $\mu^L_{\tilde{A}}(y)$, and $\mu^R_{\tilde{A}}(y)$ are the left, the right, the inverse of the left, and the inverse of the right membership functions of fuzzy numbers, respectively, as given in (2.9-2.12)

**Theorem 4.1** *If $\tilde{A}$ = (a,b,c,d) is a normal trapezoidal fuzzy number, then its centroid point on the vertical axis is shown in Eq. (4.7).*

$$y_0 = \frac{1}{3}\left[\frac{2c+d-a-2b}{c+d-a-b}\right] \tag{4.7}$$

**Proof.** By substituting Eqs. (2.9-2.10) into Eq. (4.4), the centroid point of a normal trapezoidal fuzzy number on the vertical axis is calculated as follows.

$$y_0 = \frac{\int_0^1[y(d+(c-d)y)]dy - \int_0^1[y(a+(b-a)y)]dy}{\int_0^1[d+(c-d)y]dy - \int_0^1[a+(b-a)y]dy} = \frac{\left[\frac{dy^2}{2}+\frac{(c-d)y^3}{3}\right]_0^1 - \left[\frac{ay^2}{2}+\frac{(b-a)y^3}{3}\right]_0^1}{\left[dy+\frac{(c-d)y^2}{2}\right]_0^1 - \left[ay+\frac{(b-a)y^2}{2}\right]_0^1}$$

$$= \frac{1}{3}\left[\frac{2c+d-a-2b}{c+d-a-b}\right]$$

therefore proof is complete.

**Theorem 4.2** *If $\tilde{A}$ = (a,b,c,d) is a normal trapezoidal fuzzy number, $y_0$ is its centroid point on the vertical axis, then the intersection between the line $y_0$ and the left membership function $\mu_{\tilde{A}}^{L}(x)$ on the horizontal axis is shown in Eq. (4.8).*

$$x_1 = \frac{2(a+b)^2-a(2b+c+2d)-b(2c+d)}{3(a+b-c-d)} \tag{4.8}$$

**Proof.** By substituting Eq. (4.7) into Eq. (4.5), the intersection point between the line $y_0$ and the left membership function $\mu_{\tilde{A}}^{L}(x)$ on the horizontal axis is calculated as follows.

$$x_1 = a+(b-a)\left(\frac{1}{3}\left[\frac{2c+d-a-2b}{c+d-a-b}\right]\right) = \frac{2ad+2bc+ac+bd-2(a^2+ab+b^2)}{3(c+d-a-b)}$$

$$= \frac{2(a+b)^2-a(2b+c+2d)-b(2c+d)}{3(a+b-c-d)}$$

therefore proof is complete.

**Theorem 4.3** *If $\tilde{A}$ = (a,b,c,d) is a normal trapezoidal fuzzy number, $y_0$ is its centroid point on the vertical axis, then the intersection between the line $y_0$ and the right membership function $\mu_{\tilde{A}}^{R}(x)$ on the horizontal axis is shown in Eq. (4.9).*

$$x_2 = \frac{2(c+d)^2-c(a+2b)-d(2a+b+2c)}{3(c+d-a-b)} \tag{4.9}$$

**Proof.** By substituting Eq. (4.7) into Eq. (4.6), the intersection point between the line $y_0$ and the right membership function $\mu_{\tilde{A}}^{R}(x)$ on the horizontal axis is calculated as follows.

$$x_2 = d+(c-d)\frac{1}{3}\left[\frac{d+2c-a-2b}{d+c-a-b}\right] = \frac{2(c^2+cd+d^2)-ac-2bc-2ad-bd}{3(d+c-a-b)}$$

$$= \frac{2(c+d)^2 - c(a+2b) - d(2a+b+2c)}{3(c+d-a-b)}$$

therefore proof is complete.

**Proposition 4.1** *If $\tilde{A}$ = (a,b,c,d) is a normal trapezoidal fuzzy number, then its area defuzzification technique (ADT) is given in Eq. (4.10). For a special case, when b = c, the trapezoidal fuzzy number becomes a triangular fuzzy number and its ADT is given in Eq. (4.11).*

$$ADT = d\left(\mu_{\tilde{A}}(x)\right) = \frac{(a+2b-2c-d)\left((2a+2b)^2+(c+d)(-3a+2c-d)-2c(3b+d)-4ab\right)}{18(a+b-c-d)^2} \tag{4.10}$$

$$ADT = d\left(\mu_{\tilde{A}}(x)\right) = \frac{1}{18}(4a+b+d) \tag{4.11}$$

These theorems will be validated in the following section and implemented in Chapters 5 and 6 of this thesis.

## 4.5 Area Defuzzification Technique Validation

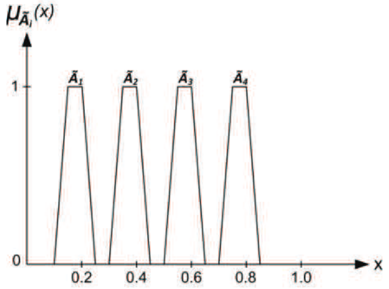
To mathematically investigate the feasibility of the area defuzzification technique to defuzzify membership functions representing nuclear event qualitative failure possibilities into the corresponding quantitative fuzzy failure rates, two types of validation are performed: validation through the five predefined essential fuzzy rules and validation through the real nuclear event failure rates obtained from nuclear power plant operating experiences.

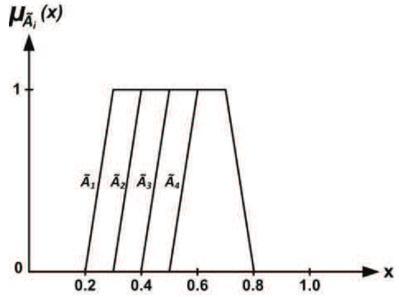
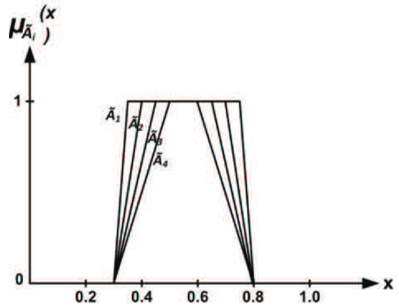
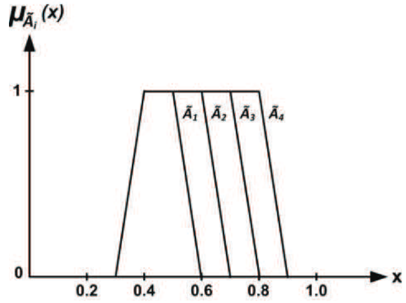
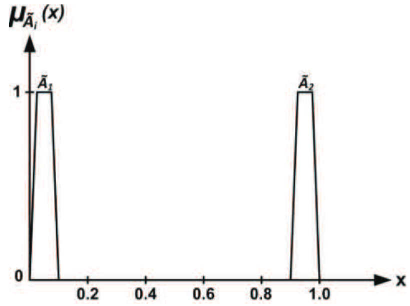
### 4.5.1 THROUGH ESSENTIAL FUZZY RULES

Five sets of fuzzy subsets are used to mathematically justify the area defuzzification technique against the five essential fuzzy rules defined in Section 4.3. The first fuzzy subset is generated by shifting the membership functions from the left to the right, as given in sub-section 4.3.1. The second fuzzy subset is generated by shifting the left membership functions from the left to the right, but the right membership function is kept in its position as given in sub-section 4.3.2. The third fuzzy subset is generated by shifting the cores of the membership functions from the left to the right, but the core width is still the same as given in sub-section 4.3.3. The fourth fuzzy subset is generated by shifting the right membership functions from the left to the right but the left membership function is kept in its position as given in sub-section 4.3.4. The last fuzzy subset is generated by modelling the membership functions to the closest possible position to and the furthest possible position from the origin, as given in sub-section 4.3.5.

The five essential fuzzy rules, the sets of the fuzzy subsets, the membership functions of the fuzzy subsets, and the quantitative fuzzy failure rates generated by the area defuzzification technique using Eq. (4.10) are given in Table 4.1.

**Table 4.1 Membership functions and the corresponding fuzzy failure rates.**

| Rule# | $\tilde{A}_i$ | $\mu_{\tilde{A}i}$ | $R_i$ | |
|---|---|---|---|---|
| (1) |  | (0.1, 0.15, 0.2, 0.25)<br>(0.3, 0.35, 0.4, 0.45)<br>(0.5, 0.55, 0.6, 0.65)<br>(0.7, 0.75, 0.8, 0.85) | 1.1234E-06<br>5.7888E-05<br>3.1662E-04<br>9.3452E-04 | $R(\tilde{A}_1)$<br>$R(\tilde{A}_2)$<br>$R(\tilde{A}_3)$<br>$R(\tilde{A}_4)$ |

| | | | | |
|---|---|---|---|---|
| (2) |  | (0.2, 0.3, 0.7, 0.8)<br>(0.3, 0.4, 0.7, 0.8)<br>(0.4, 0.5, 0.7, 0.8)<br>(0.5, 0.6, 0.7, 0.8) | 4.0897E-05<br>1.2226E-04<br>2.5268E-04<br>3.8533E-04 | *R*($\tilde{A}_1$)<br>*R*($\tilde{A}_2$)<br>*R*($\tilde{A}_3$)<br>*R*($\tilde{A}_4$) |
| (3) |  | (0.3, 0.4, 0.5, 0.9)<br>(0.3, 0.5, 0.6, 0.9)<br>(0.3, 0.6, 0.7, 0.9)<br>(0.3, 0.7, 0.8, 0.9) | 9.5293E-05<br>1.1227E-04<br>1.3116E-04<br>1.5207E-04 | *R*($\tilde{A}_1$)<br>*R*($\tilde{A}_2$)<br>*R*($\tilde{A}_3$)<br>*R*($\tilde{A}_4$) |
| (4) |  | (0.3, 0.4, 0.5, 0.6)<br>(0.3, 0.4, 0.6, 0.7)<br>(0.3, 0.4, 0.7, 0.8)<br>(0.3, 0.4, 0.8, 0.9) | 8.1067E-05<br>1.0713E-04<br>1.2226E-04<br>1.3207E-04 | *R*($\tilde{A}_1$)<br>*R*($\tilde{A}_2$)<br>*R*($\tilde{A}_3$)<br>*R*($\tilde{A}_4$) |
| (5) |  | (0, 0.025, 0.075, 0.1)<br>(0.95, 0.97, 0.98, 1) | 1.6799E-12<br>1.8531E-03 | *R*($\tilde{A}_1$)<br>*R*($\hat{A}_2$) |

We can see from Table 4.1 that the quantitative fuzzy failure rates generated by the area defuzzification technique from the membership function of the five fuzzy subsets meet all the predefined fuzzy rules. These results confirm that the area defuzzification technique is suitable for evaluating nuclear event failures expressed by qualitative failure possibilities and mathematically represented by the membership function of fuzzy numbers.

### 4.5.2 THROUGH REAL NUCLEAR EVENT FAILURE DATA

In this type of validation, real nuclear event failure probabilities collected from the reactor protection system (RPS) at the United States Babcock & Wilcox commercial reactors during the period 1984 through 1998 operating experiences, which are well documented in Wierman et al. (2001a), are compared to the quantitative fuzzy failure rates generated by five different defuzzification techniques. The purpose of this comparison is to find the most suitable technique for evaluating nuclear event failures for fault tree analysis. The five defuzzification techniques are the area defuzzification technique (*ADT*) given in Eq. (4.11), the left and right fuzzy ranking defuzzification technique (*LRDT*) given in Eq. (2.20), the centroid defuzzification technique (*CDT*) given in Eq. (2.25), the area between the centroid point and the original point defuzzification technique (*ACODT*) given in Eq. (2.26), and the centroid based Euclidean distance defuzzification technique (*CEDT*) given in Eq. (2.29). Investigation is done by assessing relative errors of the quantitative fuzzy failure rates generated by each technique to the known quantitative failure probabilities. The technique, which has the lowest number of relative errors, is the most appropriate technique because it is the closest match with the real data.

#### (1) KNOWN NUCLEAR EVENT FAILURE PROBABILITIES

The reactor protection system (RPS) is one of many safety systems in nuclear power plants which functions to rapidly insert control rods into the reactor core to stop a nuclear reaction. The Babcock & Wilcox RPS consists of numerous electronic and mechanical components to produce an automatic and manual reactor trip. The RPS trips the reactor by removing the holding power from the control rod drive motors (CRDMs). Two DC power sources, a main and a secondary power source, supply power to hold the control rods. To release the control rods, both power sources must be interrupted by either opening trip breakers on the two power sources or removing gating power from the silicon-controlled rectifiers (SCRs). The trip breakers will interrupt power to the CRD mechanisms. Nuclear event failure probabilities of the Babcock & Wilcox RPS, which are used in this validation, are shown in Table 4.2.

**Table 4.2 The Babcock & Wilcox RPS reliability data.**

| **Nuclear events** | **Failure probabilities** |
|---|---|
| *Trip breaker local hardware faults* | 1.8E-5 |
| *Shunt trip device local faults* | 6.1E-4 |
| *Channel trip unit fails to trip at its set point* | 2.9E-4 |
| *Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | 1.6E-4 |
| *Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | 1.2E-4 |
| *Manual scram switch fails to operate upon demand* | 1.3E-4 |
| *Control rod (or associated control rod drive) fails to insert fully into core upon demand* | 1.7E-5 |
| *CCF 50% or more CRD/rods fails to insert* | 4.1E-8 |
| *CCF 2 0f 4 trip breaker local hardware faults* | 7.1E-7 |
| *CCF 3 of 4 channel pressure sensor faults* | 2.1E-6 |
| *CCF specific 2 of 4 manual trip switches fault* | 5.4E-6 |
| *CCF specific 6 of 12 logic relays fault* | 5.9E-8 |
| *One regulating rod out of 20 fails to insert* | 3.4E-4 |
| *One safety rod out of 20 fails to insert* | 3.4E-4 |
| *125 Vdc power to the shunt trip fails* | 6.0E-5 |

### (2) GENERATED FUZZY FAILURE RATES

In this sub-section, how nuclear event quantitative fuzzy failure rates are generated from their corresponding qualitative failure possibilities is described and a comparison is made with the known failure probabilities in Table 4.2.

### (a) NUCLEAR EVENT FAILURE POSSIBILITY DEVELOPMENT

The granularity of the set of linguistic terms that is commonly used in engineering system safety consists of four to seven terms as described in Chapter 2. Based on the likely failure occurrences, we define seven linguistic terms to represent seven different nuclear event failure possibilities (*nefp*) as in Eq. (4.12).

$$nefp=\{very\ low,\ low,\ reasonably\ low,\ moderate,\ reasonably\ high,\ high,\ very\ high\} \tag{4.12}$$

Nuclear events with '*very low failure possibilities (VL)*' indicate that the failure rates of these events are less than $10^{-8}$ and the events are very unlikely to become failures. Nuclear events with '*very high failure possibilities (VH)*' indicate that the failure rates of these events are greater than $10^{-3}$ and these events are almost certain to become failures. Events with '*low*' (*L*), '*reasonably low*' (*RL*), '*moderate*' (*M*), '*reasonably high*' (*RH*), and '*high*' (*H*) *failure possibilities* are up-graded from '*very low*' to '*very high*' *failure possibilities* and their failure likelihoods are given in Table 4.3.

**Table 4.3 Nuclear event failure likelihoods.**

| Nuclear event failure possibilities | Failure probabilities |
|---|---|
| *Very Low (VL)* | < 1.0E-8 |
| *Low (L)* | 1.0E-8 – 1.0E-7 |
| *Reasonably Low (RL)* | 1.0E-7 – 1.0E-6 |
| *Moderate (M)* | 1.0E-6 – 1.0E-5 |
| *Reasonably High (RH)* | 1.0E-5 – 1.0E-4 |
| *High (H)* | 1.0E-4 – 1.0E-3 |
| *Very High (VH)* | > 1.0E-3 |

### (b) NUCLEAR EVENT MEMBERSHIP FUNCTION DEVELOPMENT

Ross (2004) listed six straightforward methods to assign membership values, as described in Chapter 2. In this chapter, inductive reasoning is used to develop the values of those membership functions in Eqs. (4.13-4.19) to mathematically represent nuclear event failure possibilities in Eq. (4.12). This technique generates the membership values based on the fact that the real nuclear event reliability data are mostly less than $10^{-2}$ and could be of order $10^{-5}$ to $10^{-13}$ as described in Section 4.3.

Since previous researches confirm that trapezoidal and triangular fuzzy numbers form a sound practical alternative to reflect uncertainty, inaccuracy and fuzziness of human justifications in linguistic values (Ferdous et al. 2011; Wolkenhauer 2001), we decide before the experimentation to use membership functions of trapezoidal fuzzy numbers or triangular fuzzy numbers to mathematically represent nuclear event failure possibilities. In the experimentation, we first tried to find which membership function could be used to generate a bigger failure rate range by comparing the fuzzy failure rates generated by those two membership functions. In this first experimentation, we also tried to find the left most and the right most membership functions of each fuzzy number, to generate nuclear event fuzzy failure rates within the range of real nuclear event failure probabilities. The results, which are shown in Table 4.4, confirm that the triangular membership function can generate a bigger fuzzy failure rate range than the trapezoidal membership function. The triangular membership functions can also produce smaller fuzzy failure rates than those produced by trapezoidal membership functions. These experimentation results justify that nuclear event failure possibilities should be mathematically represented by the membership functions of triangular fuzzy numbers.

**Table 4.4 The results of the experimentations to find parameters for $\mu_{VL}(x)$ and $\mu_{VH}(x)$.**

| **Experimentation goals** | **Membership functions** | **Generated fuzzy failure rates** |
|---|---|---|
| Finding a membership function representing the *very low failure possibility* | (0.00, 0.04, 0.08) | 6.36E-13 |
| | (0.00, 0.03, 0.05, 0.08) | 1.30E-12 |
| Finding a membership function representing the *very high failure possibility* | (0.92, 0.96, 1.00) | 1.03E-03 |
| | (0.92, 0.95, 0.97, 1.00) | 1.87E-03 |

The two triangular fuzzy numbers in Table 4.3 are then used to mathematically represent nuclear events with *very low failure possibility*, i.e. $\mu_{VL}(x)$, and *very high failure possibility*, i.e. $\mu_{VH}(x)$, as given in Eq. (4.13) and Eq. (4.19), respectively.

The membership parameters for the other five failure possibilities are generated by segmenting to the area between the two obtained membership functions in Table 4.3, i.e. $\mu_{VL}(x)$ and $\mu_{VH}(x)$. To find the membership parameters for *moderate failure possibility*, i.e. $\mu_M(x)$, we segmented the area between $\mu_{VL}(x)$ and $\mu_{VH}(x)$ into two areas by choosing the centre of the Cartesian plane, which is 0.50, as its core. Then, we varied the pair of its left and right supports to find the parameters that could generate the lowest fuzzy failure rates for the *moderate failure possibility*. We chose the lowest fuzzy failure rates because nuclear event failure rates are mostly very small. The results of this experimentation are shown in Table 4.5.

**Table 4.5 The results of the experimentations to find parameters for $\mu_M(x)$.**

| Experimentation goal | Membership functions | Generated fuzzy failure rates |
|---|---|---|
| Finding a membership function representing the *moderate failure possibility* | (0.35, 0.50, 0.65) | 6.39E-05 |
| | (0.40, 0.50, 0.60) | 7.91E-05 |
| | (0.45, 0.50, 0.55) | 9.65E-05 |

From Table 4.4, we chose the triangular membership function of (0.35, 0.50, 0.65) to mathematically represent nuclear events with *moderate failure possibilities*, i.e. $\mu_M(x)$, as in Eq. (4.16).

To find the membership parameters for *reasonably high failure possibility*, i.e. $\mu_{RH}(x)$, and *high failure possibility*, i.e. $\mu_H(x)$, we followed the rule that fuzzy sub sets, which are distributed in the Cartesian plane, are overlapped (Ross 2004). Based on this specific characteristic, since the right support for the $\mu_M(x)$ is 0.65, we chose 0.63 as the left support for $\mu_{RH}(x)$. We also use symmetrical membership functions to mathematically represent nuclear event failure possibilities. Therefore, the right support for the $\mu_{RH}(x)$ is 0.83. Hence, the triangular membership function of (0.63, 0.73, 0.83) is used to represent nuclear events with *reasonably high failure possibilities*, i.e.

$\mu_{RH}(x)$, as in Eq. (4.17). Meanwhile, since the left support for the $\mu_{VH}(x)$ is 0.92, then we chose 0.93 as the right support and 0.81 as the left support for the $\mu_H(x)$. Hence, the triangular membership function of (0.81, 0.87, 0.93) is used to represent nuclear events with *high failure possibilities*, i.e. $\mu_H(x)$, as in Eq. (4.18).

Using the same segmentation procedures, we finally chose those membership functions of triangular fuzzy numbers in Eqs. (4.13-4.19), which are graphically shown in Figure 4.7, to mathematically represent nuclear event qualitative failure possibilities defined in Eq. (4.12).

$$\mu_{VL}(x) = \begin{cases} \frac{x}{0.04}, & 0.00 \leq x \leq 0.04 \\ \frac{0.08-x}{0.04}, & 0.04 \leq x \leq 0.08 \\ 0, & x \geq 0.08 \end{cases} \tag{4.13}$$

$$\mu_{L}(x) = \begin{cases} \frac{x-0.07}{0.06}, & 0.07 \leq x \leq 0.13 \\ \frac{0.19-x}{0.06}, & 0.13 \leq x \leq 0.19 \\ 0, & \text{otherwise} \end{cases} \tag{4.14}$$

$$\mu_{RL}(x) = \begin{cases} \frac{x-0.17}{0.10}, & 0.17 \leq x \leq 0.27 \\ \frac{0.37-x}{0.10}, & 0.27 \leq x \leq 0.37 \\ 0, & \text{otherwise} \end{cases} \tag{4.15}$$

$$\mu_{M}(x) = \begin{cases} \frac{x-0.35}{0.15}, & 0.35 \leq x \leq 0.50 \\ \frac{0.65-x}{0.15}, & 0.50 \leq x \leq 0.65 \\ 0, & \text{otherwise} \end{cases} \tag{4.16}$$

$$\mu_{RH}(x) = \begin{cases} \frac{x-0.63}{0.10}, & 0.63 \leq x \leq 0.73 \\ \frac{0.83-x}{0.10}, & 0.73 \leq x \leq 0.83 \\ 0, & \text{otherwise} \end{cases} \tag{4.17}$$

$$\mu_{H}(x) = \begin{cases} \frac{x-0.81}{0.06}, & 0.81 \leq x \leq 0.87 \\ \frac{0.93-x}{0.06}, & 0.87 \leq x \leq 0.93 \\ 0, & \text{otherwise} \end{cases} \tag{4.18}$$

$$\mu_{VH}(x) = \begin{cases} \frac{x-0.92}{0.04}, & 0.92 \leq x \leq 0.96 \\ \frac{1.00-x}{0.04}, & 0.96 \leq x \leq 1.00 \\ 0, & x \leq 0.92 \end{cases} \tag{4.19}$$

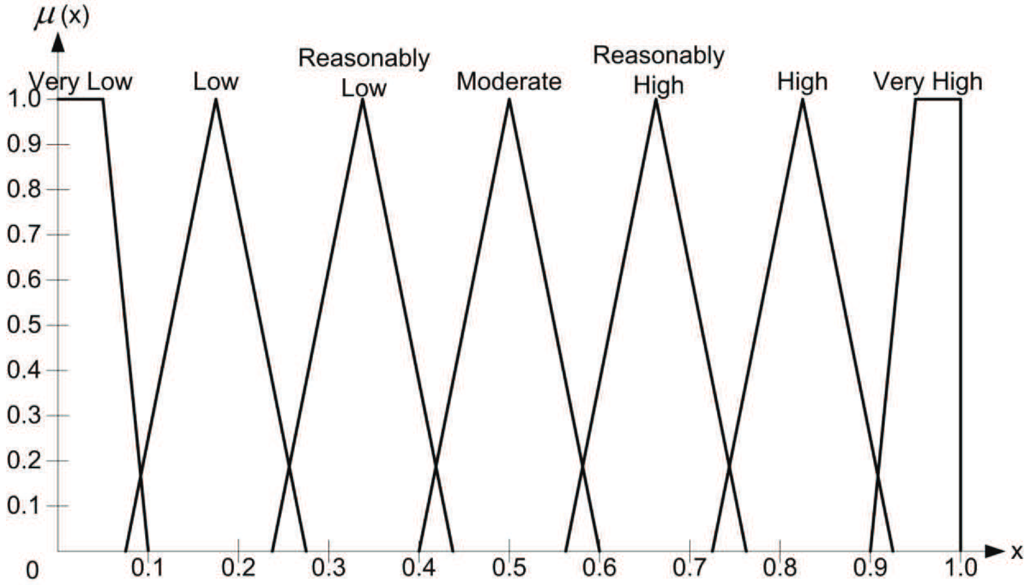


**Figure 4.7 Graphical representation of the nuclear event membership functions.**

### (c) NUCLEAR EVENT FUZZY FAILURE RATES

Let us assume that we ask five experts who are familiar with the United States Babcock & Wilcox reactor protection system and its environment to respond to our questionnaire. The questionnaire and the expert subjective evaluation results are given in Table 4.6.

**Table 4.6 Questionnaire and expert subjective evaluation results.**

| Questions | Expert 1 | Expert 2 | Expert 3 | Expert 4 | Expert 5 |
|---|---|---|---|---|---|
| *How likely the trip breaker local hardware to fail* | *RL* | *M* | *RL* | *M* | *RL* |
| *How likely the shunt trip device local to fail* | *H* | *RH* | *H* | *H* | *H* |
| *How likely the channel trip unit fails to trip at its set point* | *RH* | *RH* | *M* | *RH* | *RH* |
| *How likely the channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | *RH* | *M* | *RH* | *RH* | *M* |
| *How likely the channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | *RH* | *M* | *M* | *M* | *M* |
| *How likely the manual scram switch fails to operate upon demand* | *RH* | *M* | *M* | *M* | *RH* |
| *How likely the control rod (or associated control rod drive) fails to insert fully into core upon demand* | *M* | *RL* | *RL* | *RL* | *M* |
| *How likely the CCF 50% or more CRD/rods fails to insert* | *VL* | *L* | *L* | *L* | *L* |
| *How likely the CCF 2 0f 4 trip breaker local hardware to fail* | *L* | *RL* | *L* | *RL* | *L* |
| *How likely the CCF 3 of 4 channel pressure sensor to fail* | *L* | *L* | *RL* | *L* | *M* |
| *How likely the CCF specific 2 of 4 manual trip switches to fail* | *RL* | *L* | *RL* | *M* | *RL* |
| *How likely the CCF specific 6 of 12 logic relays to fail* | *L* | *VL* | *L* | *VL* | *RL* |
| *How likely one regulating rod out of 20 fails to insert* | *RH* | *RH* | *RH* | *RH* | *RH* |
| *How likely one safety rod out of 20 fails to insert* | *RH* | *RH* | *RH* | *RH* | *RH* |
| *How likely the 125 Vdc power to the shunt trip to fail* | *M* | *M* | *M* | *M* | *M* |

Using the arithmetic averaging in Eq. (2.12), the final membership functions for the *trip breaker local hardware failure* are calculated as follows.

$$a = \frac{0.17+0.35+0.17+0.17+0.17}{5} = (0.24)$$

$$b = \frac{0.27+0.50+0.27+0.27+0.27}{5} = (\ 0.36)$$

$$c = \frac{0.37+0.65+0.37+0.37+0.37}{5} = (0.48)$$

The final membership functions for other nuclear events in Table 4.7 are calculated using the same procedures.

**Table 4.7 Nuclear event final membership functions.**

| Nuclear events | Final membership functions |
|---|---|
| *Trip breaker local hardware faults* | (0.24,0.36,0.48) |
| *Shunt trip device local faults* | (0.77,0.84,0.91) |
| *Channel trip unit fails to trip at its set point* | (0.57,0.68,0.79) |
| *Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | (0.52,0.64,0.76) |
| *Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | (0.41,0.55,0.69) |
| *Manual scram switch fails to operate upon demand* | (0.46,0.59,0.72) |
| *Control rod (or associated control rod drive) fails to insert fully into core upon demand* | (0.24,0.36,0.48) |
| *CCF 50% or more CRD/rods fails to insert* | (0.06,0.11,0.17) |
| *CCF 2 0f 4 trip breaker local hardware faults* | (0.11,0.19,0.26) |
| *CCF 3 of 4 channel pressure sensor faults* | (0.15,0.23,0.32) |
| *CCF specific 2 of 4 manual trip switches fault* | (0.19,0.29,0.39) |
| *CCF specific 6 of 12 logic relays fault* | (0.06,0.12,0.18) |
| *One regulating rod out of 20 fails to insert* | (0.63,0.73,0.83) |
| *One safety rod out of 20 fails to insert* | (0.63,0.73,0.83) |
| *125 Vdc power to the shunt trip fails* | (0.35,0.50,0.65) |

The final membership functions in Table 4.7 are then defuzzified by the five evaluated defuzzification techniques, namely: *LRDT*, *CDT*, *ACODT*, *CEDT*, and *ADT,* to generate nuclear event failure possibility scores ($R_S$) using Eq. (4.1). The results are shown in Table 4.8.

**Table 4.8 Nuclear event failure possibility scores generated by the five different techniques.**

| **Nuclear events** | **Nuclear event failure possibility scores ($R_S$)** | | | | |
|---|---|---|---|---|---|
| | ***LRDT*** | ***CDT*** | ***ACODT*** | ***CEDT*** | ***ADT*** |
| *Trip breaker local hardware faults* | 0.3768 | 0.3620 | 0.1207 | 0.4921 | 0.1007 |
| *Shunt trip device local faults* | 0.8202 | 0.8420 | 0.2807 | 0.9056 | 0.2693 |
| *Channel trip unit fails to trip at its set point* | 0.6658 | 0.6840 | 0.2280 | 0.7609 | 0.2097 |
| *Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | 0.6232 | 0.6380 | 0.2127 | 0.7198 | 0.1927 |
| *Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | 0.5404 | 0.5460 | 0.1820 | 0.6397 | 0.1587 |
| *Manual scram switch fails to operate upon demand* | 0.5814 | 0.5920 | 0.1973 | 0.6794 | 0.1757 |
| *Control rod (or associated control rod drive) fails to insert fully into core upon demand* | 0.3768 | 0.3620 | 0.1207 | 0.4921 | 0.1007 |
| *CCF 50% or more CRD/rods fails to insert* | 0.1326 | 0.1120 | 0.0373 | 0.3516 | 0.0280 |
| *CCF 2 0f 4 trip breaker local hardware faults* | 0.2082 | 0.1860 | 0.0620 | 0.3817 | 0.0493 |
| *CCF 3 of 4 channel pressure sensor faults* | 0.2532 | 0.2320 | 0.0773 | 0.4061 | 0.0630 |
| *CCF specific 2 of 4 manual trip switches fault* | 0.3076 | 0.2880 | 0.0960 | 0.4405 | 0.0790 |
| *CCF specific 6 of 12 logic relays fault* | 0.1434 | 0.1220 | 0.0407 | 0.3550 | 0.0307 |
| *One regulating rod out of 20 fails to insert* | 0.7091 | 0.7300 | 0.2433 | 0.8025 | 0.2267 |
| *One safety rod out of 20 fails to insert* | 0.7091 | 0.7300 | 0.2433 | 0.8025 | 0.2267 |
| *125 Vdc power to the shunt trip fails* | 0.5000 | 0.5000 | 0.1667 | 0.6009 | 0.1417 |

Nuclear event fuzzy failure rates ($R$) in Table 4.9 are then generated by alternately inserting $R_s$ in Table 4.8 into Eq. (4.2).

**Table 4.9 Nuclear event fuzzy failure rates generated by the five different techniques.**

| **Nuclear events** | **Nuclear event fuzzy failure rates (*R*)** | | | | |
|---|---|---|---|---|---|
| | ***LRDT*** | ***CDT*** | ***ACODT*** | ***CEDT*** | ***ADT*** |
| *Trip breaker local hardware faults* | 1.90E-03 | 1.66E-03 | 3.46E-05 | 4.73E-03 | 1.68E-05 |
| *Shunt trip device local faults* | 4.10E-02 | 4.82E-02 | 7.10E-04 | 8.26E-02 | 6.18E-04 |
| *Channel trip unit fails to trip at its set point* | 1.48E-02 | 1.66E-02 | 3.51E-04 | 2.73E-02 | 2.62E-04 |
| *Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | 1.13E-02 | 1.24E-02 | 2.76E-04 | 2.09E-02 | 1.95E-04 |
| *Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | 6.60E-03 | 6.86E-03 | 1.59E-04 | 1.26E-02 | 9.72E-05 |
| *Manual scram switch fails to operate upon demand* | 8.66E-03 | 9.28E-03 | 2.12E-04 | 1.62E-02 | 1.41E-04 |
| *Control rod (or associated control rod drive) fails to insert fully into core upon demand* | 1.90E-03 | 1.66E-03 | 3.46E-05 | 4.73E-03 | 1.68E-05 |
| *CCF 50% or more CRD/rods fails to insert* | 4.97E-05 | 2.58E-05 | 1.59E-07 | 1.51E-03 | 3.12E-08 |
| *CCF 2 0f 4 trip breaker local hardware faults* | 2.56E-04 | 1.72E-04 | 2.04E-06 | 1.98E-03 | 6.78E-07 |
| *CCF 3 of 4 channel pressure sensor faults* | 5.01E-04 | 3.72E-04 | 5.52E-06 | 2.44E-03 | 2.19E-06 |
| *CCF specific 2 of 4 manual trip switches fault* | 9.65E-04 | 7.74E-04 | 1.38E-05 | 3.22E-03 | 6.06E-06 |
| *CCF specific 6 of 12 logic relays fault* | 6.68E-05 | 3.61E-05 | 2.52E-07 | 1.56E-03 | 5.30E-08 |
| *One regulating rod out of 20 fails to insert* | 1.95E-02 | 2.23E-02 | 4.38E-04 | 3.61E-02 | 3.44E-04 |
| *One safety rod out of 20 fails to insert* | 1.95E-02 | 2.23E-02 | 4.38E-04 | 3.61E-02 | 3.44E-04 |
| *125 Vdc power to the shunt trip fails* | 5.00E-03 | 5.00E-03 | 1.16E-04 | 9.83E-03 | 6.39E-05 |

### (3) Failure Rate Comparisons

To find the most appropriate defuzzification technique, we then assess the relative errors of all the techniques. An error is simply the difference between the fuzzy failure rates generated by each technique and the known failure probabilities. Relative errors can express the accuracy of the calculation. The lowest relative error means that the generated fuzzy failure rate is the closest to the real failure probability collected from reactor operating experiences. Therefore, the technique which produces the lowest number of relative errors is the most suitable technique for nuclear safety assessment involving qualitative failure possibilities and membership functions of fuzzy numbers. The relative errors generated by each defuzzification technique are shown in Table 4.10.

**Table 4.10 Relative errors for each defuzzification technique.**

| **Nuclear events** | **Relative errors** | | | | |
|---|---|---|---|---|---|
| | ***LRDT*** | ***CDT*** | ***ACODT*** | ***CEDT*** | ***ADT*** |
| *Trip breaker local hardware faults* | 104.5610 | 91.3227 | 0.9216 | 261.6257 | 0.0663 |
| *Shunt trip device local faults* | 66.1942 | 77.9458 | 0.1634 | 134.4156 | 0.0127 |
| *Channel trip unit fails to trip at its set point* | 50.1481 | 56.3856 | 0.2088 | 93.0262 | 0.0952 |
| *Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and send a signal to the trip unit* | 69.8290 | 76.7945 | 0.7229 | 129.5756 | 0.2197 |
| *Channel reactor vessel level sensor/transmitter fails to detect a low level and send a signal to the trip unit* | 54.0300 | 56.1587 | 0.3289 | 103.8538 | 0.1902 |
| *Manual scram switch fails to operate upon demand* | 65.6457 | 70.3776 | 0.6330 | 123.3438 | 0.0808 |
| *Control rod (or associated control rod drive) fails to insert fully into core upon demand* | 110.7705 | 96.7535 | 1.0346 | 277.0742 | 0.0113 |
| *CCF 50% or more CRD/rods fails to insert* | 1211.1177 | 628.4388 | 2.8841 | 36784.9718 | 0.2396 |
| *CCF 2 0f 4 trip breaker local hardware faults* | 359.5188 | 241.6579 | 1.8692 | 2794.4278 | 0.0455 |
| *CCF 3 of 4 channel pressure sensor faults* | 237.8051 | 176.1998 | 1.6298 | 1163.2315 | 0.0449 |
| *CCF specific 2 of 4 manual trip switches fault* | 177.6956 | 142.3106 | 1.5620 | 595.6776 | 0.1223 |
| *CCF specific 6 of 12 logic relays fault* | 1131.5968 | 610.8435 | 3.2649 | 26375.2569 | 0.1009 |
| *One regulating rod out of 20 fails to insert* | 56.3801 | 64.5880 | 0.2882 | 105.3057 | 0.0105 |
| *One safety rod out of 20 fails to insert* | 56.3801 | 64.5880 | 0.2882 | 105.3057 | 0.0105 |
| *125 Vdc power to the shunt trip fails* | 82.3391 | 82.3391 | 0.9373 | 162.8032 | 0.0642 |

It can be seen from Table 4.10 that *ADT* produces the smallest relative errors amongst the five techniques investigated. Therefore, these results confirm that the area defuzzification technique is the most suitable technique for assessing nuclear event failures, which are expressed in qualitative failure possibilities and mathematically represented by membership functions of fuzzy numbers. These results also verify that fuzzy failure rates are very good alternatives for failure probabilities when historical nuclear event data is inadequate or unavailable.

## 4.6 SUMMARY

In this chapter, we describe an area defuzzification technique to evaluate nuclear event failures which do not have quantitative historical failure data for probabilistic calculation. We define five essential fuzzy rules that need to be satisfied by the technique. Two types of validations are performed to mathematically justify the applicability and effectiveness of the area defuzzification technique. In the first type of validation, we verified the area defuzzification technique against the five predefined essential fuzzy rules. In the second type of validation, we verified the technique by comparing fuzzy failure rates generated by the technique to real failure probabilities collected from nuclear power plant operating experiences. The results of the two validations confirm that the area defuzzification technique is suitable for evaluating nuclear event failures, which are expressed in qualitative failure possibilities and mathematically represented by membership functions of fuzzy numbers. In addition, the results of the second validation also confirm that fuzzy failure rates are very good alternatives for probabilistic failure rates when historical nuclear event data is inadequate or unavailable for the probabilistic approach.

Chapter 5

# A FUZZY RELIABILITY APPROACH TO ASSESS BASIC EVENTS OF FAULT TREES THROUGH QUALITATIVE DATA PROCESSING

## 5.1 INTRODUCTION

In conventional reliability theory, it is assumed that components of a complex engineering system always have precise failure probabilities. However, this is not the case in some real applications. If a system to be evaluated is new, there will not be sufficient statistical data to estimate component reliabilities. Therefore, the assumption of component precise failure probabilities may be unreasonable. These difficulties highlight the need for new techniques that will enable effective generation of accurate basic event failure rates without the need for quantitative historical failure data. On the other hand, when quantitative historical data is inadequate or unavailable, expert subjective opinion is often used as the only resource for obtaining basic event failure information. Therefore, it is necessary to capture the subjectivity and imprecision of basic event failures.

