Risk-informed Maintenance for Non-coherent Systems

by

Ye Tao

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

Master of Applied Science

In

The Faculty of the Engineering and Applied Science

Electrical and Computer Engineering

University of Ontario Institute of Technology

Accepted December 2010

ABSTRACT

Probabilistic Safety Assessment (PSA) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. The information provided by PSA has been increasingly implemented for regulatory purposes but rarely used in providing information for operation and maintenance activities. As one of the key parts in PSA, Fault Tree Analysis (FTA) attempts to model and analyze failure processes of engineering and biological systems. The fault trees are composed of logic diagrams that display the state of the system and are constructed using graphical design techniques.

Risk Importance Measures (RIMs) are information that can be obtained from both qualitative and quantitative aspects of FTA. Components within a system can be ranked with respect to each specific criterion defined by each RIM. Through a RIM, a ranking of the components or basic events can be obtained and provide valuable information for risk-informed decision making. Various RIMs have been applied in various applications. In order to provide a thorough understanding of RIMs and interpret the results, they are categorized with respect to risk significance (RS) and safety significance (SS) in this thesis. This has also tied them into different maintenance activities. When RIMs are used for maintenance purposes, it is called risk-informed maintenance.

On the other hand, the majority of work produced on the FTA method has been concentrated on failure logic diagrams restricted to the direct or implied use of AND and OR operators. Such systems are considered as coherent systems. However, the NOT logic can also contribute to the information produced by PSA. The importance analysis of non-coherent systems is rather limited, even though the field has received more and more

attention over the years. The non-coherent systems introduce difficulties in both qualitative and quantitative assessment of the fault tree compared with the coherent systems.

In this thesis, a set of RIMs is analyzed and investigated. The 8 commonly used RIMs (Birnbaum's Measure, Criticality Importance Factor, Fussell-Vesely Measure, Improvement Potential, Conditional Probability, Risk Achievement, Risk Achievement Worth, and Risk Reduction Worth) are extended to non-coherent forms. Both coherent and non-coherent forms are classified into different categories in order to assist different types of maintenance activities. The real systems such as the Steam Generator Level Control System in CANDU Nuclear Power Plant (NPP), a Gas Detection System, and the Automatic Power Control System of the experimental nuclear reactor are presented to demonstrate the application of the results as case studies.

ACKNOWLEDGEMENTS

First I would like to thank my supervisor Professor Lixuan Lu for her invaluable help, guidance, mentoring, inspiration and friendship over the past three years.

Thanks are also extended to my colleagues and the staff in the Faculty of Engineering and Applied Science, as well as the staff in the Faculty of Energy System and Nuclear Science, who helped me at various stages throughout my research.

I am also grateful to my family and friends; it would not be possible to finish this research work without all their love, support and encouragement.