This chapter describes a fuzzy reliability approach to assess basic event failure rates through qualitative data processing. To demonstrate the feasibility of the proposed approach, nuclear event failure rates generated by the approach are compared to the real reliability data taken from nuclear power plant operating experiences. The remainder of this chapter is organized as follows. Section 5.2 describes the quantification processes of the proposed fuzzy reliability approach. Meanwhile, the validation of the approach is given in Section 5.3 and the result analysis is presented in Section 5.4. Finally, the chapter is summarized in Section 5.5. The work presented in this chapter has been reported in two of our publications listed in Section 1.7, i.e. publication numbers 5 and 8.

## 5.2 Quantification Processes

Since the objective of the approach is to integrate basic event qualitative data into the quantitative phase of the fault tree analysis, the fuzzy reliability approach applies both fuzzification and defuzzification techniques. The objective of the fuzzification technique is to convert basic event qualitative data into their corresponding mathematical form represented by the membership functions of fuzzy numbers. Meanwhile, the objective of the defuzzification technique is to transform the membership functions of the fuzzy numbers into a single scalar quantity to generate basic event failure rates as the outputs of the approach. Therefore, the defuzzification technique is used to defuzzify the output of the fuzzification technique to be further used for generating a failure rate.

Inputs to the approach are linguistic values, membership functions of fuzzy sets, basic events of the fault tree of the system under evaluation, experts and their justification weights, and expert subjective evaluation, as in Eqs. (5.1-5.6). The output of the approach is a set of fuzzy failure rates representing the all $I$ basic event failure rates, as in Eq. (5.13).

The proposed fuzzy reliability approach consists of five quantification processes which are described in details in the following sub-sections. An overall architecture of the approach quantification processes is shown in Figure 5.1.

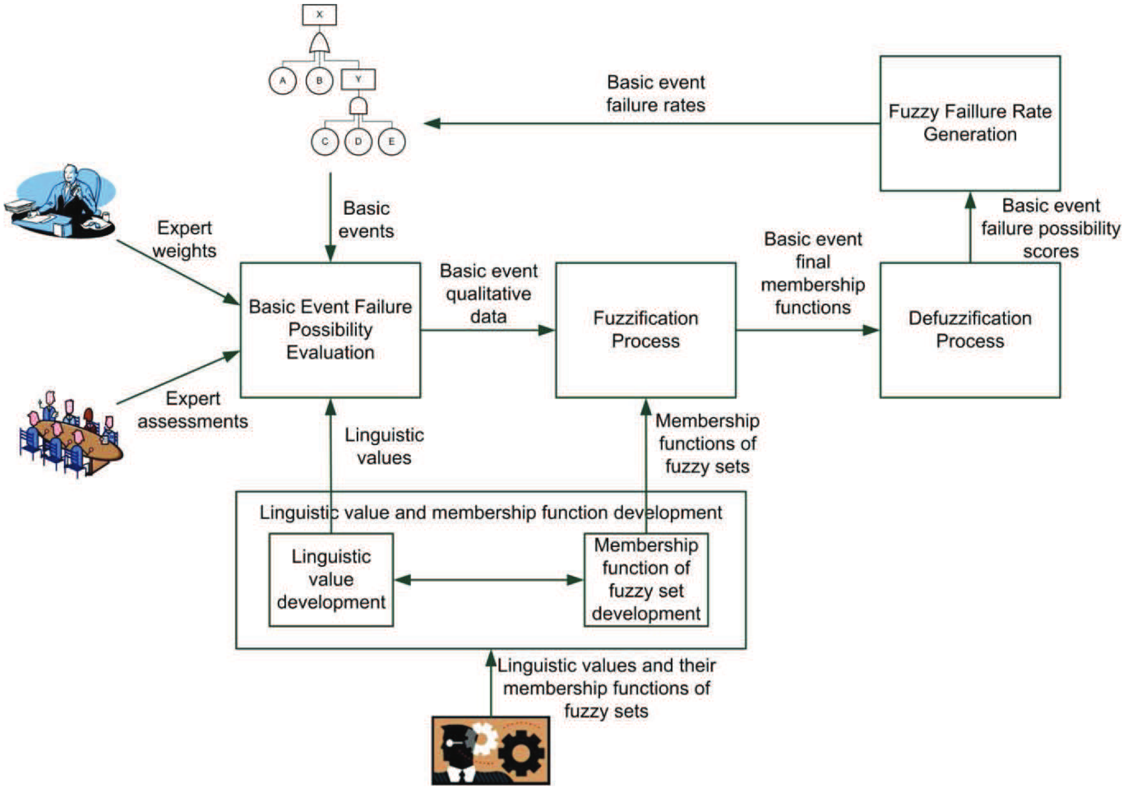

X
A
B
Y
C
D
E
Basic event failure rates
Fuzzy Faillure Rate Generation
Expert weights
Basic events
Basic event failure possibility scores
Basic event final membership functions
Basic Event Failure Possibility Evaluation
Basic event qualitative data
Fuzzification Process
Defuzzification Process
Expert assessments
Linguistic values
Membership functions of fuzzy sets
Linguistic value and membership function development
Linguistic value development
Membership function of fuzzy set development
Linguistic values and their membership functions of fuzzy sets

**Figure 5.1 Structure of the quantification processes of the fuzzy reliability approach.**

### 5.2.1 Linguistic Value And Membership Function Development

This process develops the terms of linguistic values used to represent basic event failure possibilities and their corresponding mathematical representation. The inputs for this process come from safety analysts, who understand the systems, as well as qualitative data modeling. It consists of two sub-processes, i.e., *linguistic value development* and *membership function of fuzzy set development*.

The output of the linguistic value development is a set of qualitative linguistic values (*H*), as in Eq. (5.1) to express basic event failure possibilities. This set of qualitative linguistic values will be used by experts to subjectively assess basic event failure likelihoods in the basic event failure possibility evaluation process in Figure 5.1.

To develop the set of qualitative linguistic values in Eq. (5.1), basic event failure possibilities could be graded based on the type of the components or the likely failure occurrences. Based on the component types, for example, *very low failure possibility* can be used to represent components which are rigid and very unlikely to be failure even once. Meanwhile, *very high failure possibility* can be used to represent components which have many moving parts and are near certain to be failure several times. Based on the likely failure occurrences, for example, *very low failure possibility* can be used to represent components whose failure rates could be less than $10^{-8}$. Meanwhile, *very high failure possibility* can be used to represent components whose failure rates could be greater than $10^{-3}$. This grading will, of course, be different on different application. For instance, $10^{-3}$ could be defined as *high failure possibility* for nuclear accidents but as *low failure possibility* for motor cycle accidents. Therefore, safety analysts have to develop this failure possibility grading based on the system problems on hands.

The outputs of the membership function of fuzzy set development are the membership functions of the fuzzy numbers to mathematically represent each member of *H,* as in Eq. (5.2). These membership functions are developed in the [0, 1] universe of discourse. This means that the closer the fuzzy probabilities are to 0, the less likely the basic events are to fail. On the other hand, the closer the fuzzy probabilities are to 1, the more likely the basic events are to fail. Meanwhile, the horizontal axis represents the fuzzy failure rates of basic events, which is also defined between 0 and 1. This means that the closer the fuzzy numbers are to the point of origin, the lower the basic event fuzzy failure rates are. On the other hand, the farther the fuzzy numbers are from the point of origin, the higher the basic event fuzzy failure rates are. It is also important to note that membership functions developed in this process can have different form for different engineering systems. The membership functions developed in this process will be used to generate basic event final membership functions in the fuzzification process in Figure 5.1.

To assign values for those failure possibility membership functions in Eq. (5.2), safety analysts may choose a method from the six straightforward methods described in Chapter 2, i.e. intuition, inference, rank ordering, neural networks, genetic algorithms, and inductive reasoning.

$$H = \{\textit{very low, low, reasonably low, moderate, reasonably high, high, very high}\} \tag{5.1}$$

$$\begin{aligned} M = \{&very\ low(\mu), low(\mu), reasonably\ low(\mu), moderate(\mu), \\ &reasonably\ high(\mu), high(\mu), very\ high(\mu)\} \end{aligned} \tag{5.2}$$

As noted earlier, for example, there are seven linguistic terms, i.e. *very low*, *low*, *reasonably low*, *moderate*, *reasonably high*, *high*, *very high* where each of them is mathematically described by the membership functions of the fuzzy sets, i.e. *very low (μ)*, *low (μ)*, *reasonably low (μ)*, *moderate (μ)*, *reasonably high (μ), high (μ)*, and *very high (μ)*.

The links between the linguistic values and the membership functions of fuzzy sets in Eqs. (5.1-5.2) are visualized in Figure 5.2.

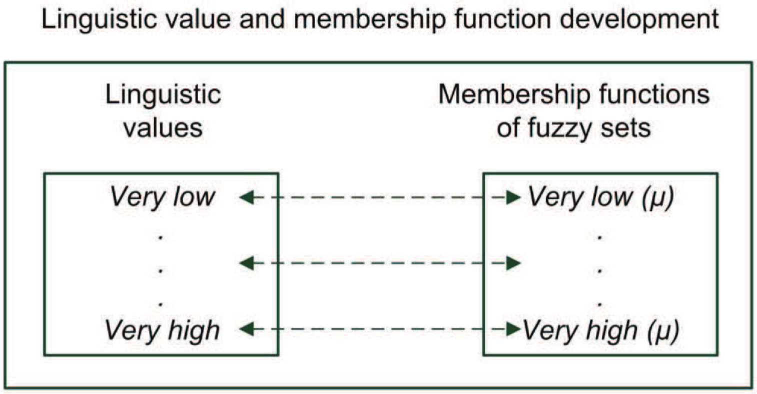

Linguistic value and membership function development
Linguistic values
Membership functions of fuzzy sets
Very low
Very high
Very low (μ)
Very high (μ)

**Figure 5.2 Links between the linguistic values and the membership functions of the fuzzy sets.**

### 5.2.2 Basic Event Failure Possibility Evaluation

This process evaluates the failure possibilities of basic events of the system fault tree subjectively assessed by experts using the qualitative linguistic values in Eq. (5.1). The inputs to this process are a set of basic events from the system fault tree, as in Eq. (5.3), a set of experts to subjectively evaluate basic event failure, as in Eq. (5.4) and their corresponding weights, as in Eq. (5.5), and a set of basic event subjective assessments coming from the experts, as in Eq. (5.6). In this evaluation process, experts answer specific questions about basic event failure possibilities by choosing one failure possibility from seven predefined failure possibilities in Eq. (5.1) as follows, for example.

*How likely is the basic event $b_i$ to fail?*
*Is it very low, low, reasonably low, moderate, reasonably high, high, or very high?*

An expert is a person who is familiar with the system, understands the system working environment, and has considerable training in and knowledge of the system operation. Three measures described in Chapter 2, i.e. the number of scientific publications, recommendations from a wide range of experts, and experiences with previous similar studies, can be used to select experts whose expertise are in the study to what it is intended for. However, in real applications, the experts may have different levels of expertise, background and working experience. Hence, they may demonstrate different perceptions about the same events and subjectively provide different assessment. To reflect their differences of assessments, different justification weights from 0 to 1 may be assigned to every expert, as in Eq. (5.5). Two key performance-based indicators described in Chapter 2, i.e. calibration and informativeness, can be used to weight selected experts.

$$B = \{b_1, b_2, \cdots, b_l\} \text{ and } B \in FT \tag{5.3}$$

$$E = \{e_1, e_2, \cdots, e_n\} \tag{5.4}$$

$$W = \{w_1, w_2, \cdots, w_3\ ; 0 \leq w_i \leq 1 \text{ and } \textstyle\sum_{i=1}^{n} w_i = 1\} \tag{5.5}$$

$$Y = \{\{very\ low, low, \cdots, low\}, \{\cdots\}, \cdots, \{\cdots\}\} \tag{5.6}$$

As noted earlier, for example, there are *l* basic events in the system fault tree *FT*, say $b_1, b_2, \ldots, b_l$ which are subjectively evaluated by *n* experts, say $e_1, e_2, \ldots, e_n$ which have justification weights of say, $w_1, w_2, \ldots, w_n$ where each weight is defined in space [0, 1] and the total weight must be 1. Meanwhile, *Y* is the set of the basic event failure possibilities which are subjectively evaluated by the experts. For example, the experts $e_1$, $e_2$, …, and $e_n$ subjectively justify the failure possibility of the basic event $b_1$ as *very low*, *low*, …, and *low*, respectively.

The output of this process is a matrix of basic event qualitative data (*Ql*), as in Eq. (5.7). For example, the qualitative data for the basic event $b_1$ are *very low*, *low*, …, and *low.*

$$Ql = \begin{bmatrix} very\ low & low & \cdots & low \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix} \tag{5.7}$$

The description of links amongst Eqs. (5.1, 5.3-5.7) are visualized in Figure 5.3.

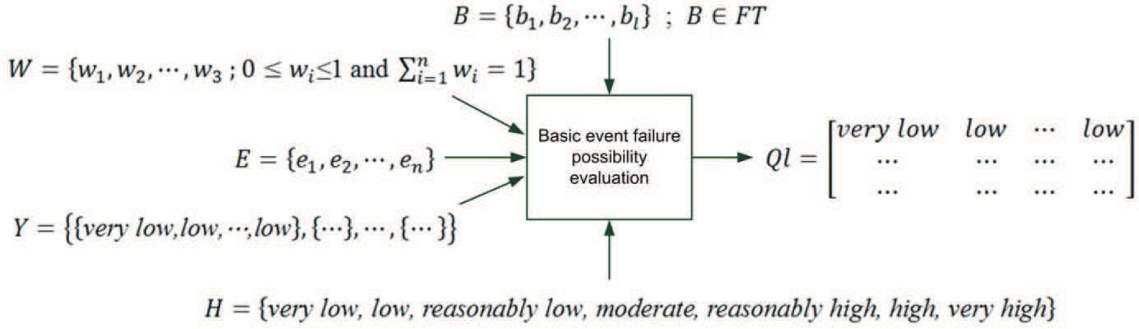

$B = \{b_1, b_2, \cdots, b_l\}$ ; $B \in FT$
$W = \{w_1, w_2, \cdots, w_3 ; 0 \leq w_i \leq 1$ and $\sum_{i=1}^{n} w_i = 1\}$
Basic event failure possibility evaluation
$E = \{e_1, e_2, \cdots, e_n\}$
$Ql = \begin{bmatrix} very\ low & low & \cdots & low \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$
$Y = \{\{very\ low, low, \cdots, low\}, \{\cdots\}, \cdots, \{\cdots\}\}$
$H = \{very\ low,\ low,\ reasonably\ low,\ moderate,\ reasonably\ high,\ high,\ very\ high\}$

**Figure 5.3 Description of links amongst Eqs. (5.1, 5.3-5.7).**

The basic event qualitative data generated in this process will be used to generate the corresponding set of basic event quantitative data in the fuzzification process in Figure 5.1.

### 5.2.3 FUZZIFICATION PROCESS

This process quantifies basic event qualitative data taken from the basic event failure possibility evaluation process, as in Eq. (5.7) into their corresponding quantitative data in the form of the membership functions of the fuzzy numbers, as in Eq. (5.8) and then aggregates those subjective quantitative data to generate a vector of basic event final quantitative data, as in Eq. (5.9).

$$Qn = \begin{bmatrix} very\ low(\mu) & low(\mu) & \cdots & low(\mu) \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix} \tag{5.8}$$

*Qn* is the corresponding quantitative data of the qualitative data *Ql* in Eq. (5.7), for example, the quantitative data for the basic event $b_1$ are *very low(μ), low(μ), …,* and *low(μ)*.

$$M^B = \begin{bmatrix} b_1(\mu) \\ b_2(\mu) \\ \vdots \\ b_l(\mu) \end{bmatrix} \tag{5.9}$$

$M^B$ is the output of this process which is a vector of *l* basic event final quantitative data. Each data in this vector is aggregated from the *n* quantitative data subjectively evaluated by the *n* experts. For example, $b_1(\mu)$ is the final quantitative data for the basic event $b_1$, which is aggregated from its *n* quantitative data, i.e. *very low(μ), low(μ), …, low(μ)*. This $b_1(\mu)$ is also given in the form of a membership function of a fuzzy set.

We consider the weighted averaging operator described in Chapter 2 as the most appropriate aggregation technique for this process. It represents real situation in which experts may justify the same basic event with different failure possibilities by weighting each experts to correlate their judgments to their expertise. Therefore, Eq. (5.9) can be extended, as in Eq. (5.10).

$$M^B = \begin{bmatrix} b_1(\mu) \\ b_2(\mu) \\ \vdots \\ b_l(\mu) \end{bmatrix} = Qn \times \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ \vdots \\ w_n \end{bmatrix} \tag{5.10}$$

where *l* is the number of basic events, *n* is the number of experts, *Qn* is the matrix of quantitative data, as in Eq. (5.8), and $w_i$ is the weight of the $i^{th}$ expert, as in Eq. (5.5).

### 5.2.4 Defuzzification Process

The final quantitative data taken from the fuzzification process is still in the form of fuzzy numbers whereas the calculation of the actual reliability requires a single scalar quantity. Therefore, the output generated by the fuzzification process need to be transformed into a scalar quantity. This process defuzzifies the vector $M^B$ in Eq. (5.10) into its corresponding vector of basic event failure possibility scores, as in Eq. (5.11).

$$\begin{bmatrix} R_s^{b_1} \\ R_s^{b_2} \\ R_s^{b_3} \\ \vdots \\ R_s^{b_l} \end{bmatrix} = \begin{bmatrix} d\big(b_1(\mu)\big) \\ d\big(b_2(\mu)\big) \\ d\big(b_3(\mu)\big) \\ \vdots \\ d\big(b_l(\mu)\big) \end{bmatrix} \tag{5.11}$$

where the $R_s^{b_i}$ is a failure possibility score for the $i^{th}$ basic event, which is defuzzified from its final quantitative data, i.e. $d\big(b_i(\mu)\big)$, and *l* is the number of basic events.

In Chapter 4, the area defuzzification technique (*ADT*) has been validated as the most suitable technique to defuzzify the membership functions of fuzzy sets, which are used to mathematically represent nuclear event failure possibilities, into the corresponding nuclear event failure possibility scores. Therefore, Eq. (5.11) can be rewritten, as in Eq. (5.12).

$$\begin{bmatrix} R_s^{b_1} \\ R_s^{b_2} \\ R_s^{b_3} \\ \vdots \\ R_s^{b_l} \end{bmatrix} = \begin{bmatrix} ADT\big(b_1(\mu)\big) \\ ADT\big(b_2(\mu)\big) \\ ADT\big(b_3(\mu)\big) \\ \vdots \\ ADT\big(b_l(\mu)\big) \end{bmatrix} \tag{5.12}$$

### 5.2.5 Fuzzy Failure Rate Generation

This process generates a vector of basic event fuzzy failure rates ($R^{b_k}$) from their corresponding failure possibility scores taken from the defuzzification process in Figure 5.1, as in Eq. (5.13).

$$R^B = \begin{bmatrix} R^{b_1} \\ R^{b_2} \\ \vdots \\ R^{b_l} \end{bmatrix} \tag{5.13}$$

$R^B$ is a vector of *l* basis event fuzzy failure rates where each of them is generated from its failure possibility score. For example, $R^{b_1}$ is the fuzzy failure rate for the basic event $b_1$ which is generated from $R_s^{b_1}$ using the Onisawa's logarithmic function described in Chapter 2, as in Eq. (5.14).

$$R^{b_i} = \begin{cases} \frac{1}{10^z}, & R_s^{b_i} \neq 0 \\ 0, & R_s^{b_i} = 0 \end{cases} \tag{5.14}$$

where $R^{b_i}$ is a fuzzy failure rate for the *i<sup>th</sup>* basic event and $z = \left[\frac{1-R_s^{b_i}}{R_s^{b_i}}\right]^{1/3} \times 2.301$.

We call the output of the proposed fuzzy reliability approach as fuzzy failure rate to make it different from the probabilistic failure rate. Fuzzy failure rates are generated by the proposed approach from the membership functions of the fuzzy numbers whereas probabilistic failure rates are probabilistically calculated from historical failure data.

## 5.3 VALIDATION

When a new approach is developed, testing and validation are needed to ensure its soundness. This section mathematically investigates the feasibility of the proposed approach to evaluate basic event failure rates through the qualitative data processing as described in the previous section. In this validation, basic event failure rates generated by the proposed fuzzy reliability approach are compared to the known probabilistic failure rates taken from the U.S. Combustion Engineering Reactor Protection System (CERPS) during the period 1984 through 1998 operating experience which are well documented in Wierman et al. (2001).

Component failure probabilities in Wierman et al. (2001) are presented in three different values, i.e. *best estimate*, *lower bound*, and *upper bound* reliability values. The best estimate reliability value is the recommended reliability data to be used in the fault tree analysis. Meanwhile, the upper and the lower bound reliability values represent a range of reliability data estimation. To verify the feasibility and the applicability of the proposed approach, the basic event failure rates generated by the proposed approach have to be between the upper and the lower bound reliability values and as close as possible to the best estimate reliability value.

This section describes the basic event data sets used to verify the proposed approach and the mathematical illustration to show the approach performance and feasibility to assess basic event failure rates through qualitative data processing.

### 5.3.1 BASIC EVENT DATA SETS

Reactor protection system is one of many safety systems in commercial reactors that comprises numerous electronic and mechanical components to produce an automatic or manual rapid shutdown when the reactor experiences disturbed conditions and requires a trip to stop the nuclear reaction. Basic events in this illustration are taken from the CERPS fault tree in Wierman et al. (2001). We can see from Table 5.1 that there are 37 basic events to be assessed by the proposed fuzzy reliability approach.

**Table 5.1 The basic event failure rates of the CERPS fault tree.**

| **Basic events** | **Failure description** | **Known reliability** | | |
|---|---|---|---|---|
| | | **Lower bound** | **Best estimate** | **Upper bound** |
| $b_1$ | Trip breaker local hardware faults | 4.3E-6 | 1.8E-5 | 4.5E-5 |
| $b_2$ | Shunt trip device local faults | 6.3E-6 | 1.5E-4 | 5.5E-4 |
| $b_3$ | Under-voltage coil device local faults | 1.4E-4 | 1.1E-3 | 3.5E-3 |
| $b_4$ | Channel trip unit (bi-stable) fails to trip at its set point | 3.4E-5 | 5.0E-4 | 1.8E-3 |
| $b_5$ | Channel analog core protection calculator fails to send a signal to the trip unit | 1.6E-3 | 7.6E-3 | 2.0E-2 |
| $b_6$ | Channel digit protection calculator fails to send a signal to the trip unit | 6.5E-4 | 2.7E-3 | 6.8E-3 |
| $b_7$ | Channel reactor vessel pressure sensor/transmitter fails to detect a high pressure and sends a signal to the trip unit | 1.1E-5 | 1.1E-4 | 3.5E-4 |
| $b_8$ | Channel reactor vessel temperature/transmitter (cold or hot leg) fails to detect a low level and sends a signal to the trip unit | 4.2E-4 | 8.4E-4 | 1.5E-3 |
| $b_9$ | Manual scram switch fails to operate upon demand | 4.1E-5 | 1.3E-4 | 2.8E-4 |
| $b_{10}$ | Control rod (or associated control rod drive) fails to insert fully into core upon demand | 3.4E-7 | 1.7E-5 | 6.4E-5 |
| $b_{11}$ | Channel logic relay fails to de-energize upon demand | 2.2E-5 | 2.6E-4 | 8.8E-4 |
| $b_{12}$ | CCF 2 of 8 trip breaker local hardware faults | 1.9E-7 | 1.0E-6 | 2.7E-6 |
| $b_{13}$ | CCF 2 of 4 trip breaker local hardware faults | 8.0E-8 | 7.1E-7 | 2.2E-6 |
| $b_{14}$ | CCF 2 of 8 shunt trip device local faults | 3.9E-7 | 1.1E-6 | 4.0E-5 |
| $b_{15}$ | CCF 2 of 4 shunt trip device local faults | 2.5E-7 | 8.7E-6 | 3.3E-5 |
| $b_{16}$ | CCF 2 of 8 under-voltage coil device local faults | 5.1E-6 | 5.4E-5 | 1.8E-4 |
| $b_{17}$ | CCF 2 of 4 under-voltage coil device local faults | 2.3E-6 | 3.7E-5 | 1.3E-4 |
| $b_{18}$ | CCF specific 2 of 3 bi-stables associated with either a pressure (P) or temperature (T) signal (T&M) | 1.1E-6 | 2.6E-5 | 9.5E-5 |
| $b_{19}$ | CCF specific 3 of 4 bi-stables associated with either a pressure (P) or temperature (T) signal | 1.4E-7 | 7.2E-6 | 2.8E-5 |
| $b_{20}$ | CCF specific 4 of 6 bi-stables (T&M) | 3.7E-8 | 1.7E-6 | 6.6E-6 |
| $b_{21}$ | CCF specific 6 of 8 bi-stables | 7.1E-9 | 7.7E-7 | 2.9E-6 |

| | | | | |
|---|---|---|---|---|
| $b_{22}$ | CCF 2 of 3 analog core protection calculators (T&M) | 4.9E-5 | 3.8E-4 | 1.2E-3 |
| $b_{23}$ | CCF 3 of 4 analog core protection calculators | 1.3E-5 | 1.7E-4 | 5.6E-4 |
| $b_{24}$ | CCF 2 of 3 digital core protection calculators (T&M) | 2.3E-5 | 1.4E-4 | 3.8E-4 |
| $b_{25}$ | CCF 3 of 4 digital core protection calculators | 6.3E-6 | 5.7E-5 | 1.8E-4 |
| $b_{26}$ | CCF 2 of 3 pressure sensor/ transmitters (T&M) | 3.0E-7 | 5.0E-6 | 1.8E-5 |
| $b_{27}$ | CCF 3 of 4 pressure sensor/ transmitters | 4.0E-8 | 1.5E-6 | 5.8E-6 |
| $b_{28}$ | CCF 2 of 3 temperature sensor/ transmitters (T&M) | 8.0E-6 | 3.7E-5 | 9.8E-5 |
| $b_{29}$ | CCF 3 of 4 temperature sensor/ transmitters | 7.5E-7 | 1.0E-5 | 3.5E-5 |
| $b_{30}$ | CCF specific 2 of 4 manual trip switches | 7.4E-7 | 5.0E-6 | 1.5E-5 |
| $b_{31}$ | CCF specific 2 of 4 trip breaker shunt trip device power | 2.3E-7 | 2.5E-6 | 8.3E-6 |
| $b_{32}$ | CCF 50% (18 of 36) or more CRD/rods fail to insert | 7.5E-10 | 3.6E-8 | 1.4E-7 |
| $b_{33}$ | CCF specific 6 of 12 logic relays (T&M) | 4.8E-9 | 1.6E-7 | 6.0E-7 |
| $b_{34}$ | CCF specific 12 of 24 logic relays | 5.3E-10 | 4.3E-8 | 1.7E-7 |
| $b_{35}$ | CCF 3 of 3 logic relays (T&M) | 4.8E-9 | 4.7E-7 | 1.8E-6 |
| $b_{36}$ | CCF 6 of 6 logic relays | 8.2E-10 | 2.0E-7 | 7.2E-7 |
| $b_{37}$ | CCF 2 of 4 trip relays | 5.7E-7 | 4.8E-6 | 1.5E-5 |

### 5.3.2 BASIC EVENT SUBJECTIVE ASSESSMENT

In this section, the mathematical illustration to show the performance and feasibility of the proposed fuzzy reliability approach to assess basic event failure rates through qualitative data processing is described. Let there be seven experts, who understand the working environment and are familiar with the CERPS, subjectively assess those basic events shown in Table 5.1. For illustration purposes only, we give all the seven experts the same justification weight of 1/7. Using the processes explain in Section 5.2, the fuzzy failure rates of all basic events in Table 5.1 are generated as follows.

### (1) LINGUISTIC VALUE AND MEMBERSHIP FUNCTION DEVELOPMENT

Based on the likely failure occurrences, seven linguistic terms to qualitatively represent seven different nuclear event failure possibilities have been developed in Eq. (4.12) which can be restated, as in Eq. (5.15).

$$H = \{\textit{very low(VL), low(L), reasonably low(RL), moderate(M),}\\ \textit{reasonably high(RH), high(H), very high(VH)}\} \quad (5.15)$$

The description of the nuclear event failure possibilities in Eq. (5.15) can be seen in Table 4.3. Furthermore, the membership functions of triangular fuzzy numbers have also been developed in Chapter 4 to mathematically represent those seven nuclear event failure possibilities in Eq. (5.15) which can be restated in simple forms, as in Eqs. (5.16-5.22).

$$\mu_{very\ low}(x) = \{0.00, 0.04, 0.08\} \quad (5.16)$$

$$\mu_{low}(x) = \{0.07, 0.13, 0.19\} \quad (5.17)$$

$$\mu_{reasonably\ low}(x) = \{0.17, 0.27, 0.37\} \quad (5.18)$$

$$\mu_{moderate}(x) = \{0.35, 0.50, 0.65\} \quad (5.19)$$

$$\mu_{reasonably\ high}(x) = \{0.63, 0.73, 0.83\} \quad (5.20)$$

$$\mu_{high}(x) = \{0.81, 0.87, 0.93\} \quad (5.21)$$

$$\mu_{very\ high}(x) = \{0.92, 0.96, 1.00\} \quad (5.22)$$

### (2) BASIC EVENT FAILURE POSSIBILITY EVALUATION

There are four inputs for this process as described in Section 5.2. One of the inputs is the nuclear event failure possibility distribution, as in Eq. (5.15). The other three inputs are a set of seven experts' weights ($W$), as in Eq. (5.23), a set of 37 basic events of the CERPS fault tree ($B$), as in Eq. (5.24) and a matrix of expert subjective evaluation ($Y$) which are shown as a table in Table 5.2 to easily understand how each expert evaluates basic event failure possibilities.

$$W = \{w_i \mid i = 1,2,3, \ldots, 7 \text{ and } w_i = 1/7\} \quad (5.23)$$

$$B = \{b_i \mid i = 1,2, \ldots, 37 \text{ and } b_i \in FT(CERPS)\} \quad (5.24)$$

**Table 5.2 Expert justification results.**

| **Basic events** | **Basic event qualitative data assessed by experts** | | | | | | |
|---|---|---|---|---|---|---|---|
| | ***e₁*** | ***e₂*** | ***e₃*** | ***e₄*** | ***e₅*** | ***e₆*** | ***e₇*** |
| $b_1$ | *M* | *RL* | *M* | *RL* | *M* | *RL* | *RL* |
| $b_2$ | *RH* | *M* | *M* | *M* | *RH* | *M* | *RH* |
| $b_3$ | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* |
| $b_4$ | *RH* | *H* | *RH* | *H* | *RH* | *H* | *RH* |
| $b_5$ | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* |
| $b_6$ | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* | *VH* |
| $b_7$ | *RH* | *M* | *RH* | *M* | *M* | *M* | *M* |
| $b_8$ | *H* | *VH* | *H* | *VH* | *VH* | *H* | *H* |
| $b_9$ | *M* | *RH* | *M* | *M* | *RH* | *M* | *M* |
| $b_{10}$ | *M* | *RL* | *M* | *M* | *RL* | *RL* | *RL* |
| $b_{11}$ | *RH* | *RH* | *RH* | *RH* | *M* | *RH* | *M* |
| $b_{12}$ | *L* | *L* | *RL* | *L* | *RL* | *RL* | *L* |
| $b_{13}$ | *L* | *L* | *RL* | *RL* | *RL* | *L* | *L* |
| $b_{14}$ | *L* | *RL* | *L* | *RL* | *L* | *RL* | *RL* |
| $b_{15}$ | *RL* | *RL* | *RL* | *RL* | *RL* | *RL* | *M* |
| $b_{16}$ | *M* | *RL* | *M* | *M* | *M* | *M* | *M* |
| $b_{17}$ | *M* | *RL* | *M* | *M* | *RL* | *M* | *M* |
| $b_{18}$ | *M* | *RL* | *RL* | *M* | *RL* | *M* | *M* |
| $b_{19}$ | *RL* | *RL* | *M* | *RL* | *RL* | *RL* | *RL* |
| $b_{20}$ | *RL* | *L* | *RL* | *RL* | *RL* | *L* | *RL* |
| $b_{21}$ | *L* | *RL* | *L* | *RL* | *L* | *L* | *RL* |
| $b_{22}$ | *H* | *RH* | *RH* | *RH* | *RH* | *RH* | *RH* |
| $b_{23}$ | *M* | *RH* | *RH* | *M* | *RH* | *M* | *M* |
| $b_{24}$ | *M* | *RH* | *M* | *RH* | *M* | *RH* | *M* |
| $b_{25}$ | *M* | *M* | *M* | *M* | *RL* | *M* | *M* |
| $b_{26}$ | *RL* | *RL* | *RL* | *M* | *RL* | *RL* | *L* |
| $b_{27}$ | *L* | *L* | *RL* | *L* | *L* | *RL* | *M* |
| $b_{28}$ | *M* | *M* | *M* | *M* | *RL* | *RL* | *M* |
| $b_{29}$ | *RL* | *RL* | *RL* | *M* | *RL* | *M* | *RL* |
| $b_{30}$ | *RL* | *M* | *RL* | *RL* | *L* | *RL* | *RL* |
| $b_{31}$ | *RL* | *RL* | *RL* | *RL* | *RL* | *RL* | *L* |
| $b_{32}$ | *L* | *VL* | *L* | *L* | *L* | *L* | *L* |
| $b_{33}$ | *L* | *L* | *L* | *L* | *L* | *RL* | *L* |
| $b_{34}$ | *L* | *L* | *L* | *L* | *L* | *L* | *VL* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $b_{35}$ | *L* | *RL* | *L* | *RL* | *L* | *L* | *L* |
| $b_{36}$ | *L* | *L* | *RL* | *L* | *L* | *L* | *L* |
| $b_{37}$ | *RL* | *RL* | *RL* | *RL* | *RL* | *RL* | *RL* |

Those justification results in Table 5.2 are just of illustrative character of experts to obtain the closest match failure rates to the known best estimate values.

The output of this process is generated using Eq. (5.7). For example, the qualitative data for basic events $b_1 - b_5$ and $b_{33} - b_{37}$ are shown in Eq. (5.25). The qualitative data for other basic events in *B* are generated with the same processes.

$$Ql = \begin{bmatrix} M & RL & M & RL & M & RL & RL \\ RH & M & M & M & RH & M & RH \\ VH & VH & VH & VH & VH & VH & VH \\ RH & H & RH & H & RH & H & RH \\ VH & VH & VH & VH & VH & VH & VH \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ L & L & L & L & L & RL & L \\ L & L & L & L & L & L & VL \\ L & RL & L & RL & L & L & L \\ L & L & RL & L & L & L & L \\ RL & RL & RL & RL & RL & RL & RL \end{bmatrix} \tag{5.25}$$

(3) FUZZIFICATION PROCESS

Using Eqs. (5.16-5.22), the matrix *Ql* in Eq. (5.25) can be transformed into the corresponding quantitative data *Qn,* as in Eq. (5.26).

$$Qn = \begin{bmatrix} \mu_M(x) & \mu_{RL}(x) & \mu_M(x) & \mu_{RL}(x) & \mu_M(x) & \mu_{RL}(x) & \mu_{RL}(x) \\ \mu_{RH}(x) & \mu_M(x) & \mu_M(x) & \mu_M(x) & \mu_{RH}(x) & \mu_M(x) & \mu_{RH}(x) \\ \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) \\ \mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) \\ \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) \\ \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_{VL}(x) \\ \mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) \\ \mu_L(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) \\ \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) \end{bmatrix} \tag{5.26}$$

Using (5.10), for example, the final membership functions for basic events $b_1$ – $b_5$ and $b_{33}$ – $b_{37}$ shown in Eq. (5.27) are generated as follows.

$$
\begin{bmatrix} \mu^{b_1}(x) \\ \mu^{b_2}(x) \\ \mu^{b_3}(x) \\ \mu^{b_4}(x) \\ \mu^{b_5}(x) \\ \vdots \\ \mu^{b_{33}}(x) \\ \mu^{b_{34}}(x) \\ \mu^{b_{35}}(x) \\ \mu^{b_{36}}(x) \\ \mu^{b_{37}}(x) \end{bmatrix}
=
\begin{bmatrix}
\mu_M(x) & \mu_{RL}(x) & \mu_M(x) & \mu_{RL}(x) & \mu_M(x) & \mu_{RL}(x) & \mu_{RL}(x) \\
\mu_{RH}(x) & \mu_M(x) & \mu_M(x) & \mu_M(x) & \mu_{RH}(x) & \mu_M(x) & \mu_{RH}(x) \\
\mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) \\
\mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) & \mu_H(x) & \mu_{RH}(x) \\
\mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) & \mu_{VH}(x) \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) \\
\mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_{VL}(x) \\
\mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) \\
\mu_L(x) & \mu_L(x) & \mu_{RL}(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) & \mu_L(x) \\
\mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x) & \mu_{RL}(x)
\end{bmatrix}
\times
\begin{bmatrix} 1/7 \\ 1/7 \\ 1/7 \\ 1/7 \\ 1/7 \\ 1/7 \\ 1/7 \end{bmatrix}
$$

$$
\begin{bmatrix} \mu^{b_1}(x) \\ \mu^{b_2}(x) \\ \mu^{b_3}(x) \\ \mu^{b_4}(x) \\ \mu^{b_5}(x) \\ \vdots \\ \mu^{b_{33}}(x) \\ \mu^{b_{34}}(x) \\ \mu^{b_{35}}(x) \\ \mu^{b_{36}}(x) \\ \mu^{b_{37}}(x) \end{bmatrix}
=
\begin{bmatrix} (0.25,0.37,0.49) \\ (0.47,0.60,0.73) \\ (0.92,0.96,1.00) \\ (0.71,0.79,0.87) \\ (0.92,0.96,1.00) \\ \vdots \\ (0.08,0.15,0.22) \\ (0.06,0.12,0.17) \\ (0.10,0.17,0.24) \\ (0.08,0.15,0.22) \\ (0.17,0.27,0.37) \end{bmatrix}
\tag{5.27}
$$

The final membership functions for other basic events in Table 5.3 are generated with the same procedures.

### (4) DEFUZZIFICATION PROCESS

By substituting Eq. (4.28) and Eq. (5.27) into Eq. (5.12), the failure possibility scores for basic events $b_1$ – $b_5$ and $b_{33}$ – $b_{37}$, for example, are generated as in Eq. (5.28).

$$\begin{bmatrix} R_s^{b_1} \\ R_s^{b_2} \\ R_s^{b_3} \\ R_s^{b_4} \\ R_s^{b_5} \\ \vdots \\ R_s^{b_{33}} \\ R_s^{b_{34}} \\ R_s^{b_{35}} \\ R_s^{b_{36}} \\ R_s^{b_{37}} \end{bmatrix} = \begin{bmatrix} ADT(0.25,0.37,0.49) \\ ADT(0.47,0.60,0.73) \\ ADT(0.92,0.96,1.00) \\ ADT(0.71,0.79,0.87) \\ ADT(0.92,0.96,1.00) \\ \vdots \\ ADT(0.08,0.15,0.22) \\ ADT(0.06,0.12,0.17) \\ ADT(0.10,0.17,0.24) \\ ADT(0.08,0.15,0.22) \\ ADT(0.17,0.27,0.37) \end{bmatrix} = \begin{bmatrix} 0.102619 \\ 0.178095 \\ 0.313333 \\ 0.249524 \\ 0.313333 \\ \vdots \\ 0.039048 \\ 0.029524 \\ 0.044762 \\ 0.039048 \\ 0.073333 \end{bmatrix} \tag{5.28}$$

The failure possibility scores for other basic events in Table 5.3 are generated with the same procedures.