CONTENTS

ABSTRACT ..... **i**

ACKNOWLEDGEMENTS ..... **iii**

CONTENTS ..... **iv**

List of Figures ..... **vii**

List of Tables ..... **ix**

Abbreviations ..... **xi**

Nomenclature ..... **xiii**

Chapter 1 Introduction **1**

1.1 Overview 1

1.2 Motivation 3

1.3 Objective of the Thesis 4

1.4 Structure of the Thesis 4

Chapter 2 Background **6**

2.1 Probabilistic Safety Assessment (PSA) 6

2.1.1 Introduction 6

2.1.2 Fault Tree Analysis 7

2.1.3 Event Tree Analysis 9

2.1.4 Qualitative Analysis 10

2.1.4.1 Overview 10

2.1.4.2 Obtaining Minimal Cut Sets 11

2.1.5 Quantitative Analysis 19

2.1.5.1 Reliability Parameters 19

2.1.5.2 Calculating the Top Event Probability 21

2.1.6 Common Cause Failure Analysis 22

2.2 Risk Importance Measures 22

2.2.1 Risk Importance Measures for Basic Events 23

2.2.2 Risk Importance Measures for Failures of Systems and Functions 25

2.3 Non-coherent Systems 26

2.3.1 A Simple Example of Non-coherency 27

2.3.2 Non-coherent System In Real World 29

2.3.3 Calculational Tools for Non-coherent Fault Tree Analysis 33

2.4 Maintenance Engineering 34
2.4.1 Reliability Centered Maintenance 36
2.4.2 Risk-informed Maintenance 38
2.4.2.1 Risk-informed Decision Making Approach 38
2.4.2.2 The Nuclear Industry's Transition to Risk-informed Regulation 40
2.4.2.3 Optimized Maintenance through PSA 42
Chapter 3 Extension of Risk Importance Measures to Non-coherent Systems 43
3.1 Various Risk Importance Measures 43
3.1.1 Birnbaum's Measure 44
3.1.2 Criticality Importance Factor 46
3.1.3 Improvement Potential 47
3.1.4 Fussell-Vesely Measure 47
3.1.5 Risk Achievement 50
3.1.6 Conditional Probability 50
3.1.7 Risk Achievement Worth 51
3.1.8 Risk Reduction Worth 53
3.2 Extension of Various Risk Importance Measures to Non-coherent Systems 55
3.2.1 The Extension of Birnbaum's Measure to Non-coherent Systems 55
3.2.2 The Extension of Criticality Importance Factor to Non-coherent Systems 58
3.2.3 The Extension of Improvement Potential to Non-coherent Systems 59
3.2.4 The Extension of Fussell-Vesely Measure to Non-coherent Systems 59
3.2.5 The Extension of Risk Achievement to Non-coherent Systems 60
3.2.6 The Extension of Conditional Probability to Non-coherent Systems 64
3.2.7 The Extension of Risk Achievement Worth to Non-coherent Systems 64
3.2.8 The Extension of Risk Reduction Worth to Non-coherent Systems 65
Chapter 4 Categorization of Various Risk Importance Measures 67
4.1 Overview 67
4.2 Risk Significance and Safety Significance 68
4.2.1 Risk Significance 69
4.2.2 Safety Significance 72
4.3 Classification of Risk Importance Measures for Risk-informed Maintenance 77
4.4 The Application of RIMs in Non-coherent Systems 84
Chapter 5 Case Studies 97

5.1 The Application of Non-coherent Fault Tree Analysis on a Steam Generator Level Control System 97
5.1.1 Steam Generator Level Control System 97
5.1.2 Demonstration of Non-coherent Fault Tree Analysis on the SGLCS 98
5.2 The Application of Non-coherent Fault Tree Analysis on a Gas Detection System 108
5.2.1 Gas Detection System 108
5.2.2 Demonstration of Non-coherent Fault Tree Analysis on the SGLCS 110
5.3 The Application of Non-coherent Fault Tree Analysis on the Automatic Power Control System 128
Chapter 6 Conclusions and Future Work 128
6.1 Conclusions 128
6.2 Future Work 129
Bibliography 131
VITA 139

List of Figures

Figure 2.1: A Fault Tree Example 9
Figure 2.2: An Example of Event Tree Model 10
Figure 2.3: OR gate, AND gate and Inverter (or NOT gate) 11
Figure 2.4: Single-variable Theorems 13
Figure 2.5: Fault Tree Diagram 17
Figure 2.6: Evaluating Functional Importance 25
Figure 2.7: Traffic Light System 27
Figure 2.8: Collision Fault Trees 29
Figure 2.9: Schematic Layout of TMI-2 30
Figure 2.10: TMI-2 Fault Tree 1 31
Figure 2.11: TMI-2 Fault Tree 2 32
Figure 2.12: TMI-2 Fault Tree 3 32
Figure 2.13: Different Types of Maintenance 35
Figure 2.14: Preventive and Corrective Maintenance 36
Figure 4.1: A Simple Series System 70
Figure 4.2: A Complex System 72
Figure 4.3: A Simple Parallel System 73
Figure 4.4: System Fault Tree with Component *a* Assumed Failed 75
Figure 4.5: System Fault Tree with Component *b* Assumed Failed 76
Figure 4.6: Final System Fault Tree with component *b* assumed failed 76
Figure 4.7: Non-coherent Fault Tree 1 85
Figure 4.8: System Fault Tree when component *b* fails 87
Figure 4.9: Simplified Fault Tree for Figure 4.8 88
Figure 4.10: System Fault Tree Assuming Component *a* Fails 89
Figure 4.11: Simplified Fault Tree for Figure 4.10 89
Figure 4.12: System Fault Tree Assuming Component *c* Works 90
Figure 4.13: Simplified Fault Tree for Figure 4.12 90
Figure 4.14: System Fault Tree Assuming Component *c* Fails 91
Figure 4.15: Simplified Fault Tree for Figure 4.14 91
Figure 4.16: Non-coherent Fault Tree 2 94
Figure 5.1: Steam Generator Feed Pumps and Level Control Valves 98
Figure 5.2: One Element Control of SGLCS 99

Figure 5.3: Simplified Level Control System 100
Figure 5.4: Example System Structure in Fault Tree 101
Figure 5.5: Simplified Gas Detection System 108
Figure 5.6: Fault Tree for Gas Detection System 109
Figure 5.7: Non-coherent Fault Tree Diagram for Outcome 4 111
Figure 5.8: Simplified Fault Tree for Outcome 4 112
Figure 5.9: The Flowsheet of APCS 115
Figure 5.10: The Loop Switch of APCS 116
Figure 5.11: Fault Tree of the APCS 121

List of Tables

Table 2.1: Truth Table defining OR operation 12
Table 2.2: Truth Table defining AND operation 12
Table 2.3: Truth Table Defining NOT logic 12
Table 2.4: Boolean Algebra 16
Table 2.5: Definitions of Various RIMs 24
Table 3.1: Definitions of Birnbaum's Measure 45
Table 3.2: Definitions of Fussell-Vesely Measure 48
Table 3.3: Definitions of Risk Achievement Worth 52
Table 3.4: Definitions of Risk Reduction Worth 54
Table 3.5: The Result Obtained from the Example 62
Table 3.6: Possible and Critical States for the Events 63
Table 3.7: Expected Results 63
Table 4.1: The Definition of Various RIMs 78
Table 4.2: Various RIMs on a Parallel System 79
Table 4.3: Various RIMs on a Series System 80
Table 4.4: Comparison of Different RIMs on a Complex System 81
Table 4.5: The Categorization of Various RIMs with respect to Risk and Safety Significance 83
Table 4.6: The Extended RIMs to Non-coherent Systems 84
Table 4.7: Demonstration of various RIMs on the Non-coherent System 93
Table 4.8: The Comparison of Results of BM and RA for the Non-coherent System 95
Table 5.1: Failure/Repair Parameters of the Example System 101
Table 5.2: Measure and Ranking of Importance with Respect to RS Using Parameter Set 1 102
Table 5.3: Measure and Ranking of Importance with Respect to RS Using Parameter Set 2 103
Table 5.4: Measure and Ranking of Importance with Respect to RS Using Parameter Set 3 103
Table 5.5: Measure and Ranking of Importance with Respect to RS Using Parameter Set 4 103
Table 5.6: Measure and Ranking of Importance with Respect to RS Using Parameter Set 5 104
Table 5.7: Measure and Ranking of Importance with Respect to RS Using Parameter Set 3 104
Table 5.8: Measure and Ranking of Importance with Respect to SS Using Parameter Set 1 104
Table 5.9: Measure and Ranking of Importance with Respect to SS Using Parameter Set 2 105
Table 5.10: Measure and Ranking of Importance with Respect to SS Using Parameter Set 3 105
Table 5.11: Measure and Ranking of Importance with Respect to SS Using Parameter Set 4 105
Table 5.12: Measure and Ranking of Importance with Respect to SS Using Parameter Set 5 106

Table 5.13: Measure and Ranking of Importance with Respect to SS Using Parameter Set 6 106
Table 5.14: Gas Detection System Outcome 110
Table 5.15: Component Availability/Unavailability Values for GDS 112
Table 5.16: Measures and Rankings of Component Importance for GDS 113
Table 5.17: Basic Events and Their Unavailabilities 122
Table 5.18: RIMs for basic events in APCS 124
Table 5.19: Importance Rankings Provided by Risk Significant Measures 125
Table 5.20: Importance Rankings Provided by Safety Significant Measures 126