### (5) Basic Event Fuzzy Failure Rate Generation

Using Eqs. (5.13-5.14), for example, the generated fuzzy failure rates for basic events $b_1 - b_5$ and $b_{33} - b_{37}$ are as follows.

$$\begin{bmatrix} R_s^{b_1} \\ R_s^{b_2} \\ R_s^{b_3} \\ R_s^{b_4} \\ R_s^{b_5} \\ \vdots \\ R_s^{b_{33}} \\ R_s^{b_{34}} \\ R_s^{b_{35}} \\ R_s^{b_{36}} \\ R_s^{b_{37}} \end{bmatrix} = \begin{bmatrix} 1.82\text{E-}5 \\ 1.48\text{E-}4 \\ 1.03\text{E-}3 \\ 4.77\text{E-}4 \\ 1.03\text{E-}3 \\ \vdots \\ 2.03\text{E-}7 \\ 4.26\text{E-}8 \\ 4.15\text{E-}7 \\ 2.03\text{E-}7 \\ 4.37\text{E-}6 \end{bmatrix} \tag{5.29}$$

The fuzzy failure rates for other basic events in Table 5.3 are generated with the same procedures.

**Table 5.3 Data generated by the fuzzy reliability approach.**

| Basic events | Final membership functions | Failure possibility scores | Failure rates |
|---|---|---|---|
| $b_1$ | (0.25, 0.37, 0.49) | 0.102619 | 1.82E-5 |
| $b_2$ | (0.47, 0.60, 0.73) | 0.178095 | 1.48E-4 |
| $b_3$ | (0.92, 0.96, 1.00) | 0.313333 | 1.03E-3 |
| $b_4$ | (0.71, 0.79, 0.87) | 0.249524 | 4.77E-4 |
| $b_5$ | (0.92, 0.96, 1.00) | 0.313333 | 1.03E-3 |
| $b_6$ | (0.92, 0.96, 1.00) | 0.313333 | 1.03E-3 |
| $b_7$ | (0.43, 0.57, 0.70) | 0.165952 | 1.14E-4 |
| $b_8$ | (0.86, 0.91, 0.96) | 0.294286 | 8.32E-4 |
| $b_9$ | (0.43, 0.57, 0.70) | 0.165952 | 1.14E-4 |
| $b_{10}$ | (0.25, 0.37, 0.49) | 0.102619 | 1.82E-5 |
| $b_{11}$ | (0.55, 0.66, 0.78) | 0.202381 | 2.32E-4 |
| $b_{12}$ | (0.11, 0.19, 0.27) | 0.050476 | 7.59E-7 |
| $b_{13}$ | (0.11, 0.19, 0.27) | 0.050476 | 7.59E-7 |
| $b_{14}$ | (0.13, 0.21, 0.29) | 0.05619 | 1.28E-6 |
| $b_{15}$ | (0.20, 0.30, 0.41) | 0.083095 | 7.54E-6 |
| $b_{16}$ | (0.32, 0.47, 0.61) | 0.131905 | 4.87E-5 |
| $b_{17}$ | (0.30, 0.43, 0.57) | 0.122143 | 3.63E-5 |
| $b_{18}$ | (0.27, 0.40, 0.53) | 0.112381 | 2.62E-5 |
| $b_{19}$ | (0.20, 0.30, 0.41) | 0.083095 | 7.54E-6 |
| $b_{20}$ | (0.14, 0.23, 0.32) | 0.061905 | 2.02E-6 |
| $b_{21}$ | (0.11, 0.19, 0.27) | 0.050476 | 7.59E-7 |
| $b_{22}$ | (0.66, 0.75, 0.84) | 0.234286 | 3.85E-4 |
| $b_{23}$ | (0.47, 0.60, 0.73) | 0.178095 | 1.48E-4 |
| $b_{24}$ | (0.47, 0.60, 0.73) | 0.178095 | 1.48E-4 |
| $b_{25}$ | (0.32, 0.47, 0.61) | 0.131905 | 4.87E-5 |
| $b_{26}$ | (0.18, 0.28, 0.38) | 0.077381 | 5.54E-6 |
| $b_{27}$ | (0.14, 0.22, 0.31) | 0.060238 | 1.78E-6 |
| $b_{28}$ | (0.30, 0.43, 0.57) | 0.122143 | 3.63E-5 |
| $b_{29}$ | (0.22, 0.34, 0.45) | 0.092857 | 1.21E-5 |
| $b_{30}$ | (0.18, 0.28, 0.38) | 0.077381 | 5.54E-6 |
| $b_{31}$ | (0.16, 0.25, 0.34) | 0.067619 | 3.04E-6 |
| $b_{32}$ | (0.06, 0.12, 0.17) | 0.029524 | 4.26E-8 |
| $b_{33}$ | (0.08, 0.15, 0.22) | 0.039048 | 2.03E-7 |
| $b_{34}$ | (0.06, 0.12, 0.17) | 0.029524 | 4.26E-8 |
| $b_{35}$ | (0.10, 0.17, 0.24) | 0.044762 | 4.15E-7 |
| $b_{36}$ | (0.08, 0.15, 0.22) | 0.039048 | 2.03E-7 |
| $b_{37}$ | (0.17, 0.27, 0.37) | 0.073333 | 4.37E-6 |

We can see from Table 5.3 that the proposed fuzzy reliability approach generates basic event fuzzy failure rates which have similar forms as the probabilistic failure rates.

## 5.4 EVALUATION

This section analyzes the basic event fuzzy failure rates generated by the proposed fuzzy reliability approach to verify the feasibility of the approach to evaluate basic events which do not have quantitative historical failure data for calculating their failure probabilities. Table 5.4 shows the basic event fuzzy failure rates generated by the approach and their known failure rates together with their relative errors to express the accuracy of the calculation. The relative errors are calculated using the generated and the best estimate failure rates.

**Table 5.4 Basic event failure rates**

| Basic events | Generated failure rates | Known failure rates | | | Relative errors |
|---|---|---|---|---|---|
| | | Lower bound | Best estimate | Upper bound | |
| $b_1$ | 1.82E-5 | 4.3E-6 | 1.8E-5 | 4.5E-5 | 0.009559 |
| $b_2$ | 1.48E-4 | 6.3E-6 | 1.5E-4 | 5.5E-4 | 0.016080 |
| $b_3$ | 1.03E-3 | 1.4E-4 | 1.1E-3 | 3.5E-3 | 0.067153 |
| $b_4$ | 4.77E-4 | 3.4E-5 | 5.0E-4 | 1.8E-3 | 0.045884 |
| $b_5$ | 1.03E-3 | 1.6E-3 | 7.6E-3 | 2.0E-2 | 0.864983 |
| $b_6$ | 1.03E-3 | 6.5E-4 | 2.7E-3 | 6.8E-3 | 0.619951 |
| $b_7$ | 1.14E-4 | 1.1E-5 | 1.1E-4 | 3.5E-4 | 0.040376 |
| $b_8$ | 8.32E-4 | 4.2E-4 | 8.4E-4 | 1.5E-3 | 0.009576 |
| $b_9$ | 1.14E-4 | 4.1E-5 | 1.3E-4 | 2.8E-4 | 0.119682 |
| $b_{10}$ | 1.82E-5 | 3.4E-7 | 1.7E-5 | 6.4E-5 | 0.068945 |
| $b_{11}$ | 2.32E-4 | 2.2E-5 | 2.6E-4 | 8.8E-4 | 0.107907 |
| $b_{12}$ | 7.59E-7 | 1.9E-7 | 1.0E-6 | 2.7E-6 | 0.240724 |
| $b_{13}$ | 7.59E-7 | 8.0E-8 | 7.1E-7 | 2.2E-6 | 0.069403 |
| $b_{14}$ | 1.28E-6 | 3.9E-7 | 1.1E-6 | 4.0E-5 | 0.163532 |
| $b_{15}$ | 7.54E-6 | 2.5E-7 | 8.7E-6 | 3.3E-5 | 0.133485 |
| $b_{16}$ | 4.87E-5 | 5.1E-6 | 5.4E-5 | 1.8E-4 | 0.097310 |
| $b_{17}$ | 3.63E-5 | 2.3E-6 | 3.7E-5 | 1.3E-4 | 0.019914 |
| $b_{18}$ | 2.62E-5 | 1.1E-6 | 2.6E-5 | 9.5E-5 | 0.006028 |

| | | | | | |
|---|---|---|---|---|---|
| $b_{19}$ | 7.54E-6 | 1.4E-7 | 7.2E-6 | 2.8E-5 | 0.047039 |
| $b_{20}$ | 2.02E-6 | 3.7E-8 | 1.7E-6 | 6.6E-6 | 0.189768 |
| $b_{21}$ | 7.59E-7 | 7.1E-9 | 7.7E-7 | 2.9E-6 | 0.013927 |
| $b_{22}$ | 3.85E-4 | 4.9E-5 | 3.8E-4 | 1.2E-3 | 0.012703 |
| $b_{23}$ | 1.48E-4 | 1.3E-5 | 1.7E-4 | 5.6E-4 | 0.131835 |
| $b_{24}$ | 1.48E-4 | 2.3E-5 | 1.4E-4 | 3.8E-4 | 0.054200 |
| $b_{25}$ | 4.87E-5 | 6.3E-6 | 5.7E-5 | 1.8E-4 | 0.144820 |
| $b_{26}$ | 5.54E-6 | 3.0E-7 | 5.0E-6 | 1.8E-5 | 0.107479 |
| $b_{27}$ | 1.78E-6 | 4.0E-8 | 1.5E-6 | 5.8E-6 | 0.186810 |
| $b_{28}$ | 3.63E-5 | 8.0E-6 | 3.7E-5 | 9.8E-5 | 0.019914 |
| $b_{29}$ | 1.21E-5 | 7.5E-7 | 1.0E-5 | 3.5E-5 | 0.205248 |
| $b_{30}$ | 5.54E-6 | 7.4E-7 | 5.0E-6 | 1.5E-5 | 0.107479 |
| $b_{31}$ | 3.04E-6 | 2.3E-7 | 2.5E-6 | 8.3E-6 | 0.214396 |
| $b_{32}$ | 4.26E-8 | 7.5E-10 | 3.6E-8 | 1.4E-7 | 0.182478 |
| $b_{33}$ | 2.03E-7 | 4.8E-9 | 1.6E-7 | 6.0E-7 | 0.267381 |
| $b_{34}$ | 4.26E-8 | 5.3E-10 | 4.3E-8 | 1.7E-7 | 0.010018 |
| $b_{35}$ | 4.15E-7 | 4.8E-9 | 4.7E-7 | 1.8E-6 | 0.117941 |
| $b_{36}$ | 2.03E-7 | 8.2E-10 | 2.0E-7 | 7.2E-7 | 0.013905 |
| $b_{37}$ | 4.37E-6 | 5.7E-7 | 4.8E-6 | 1.5E-5 | 0.089537 |

From Table 5.4, it can be seen that the relative errors for two basic events, i.e. $b_5$ and $b_6$, are still very big which are 0.865 and 0.620. The relative errors for other 35 basic events are between 0.006 and 0.267.

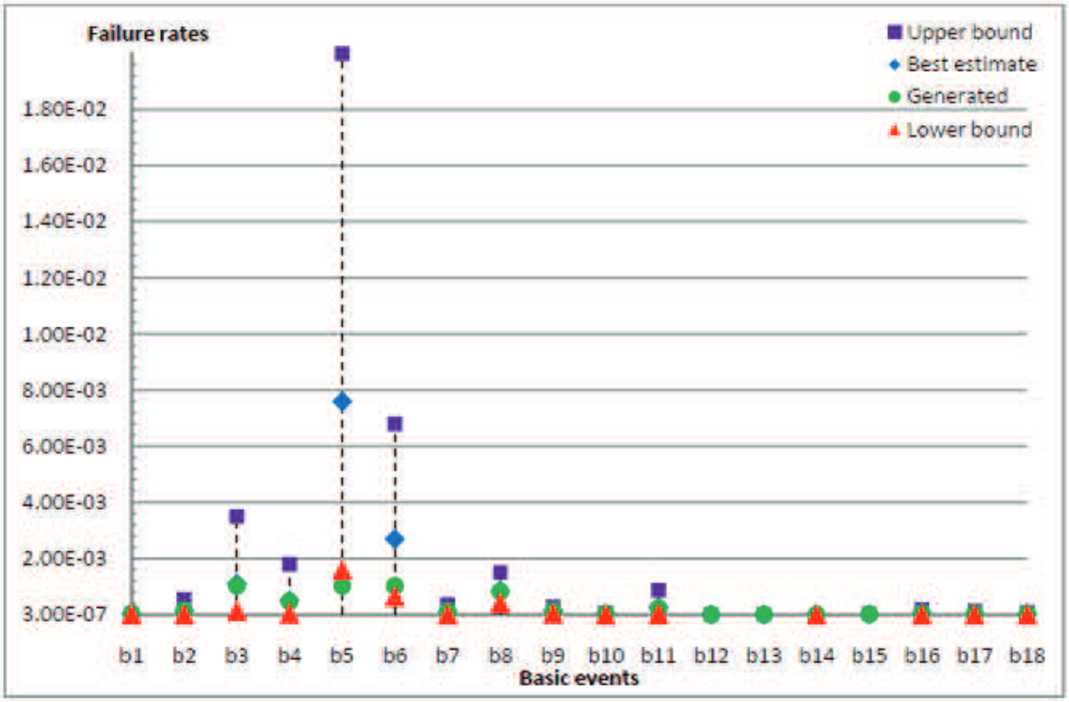


**Figure 5.4 Failure rate comparisons for basic events $b_1$ - $b_{18}$.**

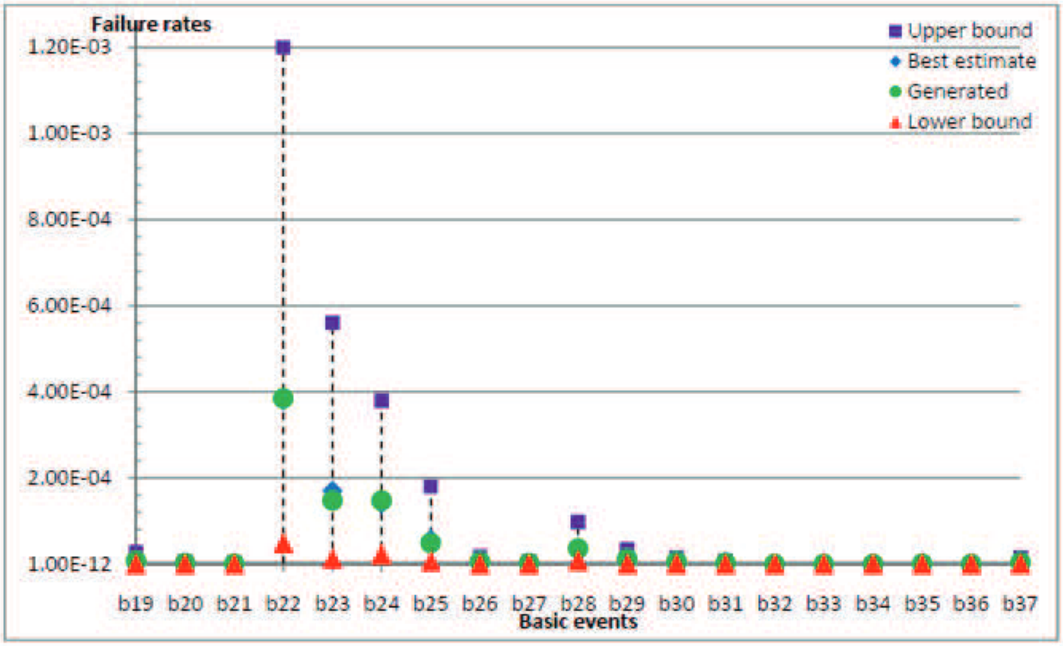


**Figure 5.5 Failure rate comparisons for basic events $b_{19}$ – $b_{37}$.**

In Figures 5.4-5.5, we can see that the failure rates generated by the proposed fuzzy reliability approach for the 35 basic events are very close to the best estimate reliability value collected from the operating experiences. However, the failure rates generated for the other two basic events, i.e. $b_5$ and $b_6$, are very close to the lower bound reliability values. These two exceptions might be caused by the incapability of the proposed approach to generate failure rates greater than *1.01E-03*. It will be interesting to see, in the future research, how the proposed fuzzy reliability approach will perform for different membership functions and/or different applications.

Generally, these results have demonstrated that the proposed fuzzy reliability approach can be feasibly used as an alternative approach for conventional probabilistic reliability approach to assess basic event failure rates. However, if the expertise disparities of the experts on the system under evaluation are very substantial, the weights amongst experts will be different and, consequently, the basic event failure possibilities justified by them will also be very different. This condition will cause the proposed approach generating higher relative errors. Hence, it is important to note that the selection of the experts to subjectively evaluate basic event failure possibilities will affect the generation of the basic event failure rates to some extents.

We also have to acknowledge that if basic events to be evaluated have historical failure data, conventional probabilistic reliability approach should be used. The calculation results of this conventional approach will represent the actual reliability of those basic events. On the other hand, if the subjective justification is the only method to evaluate basic event failures, the proposed fuzzy reliability approach offers a feasible and effective solution to generate basic event failure rates through the qualitative data processing. Experts can intuitively and easily use their expertise and working experience to evaluate basic event failure possibilities using qualitative linguistic values. From the illustrative character of the expert justification that we have done in this case study, the distribution of membership functions used in this experiment produce failure rates which are closely match with the actual failure rates.

## 5.5 SUMMARY

This chapter describes a fuzzy reliability approach to assess basic events of fault trees through qualitative data processing. Those data sets used in the case study are described in terms of nuclear event failure possibilities and mathematically represented by the membership functions of the fuzzy numbers, to characterize basic event failure likelihood. The key advantage of using linguistic values in system reliability assessment is that the developed approach can intuitively and easily accept expert opinions which otherwise cannot be represented by quantitative data. Using a case study, we demonstrated the performance of the approach by comparing the generated failure rates with the actual probabilistic failure rates collected from the operating experiences of the U.S. combustion engineering reactor protection system. The results show that the proposed fuzzy reliability approach offers a very good alternative approach to assess event reliability data when historical quantitative data is insufficient or unavailable to invoke the probabilistic approach.

Chapter 6

# AN INTELLIGENT FAULT TREE ANALYSIS SYSTEM FOR NUCLEAR POWER PLANT SAFETY ASSESSMENT

## 6.1 INTRODUCTION

Fault tree analysis provides a comprehensive and structured approach to identify and understand key plant vulnerabilities, to develop accident scenarios, to assess the level of plant safety, and to derive numerical estimates of potential risks. Due to the complexity of fault tree analysis, a number of personal computer-based software systems have been developed. However, they only accept basic event failure rates which are expressed in numerical values (Hamada et al. 2004). In real-world applications such as nuclear engineering systems, basic events may not have historical failure data for estimating their failure probabilities and only expert subjective opinions, which are expressed in qualitative failure possibilities, can be obtained.

In this chapter, newly developed fault tree analysis software called Intelligent Fault Tree Analysis System for Nuclear Safety Assessment (InFaTAS-NuSA), which can accept not only quantitative failure probabilities but also qualitative failure possibilities, is introduced. All the necessary primary features for fault tree analysis have been implemented in friendly graphical user interfaces. To verify the accuracy and effectiveness of the developed software system, a case study is performed and the results are compared with the results obtained from a well-known reliability software package, i.e. SAPHIRE (Wierman et al. 2001).

The rest of the chapter is organized as follows. The general specifications of the InFaTAS-NuSA are briefly presented in Section 6.2. Section 6.3 describes its main features and an algorithm to subjectively assess nuclear event failures is given in Section 6.4. A real world application to demonstrate the applicability of the InFaTAS-NuSA is described in detail in Section 6.5. The results of the case study are evaluated in Section 6.6. Finally, the chapter is summarized in Section 6.7. The work presented in this chapter has been reported in one of our publications listed in Section 1.7, i.e. publication number 6.

## 6.2 General Specifications

The current version of InFaTAS-NuSA has implemented the primary features of fault tree analysis, such as basic events, intermediate events, transfer pages, and “AND” and “OR” Boolean gates. It also has the capability for expansion and can be easily improved for complex fault trees.

Minimal cut set evaluations as well as their importance measures and basic event Fussell-Vesely importance measures have also been implemented in the system. The basic structure of InFaTAS-NuSA is shown in Figure 6.1.

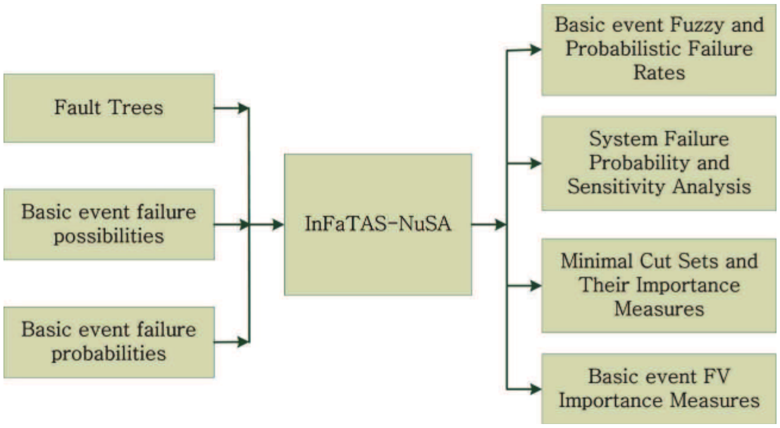

Fault Trees
Basic event failure possibilities
Basic event failure probabilities
InFaTAS-NuSA
Basic event Fuzzy and Probabilistic Failure Rates
System Failure Probability and Sensitivity Analysis
Minimal Cut Sets and Their Importance Measures
Basic event FV Importance Measures

**Figure 6.1 Basic structure of InFaTAS-NuSA.**

InFaTAS-NuSA provides a number of graphical interfaces to enable users to conduct a variety of analyses, namely:

(1) to build the fault tree of the system under evaluation;

(2) to enter basic event qualitative failure possibilities. This feature is provided for basic events in which expert subjective justifications offer the only method for evaluating their failures;

(3) to enter the basic event quantitative failure probabilities. This feature is provided for basic events which have historical failure data;

(4) to generate basic event quantitative fuzzy failure rates from their corresponding qualitative failure possibilities;

(5) to calculate system failure probability and system sensitivity to the variations of basic event failure possibilities;

(6) to evaluate minimal cut sets and their importance measures;

(7) to evaluate the Fussell-Vesely importance measures of basic events;

(8) to generate reports as needed.

## 6.3 MAIN FEATURES

InFaTAS-NuSA is the realization of the intelligent hybrid fault tree analysis framework explained in Chapter 3. This section briefly describes the eight main features of InFaTAS-NuSA.

### (1) NUCLEAR EVENT QUALITATIVE DATA

The objective of the implementation of the nuclear event qualitative data into the new developed system is to deal with nuclear events which do not have historical failure data to estimate their failure probabilities. Seven terms of qualitative failure possibilities to represent nuclear event qualitative data have been developed and described in details in Chapter 4. The nuclear event failure possibilities in Eq. (4.12) are realized in InFaTAS-NuSA to enable experts to subjectively evaluate nuclear event failures that do not have historical failure data, but expert subjective opinions are the only method to obtain their failures.

### (2) FAILURE POSSIBILITY MEMBERSHIP FUNCTIONS

The objective of the implementation of the failure possibility membership functions into the new developed system is to mathematically represent nuclear event qualitative data. The membership functions of triangular fuzzy numbers have been developed and described in details in Chapter 4 to mathematically represent nuclear event failure possibilities. The membership functions given in Eqs. (4.13-4.19) are realized in InFaTAS-NuSA to enable safety analysts to mathematically evaluate the failure probability of the undesired top event of a fault tree in which its basic event failures are subjectively assessed by experts using qualitative failure possibilities.

### (3) NUCLEAR EVENT FINAL MEMBERSHIP FUNCTION

The objective of the calculation of the nuclear event final membership function is to aggregate different expert opinions on the same nuclear events. The aggregation method given in Eq. (5.10) is realized in InFaTAS-NuSA to accommodate the weight of each expert involving in the basic event assessment.

### (4) NUCLEAR EVENT FAILURE POSSIBILITY SCORE

The objective of the calculation of the nuclear event failure possibility score is to express the most-valued expert belief that a nuclear event may fail. The defuzzification process given in Eq. (5.12) is realized in InFaTAS-NuSA. Meanwhile, the details of the area defuzzification technique applied in Eq. (5.12) are described in Chapter 4.

### (5) NUCLEAR EVENT FUZZY FAILURE RATE

The objective of the fuzzy failure rate generation is to convert nuclear event qualitative data, which have been provided by experts for each nuclear event of the fault trees under evaluation, into their corresponding quantitative fuzzy failure rates, whose forms are similar to the forms of nuclear event failure probabilities. Therefore, this feature will enable nuclear event qualitative failure possibilities to be integrated into the quantitative phase on fault tree analysis. The formula to generate nuclear event fuzzy failure rate given in Eq. (5.14) is realized in InFaTAS-NuSA.

### (6) MINIMAL CUT SET IMPORTANCE MEASURE

The objective of this feature is to evaluate the contribution percentage of every single minimal cut set to the occurrence of the top event failure. The formula given in Eq. (3.4) is realized in InFaTAS-NuSA to rank the impact of every single minimal cut set to the occurrence of the top event failure.

### (7) BASIC EVENT FUSSELL-VESELY IMPORTANCE MEASURE

The objective of this feature is to evaluate the contribution of every basic event to the failure occurrence of the top event. The formula given in Eq. (3.3) is realized in InFaTAS-NuSA to evaluate the contribution of basic events to the occurrence of the top event failure for risk reduction indicator. This measure is used to order component criticality. Basic event with the highest contributor is the most critical component. On the other hand, basic event with the lowest contributor is the least critical component for the system being evaluated.

### (8) TOP EVENT SENSITIVITY ANALYSIS

Since different experts may evaluate the same events as having different failure possibilities, these differences will off course, affect the calculation of the basic event fuzzy failure rates and also contribute to the top event failure probability calculation. By considering basic event failure possibility variations, top event sensitivity needs to be analyzed by generating the lower bound and the upper bound failure rates using the lowest and highest failure possibilities given by the experts. For example, if the failure possibilities of the basic event *A* are subjectively assessed by five experts as {*low, reasonably low, low, moderate, low*}, then the lower bound failure rate is generated using these failure possibilities "{*low, low, low, low, low*}" and the upper bound failure rate is generated using these failure possibilities "(*moderate, moderate, moderate, moderate, moderate*}". These two failure rates are then used to generate the failure probability range of the top event to find a sensitivity spectrum of the top event to the variations of basic event failure possibilities. This method is realized in InFaTAS-NuSA to analyze the sensitivity of the top event to the variations of the basic event failure possibilities provided by experts.

## 6.4 NUCLEAR EVENT ASSESSMENT ALGORITHM

Nuclear event failures are assessed in InFaTAS-NuSA after the system fault tree has been completed and before it is analyzed to estimate the top event failure probability. A nuclear event assessment algorithm to subjectively evaluate nuclear events of the system fault tree in InFaTAS-NuSA using qualitative failure possibilities described in Chapter 4 is as follows.

```
Ask for expert justification weights
    totalWeight = 0
    noExpert = 0
    WHILE still experts $\boldsymbol{e_j}$
        Read justification weight $\boldsymbol{w_j}$
        totalWeight = totalWeight + $\boldsymbol{w_j}$
        noExpert = noExpert + 1
    END WHILE
Normalize justification weight for each expert
    FOR $\boldsymbol{i}$ = 1 to noExpert
        $\boldsymbol{w_i} = \frac{w_i}{\text{totalWeight}}$
    END FOR
Evaluate basic events
    WHILE still basic events $\boldsymbol{b_i}$
        IF $\boldsymbol{b_i}$ has historical failure probability distribution
            Enter its ***lower bound***, ***best estimate*** and ***upper bound*** failure probabilities
        ELSE
            WHILE still experts $\boldsymbol{e_j}$
                Read failure possibility $\boldsymbol{h_k^{e_j b_i}}$ given by the expert $e_j$
                Find the left endpoint $\boldsymbol{x_{1k}^{e_j}}$, the core $\boldsymbol{x_{2k}^{e_j}}$ and the right endpoint $\boldsymbol{x_{3k}^{e_j}}$ of the
                corresponding membership function $\boldsymbol{\mu_k}$
                    IF $\boldsymbol{h_k^{e_j b_i}} = \boldsymbol{h_1}$ THEN $\boldsymbol{x_{1k}^{e_j}} = 0.00; \boldsymbol{x_{2k}^{e_j}} = 0.04; \boldsymbol{x_{3k}^{e_j}} = 0.08$
                    ELSE IF $\boldsymbol{h_k^{e_j b_i}} = \boldsymbol{h_2}$ THEN $\boldsymbol{x_{1k}^{e_j}} = 0.07; \boldsymbol{x_{2k}^{e_j}} = 0.13; \boldsymbol{x_{3k}^{e_j}} = 0.19$
                    ELSE IF $\boldsymbol{h_k^{e_j b_i}} = \boldsymbol{h_3}$ THEN $\boldsymbol{x_{1k}^{e_j}} = 0.17; \boldsymbol{x_{2k}^{e_j}} = 0.27; \boldsymbol{x_{3k}^{e_j}} = 0.37$
        ELSE IF $\boldsymbol{h}_k^{e_j b_i} = \boldsymbol{h}_4$ THEN $\boldsymbol{x}_{1k}^{e_j} = 0.35; \boldsymbol{x}_{2k}^{e_j} = 0.50; \boldsymbol{x}_{3k}^{e_j} = 0.65$
        ELSE IF $\boldsymbol{h}_k^{e_j b_i} = \boldsymbol{h}_5$ THEN $\boldsymbol{x}_{1k}^{e_j} = 0.63; \boldsymbol{x}_{2k}^{e_j} = 0.73; \boldsymbol{x}_{3k}^{e_j} = 0.83$
        ELSE IF $\boldsymbol{h}_k^{e_j b_i} = \boldsymbol{h}_6$ THEN $\boldsymbol{x}_{1k}^{e_j} = 0.81; \boldsymbol{x}_{2k}^{e_j} = 0.87; \boldsymbol{x}_{3k}^{e_j} = 0.93$
        ELSE IF $\boldsymbol{h}_k^{e_j b_i} = \boldsymbol{h}_7$ THEN $\boldsymbol{x}_{1k}^{e_j} = 0.92; \boldsymbol{x}_{2k}^{e_j} = 0.96; \boldsymbol{x}_{3k}^{e_j} = 1.00$
    END WHILE
    Calculate the final membership function $\boldsymbol{\mu}^{\boldsymbol{b_i}}(\boldsymbol{x}) = (\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3)$
      FOR $\boldsymbol{i}$ = 1 to 3
        $\boldsymbol{x}_l = \sum_{k=1}^{7} \sum_{j=1}^{noExpert} (\boldsymbol{w}_j \times \boldsymbol{x}_{lk}^{e_j})$
      END FOR
    Calculate the $\boldsymbol{b}^i$ event failure possibility score $\boldsymbol{R}_S^{\boldsymbol{b_i}}$
      $\boldsymbol{R}_s^{\boldsymbol{b_i}} = \frac{1}{18}(4\boldsymbol{x}_1 + \boldsymbol{x}_2 + \boldsymbol{x}_3)$
    Calculate the $\boldsymbol{b}^i$ event fuzzy failure rate $\boldsymbol{R}^{\boldsymbol{b_i}}$
      IF $\boldsymbol{R}_S^{\boldsymbol{b_i}} = \boldsymbol{0}$ THEN $\boldsymbol{R}^{\boldsymbol{b_i}} = \boldsymbol{0}$
      ELSE $\boldsymbol{R}^{\boldsymbol{b_i}} = \frac{1}{10^{\left[\frac{1-R_S^{b_i}}{R_S^{b_i}}\right]^{1/3} \times 2.301}}$
  END WHILE
END
```

$e_j$ is the $j^{th}$ expert in Eq. (5.4), $w_j$ is the justification weight of the expert $e_j$ ($0 < w_j \leq 1$) in Eq. (5.5), $b_i$ is the $i^{th}$ basic event in the fault tree in Eq. (5.3), and $h_k^{e_j b_i}$ is the $k^{th}$ failure possibility in Eq. (4.12) evaluated by the expert $e_j$ for the basic event $b_i$.

## 6.5 Real World Application

The model of the reactor protection system of the U.S. combustion engineering pressurized water reactor Group 1 will be evaluated by the developed InFaTAS-NuSA. To verify the effectiveness and applicability of InFaTAS-NuSA, the evaluation results will be compared with those of the same system generated by SAPHIRE which is well documented in Wierman et al. (2001).

### 6.5.1 PROBLEM DESCRIPTION

The RPS is one of many safety systems in nuclear power plants, which is designed to perform safe shutdown of the reactor by inserting control rod clusters into the reactor core to immediately terminate nuclear reaction, so that heat generation in the core can be eliminated. With the help of other safety systems, the integrity of the fuel and the reactor coolant pressure boundary can be maintained.

The combustion engineering reactor protection system (CERPS) comprises numerous electronic and mechanical components to produce an automatic and manual rapid reactor trip. The first model of this CERPS, which is used in this case study, consists of four channels to measure parameter plants, six trip matrices to trip the reactor trip switch gear, trip breakers to interrupt power to the control element assembly drive mechanism (CEDM) allowing gravity to insert the control rod assembly into the reactor core, and a group of control rods which will de-energized on successful CERPS actuation. The simplified diagram of this CERPS is shown in Figure 6.2.

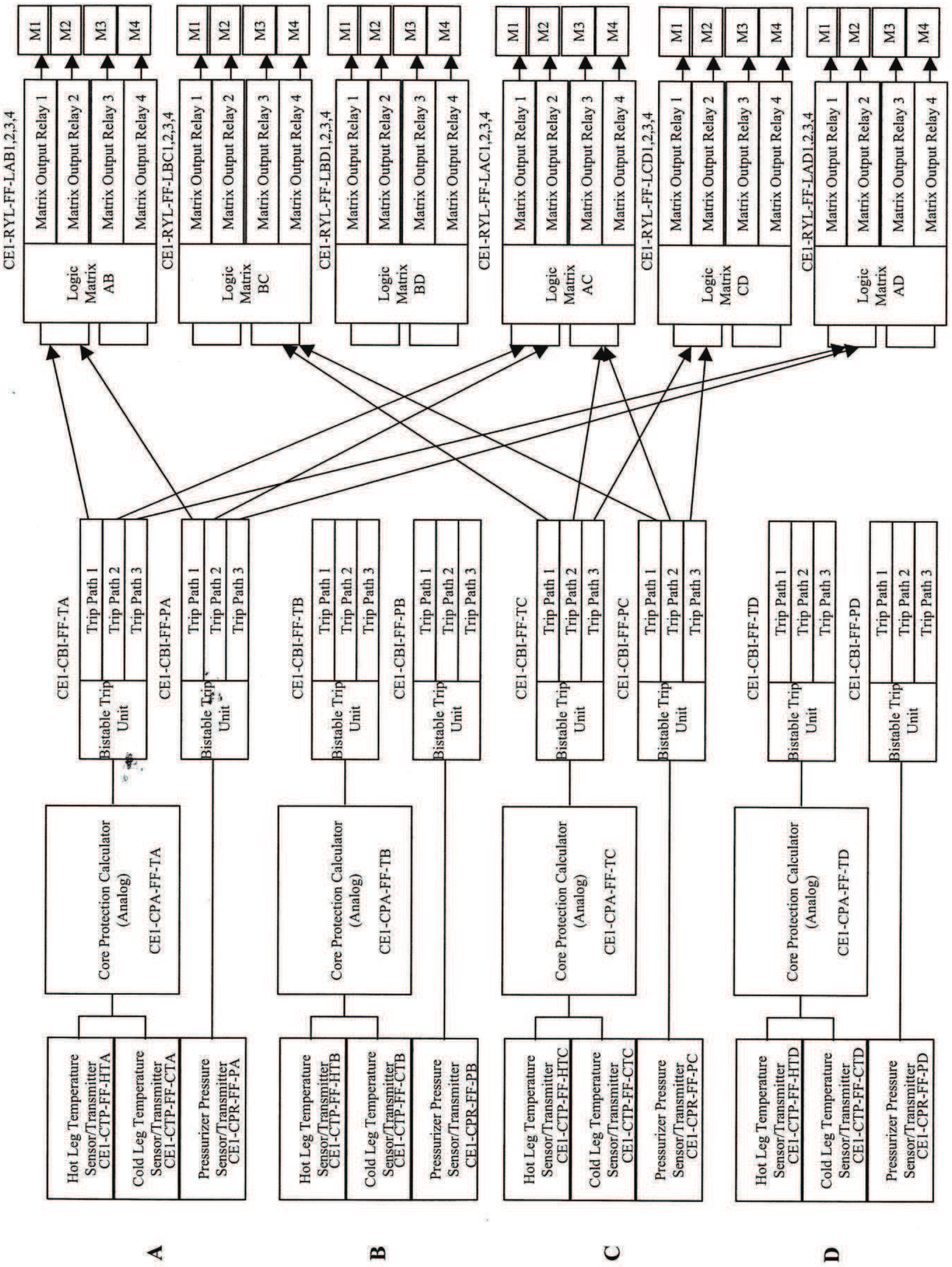

A
B
C
D
Hot Leg Temperature Sensor/Transmitter CE1-CTP-FF-HTA
Cold Leg Temperature Sensor/Transmitter CE1-CTP-FF-CTA
Pressurizer Pressure Sensor/Transmitter CE1-CPR-FF-PA
Core Protection Calculator (Analog) CE1-CPA-FF-TA
CE1-CBI-FF-TA
CE1-CBI-FF-PA
Bistable Trip Unit
Trip Path 1
Trip Path 2
Trip Path 3
Hot Leg Temperature Sensor/Transmitter CE1-CTP-FF-HTB
Cold Leg Temperature Sensor/Transmitter CE1-CTP-FF-CTB
Pressurizer Pressure Sensor/Transmitter CE1-CPR-FF-PB
Core Protection Calculator (Analog) CE1-CPA-FF-TB
CE1-CBI-FF-TB
CE1-CBI-FF-PB
Hot Leg Temperature Sensor/Transmitter CE1-CTP-FF-HTC
Cold Leg Temperature Sensor/Transmitter CE1-CTP-FF-CTC
Pressurizer Pressure Sensor/Transmitter CE1-CPR-FF-PC
Core Protection Calculator (Analog) CE1-CPA-FF-TC
CE1-CBI-FF-TC
CE1-CBI-FF-PC
Hot Leg Temperature Sensor/Transmitter CE1-CTP-FF-HTD
Cold Leg Temperature Sensor/Transmitter CE1-CTP-FF-CTD
Pressurizer Pressure Sensor/Transmitter CE1-CPR-FF-PD
Core Protection Calculator (Analog) CE1-CPA-FF-TD
CE1-CBI-FF-TD
CE1-CBI-FF-PD
CE1-RYL-FF-LAB1,2,3,4
Logic Matrix AB
CE1-RYL-FF-LBC1,2,3,4
Logic Matrix BC
CE1-RYL-FF-LBD1,2,3,4
Logic Matrix BD
CE1-RYL-FF-LAC1,2,3,4
Logic Matrix AC
CE1-RYL-FF-LCD1,2,3,4
Logic Matrix CD
CE1-RYL-FF-LAD1,2,3,4
Logic Matrix AD
Matrix Output Relay 1
Matrix Output Relay 2
Matrix Output Relay 3
Matrix Output Relay 4
M1
M2
M3
M4

**Figure 6.2 Simplified diagram of the CERPS Group 1 (Wierman et al. 2001).**

To successfully perform its functions, the CERPS has to be able to insert 20 percent or more of the shutdown rods into the reactor core in the event of plant upset conditions requiring nuclear reaction termination. The failure of this system to rapidly insert of control rods into the reactor core to stop the nuclear reaction is set as the top event of the CERPS fault tree for this case study. This system failure has been evaluated using SAPHIRE and the results are well documented in Wierman et al. (2001). These results will be used to benchmark the results generated by InFaTAS-NuSA.

### 6.5.2 CERPS ANALYSIS USING InFaTAS-NuSA

Recommended procedures for using InFaTAS-NuSA for assessing the safety system of a nuclear power plant is as follows.

(1) Create a new project
(2) Construct the system fault tree
(3) Determine the number of experts who will subjectively evaluate basic events and assign justification weights to each expert
(4) Evaluate the failure possibilities of basic events
(5) Generate the failure rates of basic events
(6) Evaluate minimal cut sets and calculate their failure probabilities
(7) Calculate the top event failure probability
(8) Evaluate the importance measures of minimal cut sets
(9) Evaluate the FV importance measures of basic events
(10) Generate reports as needed
(11) Save the project for later use

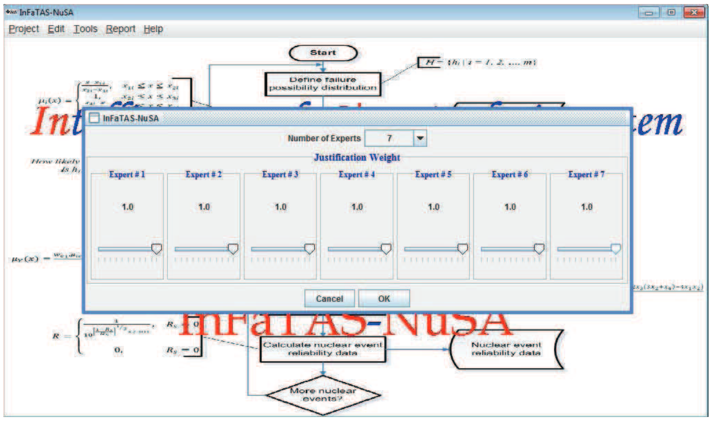
We group these procedures into three main categories: inputs, analyses and reports. Each main category has its own steps described in the sub-section below.

## (1) INPUTS

**Step 1: New project creation**. In this step, users have to provide a name for the project to store information about the fault tree structures, basic event failure possibilities, basic event probabilistic failure rates, and expert justification weights. To be easily identified from other files, InFaTAS-NuSA will add .IFTA as the extension for the given project name.

**Step 2: System fault tree construction**. System fault trees are sequentially developed from the top event to the lowest events based on sub-tree aggregation. A sub-tree is a simple fault tree, which only consists of one top event, one Boolean gate, several bottom events and transfer gates to connect the sub-trees. InFaTAS-NuSA will automatically detect any bottom event in any sub-tree that does not have a connection to other sub-trees and will generate an error if that bottom event is not a basic event.

**Step 3: Experts and their justification weights**. In this case study, let us assume that the higher management level assigns seven experts with the same level of expertise on the CERPS. All seven experts will be given the justification weight of 1, as shown in Figure 6.3.


InFaTAS-NuSA
Project Edit Tools Report Help
Start
Define failure possibility distribution
Calculate nuclear event reliability data
Nuclear event reliability data
More nuclear events?
InFaTAS-NuSA
Cancel
OK

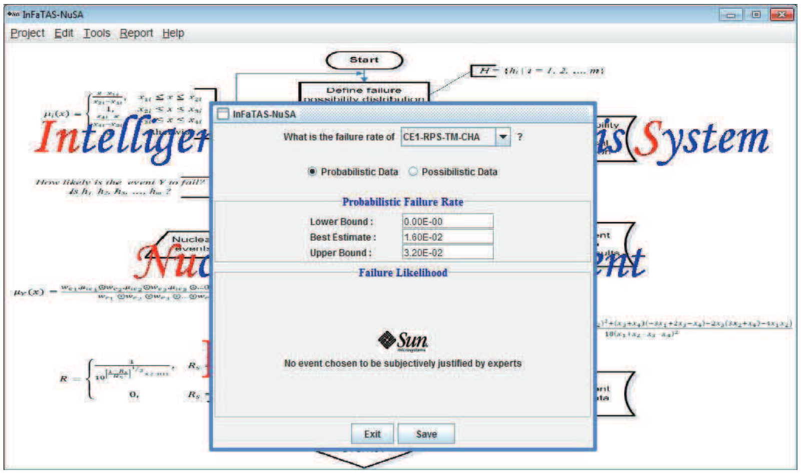
Number of Experts 7

Justification Weight

| Expert # 1 | Expert # 2 | Expert # 3 | Expert # 4 | Expert # 5 | Expert # 6 | Expert # 7 |
|---|---|---|---|---|---|---|
| 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 |

**Figure 6.3 User interface to input the number of experts and their corresponding justification weights.**

**Step 4: Basic event evaluations**. In this step, any basic events identified in Step 2 will be split into two groups: probability groups and possibility groups. When users categorize a basic event into the probability group, they have to provide three values of the basic event failure probabilities, i.e. a lower bound value, a best estimate value and an upper bound value, as shown in Figure 6.4. This group is provided for basic events which have historical failure data. The second group is provided for basic events whose failures are subjectively evaluated by the experts given in Step 3, using failure possibilities expressed in qualitative linguistic values, as shown in Figure 6.5. In this case study, let us assume that basic events in Table 6.1 do not have historical failure data and that their failure possibilities are subjectively evaluated by experts. Meanwhile, basic events that have historical failure data are given in Table 6.2. The details of the subjective evaluation results for those basic events in Table 6.1 are given in Table 6.3.


InFaTAS-NuSA
Project Edit Tools Report Help
Start
Define failure possibility distribution
Intelligen
s System
Nuc
nt
Sun
Exit
Save

InFaTAS-NuSA

What is the failure rate of CE1-RPS-TM-CHA ?

● Probabilistic Data ○ Possibilistic Data

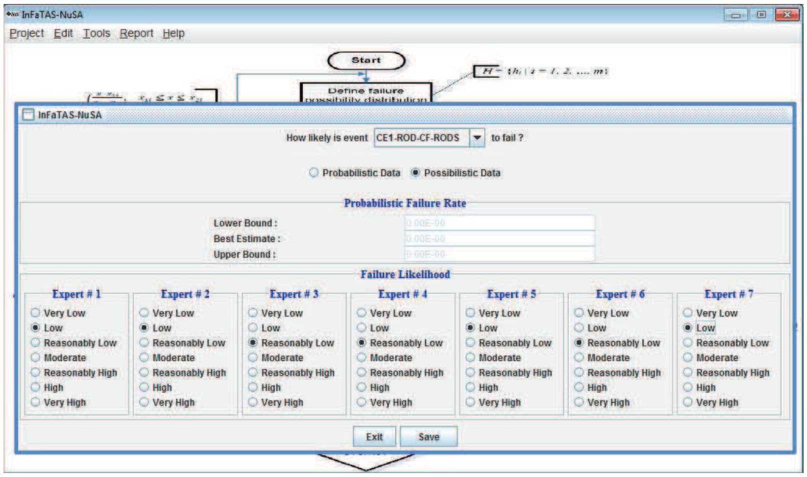
Probabilistic Failure Rate

Lower Bound : 0.00E-00
Best Estimate : 1.60E-02
Upper Bound : 3.20E-02

Failure Likelihood

No event chosen to be subjectively justified by experts

**Figure 6.4 User interface to enter basic event failure probabilities.**


InFaTAS-NuSA
Project Edit Tools Report Help
Start
Define failure possibility distribution
Exit
Save

InFaTAS-NuSA

How likely is event CE1-ROD-CF-RODS to fail ?

○ Probabilistic Data ● Possibilistic Data

Probabilistic Failure Rate

Lower Bound : 0.00E-00
Best Estimate : 0.00E-00
Upper Bound : 0.00E-00

Failure Likelihood

| Expert # 1 | Expert # 2 | Expert # 3 | Expert # 4 | Expert # 5 | Expert # 6 | Expert # 7 |
|---|---|---|---|---|---|---|
| ○ Very Low | ○ Very Low | ○ Very Low | ○ Very Low | ○ Very Low | ○ Very Low | ○ Very Low |
| ● Low | ● Low | ○ Low | ○ Low | ● Low | ○ Low | ● Low |
| ○ Reasonably Low | ○ Reasonably Low | ● Reasonably Low | ● Reasonably Low | ○ Reasonably Low | ● Reasonably Low | ○ Reasonably Low |
| ○ Moderate | ○ Moderate | ○ Moderate | ○ Moderate | ○ Moderate | ○ Moderate | ○ Moderate |
| ○ Reasonably High | ○ Reasonably High | ○ Reasonably High | ○ Reasonably High | ○ Reasonably High | ○ Reasonably High | ○ Reasonably High |
| ○ High | ○ High | ○ High | ○ High | ○ High | ○ High | ○ High |
| ○ Very High | ○ Very High | ○ Very High | ○ Very High | ○ Very High | ○ Very High | ○ Very High |

**Figure 6.5 User interface to enter basic event failure possibilities.**

**Table 6.1 CERPS fault tree basic events to be evaluated using qualitative failure possibilities.**

| Basic event name | Description |
|---|---|
| CE1-CBI-FF-PA,B,C,D<br>CE1-CBI-FF-TA,B,C,D | Channel trip unit (bi-stable) fails to trip at its set point |
| CE1-CPA-FF-TA,B,C,D | Channel analog core protection calculator fails to send a signal to the trip unit |
| CE1-CPR-FF-PA,B,C,D | Channel reactor vessel pressure sensor/ transmitter fails to detect a high pressure and sends a signal to the trip unit |
| CE1-CTP-FF-CTA,B,C,D<br>CE1-CTP-FF-HTA,B,C,D | Channel reactor vessel temperature/ transmitter (cold or hot leg) fails to detect a low level and sends a signal to the trip unit |
| CE1-MSW-FF-MT1,2 | Manual scram switch fails to operate upon demand |
| CE1-RYL-FF-LA,B,C,D–1,2,3,4 | Channel logic relay fails to de-energize upon demand |
| CE1-RYT-FF-ICM1,2,3,4 | Trip system trip relay fails to de-energize upon demand |
| CE1-CBI-CF-P(T)2OF3TM | Common cause failure specific 2 of 3 bi-stables associated with either a pressure (P) or temperature (T) signal (T&M) |
| CE1-CBI-CF-P(T)3OF4 | Common cause failure specific 3 of 4 bi-stables associated with either a pressure (P) or temperature (T) signal |
| CE1-CBI-CF-4OF6TM | Common cause failure specific 4 of 6 bi-stables (T&M) |
| CE1-CBI-CF-6OF8 | Common cause failure specific 6 of 8 bi-stables |
| CE1-CPA-CF-T2OF3TM | Common cause failure 2 of 3 analog core protection calculators (T&M) |
| CE1-CPA-CF-T3OF4 | Common cause failure 3 of 4 analog core protection calculators |
| CE1-CPR-CF-P2OF3TM | Common cause failure 2 of 3 pressure sensor/ transmitters (T&M) |
| CE1-CPR-CF-P3OF4 | Common cause failure 3 of 4 pressure sensor/ transmitters |
| CE1-CTP-CF-C(H)T2OF3TM | Common cause failure 2 of 3 temperature sensor/ transmitters (T&M) |
| CE1-CTP-CF-C(H)T3OF4 | Common cause failure 3 of 4 temperature sensor/ transmitters |
| CE1-ROD-CF-RODS | Common cause failure 20% or more CRD/rods fail to insert |
| CE1-RYL-CF-LM6OF12TM | Common cause failure specific 6 of 12 logic relays (T&M) |
| CE1-RYL-CF-LM12OF24 | Common cause failure specific 12 of 24 logic relays |
| CE1-RYL-CF-1,2,3,4LM3OF3TM | Common cause failure 3 of 3 logic relays (T&M) |
| CE1-RYL-CF-1,2,3,4LM6OF6 | Common cause failure 6 of 6 logic relays |
| CE1-RYT-CF-TR2OF4<br>CE1-RYT-CF-2OF4 | Common cause failure 2 of 4 trip relays |

**Table 6.2 CERPS fault tree basic events that have quantitative failure probabilities.**

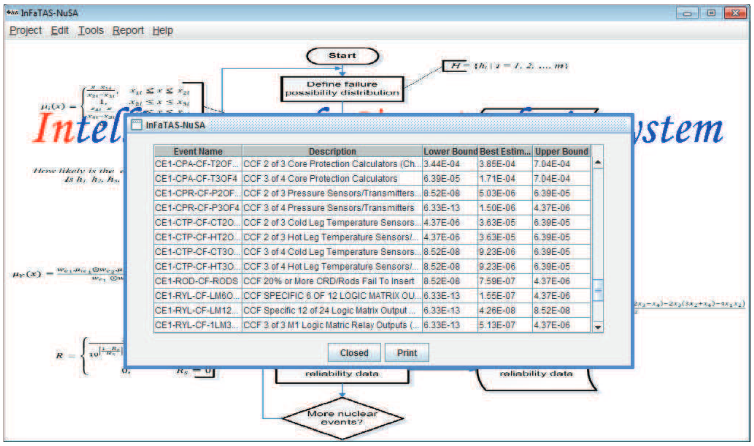
| Basic event name | Description | Failure probabilities | | |
|---|---|---|---|---|
| | | Lower bound | Best estimate | Upper bound |
| /CE1-RPS-TM-CHA | RPS channel A NOT in test and maintenance | 9.68E-1 | 9.8E-1 | 1.0 |
| CE1-RPS-TM-CHA | RPS channel A in test and maintenance | 0.0 | 1.6E-2 | 3.2E-2 |
| CE1-XHE-XE-SCRAM | Operator fails to initiate manual scram | 1.0E-2 | 1.0E-2 | 1.0E-2 |

**Table 6.3 Expert subjective evaluation results.**

| Basic event name | Basic event failure possibilities subjectively evaluated by experts | | | | | | |
|---|---|---|---|---|---|---|---|
| | **$e_1$** | **$e_2$** | **$e_3$** | **$e_4$** | **$e_5$** | **$e_6$** | **$e_7$** |
| CE1-CBI-FF-PA,B,C,D<br>CE1-CBI-FF-TA,B,C,D | *Reasonably High* | *High* | *Reasonably High* | *High* | *Reasonably High* | *High* | *Reasonably High* |
| CE1-CPA-FF-TA,B,C,D | *Very High* | *Very High* | *Very High* | *Very High* | *Very High* | *Very High* | *Very High* |
| CE1-CPR-FF-PA,B,C,D | *Reasonably High* | *Moderate* | *Moderate* | *Moderate* | *Moderate* | *Moderate* | *Reasonably High* |
| CE1-CTP-FF-CTA,B,C,D<br>CE1-CTP-FF-HTA,B,C,D | *High* | *Very High* | *High* | *Very High* | *High* | *Very High* | *High* |
| CE1-MSW-FF-MT1,2 | *Moderate* | *Reasonably High* | *Moderate* | *Moderate* | *Moderate* | *Moderate* | *High* |
| CE1-RYL-FF-LA,B,C,D–1,2,3,4 | *Reasonably High* | *Reasonably High* | *Reasonably High* | *Reasonably High* | *Moderate* | *Reasonably High* | *Reasonably High* |
| CE1-RYT-FF-ICM1,2,3,4 | *Reasonably High* | *Moderate* | *Reasonably High* | *Moderate* | *Moderate* | *Moderate* | *Moderate* |
| CE1-CBI-CF-P(T)2OF3TM | *Reasonably Low* | *Low* | *Reasonably Low* | *Low* | *Low* | *Very Low* | *Low* |
| CE1-CBI-CF-P(T)3OF4 | *Reasonably Low* | *Reasonably Low* | *Moderate* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* |
| CE1-CBI-CF-4OF6TM | *Low* | *Low* | *Low* | *Reasonably Low* | *Low* | *Reasonably Low* | *Moderate* |
| CE1-CBI-CF-6OF8 | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Low* | *Low* | *Low* | *Low* |
| CE1-CPA-CF-T2OF3TM | *Reasonably High* | *Reasonably High* | *Reasonably High* | *High* | *Reasonably High* | *Reasonably High* | *Reasonably High* |
| CE1-CPA-CF-T3OF4 | *Moderate* | *Moderate* | *Moderate* | *Reasonably High* | *Reasonably High* | *Moderate* | *High* |
| CE1-CPR-CF-P2OF3TM | *Low* | *Reasonably Low* | *Low* | *Low* | *Moderate* | *Reasonably Low* | *Moderate* |
| CE1-CPR-CF-P3OF4 | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Low* | *Reasonably Low* | *Very Low* |
| CE1-CTP-CF-C(H)T2OF3TM | *Moderate* | *Reasonably Low* | *Moderate* | *Reasonably Low* | *Moderate* | *Moderate* | *Moderate* |
| CE1-CTP-CF-C(H)T3OF4 | *Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Moderate* | *Moderate* |
| CE1-ROD-CF-RODS | *Low* | *Low* | *Reasonably Low* | *Reasonably Low* | *Low* | *Reasonably Low* | *Low* |
| CE1-RYL-CF-LM6OF12TM | *Very Low* | *Low* | *Reasonably Low* | *Reasonably Low* | *Low* | *Very Low* | *Low* |
| CE1-RYL-CF-LM12OF24 | *Low* | *Low* | *Very Low* | *Low* | *Low* | *Low* | *Low* |
| CE1-RYL-CF-1,2,3,4LM3OF3TM | *Low* | *Reasonably Low* | *Low* | *Reasonably Low* | *Low* | *Very Low* | *Reasonably Low* |
| CE1-RYL-CF-1,2,3,4LM6OF6 | *Low* | *Low* | *Reasonably Low* | *Low* | *Low* | *Low* | *Low* |
| CE1-RYT-CF-TR2OF4<br>CE1-RYT-CF-2OF4 | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* | *Reasonably Low* |

### (2) ANALYSIS

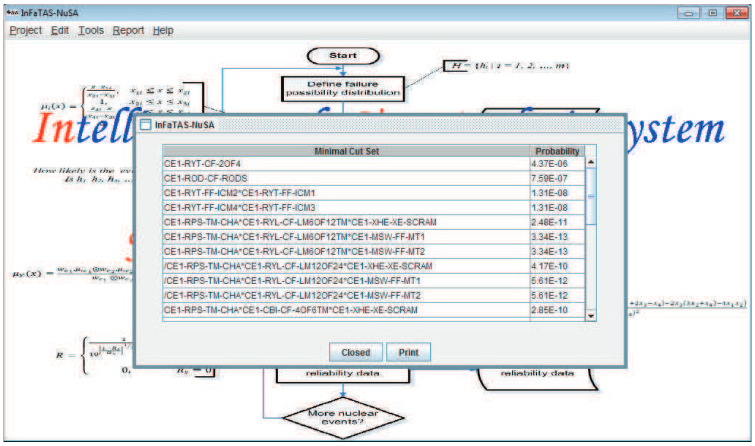
**Step 5: Basic event fuzzy failure rate generation**. Through a menu provided in the menu bar, InFaTAS-NuSA will generate basic event quantitative fuzzy failure rates from their corresponding qualitative failure possibilities given in Step 4 using the algorithm described in Section 6.4, as shown in Figure 6.6.



| Event Name | Description | Lower Bound | Best Estim... | Upper Bound |
|---|---|---|---|---|
| CE1-CPA-CF-T2OF... | CCF 2 of 3 Core Protection Calculators (Ch... | 3.44E-04 | 3.85E-04 | 7.04E-04 |
| CE1-CPA-CF-T3OF4 | CCF 3 of 4 Core Protection Calculators | 6.39E-05 | 1.71E-04 | 7.04E-04 |
| CE1-CPR-CF-P2OF... | CCF 2 of 3 Pressure Sensors/Transmitters... | 8.52E-08 | 5.03E-06 | 6.39E-05 |
| CE1-CPR-CF-P3OF4 | CCF 3 of 4 Pressure Sensors/Transmitters | 6.33E-13 | 1.50E-06 | 4.37E-06 |
| CE1-CTP-CF-CT2O... | CCF 2 of 3 Cold Leg Temperature Sensors... | 4.37E-06 | 3.63E-05 | 6.39E-05 |
| CE1-CTP-CF-HT2O... | CCF 2 of 3 Hot Leg Temperature Sensors/... | 4.37E-06 | 3.63E-05 | 6.39E-05 |
| CE1-CTP-CF-CT3O... | CCF 3 of 4 Cold Leg Temperature Sensors... | 8.52E-08 | 9.23E-06 | 6.39E-05 |
| CE1-CTP-CF-HT3O... | CCF 3 of 4 Hot Leg Temperature Sensors/... | 8.52E-08 | 9.23E-06 | 6.39E-05 |
| CE1-ROD-CF-RODS | CCF 20% or More CRD/Rods Fail To Insert | 8.52E-08 | 7.59E-07 | 4.37E-06 |
| CE1-RYL-CF-LM6O... | CCF SPECIFIC 6 OF 12 LOGIC MATRIX OU... | 6.33E-13 | 1.55E-07 | 4.37E-06 |
| CE1-RYL-CF-LM12... | CCF Specific 12 of 24 Logic Matrix Output ... | 6.33E-13 | 4.26E-08 | 8.52E-08 |
| CE1-RYL-CF-1LM3... | CCF 3 of 3 M1 Logic Matric Relay Outputs (... | 6.33E-13 | 5.13E-07 | 4.37E-06 |

**Figure 6.6 Generated basic event fuzzy failure rates.**

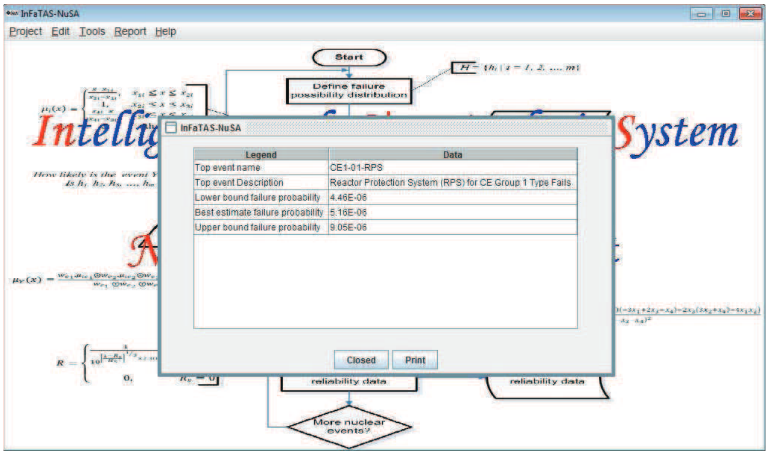
**Step 6: Minimal cut set evaluation**. Through a menu provided in the menu bar, InFaTAS-NuSA will generate minimal cut sets of the fault tree and calculate their individual failure probability, as shown in Figure 6.7.



| Minimal Cut Set | Probability |
|---|---|
| CE1-RYT-CF-2OF4 | 4.37E-06 |
| CE1-ROD-CF-RODS | 7.59E-07 |
| CE1-RYT-FF-ICM2*CE1-RYT-FF-ICM1 | 1.31E-08 |
| CE1-RYT-FF-ICM4*CE1-RYT-FF-ICM3 | 1.31E-08 |
| CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-XHE-XE-SCRAM | 2.48E-11 |
| CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-MSW-FF-MT1 | 3.34E-13 |
| CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-MSW-FF-MT2 | 3.34E-13 |
| /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-XHE-XE-SCRAM | 4.17E-10 |
| /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-MSW-FF-MT1 | 5.61E-12 |
| /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-MSW-FF-MT2 | 5.61E-12 |
| CE1-RPS-TM-CHA*CE1-CBI-CF-4OF6TM*CE1-XHE-XE-SCRAM | 2.85E-10 |

**Figure 6.7 Minimal cut sets and their failure probability.**

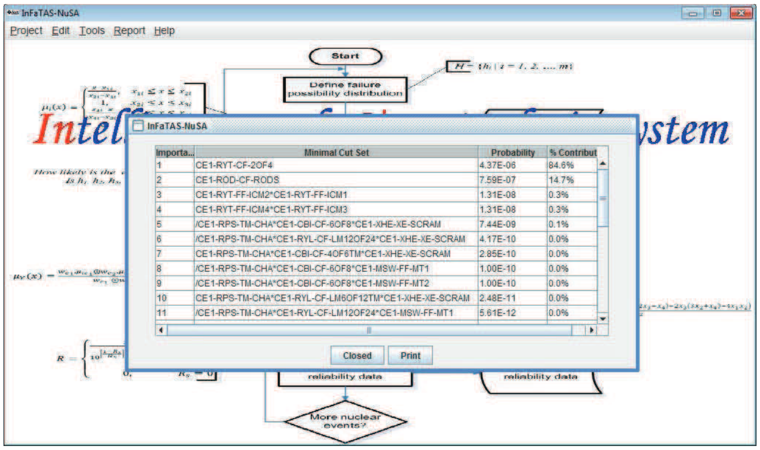
**Step 7: Top event failure probability calculation**. Through a menu provided in the menu bar, InFaTAS-NuSA will calculate the top event failure probability by summing the failure probabilities of all the minimal cut sets evaluated in Step 6, as shown in Figure 6.8.



| Legend | Data |
|---|---|
| Top event name | CE1-01-RPS |
| Top event Description | Reactor Protection System (RPS) for CE Group 1 Type Fails |
| Lower bound failure probability | 4.46E-06 |
| Best estimate failure probability | 5.16E-06 |
| Upper bound failure probability | 9.05E-06 |

**Figure 6.8 Top event failure probability.**

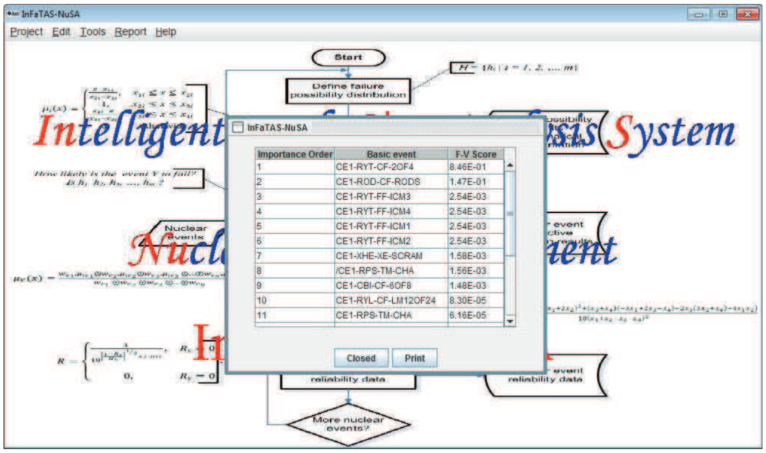
**Step 8: Minimal cut set important measure**. Through a menu provided in the menu bar, InFaTAS-NuSA will analyze the contribution of the minimal cut sets evaluated in Step 6 to the occurrence of the top event, as shown in Figure 6.9.



| Importa... | Minimal Cut Set | Probability | % Contribut |
|---|---|---|---|
| 1 | CE1-RYT-CF-2OF4 | 4.37E-06 | 84.6% |
| 2 | CE1-ROD-CF-RODS | 7.59E-07 | 14.7% |
| 3 | CE1-RYT-FF-ICM2*CE1-RYT-FF-ICM1 | 1.31E-08 | 0.3% |
| 4 | CE1-RYT-FF-ICM4*CE1-RYT-FF-ICM3 | 1.31E-08 | 0.3% |
| 5 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-XHE-XE-SCRAM | 7.44E-09 | 0.1% |
| 6 | /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-XHE-XE-SCRAM | 4.17E-10 | 0.0% |
| 7 | CE1-RPS-TM-CHA*CE1-CBI-CF-4OF6TM*CE1-XHE-XE-SCRAM | 2.85E-10 | 0.0% |
| 8 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT1 | 1.00E-10 | 0.0% |
| 9 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT2 | 1.00E-10 | 0.0% |
| 10 | CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-XHE-XE-SCRAM | 2.48E-11 | 0.0% |
| 11 | /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-MSW-FF-MT1 | 5.61E-12 | 0.0% |

**Figure 6.9 Minimal cut set important measures.**

**Step 9: Basic event Fussell-Vesely important measure**. Through a menu provided in the menu bar, InFaTAS-NuSA will analyse the contribution of every basic event to the occurrence of the top event and generate their Fussell-Vesely importance measure, as shown in Figure 6.10.



InFaTAS-NuSA

| Importance Order | Basic event | F-V Score |
|---|---|---|
| 1 | CE1-RYT-CF-2OF4 | 8.46E-01 |
| 2 | CE1-ROD-CF-RODS | 1.47E-01 |
| 3 | CE1-RYT-FF-ICM3 | 2.54E-03 |
| 4 | CE1-RYT-FF-ICM4 | 2.54E-03 |
| 5 | CE1-RYT-FF-ICM1 | 2.54E-03 |
| 6 | CE1-RYT-FF-ICM2 | 2.54E-03 |
| 7 | CE1-XHE-XE-SCRAM | 1.58E-03 |
| 8 | /CE1-RPS-TM-CHA | 1.56E-03 |
| 9 | CE1-CBI-CF-6OF8 | 1.48E-03 |
| 10 | CE1-RYL-CF-LM12OF24 | 8.30E-05 |
| 11 | CE1-RPS-TM-CHA | 6.16E-05 |

**Figure 6.10 Basic event Fussell-Vesely importance measure.**

### (3) REPORTS

**Step 10: Generate reports as needed**. Through a menu provided in the menu bar, users can generate reports to be displayed on the screen or printed. There are seven graphical user interfaces provided for report generation.

1) System fault tree in the form of a graphical report;
2) System fault tree in the form of a table report;
3) Basic event failure possibilities in the form of a table report;
4) Basic event failure probabilities in the form of a table report;
5) Top event failure probability and its sensitivity;
6) Minimal cut set important measures;
7) Basic event Fussell-Vesely important measure.

**Step 11: Save the project**. Through a menu provided in the menu bar, users can save the project to a file for later use.

## 6.6 InFaTAS-NuSA EVALUATION

To benchmark the performance of InFaTAS-NuSA, we compare four types of outputs generated by this software system to the outputs generated by SAPHIRE, i.e. basic event failure rates, as shown in Table 6.4, top event failure probability, as shown in Table 6.5, minimal cut set importance measure, as shown in Table 6.6, and basic event Fussell-Vesely importance measure, as shown in Table 6.7.

**Table 6.4 Comparison of basic event failure rates.**

| Basic event name | Failure Probability | | Relative error |
|---|---|---|---|
| | SAPHIRE | InFaTAS-NuSA | |
| CE1-CBI-FF-PA,B,C,D<br>CE1-CBI-FF-TA,B,C,D | 5.0E-4 | 4.8E-4 | 0.045884 |
| CE1-CPA-FF-TA,B,C,D | 7.6E-3 | 1.0E-3 | 0.864983 |
| CE1-CPR-FF-PA,B,C,D | 1.1E-4 | 1.1E-4 | 0.040376 |
| CE1-CTP-FF-CTA,B,C,D<br>CE1-CTP-FF-HTA,B,C,D | 8.4E-4 | 8.3E-4 | 0.009576 |
| CE1-MSW-FF-MT1,2 | 1.3E-4 | 1.3E-4 | 0.035225 |
| CE1-RYL-FF-LA,B,C,D–1,2,3,4 | 2.6E-4 | 2.8E-4 | 0.092713 |
| CE1-RYT-FF-ICM1,2,3,4 | 1.2E-4 | 1.1E-4 | 0.046322 |
| CE1-CBI-CF-P(T)2OF3TM | 2.6E-7 | 2.6E-7 | 0.004218 |
| CE1-CBI-CF-P(T)3OF4 | 7.2E-6 | 7.5E-6 | 0.047039 |
| CE1-CBI-CF-4OF6TM | 1.7E-6 | 1.8E-6 | 0.047185 |
| CE1-CBI-CF-6OF8 | 7.7E-7 | 7.6E-7 | 0.013927 |
| CE1-CPA-CF-T2OF3TM | 3.8E-4 | 3.8E-4 | 0.012703 |
| CE1-CPA-CF-T3OF4 | 1.7E-4 | 1.7E-4 | 0.007939 |
| CE1-CPR-CF-P2OF3TM | 5.0E-6 | 5.0E-6 | 0.006601 |
| CE1-CPR-CF-P3OF4 | 1.5E-6 | 1.5E-6 | 0.000282 |
| CE1-CTP-CF-C(H)T2OF3TM | 3.7E-5 | 3.6E-5 | 0.019914 |
| CE1-CTP-CF-C(H)T3OF4 | 1.0E-5 | 9.2E-6 | 0.076792 |
| CE1-ROD-CF-RODS | 8.4E-7 | 7.6E-7 | 0.096100 |
| CE1-RYL-CF-LM6OF12TM | 1.6E-7 | 1.5E-7 | 0.031932 |
| CE1-RYL-CF-LM12OF24 | 4.3E-8 | 4.3E-8 | 0.010018 |
| CE1-RYL-CF-1,2,3,4LM3OF3TM | 4.7E-7 | 5.1E-7 | 0.090759 |
| CE1-RYL-CF-1,2,3,4LM6OF6 | 2.0E-7 | 2.0E-7 | 0.013905 |
| CE1-RYT-CF-2OF4 | 4.8E-6 | 4.4E-6 | 0.089537 |

It can be seen from Table 6.4 that the basic event failure rates generated by InFaTAS-NuSA are very close to the known failure probabilities which are directly input to SAPHIRE except for the basic event CE1-CPA-FF-TA, B, C, D. This exception may be caused by the incapacity of the algorithm to generate failure rates bigger than 1.0E-3. This exception needs to be further analyzed by optimizing the membership function of the basic event failure possibilities. However, in general, these results confirm that the nuclear event assessment algorithm described in Section 4 is a sound technique for generating basic event failure rates when basic events do not have historical failure data. Furthermore, these results also confirm that expert subjective evaluations, which are expressed in qualitative failure possibilities, can be in good agreement with the real quantitative failure probabilities collected from nuclear power plant operating experiences.

**Table 6.5 Top event failure probability and its sensitivity.**

| Failure probability | SAPHIRE | InFaTAS-NuSA |
|---|---|---|
| Lower bound value (5%) | 8.8E-7 | 4.5E-6 |
| Mean value | 5.7E-6 | 5.2E-6 |
| Upper bound value (95%) | 1.7E-5 | 9.0E-6 |

It can be seen from Table 6.5 that the mean value generated by InFaTAS-NuSA (5.2E-6) is very much closer to the mean value generated by SAPHIRE (5.7E-6). The difference of this value is caused by the difference in the basic event failure data generated by InFaTAS-NuSA and the data directly input to SAPHIRE. However, the top event failure probability range generated by InFaTAS-NuSA is still inside the acceptable range of the system failure probability calculated by SAPHIRE.

**Table 6.6 Minimal cut set importance measures.**

| Minimal cut sets | SAPHIRE | | InFaTAS-NuSA | |
|---|---|---|---|---|
| | Failure probability | Contribution percentage | Failure probability | Contribution percentage |
| CE1-RYT-CF-2OF4 | 4.80E-06 | 84.5% | 4.37E-6 | 84.6% |
| CE1-ROD-CF-RODS | 8.40E-07 | 14.9% | 7.59E-7 | 14.7% |
| CE1-RYT-FF-ICM2*CE1-RYT-FF-ICM1 | 1.40E-08 | 0.3% | 1.31E-8 | 0.3% |
| CE1-RYT-FF-ICM4*CE1-RYT-FF-ICM3 | 1.40E-08 | 0.3% | 1.31E-8 | 0.3% |
| /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-XHE-XE-SCRAM | 7.50E-09 | 0.1% | 7.44E-9 | 0.1% |
| /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-XHE-XE-SCRAM | 4.20E-10 | 0.0% | 4.17E-10 | 0.0% |
| CE1-CBI-CF-4OF6TM*CE1-RPS-TM-CHA*CE1-XHE-XE-SCRAM | 2.80E-10 | 0.0% | 2.85E-10 | 0.0% |
| /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT1 | 9.80E-11 | 0.0% | 1.00E-10 | 0.0% |
| /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT2 | 9.80E-11 | 0.0% | 1.00E-10 | 0.0% |
| CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-XHE-XE-SCRAM | 2.50E-11 | 0.0% | 2.48E-11 | 0.0% |

It can be seen from Table 6.6 that the importance measures of the minimal cut sets generated by InFaTAS-NuSA are in the same order as the minimal cut sets generated by SAPHIRE. The fact that the contribution percentage shown in this table equals zero does not mean that it is zero but that it is very small due to the round-off in the algorithm used.

**Table 6.7 Basic event Fussell-Vesely importance measures.**

| **Basic events** | **InFaTAS-NuSA** |
|---|---|
| CE1-RYT-CF-2OF4 | 8.46E-1 |
| CE1-ROD-CF-RODS | 1.47E-1 |
| CE1-RYT-FF-ICM1 | 2.54E-3 |
| CE1-RYT-FF-ICM2 | 2.54E-3 |
| CE1-RYT-FF-ICM3 | 2.54E-3 |
| CE1-RYT-FF-ICM4 | 2.54E-3 |
| CE1-XHE-XE-SCRAM | 1.58E-3 |
| /CE1-RPS-TM-CHA | 1.56E-3 |
| CE1-CBI-CF-6OF8 | 1.48E-3 |
| CE1-RYL-CF-LM12OF24 | 8.30E-5 |

Table 6.7 shows the top ten basic events which contribute the most to the failure of the CERPS Group 1. Unfortunately, the details of this evaluation generated by SAPHIRE are not provided in Wierman et al. (2001), but it was mentioned that the trips of CE1-RYT-FF-ICM1, CE1-RYT-FF-ICM2, CE1-RYT-FF-ICM3, and CE1-RYT-FF-ICM4 are four dominant contributors to the failure of this RPS, as can also be seen in Table 7. In this important measure, the ranking of the basic events is more important than the FV scores.

## 6.7 SUMMARY

This chapter describes an intelligent fault tree analysis software system to assess nuclear power plant safety. The newly-developed system, InFaTAS-NuSA, introduces the concept of failure possibilities, which are expressed in qualitative linguistic values, into the quantitative phase of conventional fault tree analysis to evaluate basic events which do not have historical failure data. The first model of the CERPS has been used to verify the effectiveness and applicability of InFaTAS-NuSA. The results confirm that InFaTAS-NuSA has yielded similar outputs as SAPHIRE. The experiment results also show that the nuclear event assessment algorithm to enable experts to subjectively evaluate basic event failures seems to be a sound alternative for quantitative failure probability to overcome the limitation of conventional fault tree analysis. The advantage of using qualitative failure possibilities is that it can intuitively and easily express expert opinions which cannot be represented by numerical values.