Abbreviations

PSA	Probabilistic Safety Assessment
FTA	Fault Tree Analysis
NPP	Nuclear Power Plant
CANDU	Canada Deuterium Uranium
INPO	Institute of Nuclear Power Operations
TMI	Three Mile Island
NRC	Nuclear Regulatory Commission
RIM	Risk Importance Measure
PM	Preventive Maintenance
CM	Corrective Maintenance
ETA	Event Tree Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
RIDM	Risk Informed Decision Making
SSC	Structure, System and Components
RCM	Reliability Centered Maintenance
BWR	Boiling Water Reactor
IDCOR	Industry Degraded Core Rulemaking Program
IPE	Individual Plant Examination
GDS	Gas Detector System
SGLCS	Steam Generator Level Control System
APCS	Automatic Power Control System
MTTF	Mean Time to Failure
CCF	Common Cause Failure
BM	Birnbaum's Measure

CIF	Criticality Importance Factor
IP	Improvement Potential
FV	Fussell-Vesely Measure
RA	Risk Achievement
RAW	Risk Achievement Worth
CP	Conditional Probability
RRW	Risk Reduction Worth
RS	Risk Significance
SS	Safety Significance

Nomenclature

Q_i: unavailability of component *i*

λ_i: failure rate of component *i*

μ_i: repair rate of component *i*

$\omega_j^*(t)$: conditional failure intensity for a cut set *j* at time *t*

λ_j^*: failure rate for the cut set *j*

C_i: minimal cut set *i* prime implicant set *i*

Q_{sys}: unavailability of the system

G_{BM}: Birnbaum's Measure (BM)

G_{CIF}: Criticality Importance Factor (CIF)

G_{IP}: Improvement Potential (IP)

G_{FV}: Fussell-Vesely Measure (FV)

G_{RRW}: Risk Reduction Worth (RRW)

G_{RA}: Risk Achievement (RA)

G_{RAW}: Risk Achievement Worth (RAW)

G_{CP}: Conditional Probability (CP)

Φ: structure function

q_i: probability of the basic event *i* happening/failure probability of component *i*

p_i: probability of the basic event *i* not happening/repair probability of component *i*

Chapter 1

Introduction

1.1 Overview

The assurance of quality for safety related structure, system and components (SSCs) has always been an initial part of design and regulation of Nuclear Power Plants (NPPs). Traditionally, the safety and regulation of NPPs has been based upon deterministic approaches that consider how a set of challenges should be handled. The deterministic approach has been successfully implemented over the years as no major failure and damage has occurred [1]. However, there are downsides of the approach. The arbitrary nature of the safety criteria, the potential inconsistencies in the judgments on relative probabilities, and the lack of definition for 'safety' became increasingly evident during the 1960s. Thus, probabilistic approaches to plant safety were proposed [2][3][4].

A probabilistic approach to regulation enhances and extends the traditional deterministic approach by introducing the concept of risk and safety significance that allows the designer and operator to focus on important issues. Emphasis was initially placed on relative risks but now regulatory decision making is employing both relative and absolute risk by defining the measures of risks. The probabilistic approach is called Probabilistic Safety Assessment (PSA). It is now a fundamental tool that provides guidance to safety related

decision making and is being used to complement the deterministic approach to achieve nuclear safety.

As one of the broad PSA applications is numerical rankings of the risk and safety significance of structure, system and components (SSCs), i.e. the quantification of the contribution of SSCs to plant safety and reliability, PSA can not only be used for regulatory purposes, it is also a suitable method to handle operational issues such as surveillance testing and maintenance activities [5]. Thus risk-informed maintenance provides PSA insights to help focus monitoring of SSC performance and to ensure that the system performs effectively during maintenance activities.

The PSA methodology in the application of maintenance rules has four steps [1]:

1. After calculating their risk importance measures (RIMs), rank components according to their significance. Assign components to high and low risk/safety significance categories;
2. Assess the adequacy and completeness of the supporting PSA and other risk models by a series of sensitivity analysis.
3. Evaluation of the cumulative impact on plant risk of extending the in-service test intervals for many low significant components.
4. Review the process and results with the expert panel. This review should blend deterministic safety insights with quantitative risk measures to ensure that risk/safety significance was appropriately identified.