Chapter 7

# CONCLUSIONS AND FUTURE STUDIES

## 7.1 CONCLUSIONS

An Intelligent Fault Tree Analysis System for Nuclear Safety Assessment (InFaTAS-NuSA) has been developed in this study. InFaTAS-NuSA is a realization of the intelligent hybrid fault tree analysis framework to overcome the limitations of the nuclear power plant probabilistic safety assessment by fault tree analysis. It integrates the failure possibility-based approach into the quantitative phase of the fault tree analysis to deal with basic events, which do not have historical failure data for calculating their quantitative failure probabilities. To enable experts to subjectively and intuitively evaluate these basic events, qualitative failure possibilities have been developed and implemented in InFaTAS-NuSA. Moreover, to enable safety analysts to quantitatively estimate the failure probability of the top event of fault trees using basic event qualitative failure possibilities, the corresponding mathematical representation of those qualitative failure possibilities, an area defuzzification technique to decode membership functions of fuzzy sets into a single numerical value and a fuzzy reliability approach to convert qualitative failure possibilities into quantitative failure rates have also been developed and integrated into InFaTAS-NuSA. In this study, seven linguistic terms have been defined to represent nuclear event failure possibilities, i.e. *very low*, *low*, *reasonably low*, *moderate*, *reasonably high*, *high*, and *very high* and the corresponding mathematical forms are represented by triangular fuzzy numbers, which are defined in the [0, 1] universe of discourse based on nuclear event failure data documented in literatures using inductive reasoning. This means that the closer the fuzzy probabilities are to 0, the less likely the basic events are to fail. On the other hand, the closer the fuzzy probabilities are to 1, the more likely the basic events are to fail. Meanwhile, the horizontal axis represents the fuzzy failure rates of basic events, which is also defined between 0 and 1. This means that the closer the fuzzy numbers are to the point of origin, the lower the basic event fuzzy failure rates are. On the other hand, the farther the fuzzy numbers are from the point of origin, the higher the basic event fuzzy failure rates are. The first model of the U.S. combustion engineering reactor protection system has been used to verify the effectiveness and applicability of InFaTAS-NuSA. The results confirm that InFaTAS-NuSA has yielded similar outputs as SAPHIRE and therefore InFaTAS-NuSA has been able to overcome the limitation of the existing fault tree analysis software system which can accept only quantitative failure rates. The experiment results also show that the fuzzy reliability approach seems to be a sound alternative for conventional reliability approach to deal with basic events which do not have historical failure data and expert subjective opinions are the only means to obtain their failure information. The advantage of using qualitative failure possibilities is that it can intuitively and easily express expert opinions, which cannot be represented by numerical values.

## 7.2 FUTURE STUDIES

While the study has offered a sound solution to the current problems of nuclear power plant probabilistic safety assessment by fault tree analysis, there are still a number of interesting avenues to pursue. Therefore, we still need to continue this study for these four reasons. Firstly, the underlying failure possibilities and their corresponding mathematical representation will be further refined and enriched by admitting various classes of membership functions of fuzzy numbers. This further enrichment will validate the effectiveness and the applicability of the proposed fuzzy reliability approach to evaluate basic events using different type of membership functions for different kind of engineering applications. Secondly, more experimentation using various data sets coming from other nuclear power plants operating experiences would be advantageous to explore and to gain a better assessment of the performance of InFaTAS-NuSA. This further experimentation will also be good for future improvements and/or to find new direction for new development. Thirdly, since the fact that nuclear power plant accidents are not free from human errors, such as the Three Mile Island and Chernobyl accidents, human reliability analysis using the concept of error possibility proposed by Onisawa (1988) is also important to be studied in the future research to complement this study.

Finally, to enable InFaTAS-NuSA to deal with complicated fault trees, other types of fault tree components also need to be added into the next version of InFaTAS-NuSA. For example, a component of undeveloped event needs to be added to deal with events that cannot be further analyzed due to lack of information. “PRIORITY AND” and “EXCLUSIVE OR” Boolean gates need to be added to deal with events which have requirement conditions to make them happened. Moreover, other importance measures, such as the risk achievement worth, the risk reduction worth, the criticality importance factor and the Birnbaum importance measure also need to be provided in the next version of InFaTAS-NuSA to accommodate risk analysts needs.

# REFERENCES

Abbasbandy, S. & Asady, B. 2006, 'Ranking of fuzzy numbers by sign distance', *Inform. Sci.*, vol. 176, no. 16, pp. 2405-2416.

Abbasbandy, S. & Hajjari, T. 2009, 'A new approach for ranking of trapezoidal fuzzy numbers', *Comput. Math. Appl.*, vol. 57, no. 3, pp. 413-419.

Apostolakis, G.E. 1995, 'A commentary on modeling uncertainty', in *Proceedings of Workshop I in Advanced Topics in Risk and Reliability Analysis, Model Uncertainty: Its Characterization and Quantification,* University of Maryland Press, Maryland - USA.

Arshi, S.S., Nematollahi, M. & Sepanloo, K. 2010, 'Coupling CFAST fire modeling and SAPHIRE probabilistic assessment software for internal fire safety evaluation of a typical TRIGA research reactor', *Reliab. Eng. Syst. Saf.*, vol. 95, no. 3, pp. 166-172.

Arul, A.J., Kumar, C.S., Athmalingam, S., Singh, O.P. & Rao, K.S. 2006, 'Reliability analysis of safety grade decay heat removal system of Indian prototype fast breeder reactor', *Ann. Nucl. Energy*, vol. 33, no. 2, pp. 180-188.

Asady, B. & Zendehnam, A. 2007, 'Ranking fuzzy numbers by distance minimization', *Appl. Math. Modell.*, vol. 31, no. 11, pp. 2589-2598.

Bartha, T., Varga, I., Soumelidis, A. & Szabé, G. 2005, 'Implementation of a testing and diagnostic concept for an NPP reactor protection system', in M.D. Cin, M. Kaâniche & A. Pataricza (eds), *Dependable Computing - EDCC-5, Lecture Notes in Computer Science*, vol. 3463, Springer, Berlin, pp. 391-402.

Bector, C.R. & Chandra, S. 2005, 'Fuzzy numbers and fuzzy arithmetic', in J. Kacprzyk (ed.), *Fuzzy Mathematical Programming and Fuzzy Matrix Games*, Springer, Berlin, pp. 39-56.

Ben-Arieh, D. 2005, 'Sensitivity of multi-criteria decision making to linguistic quantifiers and aggregation means', *Comput. Ind. Eng.*, vol. 48, no. 2, pp. 289-309.

Bickel, J.H. 2008, 'Risk implications of digital reactor protection system operating experience', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 1, pp. 107-124.

Bing, L., Meilin, Z. & Kai, X. 2000, 'A practical engineering method for fuzzy reliability analysis of mechanical structures', *Reliab. Eng. Syst. Saf.*, vol. 67, no. 3, pp. 311-315.

Bodansky, D. 2004, 'Nuclear reactor safety', in *Nuclear Energy: Principles, Practices, and Prospects*, 2nd edn., Springer-Verlag, New York, pp. 371-410.

Bondavalli, A. & Filippini, R. 2004, 'Modelling and analysis of a scheduled maintenance system: A DSPN approach', *Comput. J.*, vol. 47, no. 6, pp. 634-650.

Borgonovo, E. 2007a, 'Differential, criticality and Birnbaum importance measures: An application to basic event, groups and SSCs in event trees and binary decision diagrams', *Reliab. Eng. Syst. Saf.*, vol. 92, no. 10, pp. 1458-1467.

Borgonovo, E. 2007b, 'A new uncertainty importance measure', *Reliab. Eng. Syst. Saf.*, vol. 92, no. 6, pp. 771-784.

Bortolan, G. & Degani, R. 1985, 'A review of some methods for ranking fuzzy subsets', *Fuzzy Sets Syst.*, vol. 15, no. 1, pp. 1-19.

Bowles, J.B. & Pelaez, C.E. 1995, 'Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis', *Reliab. Eng. Syst. Saf.*, vol. 50, no. 2, pp. 203-213.

Canos, L. & Liern, V. 2008, 'Soft computing-based aggregation methods for human resource management', *Eur. J. Oper. Res.*, vol. 189, no. 3, pp. 669-681.

Celik, M., Lavasani, S.M. & Wang, J. 2010, 'A risk-based modelling approach to enhance shipping accident investigation', *Saf. Sci.*, vol. 48, no. 1, pp. 18-27.

Chanda, R.S. & Bhattacharjee, P.K. 1998, 'A reliability approach to transmission expansion planning using fuzzy fault-tree model', *Electr. Power Syst. Res.*, vol. 45, no. 2, pp. 101-108.

Chen, C.C. & Tang, H.C. 2008, 'Ranking nonnormal p-norm trapezoidal fuzzy numbers with integral value', *Comput. Math. Appl.*, vol. 56, no. 9, pp. 2340-2346.

Chen, S.H. 1985, 'Ranking fuzzy numbers with maximizing set and minimizing set', *Fuzzy Sets Syst.*, vol. 17, no. 2, pp. 113-129.

Cheng, C.H. 1998, 'A new approach for ranking fuzzy numbers by distance method', *Fuzzy Sets Syst.*, vol. 95, no. 3, pp. 307-317.

Cheok, M.C., Parry, G.W. & Sherry, R.R. 1998, 'Use of importance measures in risk-informed regulatory applications', *Reliab. Eng. Syst. Saf.*, vol. 60, no. 3, pp. 213-226.

Chin, K.S., Wang, Y.M., Poon, G.K.K. & Yang, J.B. 2009, 'Failure mode and effects analysis using a group-based evidential reasoning approach', *Comput. Oper. Res.*, vol. 36, no. 6, pp. 1768-1779.

Cho, H.N., Choi, H.H. & Kim, Y.B. 2002, 'A risk assessment methodology for incorporating uncertainties using fuzzy concepts', *Reliab. Eng. Syst. Saf.*, vol. 78, no. 2, pp. 173-183.

Chu, T.C. & Tsao, C.T. 2002, 'Ranking fuzzy numbers with an area between the centroid point and original point', *Comput. Math. Appl.*, vol. 43, no. 1-2, pp. 111-117.

Coletti, G. & Scozzafava, R. 2004, 'Conditional probability, fuzzy sets, and possibility: A Unifying View', *Fuzzy Sets Syst.*, vol. 144, no. 1, pp. 227-249.

Cooke, R.M., ElSaadany, S. & Huang, X. 2008, 'On the performance of social network and likelihood-based expert weighting schemes', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 5, pp. 745-756.

Cooke, R.M. & Goossens, L.L.H.J. 2008, 'TU Delft expert judgment data base', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 5, pp. 657-674.

Delaney, M.J., Apostolakis, G.E. & Driscoll, M.J. 2005, 'Risk-informed design guidance for future reactor systems', *Nucl. Eng. Des.*, vol. 235, no. 14, pp. 1537-1556.

Deshpande, A.W. & Khanna, P. 1995, 'Fuzzy fault tree analysis: Case studies', in T. Onisawa & J. Kacprzyk (eds), *Reliability and Safety Analysis under Fuzziness*, Physica-Verlag, Heidelberg, pp. 126-141.

Dhillon, B.S. 1999, 'Fault tree analysis', in S. Fox (ed.), *Design Reliability: Fundamentals and Applications*, CRC Press LLC, Florida, pp. 126-143.

Dhillon, B.S. 2005, 'Reliability evaluation methods', in *Reliability, Quality, and Safety for Engineers*, CRC Press LLC, Florida, pp. 87-105.

Ding, Y. & Lisnianski, A. 2008, 'Fuzzy universal generating functions for multi-state system reliability assessment ', *Fuzzy Sets Syst.*, vol. 159, no. 3, pp. 307-324.

Ding, Y., Zuo, M.J., Lisnianski, A. & Li, W. 2010, 'A framework for reliability approximation of multi-state weighted k-out-of-n systems', *IEEE Trans. Reliab.*, vol. 59, no. 2, pp. 297-308.

Ding, Y., Zuo, M.J., Lisnianski, A. & Tian, Z. 2008, 'Fuzzy multi-state systems: General definitions, and performance assessment', *IEEE Trans. Reliab.*, vol. 57, no. 4, pp. 589-594.

Dubois, D. & Prade, H. 1978, 'Operations on fuzzy numbers', *Int. J. Syst. Sci.*, vol. 9, pp. 613-626.

Dubois, D. & Prade, H. 1994, 'Possibility theory and data fusion in poorly informed environments', *Control Eng. Pract.*, vol. 2, no. 5, pp. 811-823.

Dumitrescu, M., Munteanu, T., Voncila, I., Gurguiatu, G., Floricau, D. & Ulmeanu, A.P. 2006, 'Application of fuzzy logic in safety computing for a power protection system', in L. Wang, L. Jiao, G. Shi, X. Li & J. Liu (eds), *Fuzzy Systems and Knowledge Discovery*, vol. 4223, Springer Verlag, Berlin Heidelberg, pp. 980-989.

Dutuit, Y. & Rauzy, A. 1996, 'A linear time algorithm to find modules of fault trees', *IEEE Trans. Reliab.*, vol. 45, no. 3, pp. 422-425.

Epstein, S. & Rauzy, A. 2005, 'Can we trust PRA?', *Reliab. Eng. Syst. Saf.*, vol. 88, no. 3, pp. 195-205.

Ericson, C.A. 2005, 'Fault tree analysis', in Ericson (ed.), *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Virginia, pp. 183-221.

Faghihi, F., Ramezani, E., Yousefpour, F. & Mirvakili, S.M. 2008, 'Level-1 probability safety assessment of the Iranian heavy water reactor using SAPHIRE software', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 10, pp. 1377-1409.

Ferdous, P., Khan, F.I., Veitch, B. & Amyotte, P.R. 2007, 'Methodology for computer-aided fault tree analysis', *Process Saf. Environ.*, vol. 85, no. 1, pp. 70-80.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P. & Veitch, B. 2011, 'Fault and event tree analyses for process systems risk analysis: Uncertainty handling formulations', *Risk Anal.*, vol. 31, no. 1, pp. 86-107.

Gargama, H. & Chaturvedi, S.K. 2011, 'Criticality assessment models for failure mode effects and criticality analysis using fuzzy logic', *IEEE Trans. Reliab.*, vol. 60, no. 1, pp. 102-110.

Garrick, B.J. & Christie, R.F. 2002, 'Probabilistic risk assessment practices in the USA for nuclear power plants', *Saf. Sci.*, vol. 40, pp. 177-201.

Gentile, M., Rogers, W.J. & Mannan, M.S. 2003, 'Development of a fuzzy logic-based inherent safety index', *Process Saf. Environ.*, vol. 81, no. 6, pp. 444-456.

Guh, Y.Y., Po, R.W. & Lee, E.S. 2008, 'The fuzzy weighted average within a generalized means function', *Comput. Math. Appl.*, vol. 55, no. 12, pp. 2699-2706.

Guimaraes, A.C.F. & Ebecken, N.F.F. 1999, 'FuzzyFTA: A fuzzy fault tree system for uncertainty analysis', *Ann. Nucl. Energy*, vol. 26, no. 6, pp. 523-532.

Guimaraes, A.C.F. & Lapa, C.M.F. 2004, 'Fuzzy FMEA applied to PWR chemical and volume control system', *Prog. Nucl. Energy*, vol. 44, no. 3, pp. 191-213.

Guimaraes, A.C.F. & Lapa, C.M.F. 2007, 'Fuzzy inference to risk assessment on nuclear engineering systems', *Appl. Soft Comput.*, vol. 7, no. 1, pp. 17-28.

Guimaraes, A.C.F. & Lapa, C.M.F. 2008, 'Parametric fuzzy study for effects analysis of age on PWR containment cooling system', *Appl. Soft Comput.*, vol. 8, no. 1, pp. 1562–1571.

Gupta, S. & Bhattacharya, J. 2007, 'Reliability analysis of a conveyor system using hybrid data', *Qual. Reliab. Eng. Int.*, vol. 23, no. 7, pp. 867-882.

Hadavi, S.M.H. 2008, 'WWER-1000 shutdown probabilistic risk assessment: An introductory insight', *Ann. Nucl. Energy*, vol. 35, no. 2, pp. 196-208.

Haimes, Y.Y. 2004, 'Fault trees', in *Risk Modeling, Assessment, and Management*, 2nd edn, John Wiley & Sons, New Jersey, pp. 525-569.

Hamada, M., Martz, H.F., Reese, C.S., Graves, T., Johnson, V. & Wilson, A.G. 2004, 'A fully Bayesian approach for combining multilevel failure information in fault tree quantification and optimal follow-on resource allocation', *Reliab. Eng. Syst. Saf.*, vol. 86, no. 3, pp. 297-305.

Harvego, E.A., Reza, S.M.M., Richards, M. & Shenoy, A. 2006, 'An evaluation of reactor cooling and coupled hydrogen production processes using the modular helium reactor', *Nucl. Eng. Des.*, vol. 236, no. 14-16, pp. 1481-1489.

Hryniewicz, O. 2007, 'Fuzzy sets in the evaluation of reliability', in G. Levitin (ed.), *Computational Intelligence in Reliability Engineering New Metaheuristics, Neural and Fuzzy Techniques in Reliability*, Springer-Verlag, Berlin Heidelberg, pp. 363-386.

Hsu, F. & Musicki, Z. 2005, 'Issues and insights of PRA methodology in nuclear and space applications', in *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp. 510-517.

Huang, C.Y. & Chang, Y.R. 2007, 'An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees', *Reliab. Eng. Syst. Saf.*, vol. 92, no. 10, pp. 1403-1412.

Huang, D., Chen, T. & Wang, M.J.J. 2001a, 'A fuzzy set approach for event tree analysis', *Fuzzy Sets Syst.*, vol. 118, no. 1, pp. 153-165.

Huang, D., Chen, T. & Wang, M.J.J. 2001b, 'A fuzzy set approach for event tree analysis', *Fuzzy Sets Syst.*, vol. 118, no. 1, pp. 153-165.

Huang, H.Z., Tonga, X. & Zuo, M.J. 2004, 'Posbist fault tree analysis of coherent systems', *Reliab. Eng. Syst. Saf.*, vol. 84, no. 1, pp. 141-148.

IAEA 1988, *Component reliability data for use in probabilistic safety assessment*, in *IAEA-TECDOC-478*, IAEA, Vienna, Austria.

IAEA 1997, *Generic component reliability data for research reactor PSA*, in *IAEA-TECDOC-930*, IAEA, Vienna, Austria.

IAEA 1999, *Living probabilistic safety assessment (LPSA)*, in *IAEA-TECDOC-1106*, IAEA, Vienna, Austria.

IAEA 2007, *IAEA safety glossary, terminology used in nuclear safety and radiation protection*, IAEA, Vienna, Austria.

Kang, D.I. & Han, S.H. 2006, 'Estimation of the alpha factor parameters for the emergency diesel generators of Ulchin unit 3', in *Proceeding of the International Conference on Nuclear Engineering (ICONE14)*, ASME, Florida, USA, <http://scholar.googleusercontent.com/scholar?q=cache:lSZPZeO1YhAJ:scholar.google.com/+%22Reliability+Study:+Combustion+Engineering+Reactor+Protection+System%22&hl=en&as_sdt=0,5>.

Karimi, I. & Hüllermeier, E. 2007, 'Risk assessment system of natural hazards: A new approach based on fuzzy probability', *Fuzzy Sets Syst.*, vol. 158, no. 9, pp. 987-999.

Kim, B.J. & Bishu, R.R. 2006 'Uncertainty of human error and fuzzy approach to human reliability analysis', *Int. J. Uncertainty Fuzziness Knowledge Based Syst.*, vol. 14, no. 1, pp. 111-129.

Kim, K. & Park, K.S. 1990, 'Ranking fuzzy numbers with index of optimism', *Fuzzy Sets Syst.*, vol. 35, no. 2, pp. 143-150.

Kishi, T., Kikuchi, H., Miura, S., Fukuda, M., Hirano, M. & Watanabe, N. 2004, 'Application of probabilistic safety assessment to the pipe rupture incident at Hamaoka Unit-1', *J. Nucl. Sci. Technol.*, vol. 41, no. 1, pp. 77-85.

Klir, J.G. & Yuan, B. 2001, *Fuzzy Sets and Fuzzy Logic Theory and Applications*, Prentice Hall, Upper Saddle River, NJ.

Lederman, L., Niehaus, F. & Tomic, B. 1996, 'Probabilistic safety assessment past, present and future: An IAEA perspective', *Nucl. Eng. Des.*, vol. 160, no. 3, pp. 273-285.

Lederman, L., Vallerga, H. & Bojadjiev, A. 1990, 'IAEA activities on extending PSAPACK as a tool for use in NPP safety management', *Reliab. Eng. Syst. Saf.*, vol. 30, no. 1-3, pp. 447-454.

Lin, C.T. & Wang, M.J.J. 1997, 'Hybrid fault tree analysis using fuzzy sets', *Reliab. Eng. Syst. Saf.*, vol. 58, no. 3, pp. 205-213.

Lin, S.W. & Bier, V.M. 2008, 'A study of expert overconfidence', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 5, pp. 711-721.

Liou, T.S. & Wang, M.J.J. 1992, 'Ranking fuzzy numbers with integral value', *Fuzzy Sets Syst.*, vol. 50, no. 3, pp. 247-255.

Liu, J., Lopez, L.M., Yang, J.B. & Wang, J. 2008a, 'Linguistic assessment approach for hierarchical safety analysis and synthesis', in D. Ruan, F. Hardeman & K. van der Meer (eds), *Intelligent Decision and Policy Making Support Systems*, vol. 117, Springer-Verlag, Berlin Heidelberg, pp. 211-230.

Liu, J., Martinez, L. & Wang, Y.M. 2008, 'Extended belief rule base inference methodology', in *Proceedings of 3rd International Conference on Intelligent System and Knowledge Engineering*, vol. 1, pp. 1415-1420.

Liu, J., Yang, J.B., Ruan, D., Martinez, L. & Wang, J. 2008b, 'Self-tuning of fuzzy belief rule bases for engineering system safety analysis', *Ann. Oper. Res.*, vol. 163, no. 1, pp. 143-168.

Liu, J., Yang, J.B., Wang, J. & Sii, H.S. 2005, 'Engineering system safety analysis and synthesis using the fuzzy rule-based evidential reasoning approach', *Qual. Reliab. Eng. Int.*, vol. 21, no. 4, pp. 387-411.

Liu, J., Yang, J.B., Wang, J., Sii, H.S. & Wang, Y.M. 2004, 'Fuzzy rule-based evidential reasoning approach for safety analysis', *Int. J. Gen. Syst.*, vol. 33, no. 2-3, pp. 183-204.

Liu, T., Tong, J. & Zhao, J. 2008, 'Probabilistic risk assessment framework development for nuclear power plant', in *Proceedings of IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1330-1334.

Lu, J., Zhang, G. & Ruan, D. 2008, ' Intelligent multi-criteria fuzzy group decision-making for situation assessments', *Soft Computing - A Fusion of Foundations, Methodologies and Applications*, vol. 12, no. 3, pp. 289-299.

Lu, J., Zhang, G., Ruan, D. & Wu, F. 2007, *Multi-Objective Group Decision Making: Methods, Software and Applications with Fuzzy Set Techniques*, Imperial College Press, London.

Markowski, A.S. & Mannan, M.S. 2008, 'Fuzzy risk matrix', *J. Hazard. Mater.*, vol. 159, no. 1, pp. 152-157.

Markowski, A.S., Mannan, M.S. & Bigoszewska, A. 2009, 'Fuzzy logic for process safety analysis', *J. Loss Prev. Process Ind.*, vol. 22, no. 6, pp. 695-702.

Martinez, L., Liu, J., Ruan, D. & Yang, J.B. 2007, 'Dealing with heterogeneous information in engineering evaluation processes', *Inform. Sci.*, vol. 177, no. 7, pp. 1533-1542.

Mazzuchi, T.A., Linzey, W.G. & Bruning, A. 2008, 'A paired comparison experiment for gathering expert judgment for an aircraft wiring risk assessment', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 5, pp. 722-731.

Mentes, A. & Helvacioglu, I.H. 2011, 'An application of fuzzy fault tree analysis for spread mooring systems', *Ocean Eng.*, vol. 38, no. 2-3, pp. 285-294.

Misra, K.B. & Weber, G.G. 1990, 'Use of fuzzy set theory for level-I studies in probabilistic risk assessment', *Fuzzy Sets Syst.*, vol. 37, no. 2, pp. 139-160.

Moller, B., Beer, M., Graf, W. & Hoffmann, A. 1999, 'Possibility theory based safety assessment', *Comput.-Aided Civ. Infrastruct. Eng.*, vol. 14, no. 2, pp. 81-91.

Moon, J.H. & Kang, C.S. 1999, 'Use of fuzzy set theory in the aggregation of expert judgments', *Ann. Nucl. Energy*, vol. 26, no. 6, pp. 461-469.

NEA 2005, *Living PSA and its Use in the Nuclear Safety Decision-making Process*, Nuclear Energy Agency, Paris.

Niehaus, F. 1989, 'Prospects for use of probabilistic safety criteria', *Nucl. Eng. Des.*, vol. 115, no. 1, pp. 181-190.

Onisawa, T. 1988, 'An approach to human reliability in man-machine systems using error possibility', *Fuzzy Sets Syst.*, vol. 27, no. 2, pp. 87-103.

Onisawa, T. 1989, 'Fuzzy theory in reliability analysis', *Fuzzy Sets Syst.*, vol. 30, no. 3, pp. 361-363.

Opricovic, S. & Tzeng, G.H. 2003, 'Defuzzification within a multicriteria decision model', *Int. J. Uncertainty Fuzziness Knowledge Based Syst.*, vol. 11, no. 5, pp. 635-652.

Ou, Y. & Dugan, J.B. 2003, 'Approximate sensitivity analysis for acyclic Markov reliability models', *IEEE Trans. Reliab.*, vol. 52, no. 2, pp. 220-230.

Pan, H. & Yeh, C.H. 2003a, 'Fuzzy project scheduling', in *Proceedings* of *12th IEEE International Conference on Fuzzy Systems*, vol. 1, pp. 755-760.

Pan, H. & Yeh, C.H. 2003b, 'A metaheuristic approach to fuzzy project scheduling', in V. Palade, R.J. Howlett & L.C. Jain (eds), *Knowledge-Based Intelligent Information and Engineering Systems*, vol. 1, Springer, Berlin / Heidelberg, pp. 1081-1087.

Pan, N.F. 2006, 'Evaluation of building performance using fuzzy FTA', *Constr. Manag. Econ.*, vol. 24, no. 12, pp. 1241-1252.

Pan, N.F. & Wang, H. 2007, 'Assessing failure of bridge construction using fuzzy fault tree analysis', in *Proceedings of IEEE International Conference on Fuzzy Systems and Knowledge Discovery*, vol. 1, pp. 96-100.

Pandey, D. & Tyagi, S.K. 2007, 'Profust reliability of a gracefully degradable system', *Fuzzy Sets Syst.*, vol. 158, no. 7, pp. 794-803.

Pannell, D.J. 1997, 'Sensitivity analysis of normative economic models: Theoretical framework and practical strategies', *Agric. Econ.*, vol. 16, pp. 139-152.

Papazoglou, I.A., Bari, R.A., Buslik, A.J., Hall, R.E., Ilberg, D., Samanta, P.K., Teichmann, T., Youngblood, R.W., EI-Bassioni, A., Fragola, J., Lofgren, E. & W. Vesely, W. 1984, *Probabilistic Safety Analysis: Procedures Guide*, *NUREG/CR-2815*, Department of Nuclear Energy, Brookhaven National Laboratory, Upton - NY.

Paredes, G.E., Carrera, A.N., Rodriguez, A.V. & Martinez, E.G.E. 2009, 'Modeling of the high pressure core spray systems with fuzzy cognitive maps for operational transient analysis in nuclear power reactors', *Prog. Nucl. Energy*, vol. 51, no. 3, pp. 434-442.

Pillay, A. & Wang, J. 2003, 'Modified failure mode and effects analysis using approximate reasoning', *Reliab. Eng. Syst. Saf.*, vol. 79, no. 1, pp. 69-85.

Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2010a, 'A hybrid approach for fault tree analysis combining probabilistic method with fuzzy numbers', in L. Rutkowski, R. Scherer, R. Tadeusiewicz, L.A. Zadeh & J.M. Zurada (eds), *Artificial Intelligence and Soft Computing*, vol. 1, Springer, Berlin / Heidelberg, pp. 194-201.

Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2010b, 'Probabilistic safety assessment in nuclear power plants by fuzzy numbers', in *Proceedings of 9th International FLINS Conference*, vol. 4, pp. 256-262.

Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2011, 'Failure possibilities for nuclear safety assessment by fault tree analysis', *Int. J. Nucl. Knowl. Manag.*, vol. 5, no. 2, pp. 162-177.

Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2012a, 'An area defuzzification technique to assess nuclear event reliability data from failure possibilities', *Int. J. Comput. Intell. Appl.*, vol. 11, no. 4, 1250022 (16 pp).

Purba, J.H., Lu, J., Ruan, D. & Zhang, G. 2012b, 'A failure possibility-based reliability algorithm for nuclear safety assessment by fault tree analysis', in *Proceedings of 1st International Workshop on Safety & Security Risk Assessment and Organizational Cultures (SSRAOC2012)*, pp. 29-36.

Purba, J.H., Lu, J. & Zhang, G. 2012a, 'An area defuzzification technique and essential fuzzy rules for defuzzifying nuclear event failure possibilities into reliability data', in *Proceedings of 10th International FLINS Conference*, vol. 7, pp. 1208-1213.

Purba, J.H., Lu, J. & Zhang, G. 2012b, 'Fuzzy failure rate for nuclear power plant probabilistic safety assessment by fault tree analysis', in C. Kahraman (ed.), *Computational Intelligence Systems in Industrial Engineering*, vol. 6, Atlantis Press, pp. 131-154.

Purba, J.H., Lu, J. & Zhang, G. 2013, 'An intelligent fault tree analysis for nuclear safety assessment', *Risk Anal. (under review)*.

Purba, J.H., Lu, J., Zhang, G. & Pedrycz, W. 2012c, 'A fuzzy reliability assessment of basic events of fault trees through qualitative data processing', *Fuzzy Sets Syst. (Available online 18 June 2013)*.

Ren, J., Jenkinson, I., H.S., S., Xu, D.L., Wang, J. & Yang, J.B. 2005, 'An offshore safety assessment framework using fuzzy reasoning and evidential synthesis approaches', *J. Mar. Eng. Tech. (IMarEST)*, vol. A6, no. 1, pp. 3-16.

Ross, T.J. 2004a, 'Development of Membership functions', in *Fuzzy Logic With Engineering Applications*, 2nd edn, John Wiley & Sons, Chichester, pp. 178-211.

Ross, T.J. 2004b, 'Properties of membership functions, fuzzifications, and defuzzification', in *Fuzzy Logic With Engineering Applications*, 2nd edn, John Wiley & Sons, Chichester, pp. 90-119.

Saltelli, A. 2002, 'Sensitivity analysis for importance assessment', *Risk Anal.*, vol. 22, no. 3, p. 579.

Sharma, U. & Sudhakar, M. 1993, 'Use of recursive methods in fuzzy fault tree analysis: An aid to quantitative risk analysis', *Reliab. Eng. Syst. Saf.*, vol. 41, no. 3, pp. 231-237.

Shu, L., Li, J. & Qiu, M. 2008, 'Study on applying fault tree analysis based on fuzzy reasoning in risk analysis of construction quality', in *Proceedings of International Conference on Risk Management & Engineering Management*, pp. 393-397.

Smith, C., Knudsen, J., Kvarfordt, K. & Wood, T. 2008, 'Key attributes of the SAPHIRE risk and reliability analysis software for risk-informed probabilistic applications', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 8, pp. 1151-1164.

Song, H., Zhang, H.Y. & Chan, C.W. 2009, 'Fuzzy fault tree analysis based on T–S model with application to INS/GPS navigation system', in *Soft Computing - A Fusion of Foundations, Methodologies and Applications*, vol. 13, no. 1, pp. 31-40.

Stacey, W.M. 2007, 'Reactor safety', in *Nuclear Reactor Physics*, 2nd edn, Wiley-VCH, Verlag GmbH KGaA, Weinheim, pp. 283-302.

Suresh, P.V., Babar, A.K. & Venkat Raj, V. 1996, 'Uncertainty in fault tree analysis: A fuzzy approach', *Fuzzy Sets Syst.*, vol. 83, no. 2, pp. 135-141.

Swain, A.D. & Guttmann, H.E. 1983, *Handbook of Human Reliability with the Emphasis on Nuclear Power Plant Applications*, USNRC, Washington DC.

Tsiporkova, E. & Boeva, V. 2006, 'Multi-step ranking of alternatives in a multi-criteria and multi-expert decision making environment', *Inform. Sci.*, vol. 176, no. 18, pp. 2673-2697.

Tuomisto, J.T., Wilson, A., J.S., E. & Tainio, M. 2008, 'Uncertainty in mortality response to airborne fine particulate matter: Combining European air pollution experts', *Reliab. Eng. Syst. Saf.*, vol. 93, no. 5, pp. 732-744.

Uryas'ev, S. & Vallerga, H. 1993, 'Optimization of test strategies: A general approach', *Reliab. Eng. Syst. Saf.*, vol. 41, no. 2, pp. 155-165.

van der Borst, M. & Schoonakker, H. 2001, 'An overview of PSA importance measures', *Reliab. Eng. Syst. Saf.*, vol. 72, no. 3, pp. 241-245.

Van Leekwijck, W. & Kerre, E.E. 1999, 'Defuzzification: Criteria and classification', *Fuzzy Sets Syst.*, vol. 108, no. 2, pp. 159-178.

Verma, A.K., Srividya, A. & Karanki, D.R. 2010, 'System reliability modeling', in *Reliability and Safety Engineering*, Springer-Verlag, London, pp. 71-168.

Vesely, W.E., Goldberg, F.F., Roberts, N.N. & Haasl, D.F. 1981, *Fault Tree Handbook*, Systems and Reliability Research, in U.S.N.R. Commission (ed.) vol. Nureg-0492, Washington, D.C.

Vinod, G., Kushwaha, H.S., Verma, A.K. & Srividya, A. 2003, 'Importance measures in ranking piping components for risk informed in-service inspection', *Reliab. Eng. Syst. Saf.*, vol. 80, no. 2, pp. 107-113.

Wall, I.B., Haugh, J.J. & Worlege, D.H. 2001, 'Recent applications of PSA for managing nuclear power plant safety', *Prog. Nucl. Energy*, vol. 39, no. 3-4, pp. 367-425.

Wang, A., Luo, Y., Tu, G. & Pei Liu, P. 2011, 'Quantitative evaluation of human-reliability based on fuzzy-clonal selection', *IEEE Trans. Reliab.*, vol. 60, no. 3, pp. 517-527.

Wang, Y.J. & Lee, H.S. 2008, 'The revised method of ranking fuzzy numbers with an area between the centroid and original points', *Comput. Math. Appl.*, vol. 55, no. 9, pp. 2033-2042.

Wang, Y.M. 2009, 'Centroid defuzzification and the maximizing set and minimizing set ranking based on alpha level sets', *Comput. Ind. Eng.*, vol. 57, no. 1, pp. 228-236.

Wang, Y.M., Chin, K.S., Poon, G.K.K. & Yang, J.B. 2009, 'Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean', *Expert Syst. Appl.*, vol. 36, no. 2, pp. 1195-1207.

Wang, Y.M., Yang, J.B., Xu, D.L. & Chin, K.S. 2006, 'On the centroids of fuzzy numbers', *Fuzzy Sets Syst.*, vol. 157, no. 7, pp. 919-926.

Wierman, T.E., Beck, S.T., Calley, M.B., Eide, S.A., Gentillon, C.D. & Kohn, W.E. 2001a, 'Reliability study: Babcock & Wilcox reactor protection system, 1984–1998', NUREG/CR-5500, Vol. 11, USNRC, Washington DC.

Wierman, T.E., Beck, S.T., Calley, M.B., Eide, S.A., Gentillon, C.D. & Kohn, W.E. 2001b, 'Reliability study: Combustion engineering reactor protection system, 1984–1998', NUREG/CR-5500, Vol. 10, USNRC, Washington DC.

Wolkenhauer, O. 2001, 'Fuzzy mathematics', in *Data Engineering: Fuzzy Mathematics in Systems Theory and Data Analysis*, John Wiley & Sons, New York, pp. 197-212.

Wu, J.S., Apostolakis, G.E. & Okrent, D. 1990, 'Uncertainties in system analysis: Probabilistic versus nonprobabilistic theories', *Reliab. Eng. Syst. Saf.*, vol. 30, no. 1-3, pp. 163-181.

Wu, T., Tu, G., Bo, Z.Q. & Klimek, A. 2007, 'Fuzzy set theory and fault tree analysis based method suitable for fault diagnosis of power transformer', in *Proceedings of IEEE International Conference on Intelligent Systems Applications to Power Systems*, pp. 1-5.

Xu, K., Tang, L.C., Xie, M., Ho, S.L. & Zhu, M.L. 2002, 'Fuzzy assessment of FMEA for engine systems', *Reliab. Eng. Syst. Saf.*, vol. 75, no. 1, pp. 17-29.

Yang, G. 2007, 'Potential failure mode avoidance', in *Life Cycle Reliability Engineering*, John Wiley & Sons, Hoboken, NJ, pp. 194-235.

Yang, J.B., Wang, Y.M., Xu, D.L. & Chin, K.S. 2006, 'The evidential reasoning approach for MADA under both probabilistic and fuzzy uncertainties', *Eur. J. Oper. Res.*, vol. 171, no. 1, pp. 309-343.

Yang, Z., Bonsall, S. & Wang, J. 2008, 'Fuzzy rule-based Bayesian reasoning approach for prioritization of failures in FMEA', *IEEE Trans. Reliab.*, vol. 57, no. 3, pp. 517-528.

Yuhua, D. & Datao, Y. 2005, 'Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis', *J. Loss Prev. Process Ind.*, vol. 18, pp. 83-88.

Zadeh, L.A. 1965, 'Fuzzy sets', *Inform. Control*, vol. 8, pp. 338-353.

Zadeh, L.A. 1978, 'Fuzzy sets as a basis for a theory of possibility', *Fuzzy Sets Syst.*, vol. 1, no. 1, pp. 3-28.

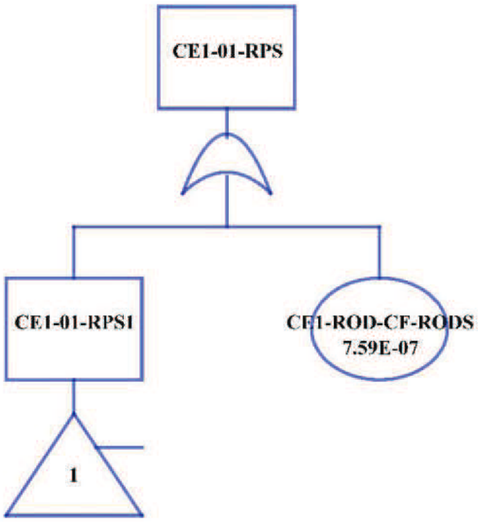
Zhang, G., Ma, J. & Lu, J. 2009, 'Emergency management evaluation by a fuzzy multi-criteria group decision support system ', *Stoch. Env. Res.Risk A.*, vol. 23, no. 4, pp. 517-527.

Zio, E., Baraldi, P., Librizzi, M., Podofillini, L. & Dang, V.N. 2009, 'A fuzzy set-based approach for modeling dependence among human errors', *Fuzzy Sets Syst.*, vol. 160, no. 13, pp. 1947-1964.

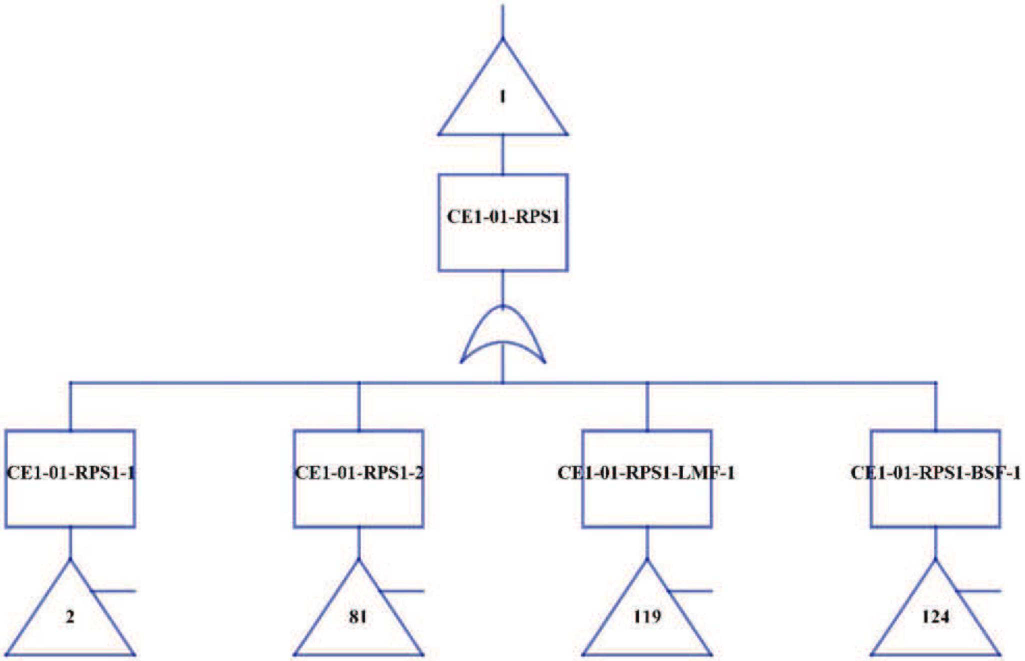
# Appendix A

# FAULT TREES OF THE COMBUSTION ENGINEERING REACTOR PROTECTION SYSTEMS (CERPS) GROUP 1 DESIGNS

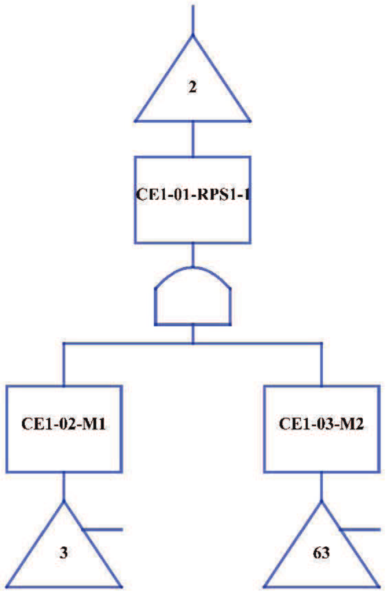
This appendix presents the reactor protection system (RPS) fault trees representing the Combustion Engineering RPS (CERPS) Group 1 designs, which is used to evaluate InFaTAS-NuSA. All fault trees shown in this appendix are generated by InFaTAS-NuSA.



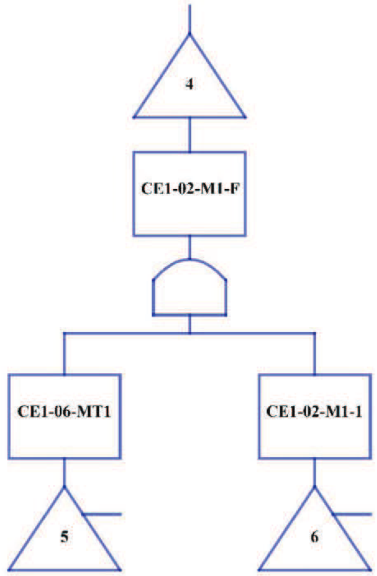
CE1-01-RPS: Reactor Protection System (RPS) for CE Group 1 Type Fails



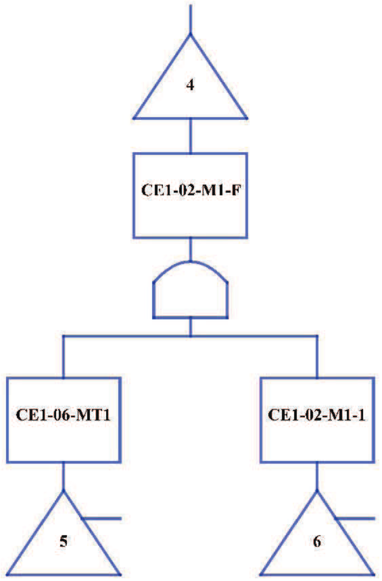
CE1-01-RPS1: Clutch Power Supply Buses Fail to De-Energize



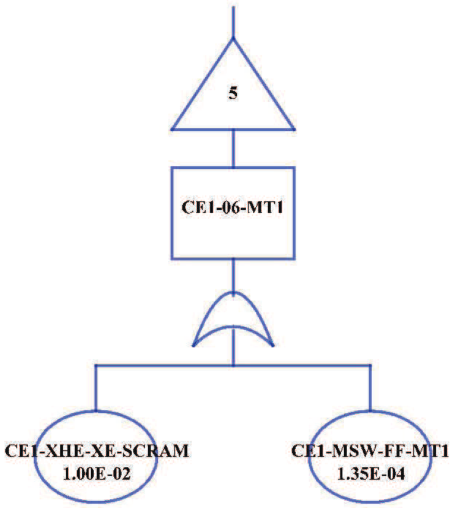
**CE1-01-RPS1-1: Failure of Trip Contactor M1 and M2**



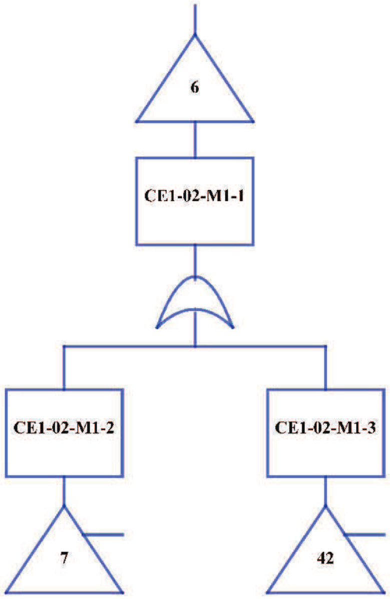
**CE1-02-M1 : Failure of Trip Contact M1**



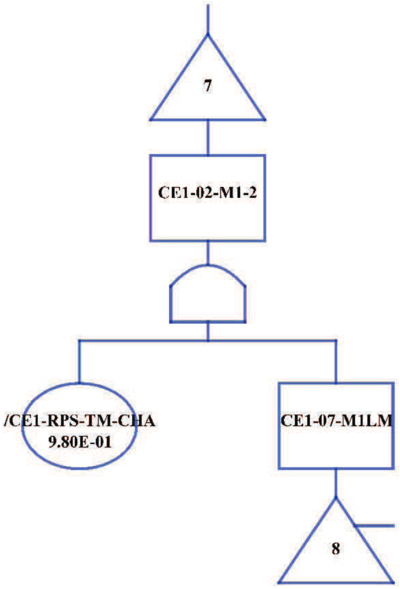
**CE1-02-M1-F: Trip Contact M1 Failures**



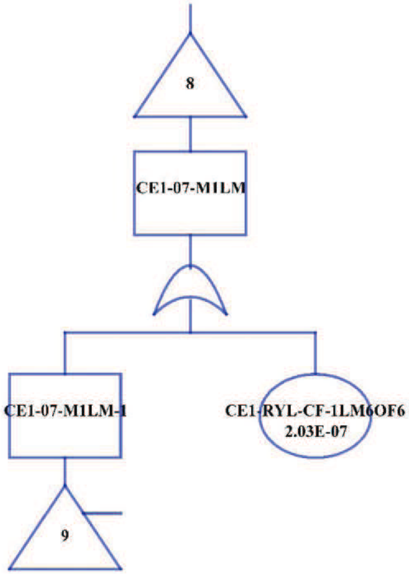
**CE1-06-MT1: Failure of Manual Switch 1**



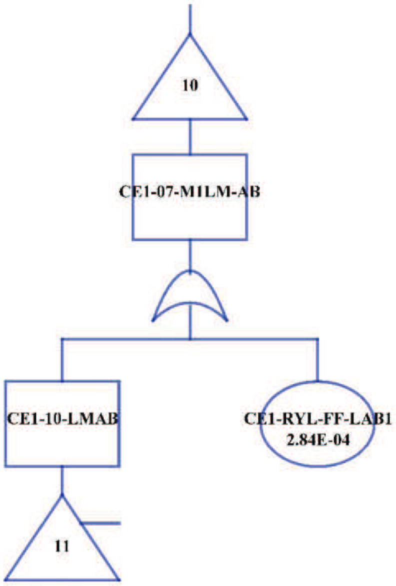
**CE1-02-M1-1: Reactor Trip Logic Matrix Relays for M1 Signal Fail**



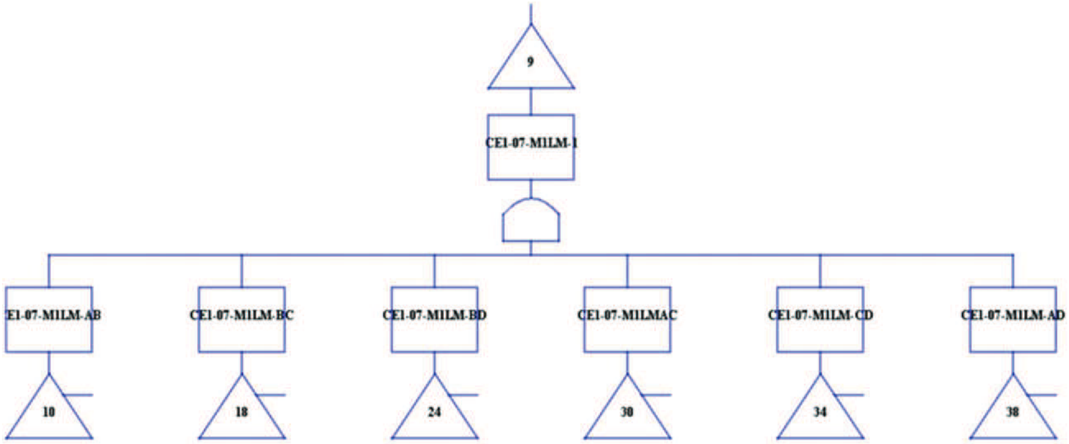
**CE1-02-M1-2: Logic Matrix Relays for M1 Fail (NO RPS T&M)**



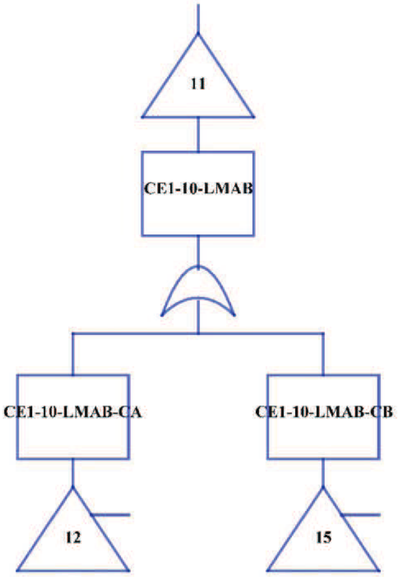
**CE1-07-M1LM: Failure of Logic Matrix Relay For M1 Signal (Ch A not in T&M)**



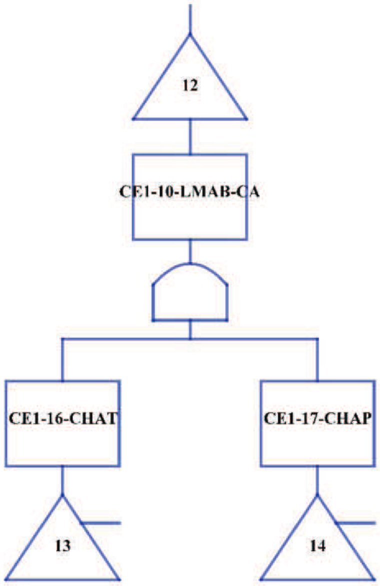
**CE1-07-M1LM-AB: Logic Matrix A Output Relays to M1 Fail**



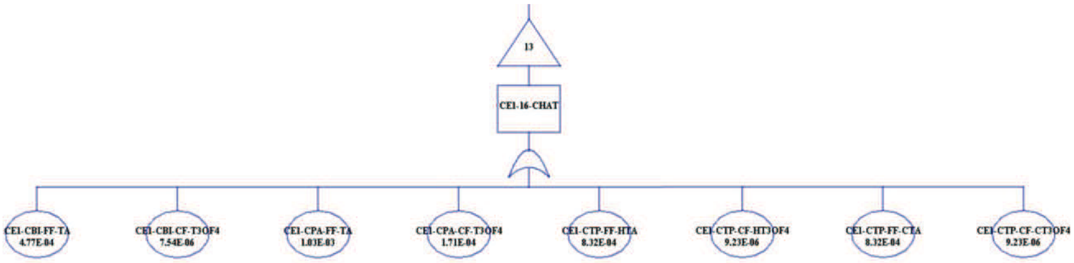
CE1-07-M1LM-1: Logic Matrix Output Relays for M1 Signal Fail



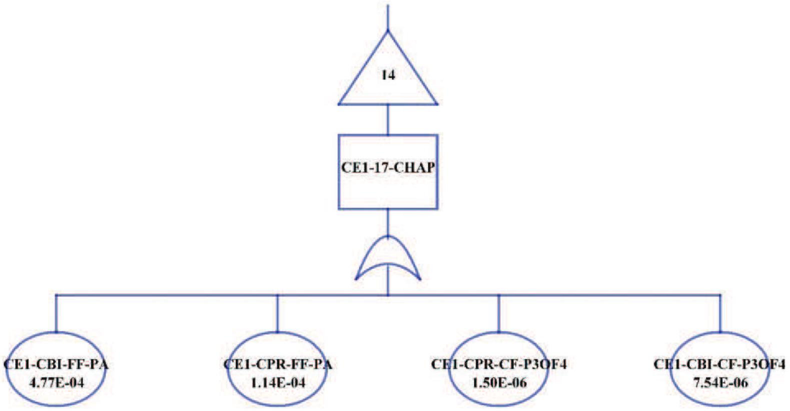
CE1-10-LMAB: Input to Logic Matrix AB Fails



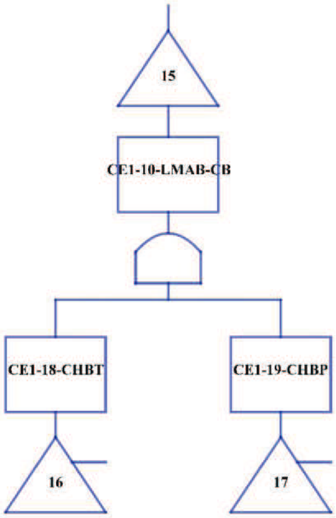
CE1-10-LMAB-CA: Input Signal to Logic Matrix AB From Channel A Fails

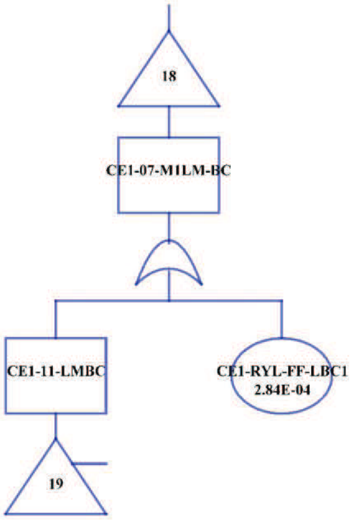


**CE1-16-CHAT: Channel A Temperature Bistable Fails**



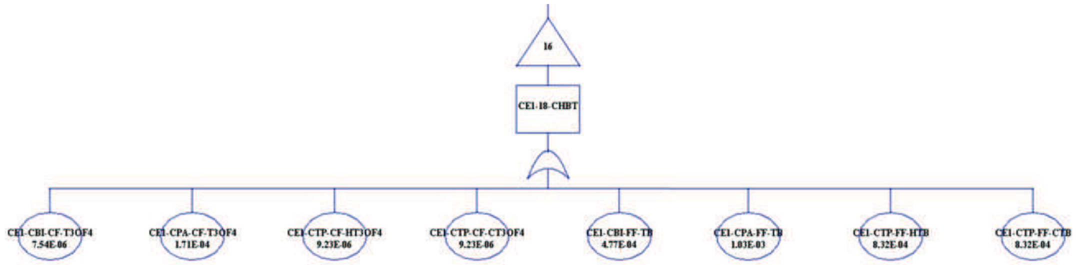
**CE1-17-CHAP: Channel A Pressure Bistable Fails**



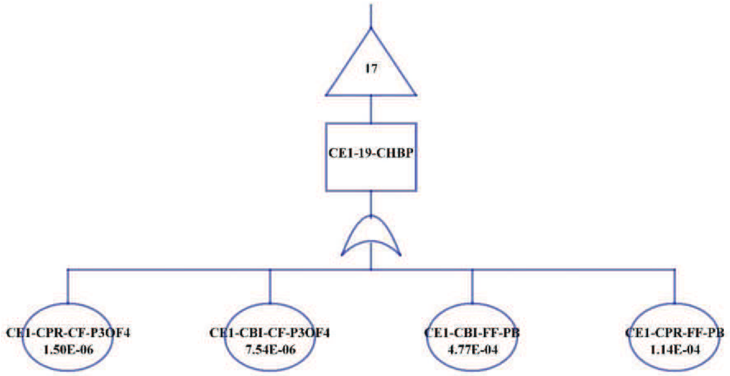


**CE1-10-LMAB-CB: Input Signal to Logic Matrix AB from Channel B Fails**

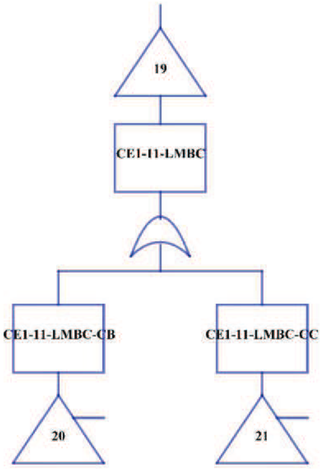
**CE1-07-M1LM-BC: Logic Matrix BC Output Relays to M1 Fail**



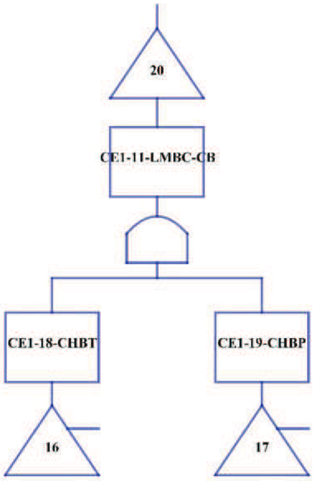
**CE1-18-CHBT: Channel B Temperature Bistable Fails**



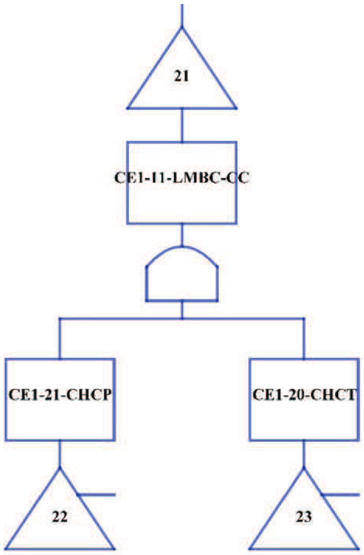
**CE1-19-CHBP: Channel B Pressure Bistable Fails**



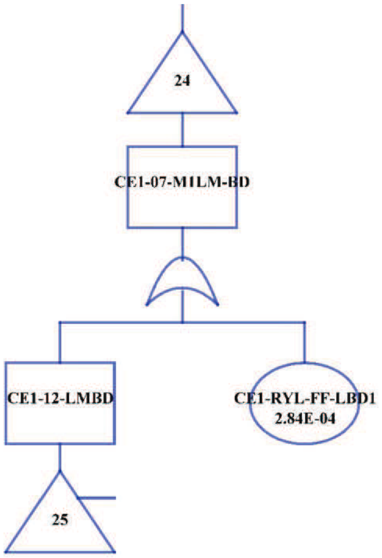
**CE1-11-LMBC: Input to Logic Matrix BC Fails**



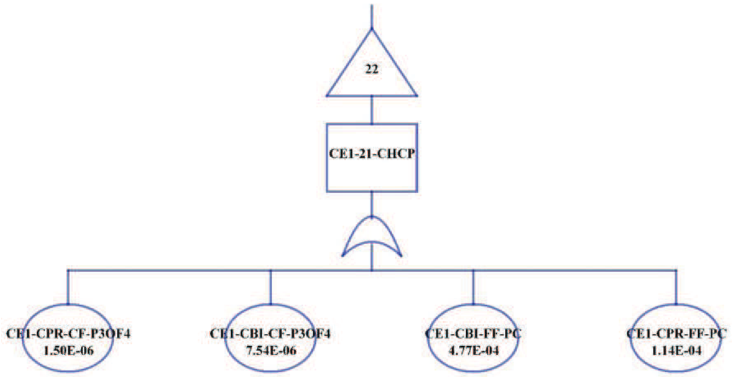
**CE1-11-LMBC-CB: Input Signal to Logic Matrix BC from Channel B Fails**



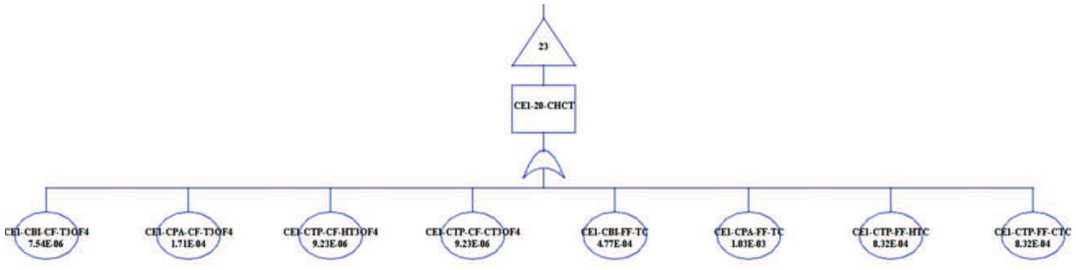
**CE1-11-LMBC-CC: Input Signal to Logic Matrix BC from Channel C Fails**



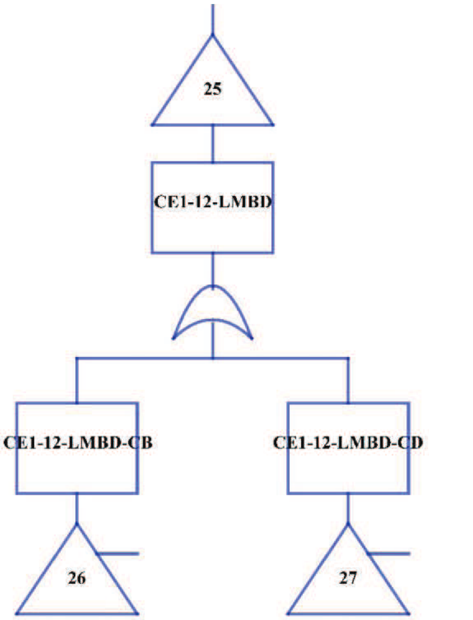
**CE1-07-M1LM-BD: Logic Matrix BD Output Relays to M1 Fail**



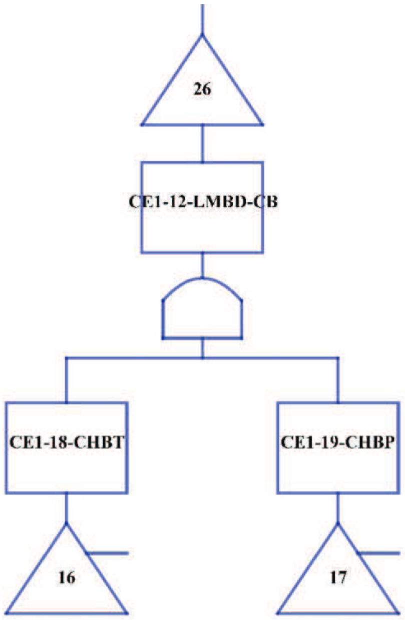
**CE1-21-CHCP: Channel C Pressure Bistable Fails**



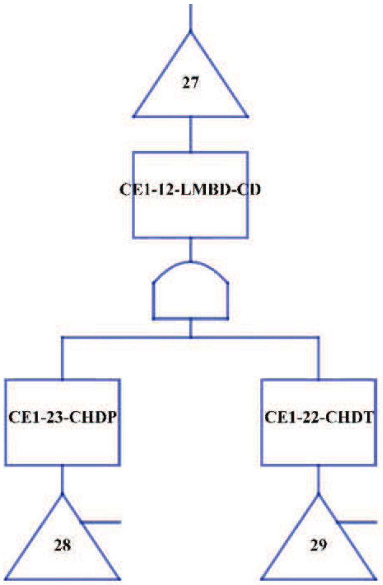
**CE1-20-CHCT: Channel C Temperature Bistable Fails**



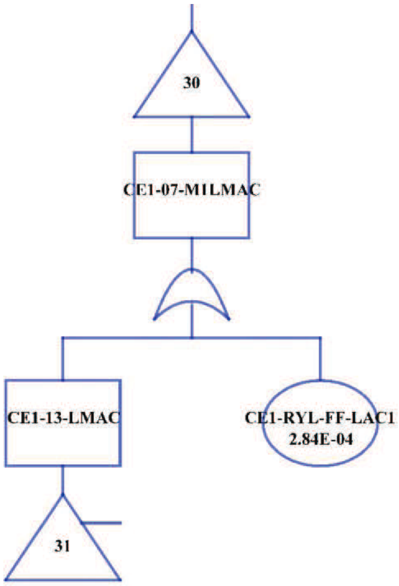
CE1-12-LMBD: Input to Logic Matrix BD Fails



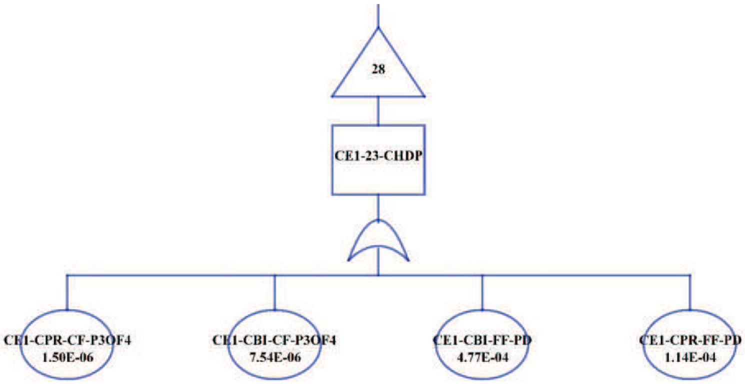
CE1-12-LMBD-CB: Input Signal to Logic Matrix BD from Channel B Fails



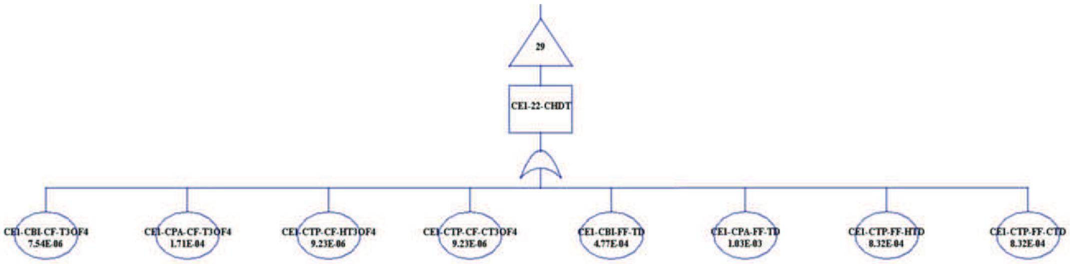
CE1-12-LMBD-CD: Input Signal to Logic Matrix BD from Channel D Fails



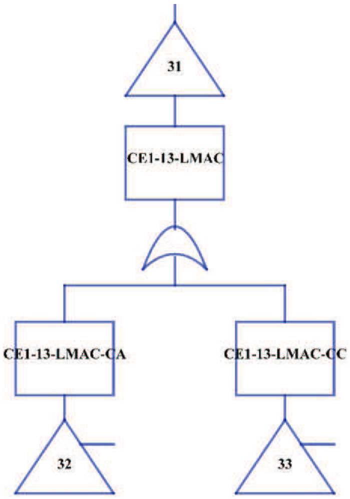
CE1-07-M1LMAC: Logic Matrix AC Output Relays to M1 Fail



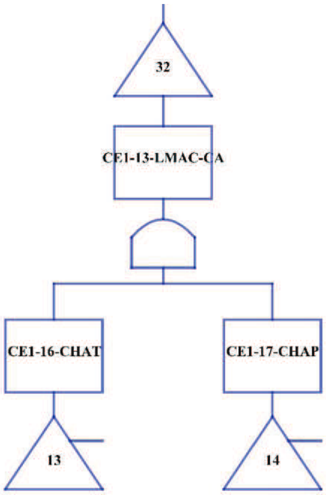
**CE1-23-CHDP: Channel D Pressure Bistable Fails**



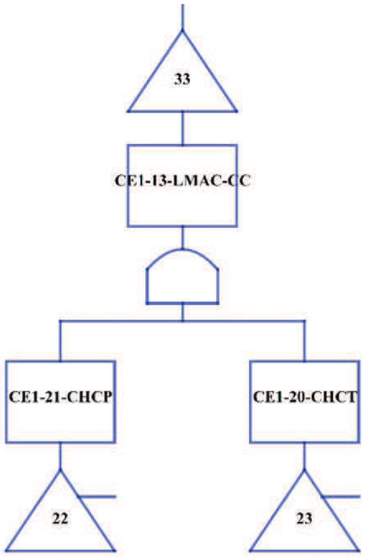
**CE1-22-CHDT: Channel D Temperature Bistable Fails**



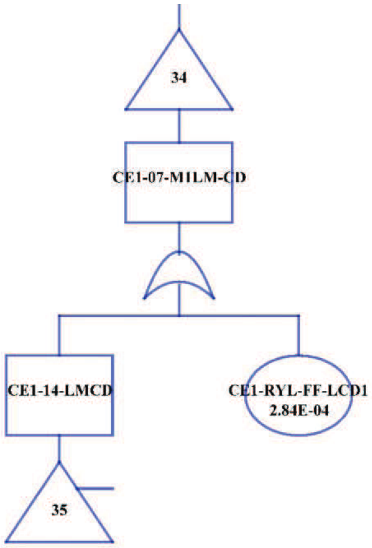
**CE1-13-LMAC: Input to Logic Matrix AC Fails**



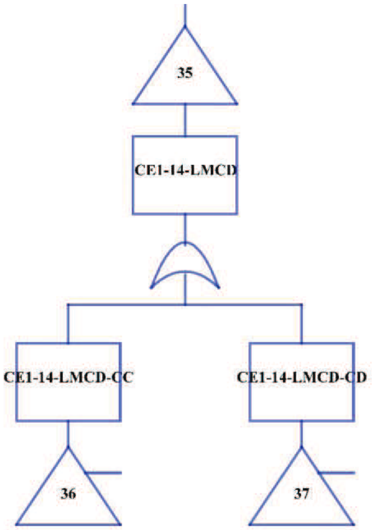
**CE1-13-LMAC-CA: Input Signal to Logic Matrix AC from Channel A Fails**



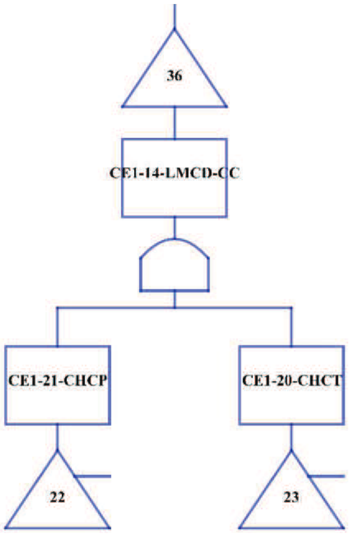
**CE1-13-LMAC-CC: Input Signal to Logic Matrix AC from Channel C Fails**



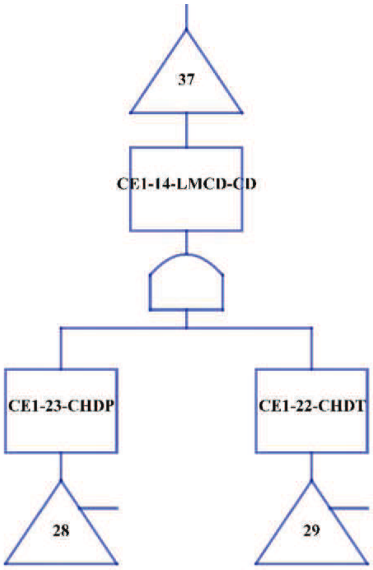
**CE1-07-M1LM-CD: Logic Matrix CD Output Relays to M1 Fail**



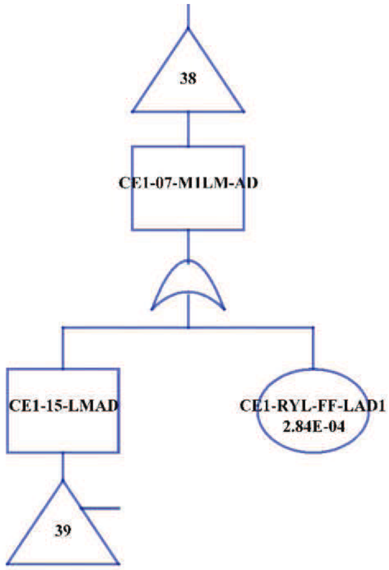
**CE1-14-LMCD: Input to Logic Matrix CD Fails**



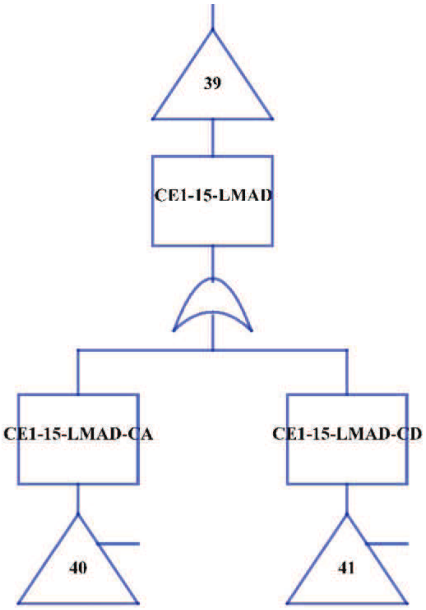
**CE1-14-LMCD-CC: Input Signal to Logic Matrix CD from Channel C Fails**



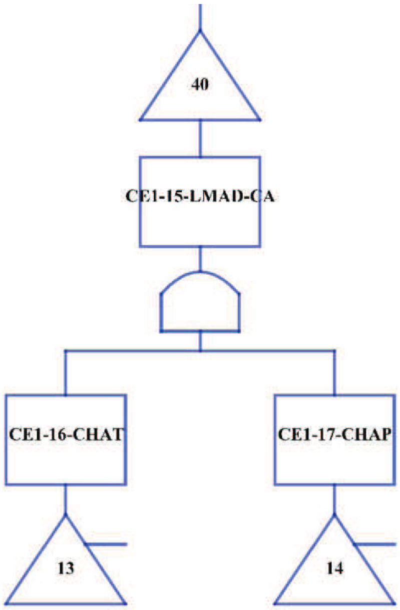
**CE1-14-LMCD-CD: Input Signal to Logic Matrix CD from Channel D Fails**



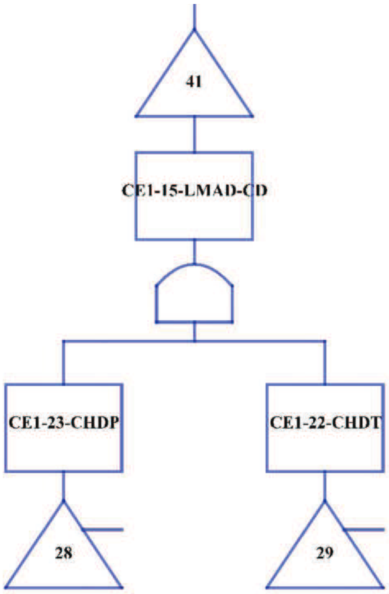
**CE1-07-M1LM-AD: Logic Matrix AD Output Relays to M1 Fail**



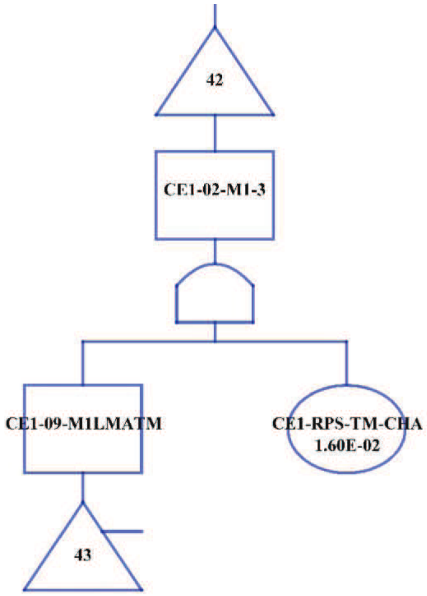
**CE1-15-LMAD: Input to Logic Matrix AD Fails**



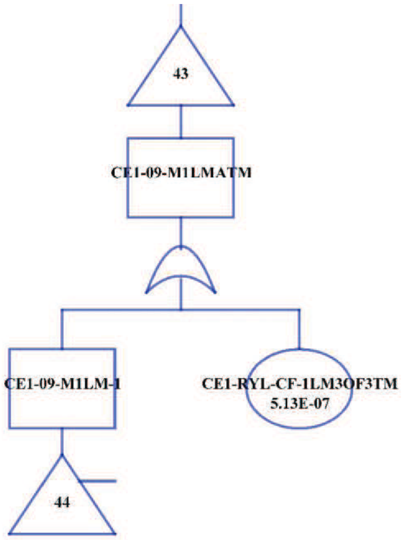
**CE1-15-LMAD-CA: Input Signal to Logic Matrix AD from Channel A Fails**



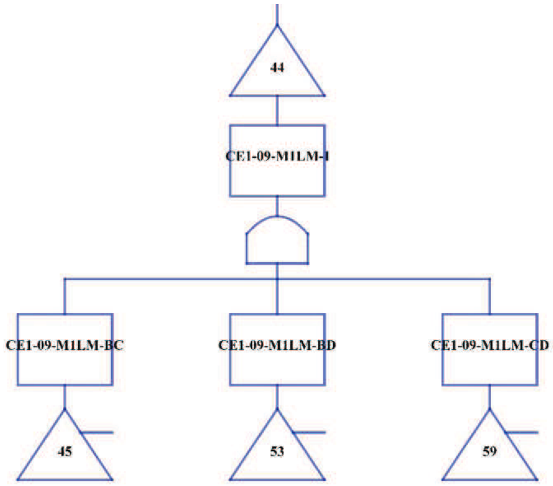
**CE1-15-LMAD-CD: Input Signal to Logic Matrix AD from Channel D Fails**



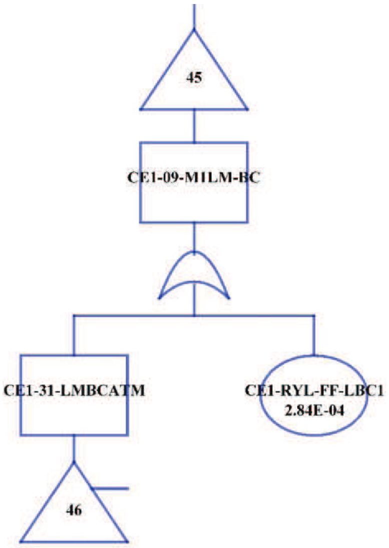
**CE1-02-M1-3: Logic Matrix Relays for M1 Fails (Channel A in T&M)**



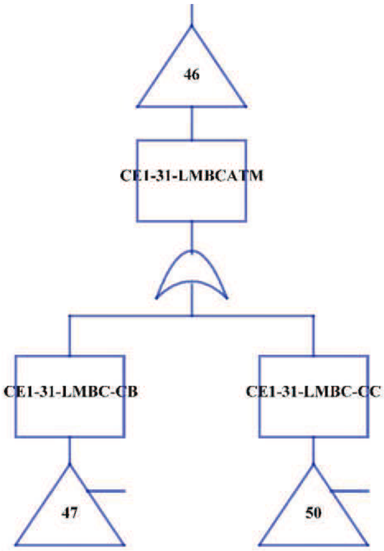
**CE1-09-M1LMATM: Failure of Logic Matrix Relay for M1 Signal (Ch A in T&M)**



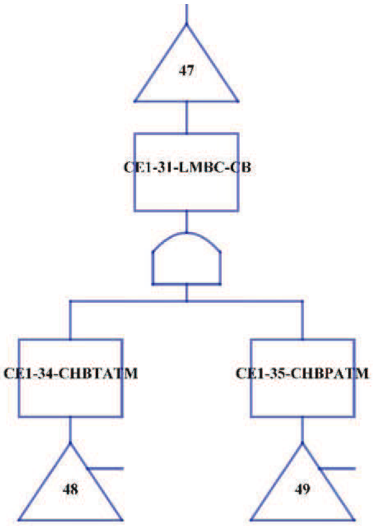
**CE1-09-M1LM-1: Logic Matrix Output Relays for M1 Signal Fail (Ch A T&M)**



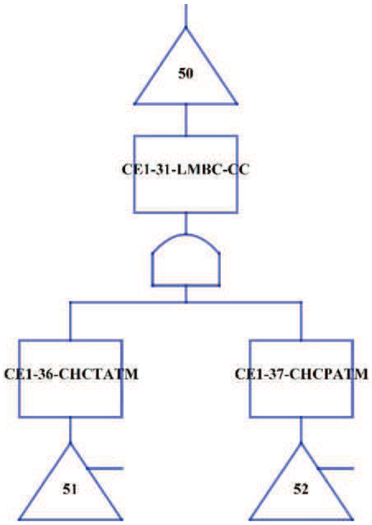
CE1-09-M1LM-BC: Logic Matrix BC Output Relays to M1 Fail



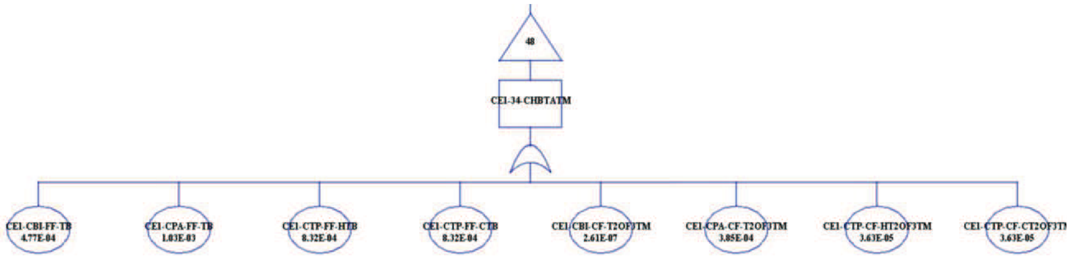
CE1-31-LMBCATM: Input to Logic Matrix BC Fails (Ch A T&M)



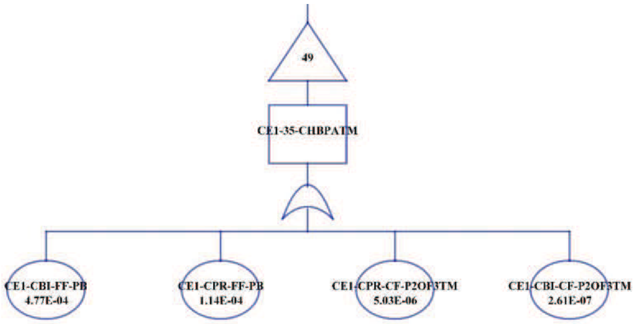
CE1-31-LMBC-CB: Input to Logic Matrix BC from Channel B Fails (Ch A T&M)



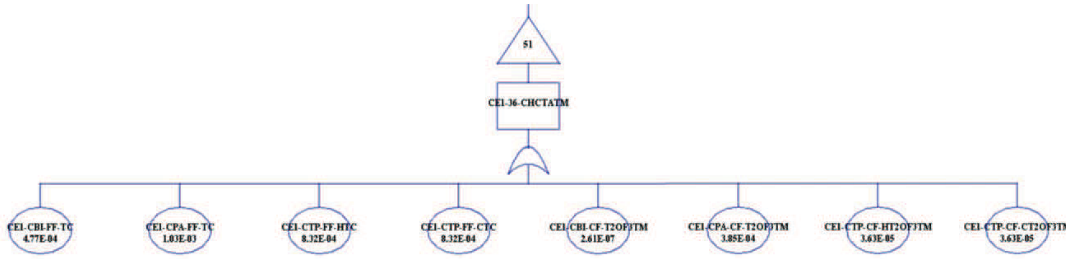
CE1-31-LMBC-CC: Input to Logic Matrix BC from Channel C Fails (Ch A T&M)



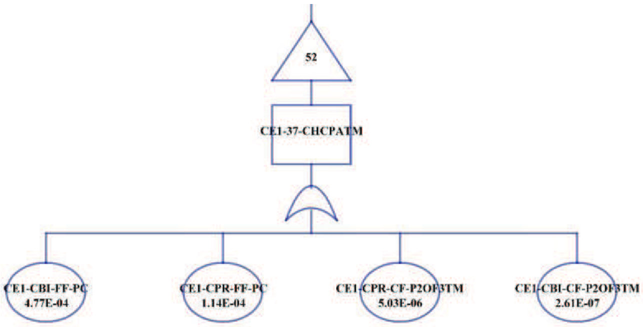
CE1-34-CHBTATM: Channel B Temperature Bistable Fails (Ch A T&M)



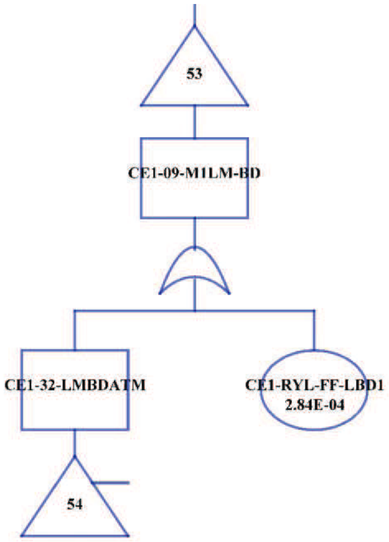
CE1-35-CHBPATM: Channel B Pressure Bistable Fails (Ch A T&M)



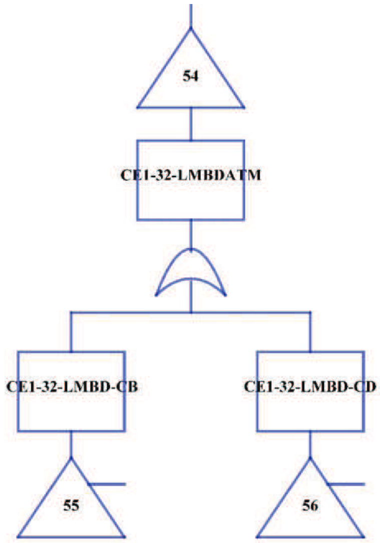
CE1-36-CHCTATM: Channel C Temperature Bistable Fails (Ch A T&M)



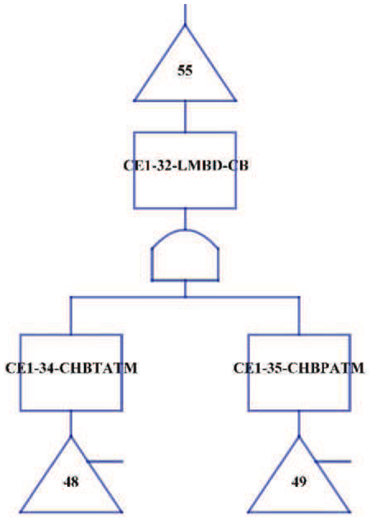
CE1-37-CHCPATM: Channel C Pressure Bistable Fails (Ch A T&M)



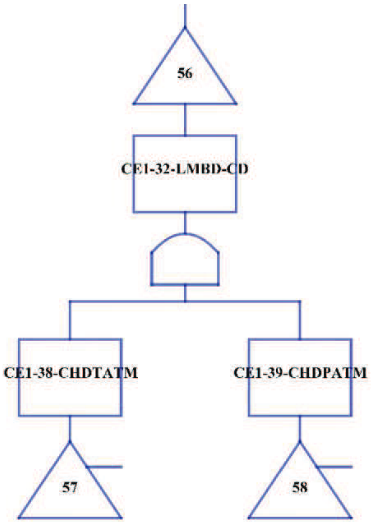
**CE1-09-M1LM-BD: Logic Matrix BD Output Relays to M1 Fail**



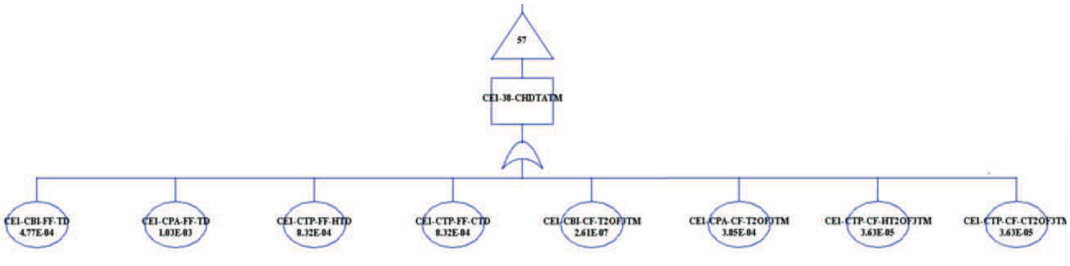
**CE1-32-LMBDATM: Input to Logic Matrix BD Fails (Ch A T&M)**



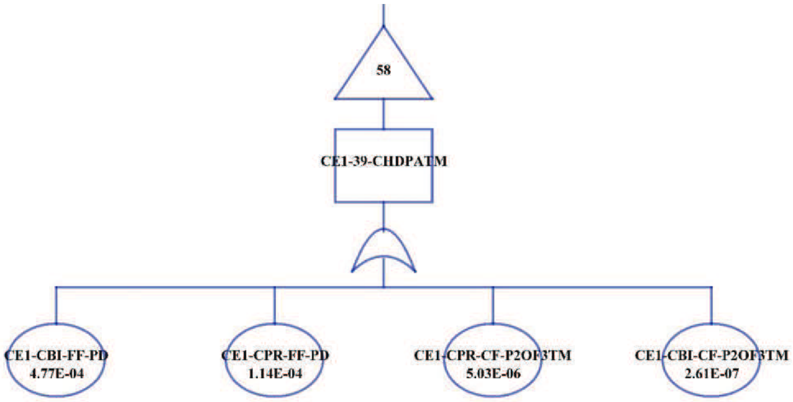
**CE1-32-LMBD-CB: Input to Logic Matrix BD from Channel B Fails (Ch A T&M)**



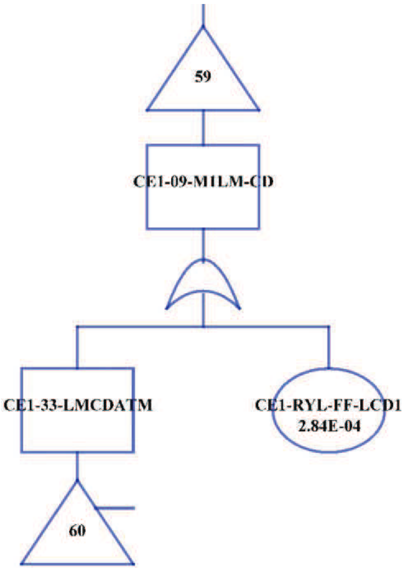
**CE1-32-LMBD-CD: Input to Logic Matrix BD from Channel D Fails (Ch A T&M)**



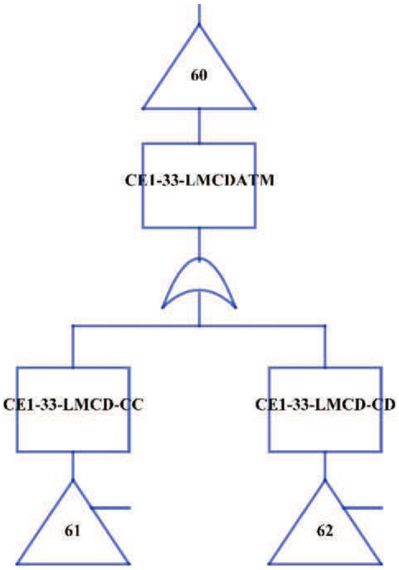
**CE1-38-CHDTATM: Channel D Temperature Bistable Fails (Ch A T&M)**



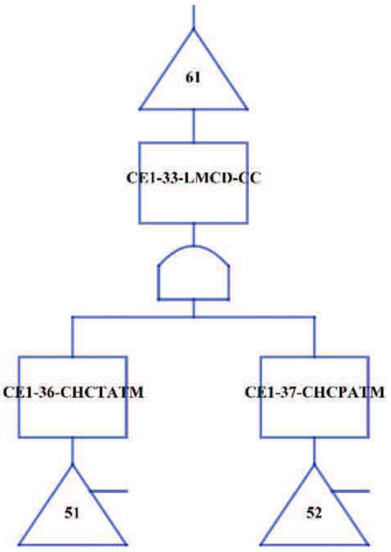
**CE1-39-CHDPATM: Channel D Pressure Bistable Fails (Ch A T&M)**



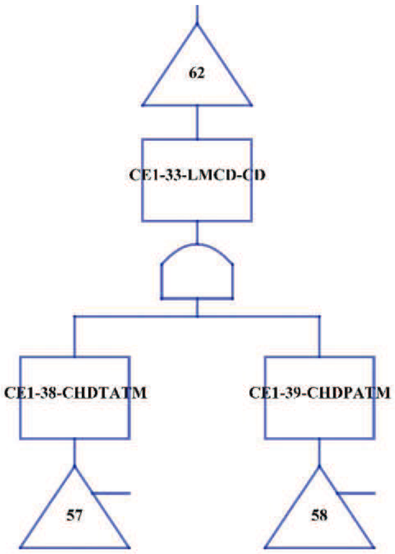
**CE1-09-M1LM-CD: Logic Matrix CD Output Relays to M1 Fail**



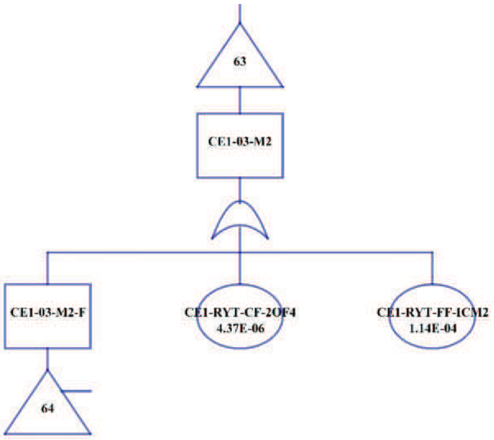
**CE1-33-LMCDATM: Input to Logic Matrix CD Fails (Ch A T&M)**



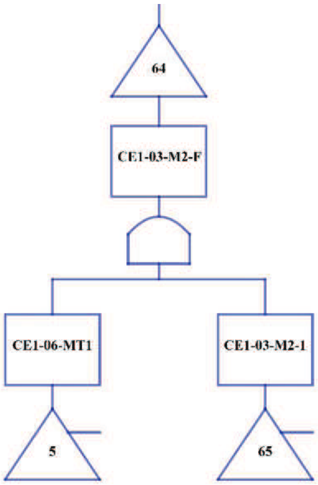
**CE1-33-LMCD-CC: Input to Logic Matrix CD from Channel C Fails (Ch A T&M)**



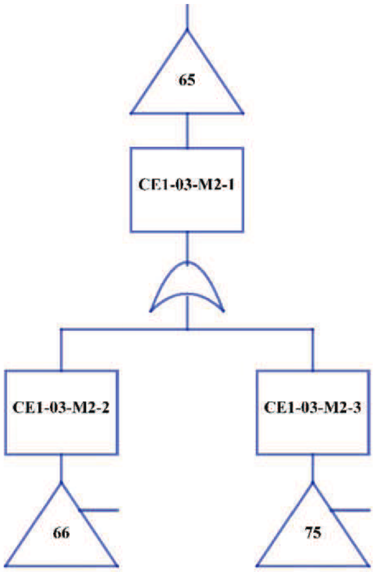
**CE1-33-LMCD-CD: Input to Logic Matrix CD from Channel D Fails (Ch A T&M)**



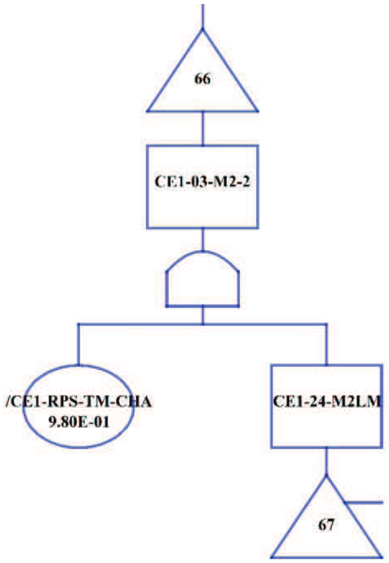
**CE1-03-M2: Failure of Trip Contact M2**



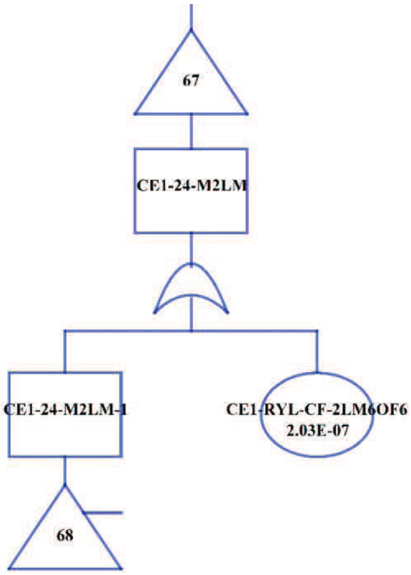
**CE1-03-M2-F: Trip Contact M2 Failures**



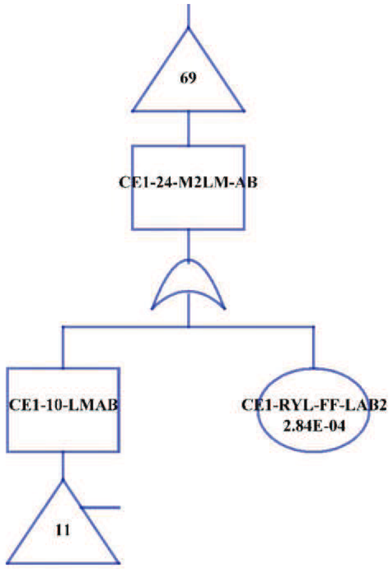
**CE1-03-M2-1: Reactor Trip Logic Matrix Relays for M2 Signal Fail**



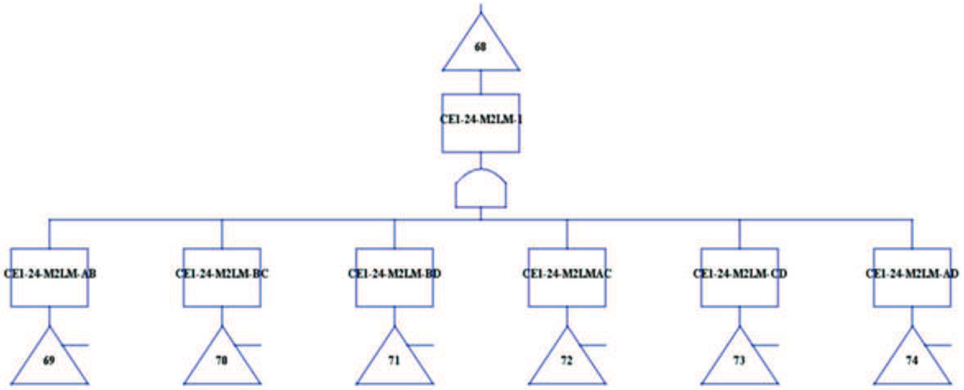
**CE1-03-M2-2: Logic Matrix Relays For M2 Fail (No RPS T&M)**



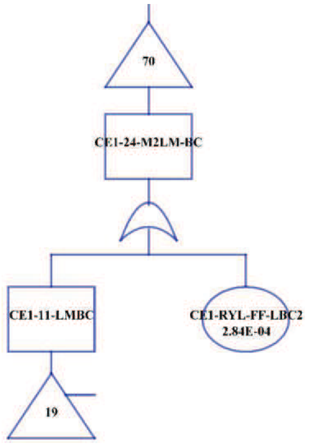
**CE1-24-M2LM: Failure of Logic Matrix Relay for M2 Signal (Ch A not in T&M)**



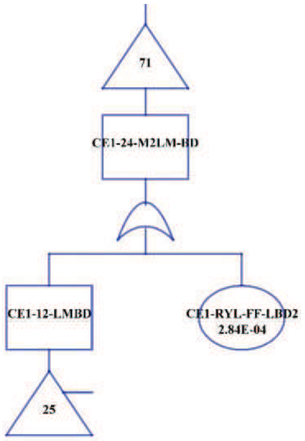
**CE1-24-M2LM-AB: Logic Matrix AB Output Relays to M2 Fail**



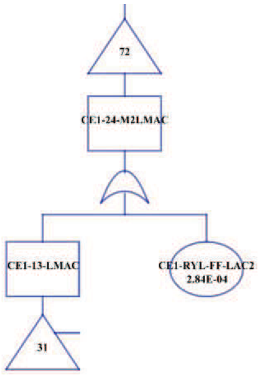
**CE1-24-M2LM-1: Logic Matrix Output Relays for M2 Signal Fail**



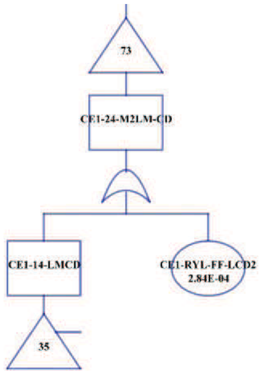
**CE1-24-M2LM-BC: Logic Matrix BC Output Relays to M2 Fail**



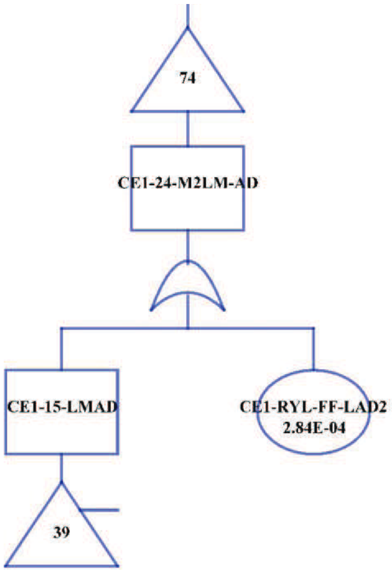
**CE1-24-M2LM-BD: Logic Matrix BD Output Relays to M2 Fail**



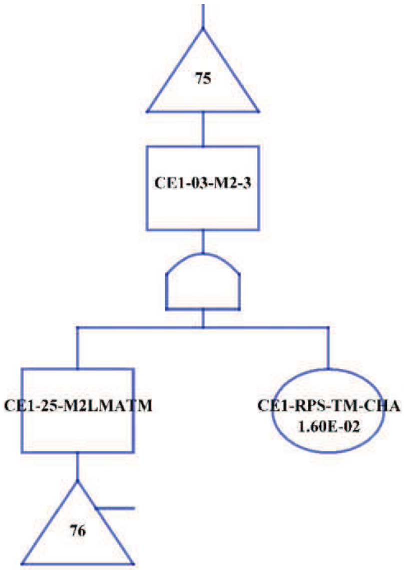
**CE1-24-M2LMAC: Logic Matrix AC Output Relays to M2 Fail**



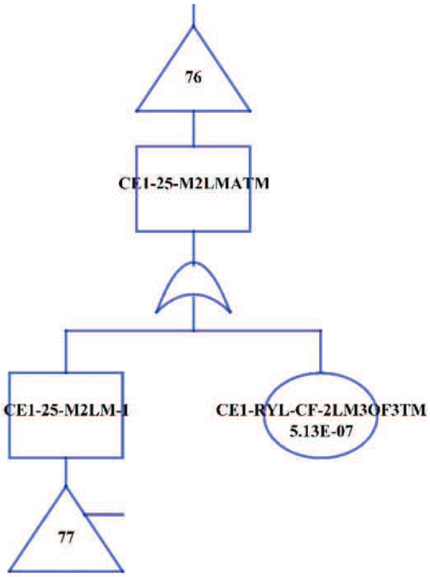
**CE1-24-M2LM-CD: Logic Matrix CD Output Relays to M2 Fail**



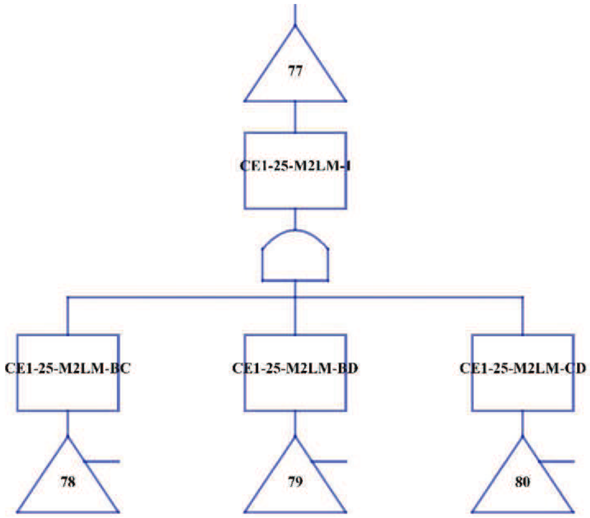
**CE1-24-M2LM-AD: Logic Matrix AD Output Relays to M2 Fail**



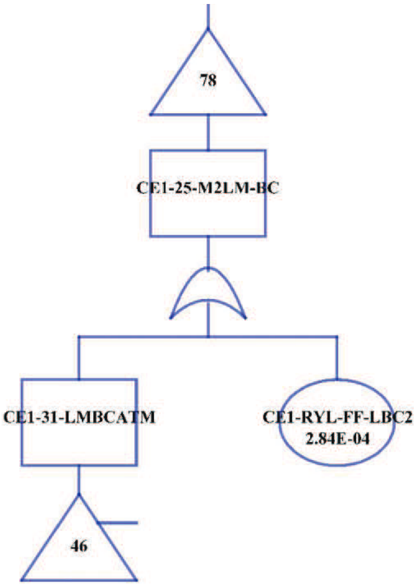
**CE1-03-M2-3: Logic Matrix Relays for M2 Fails (Channel A in T&M)**



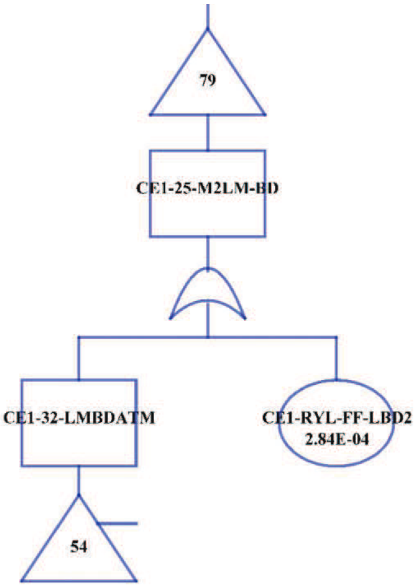
**CE1-25-M2LMATM: Failure of Logic Matrix Relay for M2 Signal (Ch A in T&M)**



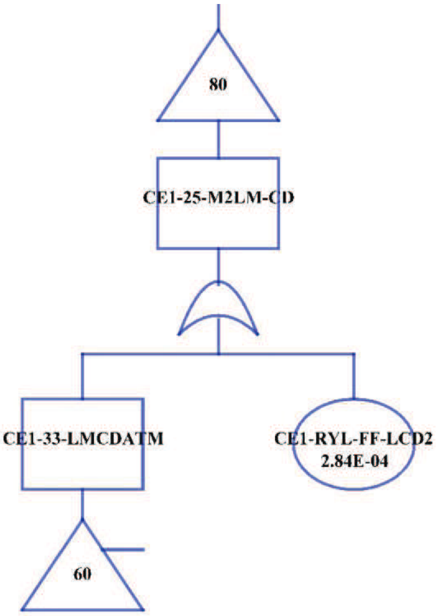
**CE1-25-M2LM-1: Logic Matrix Output Relays for M2 Signal Fail (Ch A T&M)**



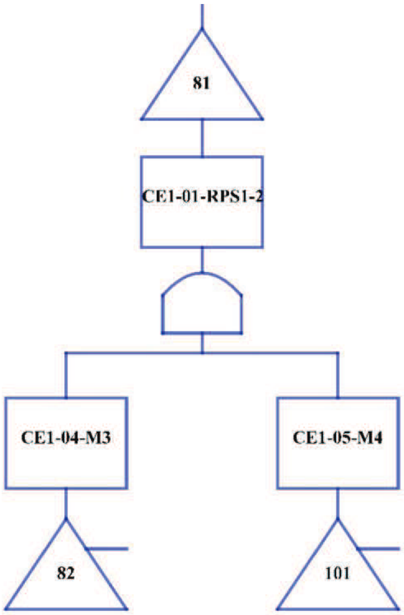
CE1-25-M2LM-BC: Logic Matrix BC Output Relays to M2 Fail



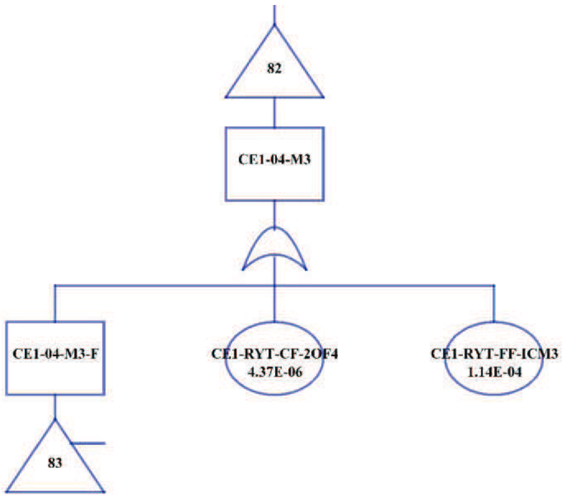
CE1-25-M2LM-BD: Logic Matrix BD Output Relays to M2 Fail



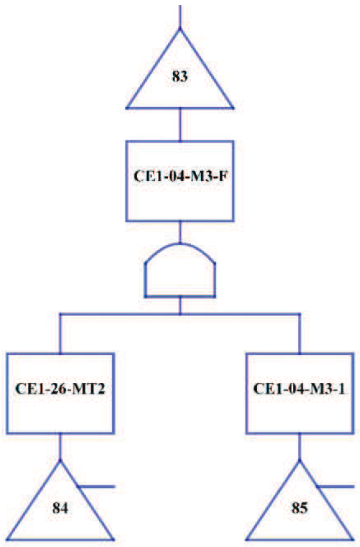
CE1-25-M2LM-CD: Logic Matrix CD Output Relays to M2 Fail



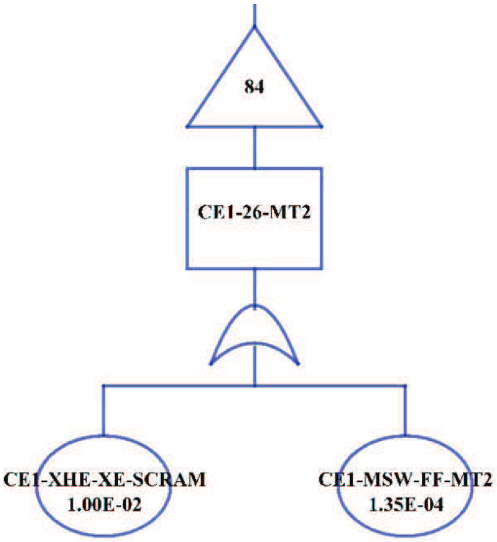
CE1-01-RPS1-2: Failure of Trip Contactor M3 and M4



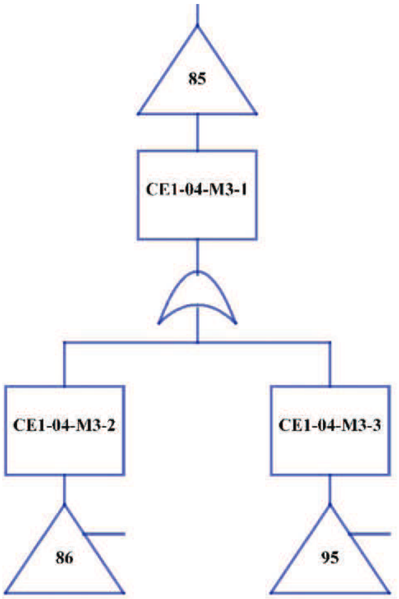
**CE1-04-M3: Failure of Trip Contact M3**



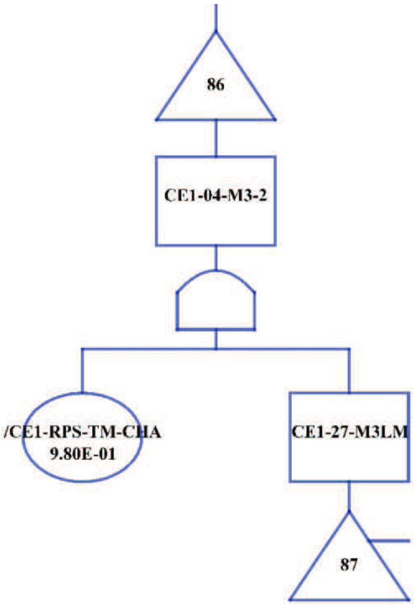
**CE1-04-M3-F: Trip Contact M3 Failures**



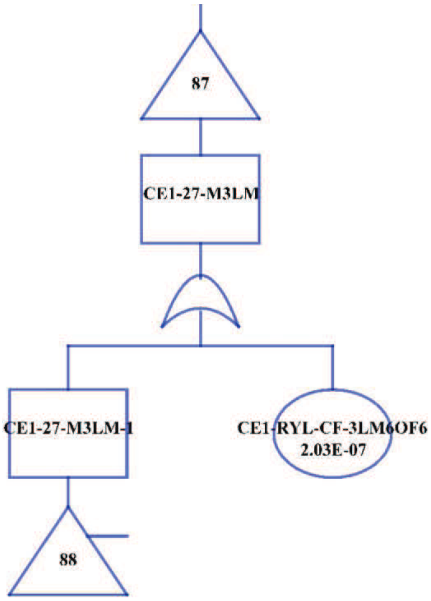
**CE1-26-MT2: Failure of Manual Switch 2**



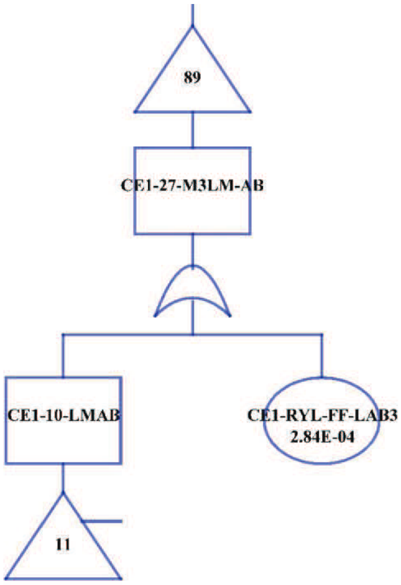
**CE1-04-M3-1: Reactor Trip Logic Matrix Relays for M3 Signal Fail**



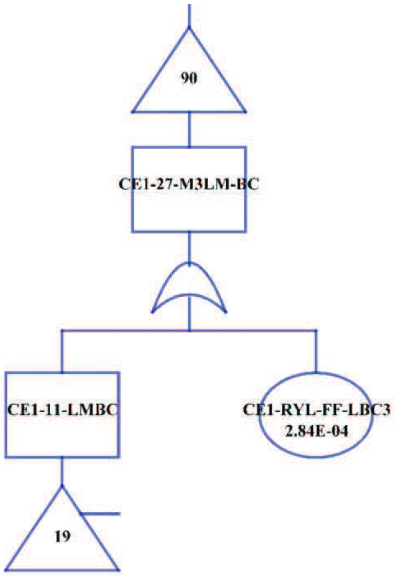
**CE1-04-M3-2: Logic Matrix Relays for M3 Fail (No RPS T&M)**



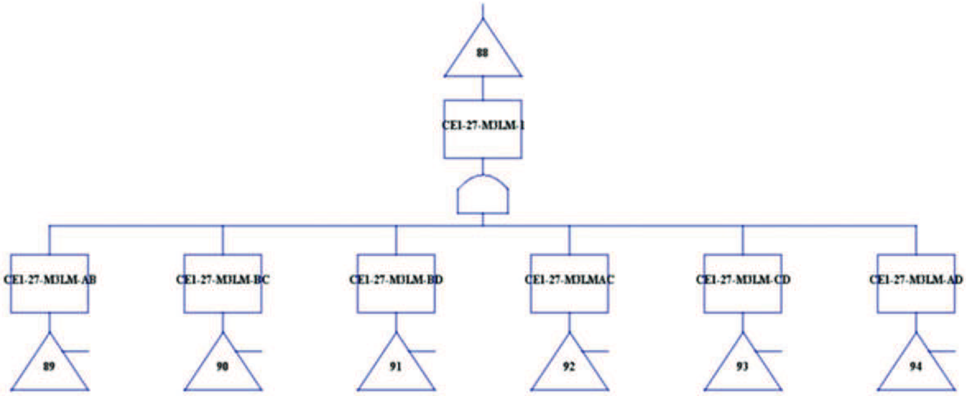
**CE1-27-M3LM: Failure of Logic Matrix Relay for M3 Signal (Ch A not in T&M)**



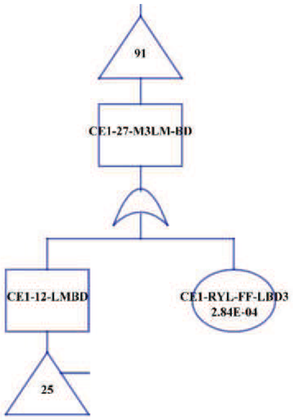
**CE1-27-M3LM-AB: Logic Matrix AB Output Relays to M3 Fail**



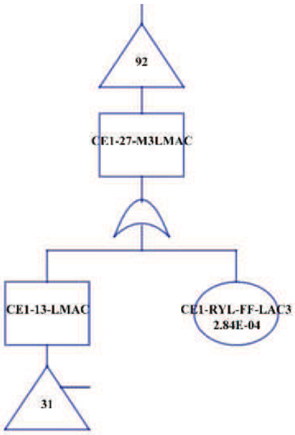
**CE1-27-M3LM-BC: Logic Matrix BC Output Relays to M3 Fail**



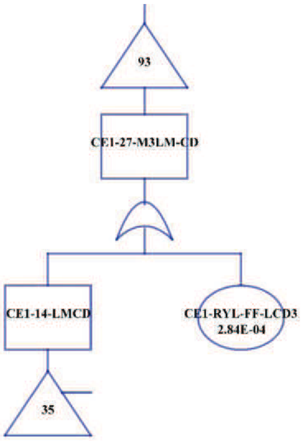
**CE1-27-M3LM-1: Logic Matrix Output Relays for M3 Signal Fail**



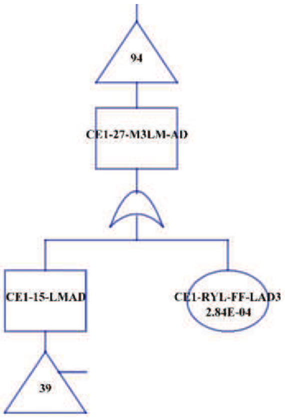
**CE1-27-M3LM-BD: Logic Matrix BD Output Relays to M3 Fail**



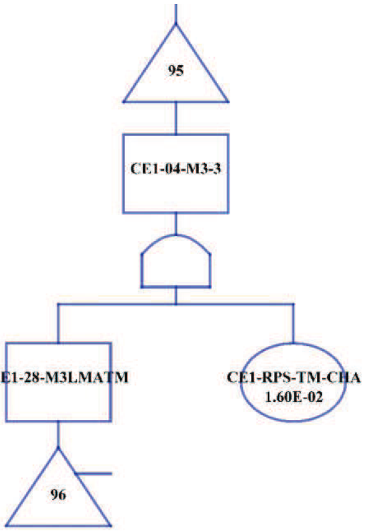
**CE1-27-M3LMAC: Logic Matrix AC Output Relays to M3 Fail**



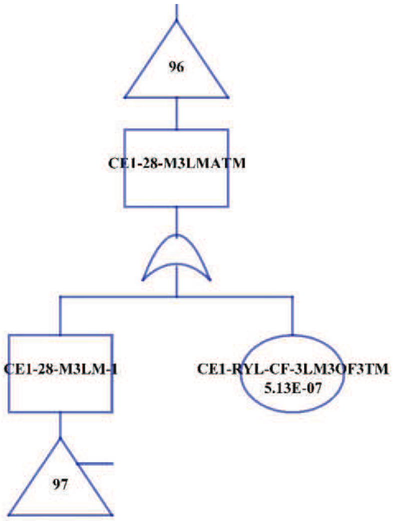
**CE1-27-M3LM-CD: Logic Matrix CD Output Relays to M3 Fail**



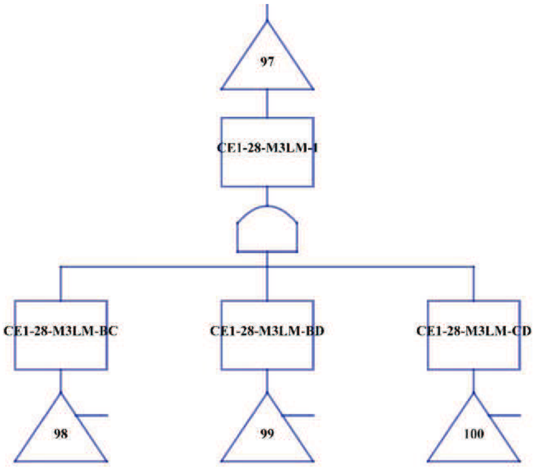
**CE1-27-M3LM-AD: Logic Matrix AD Output Relays to M3 Fail**



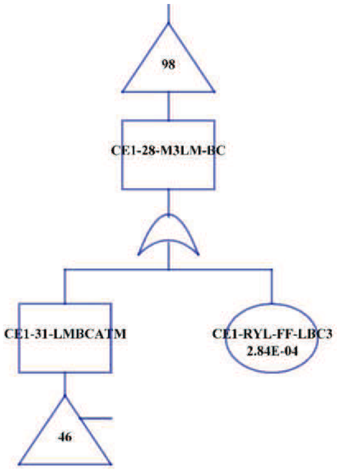
**CE1-04-M3-3: Logic Matrix Relays for M3 Fails (Channel A in T&M)**



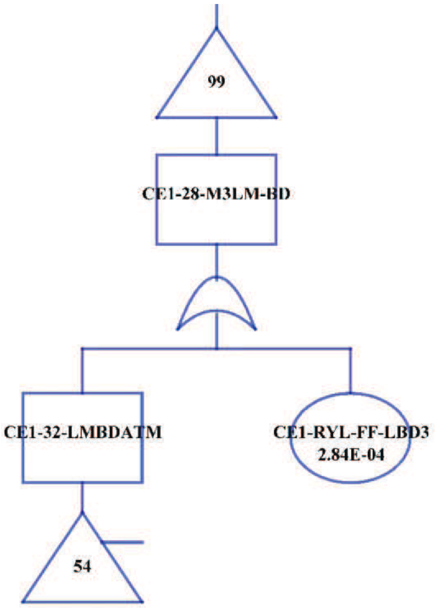
**CE1-28-M3LMATM: Failure of Logic Matrix Relay for M3 Signal (Ch A in T&M)**



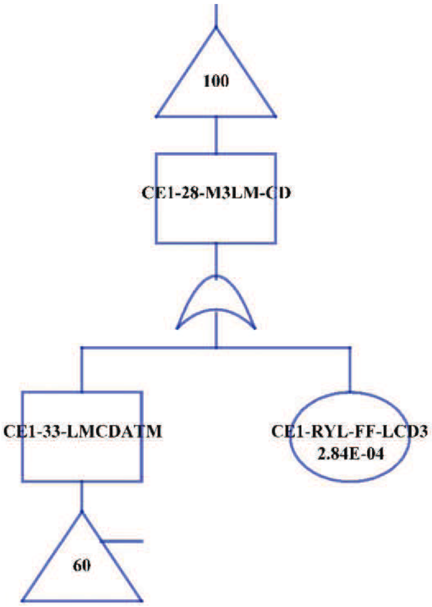
**CE1-28-M3LM-1: Logic Matrix Output Relays for M3 Signal Fail (Ch A T&M)**



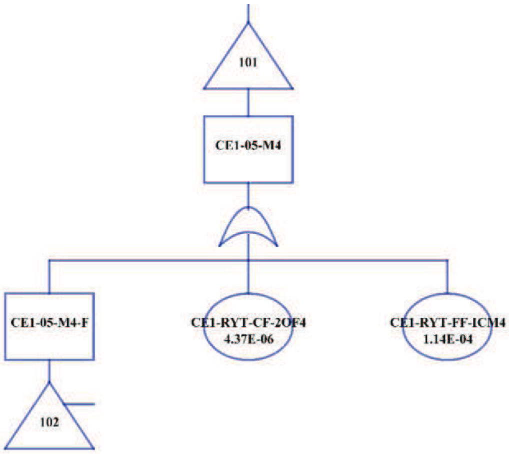
**CE1-28-M3LM-BC: Logic Matrix BC Output Relays to M3 Fail**



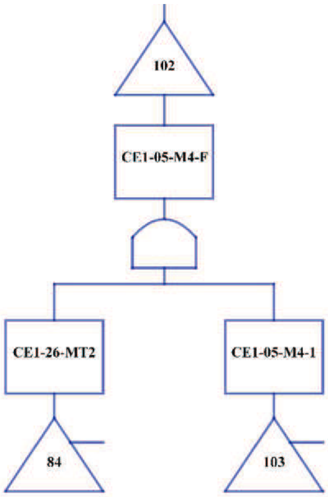
CE1-28-M3LM-BD: Logic Matrix BD Output Relays to M3 Fail



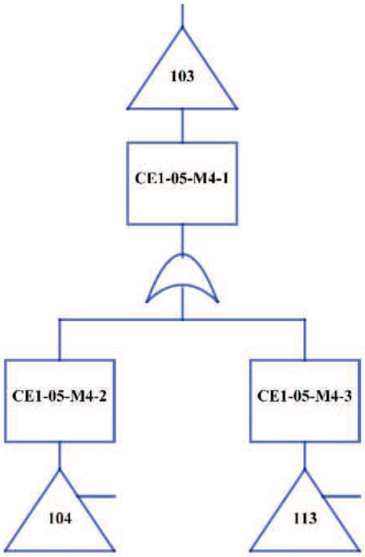
CE1-28-M3LM-CD: Logic Matrix CD Output Relays to M3 Fail



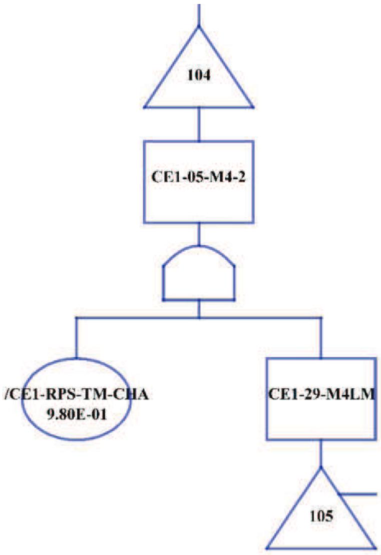
CE1-05-M4: Failure of Trip Contact M4



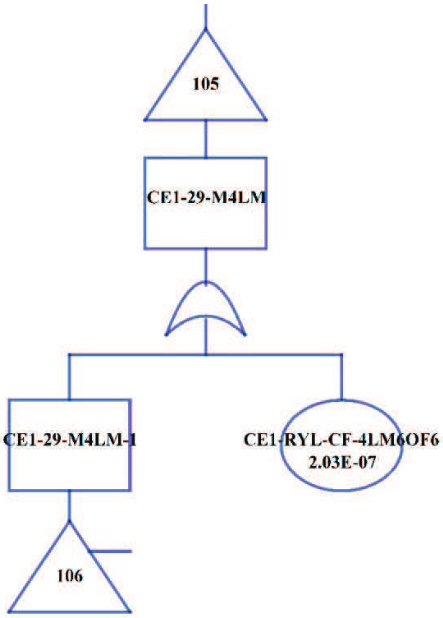
CE1-05-M4-F: Trip Contact M4 Failures



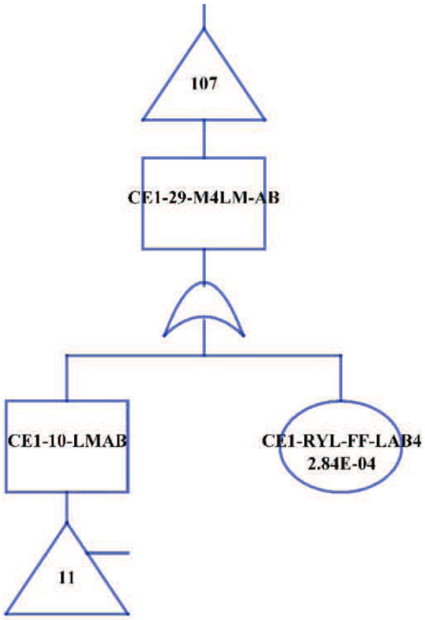
**CE1-05-M4-1: Reactor Trip Logic Matrix Relays for M4 Signal Fail**



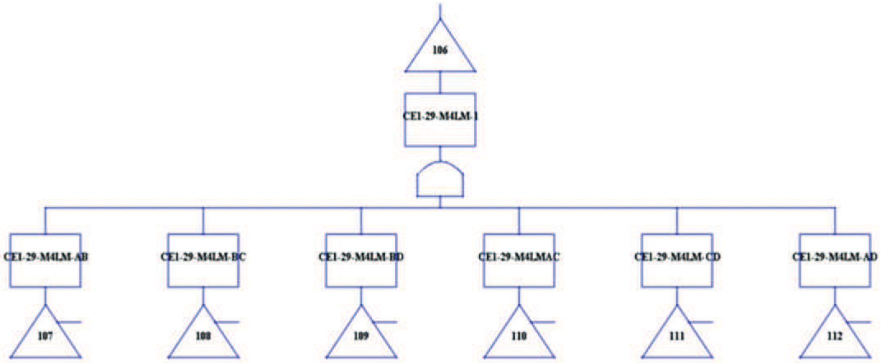
**CE1-05-M4-2: Logic Matrix Relays for M4 Fail (No RPS T&M)**



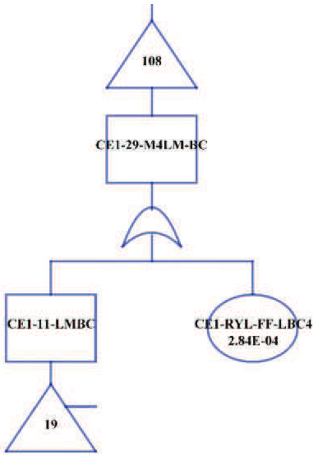
**CE1-29-M4LM: Failure of Logic Matrix Relay for M4 Signal (Ch A not in T&M)**



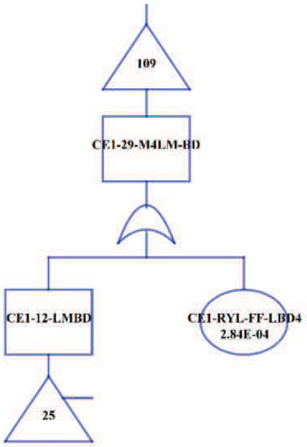
**CE1-29-M4LM-AB: Logic Matrix AB Output Relays to M4 Fail**



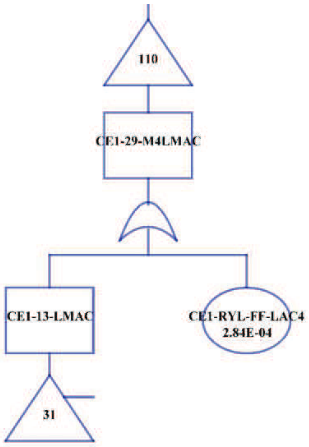
**CE1-29-M4LM-1: Logic Matrix Output Relays for M4 Signal Fail**



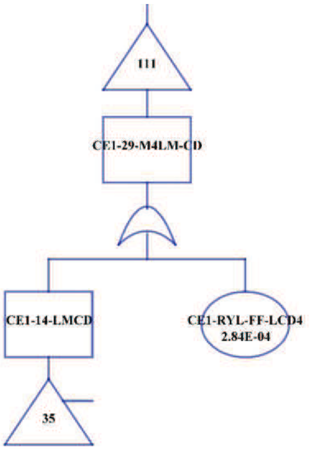
**CE1-29-M4LM-BC: Logic Matrix BC Output Relays to M4 Fail**



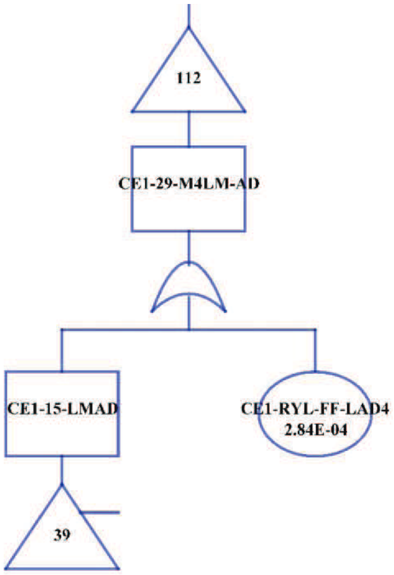
**CE1-29-M4LM-BD: Logic Matrix BD Output Relays to M4 Fail**



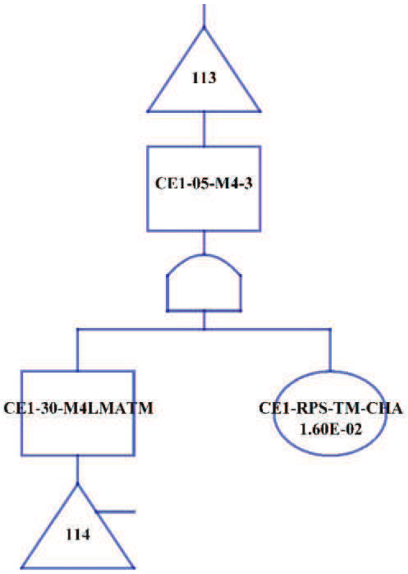
**CE1-29-M4LMAC: Logic Matrix AC Output Relays to M4 Fail**



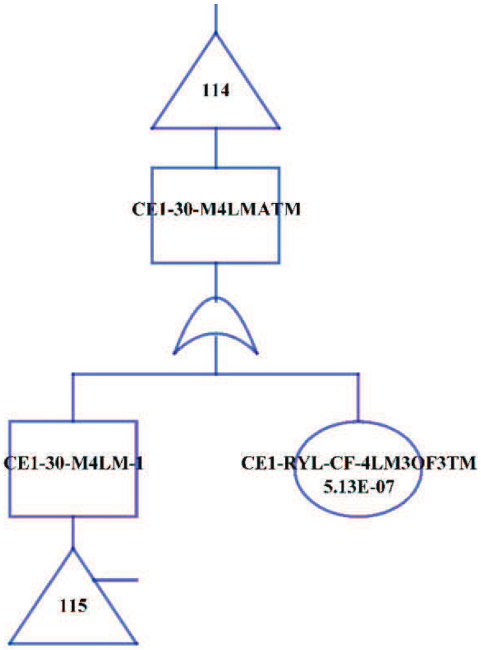
**CE1-29-M4LM-CD: Logic Matrix CD Output Relays to M4 Fail**



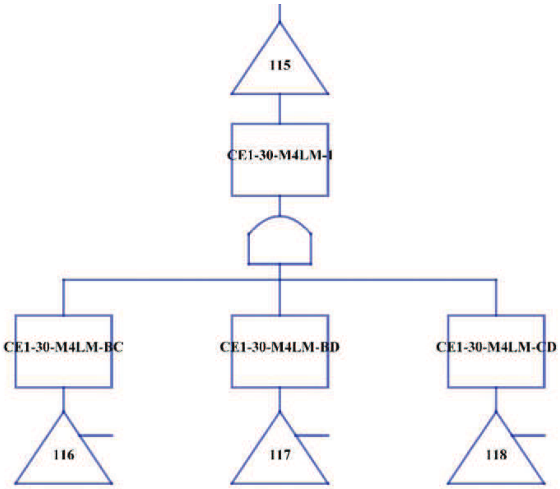
**CE1-29-M4LM-AD: Logic Matrix AD Output Relays to M4 Fail**



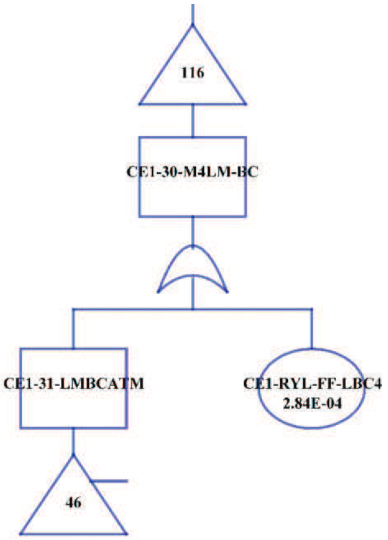
**CE1-05-M4-3: Logic Matrix Relays for M4 Fails (Channel A in T&M)**



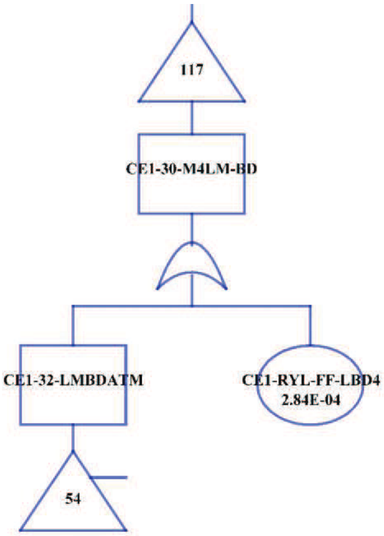
**CE1-30-M4LMATM: Failure of Logic Matrix Relay for M4 Signal (Ch A in T&M)**



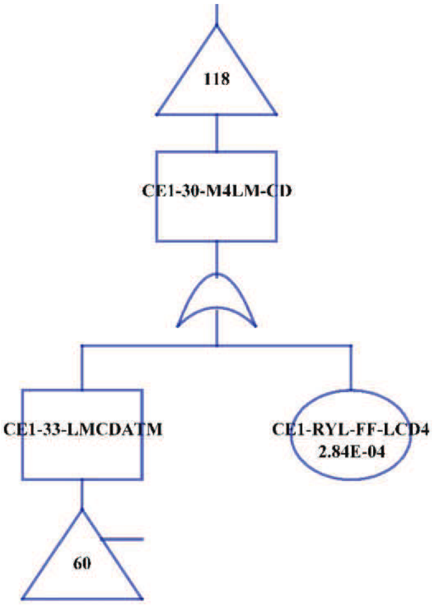
**CE1-30-M4LM-1: Logic Matrix Output Relays for M4 Signal Fail (Ch A T&M)**



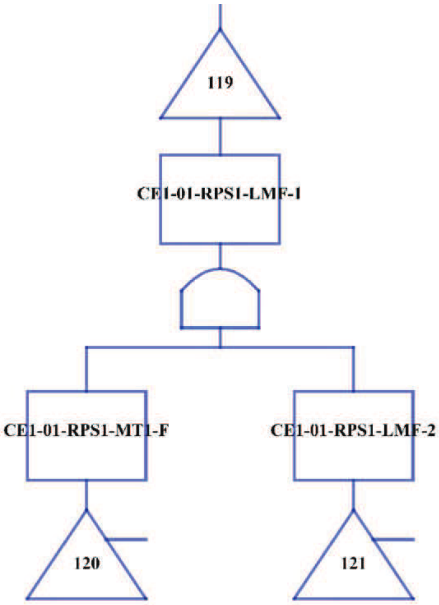
**CE1-30-M4LM-BC: Logic Matrix BC Output Relays to M4 Fail**



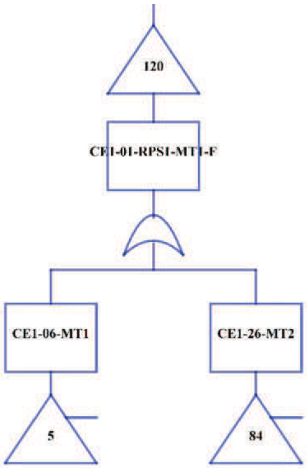
**CE1-30-M4LM-BD: Logic Matrix BD Output Relays to M4 Fail**



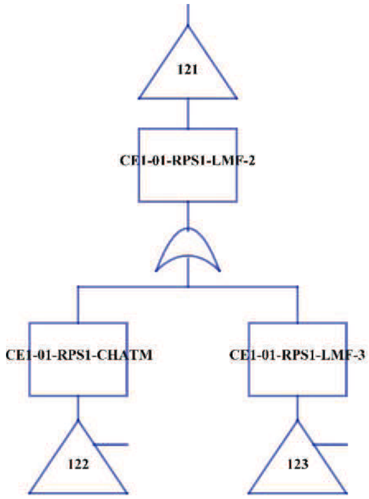
**CE1-30-M4LM-CD: Logic Matrix CD Output Relays to M4 Fail**



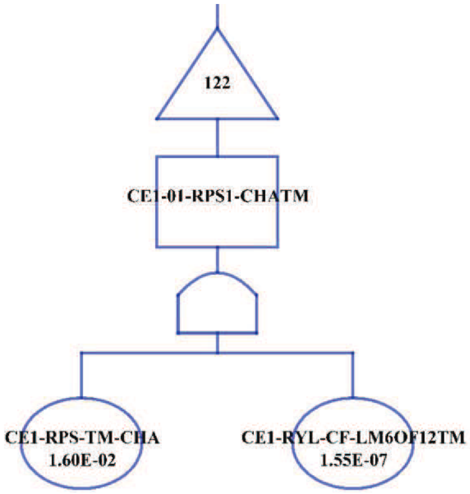
**CE1-01-RPS1-LMF-1: Common Cause Failures of Logic Matrix Relays**



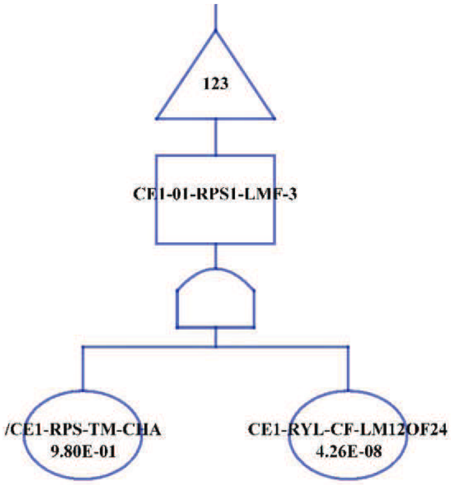
**CE1-01-RPS1-MT1-F: Operator Fails to Manual Trip RPS**



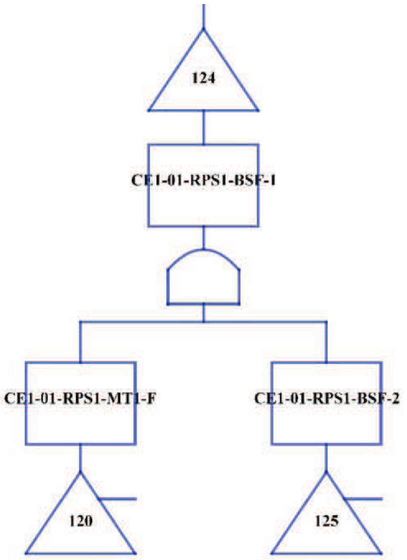
**CE1-01-RPS1-LMF-2: CCF of Logic Matric Relays**



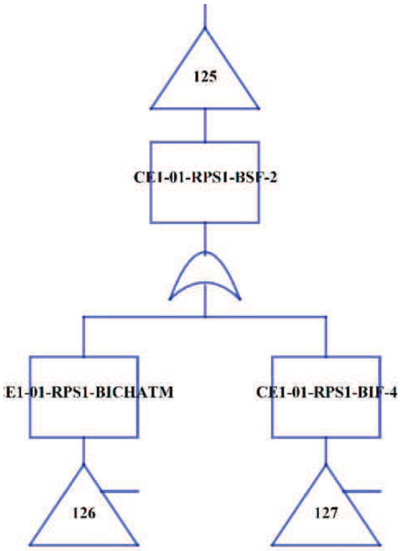
**CE1-01-RPS1-CHATM: CCF of Logic Matrix Relays During Ch A T&M**



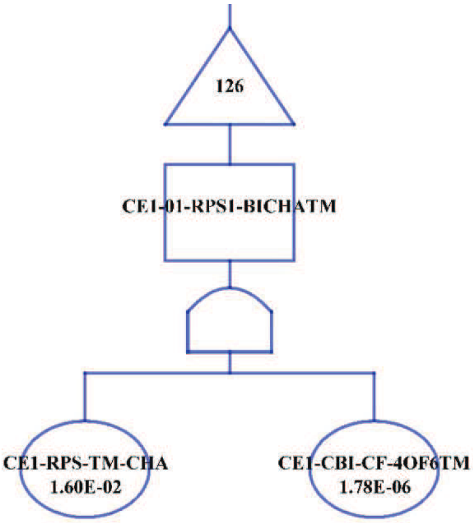
**CE1-01-RPS1-LMF-3: CCF of Logic Matrix Relays (Ch A not in T&M)**



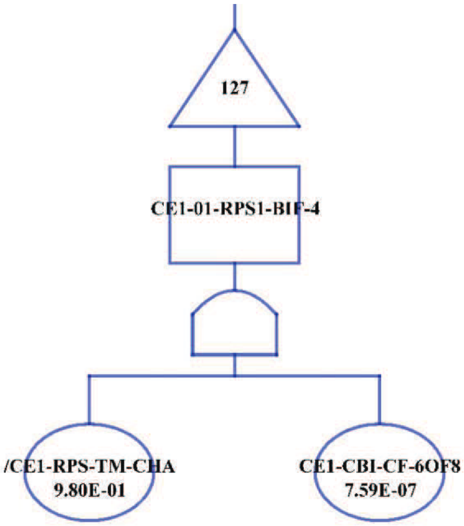
**CE1-01-RPS1-BSF-1: Common Cause Failure of Bistable Trip Units**



**CE1-01-RPS1-BSF-2: CCF of Bistable Trip Units**



**CE1-01-RPS1-BICHATM: CCF of Bistable Trip Units During Ch A T&M**

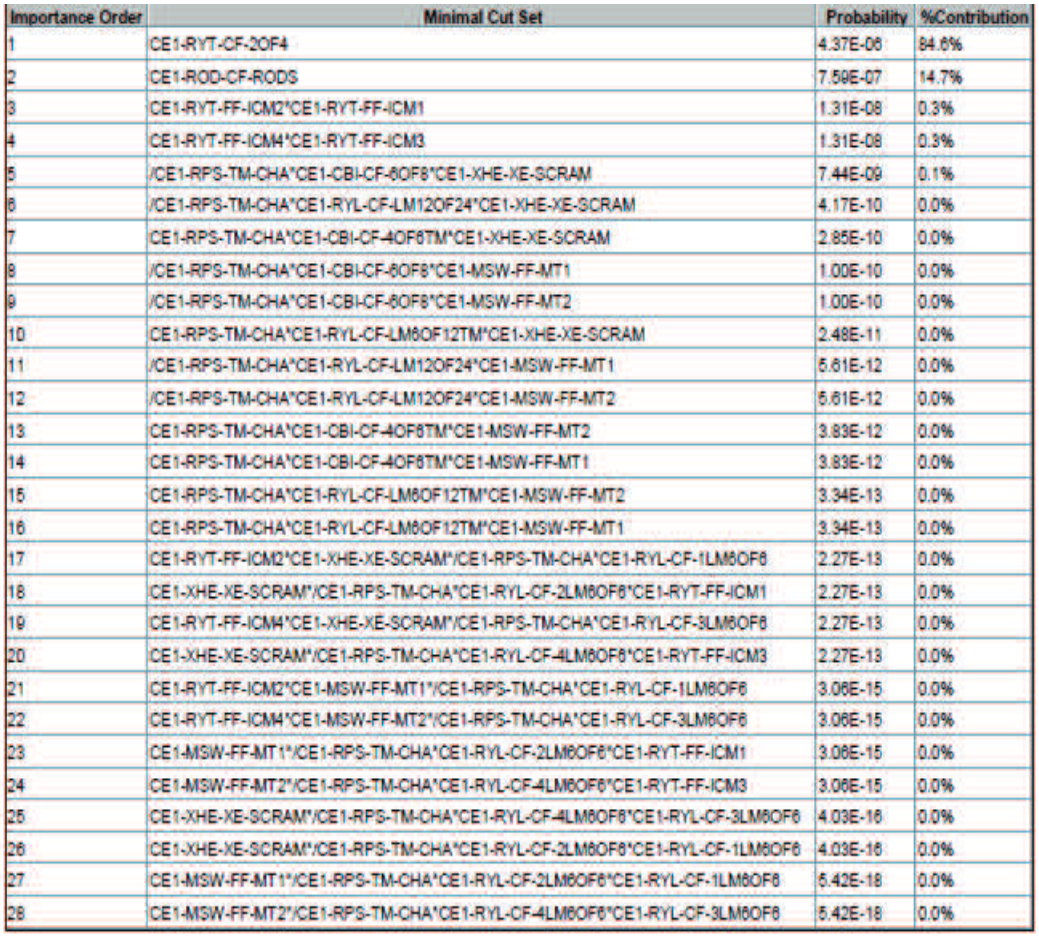


**CE1-01-RPS1-BIF-4: CCF of Bistable Trip Units (Ch A not in T&M)**

# Appendix B

# MINIMAL CUT SET IMPORTANCE MEASURES OF THE CERPS GROUP 1 DESIGNS

This appendix presents the minimal cut set importance measures of the Combustion Engineering RPS (CERPS) Group 1 designs, which is generated by InFaTAS-NuSA.

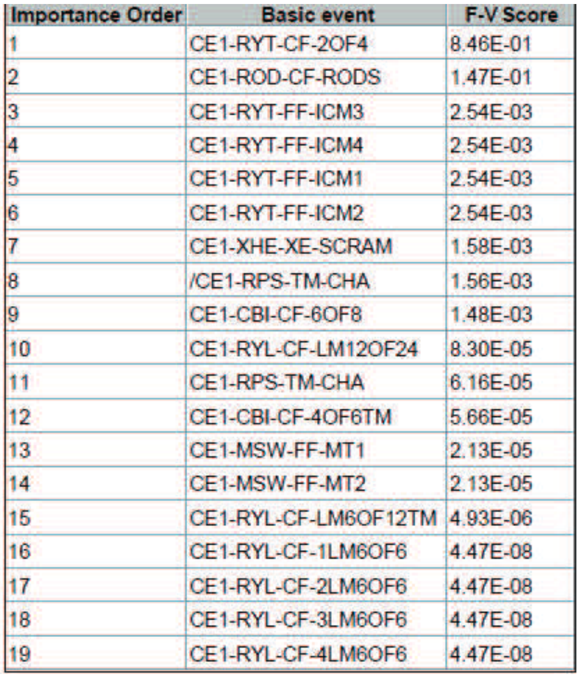


| Importance Order | Minimal Cut Set | Probability | %Contribution |
|---|---|---|---|
| 1 | CE1-RYT-CF-2OF4 | 4.37E-06 | 84.6% |
| 2 | CE1-ROD-CF-RODS | 7.59E-07 | 14.7% |
| 3 | CE1-RYT-FF-ICM2*CE1-RYT-FF-ICM1 | 1.31E-08 | 0.3% |
| 4 | CE1-RYT-FF-ICM4*CE1-RYT-FF-ICM3 | 1.31E-08 | 0.3% |
| 5 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-XHE-XE-SCRAM | 7.44E-09 | 0.1% |
| 6 | /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-XHE-XE-SCRAM | 4.17E-10 | 0.0% |
| 7 | CE1-RPS-TM-CHA*CE1-CBI-CF-4OF8TM*CE1-XHE-XE-SCRAM | 2.85E-10 | 0.0% |
| 8 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT1 | 1.00E-10 | 0.0% |
| 9 | /CE1-RPS-TM-CHA*CE1-CBI-CF-6OF8*CE1-MSW-FF-MT2 | 1.00E-10 | 0.0% |
| 10 | CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-XHE-XE-SCRAM | 2.48E-11 | 0.0% |
| 11 | /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-MSW-FF-MT1 | 5.61E-12 | 0.0% |
| 12 | /CE1-RPS-TM-CHA*CE1-RYL-CF-LM12OF24*CE1-MSW-FF-MT2 | 5.61E-12 | 0.0% |
| 13 | CE1-RPS-TM-CHA*CE1-CBI-CF-4OF8TM*CE1-MSW-FF-MT2 | 3.83E-12 | 0.0% |
| 14 | CE1-RPS-TM-CHA*CE1-CBI-CF-4OF8TM*CE1-MSW-FF-MT1 | 3.83E-12 | 0.0% |
| 15 | CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-MSW-FF-MT2 | 3.34E-13 | 0.0% |
| 16 | CE1-RPS-TM-CHA*CE1-RYL-CF-LM6OF12TM*CE1-MSW-FF-MT1 | 3.34E-13 | 0.0% |
| 17 | CE1-RYT-FF-ICM2*CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-1LM6OF6 | 2.27E-13 | 0.0% |
| 18 | CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-2LM6OF6*CE1-RYT-FF-ICM1 | 2.27E-13 | 0.0% |
| 19 | CE1-RYT-FF-ICM4*CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-3LM6OF6 | 2.27E-13 | 0.0% |
| 20 | CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-4LM6OF6*CE1-RYT-FF-ICM3 | 2.27E-13 | 0.0% |
| 21 | CE1-RYT-FF-ICM2*CE1-MSW-FF-MT1*/CE1-RPS-TM-CHA*CE1-RYL-CF-1LM6OF6 | 3.06E-15 | 0.0% |
| 22 | CE1-RYT-FF-ICM4*CE1-MSW-FF-MT2*/CE1-RPS-TM-CHA*CE1-RYL-CF-3LM6OF6 | 3.06E-15 | 0.0% |
| 23 | CE1-MSW-FF-MT1*/CE1-RPS-TM-CHA*CE1-RYL-CF-2LM6OF6*CE1-RYT-FF-ICM1 | 3.06E-15 | 0.0% |
| 24 | CE1-MSW-FF-MT2*/CE1-RPS-TM-CHA*CE1-RYL-CF-4LM6OF6*CE1-RYT-FF-ICM3 | 3.06E-15 | 0.0% |
| 25 | CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-4LM6OF6*CE1-RYL-CF-3LM6OF6 | 4.03E-16 | 0.0% |
| 26 | CE1-XHE-XE-SCRAM*/CE1-RPS-TM-CHA*CE1-RYL-CF-2LM6OF6*CE1-RYL-CF-1LM6OF6 | 4.03E-16 | 0.0% |
| 27 | CE1-MSW-FF-MT1*/CE1-RPS-TM-CHA*CE1-RYL-CF-2LM6OF6*CE1-RYL-CF-1LM6OF6 | 5.42E-18 | 0.0% |
| 28 | CE1-MSW-FF-MT2*/CE1-RPS-TM-CHA*CE1-RYL-CF-4LM6OF6*CE1-RYL-CF-3LM6OF6 | 5.42E-18 | 0.0% |
)

# Appendix C

## FUSSELL-VESELY IMPORTANCE MEASURES OF THE CERPS GROUP 1 DESIGNS

This appendix presents the Fussell-Vesely importance measures of the basic events of the Combustion Engineering RPS (CERPS) Group 1 designs, which is generated by InFaTAS-NuSA.



| Importance Order | Basic event | F-V Score |
|---|---|---|
| 1 | CE1-RYT-CF-2OF4 | 8.46E-01 |
| 2 | CE1-ROD-CF-RODS | 1.47E-01 |
| 3 | CE1-RYT-FF-ICM3 | 2.54E-03 |
| 4 | CE1-RYT-FF-ICM4 | 2.54E-03 |
| 5 | CE1-RYT-FF-ICM1 | 2.54E-03 |
| 6 | CE1-RYT-FF-ICM2 | 2.54E-03 |
| 7 | CE1-XHE-XE-SCRAM | 1.58E-03 |
| 8 | /CE1-RPS-TM-CHA | 1.56E-03 |
| 9 | CE1-CBI-CF-6OF8 | 1.48E-03 |
| 10 | CE1-RYL-CF-LM12OF24 | 8.30E-05 |
| 11 | CE1-RPS-TM-CHA | 6.16E-05 |
| 12 | CE1-CBI-CF-4OF6TM | 5.66E-05 |
| 13 | CE1-MSW-FF-MT1 | 2.13E-05 |
| 14 | CE1-MSW-FF-MT2 | 2.13E-05 |
| 15 | CE1-RYL-CF-LM6OF12TM | 4.93E-06 |
| 16 | CE1-RYL-CF-1LM6OF6 | 4.47E-08 |
| 17 | CE1-RYL-CF-2LM6OF6 | 4.47E-08 |
| 18 | CE1-RYL-CF-3LM6OF6 | 4.47E-08 |
| 19 | CE1-RYL-CF-4LM6OF6 | 4.47E-08 |