1.2 Motivation

The transition of the United States nuclear industry from a prescriptive regulatory to a more risk-informed approach to operations and regulations occurred over a 20 year period in which gradual changes were made in the fundamental regulations and to the approach to nuclear safety and operations. The experience of risk-informed approach in regulatory decision making has shown positive results in both safety and economics in United States. The use of risk information in operations and regulation is marginally better with no degradation in safety when plants that have embraced risk-informed approaches are compared to those that have not. The use of risk-informed approaches allows both the regulator and the industry to focus on important safety issues. The transition to risk-informed regulation also required a "culture change" by both the regulators and the utilities. Caution should be taken, however, since the basis of the US transition to risk-informed regulation is founded on a long history of a regulatory structure and practices that have matured the industry to a point where the next step could be taken [6]. The use of risk insights in maintenance activities was mentioned at the early 1990s, when the maintenance rule enabled utilities to take advantages of their Individual Plant Examinations (IPEs) in developing a risk-informed maintenance program [7].

On the other hand, the use of PSA for regulatory decision making has been growing at 1980s since the Three Mile Island Accident (TMI-2) occurred in 1979. The investigation on the event has revealed the critical human factor problems about the industrial design of the reactor control system's user interface. The ambiguous nature of indicators did not show the maintenance or repair priority among the components that have all been indicated as

failed at the same time. Therefore, the maintenance activity involving PSA insights is an area that warrants further investigation.

1.3 Objective of the Thesis

In a risk-informed maintenance framework, Fault Tree Analysis (FTA) is one of the techniques adopted to gain insight into the dependence of each sub-system in the safety systems. The risk importance measures (RIMs) from PSA analysis are utilized to provide sufficient information about potential weak spot in the system so that appropriate maintenance decisions can be made. Fault trees are used to model the different safety systems that mitigate or cause initiating events in PSA. The aim of the fault tree is to determine the occurrence of the top event in terms of occurrence or non-occurrence of the events. While most of the systems have coherent structures, some systems have non-coherent structure due to the nature of the system or bad real world design. Thus, the investigation on various RIMs as well as the extension of RIMs to the non-coherent systems is necessary. On the other hand, different RIMs have different use in maintenance activities and they should be classified into different categorizes for different purposes.

1.4 Structure of the Thesis

This thesis is organized as follows. Chapter 2 presents the background survey including the further introduction of PSA, FTA and maintenance engineering. Chapter 3 presents various risk importance measures (RIMs) along with their extension for non-coherent FTA. The various RIMs are classified into different categories for different purposes with further discussion, both in coherent and non-coherent systems in Chapter 4. Chapter 5 uses three real-world applications as case studies to back up the methodology. In

Chapter 6, the conclusions of the current research will be summarized, as well as discussion of future work.

Chapter 2

Background

2.1 Probabilistic Safety Assessment (PSA)

2.1.1 Introduction

Probabilistic Safety Assessment (PSA) was widely adopted in safety critical areas such as nuclear power generation, aerospace systems, chemical industry, etc. It has become an analytical tool used to assess the safety of safety critical facilities under various events, which also identifies potential modes of system failures by determining the likelihood and consequences of their occurrence.

In the nuclear industry, PSA usually attempts to answers three basic questions:

I. What can go wrong with the studied technological entity, or what are the initiators or initiating events (undesirable starting events) that lead to adverse consequence(s)?

II. What and how severe are the potential detriments, or the adverse consequences that the technological entity may be eventually subjected to as a result of the occurrence of the initiator?

III. How likely are these undesirable consequences to occur, or what are their probabilities or frequencies?

PSA can be classified into three levels progressively:

Level 1: analysis of the probability of certain critical states being reached (e.g. "loss of coolant" in an NPP);

Level 2: analysis of the consequences of various critical states being reached, with the associated probabilities;

Level 3: further analysis of the probable (adverse) effects on humans, including an estimation of the extent of the loss of life and when this might occur.

PSA typically involves both qualitative and quantitative analysis by using Fault Tree Analysis (FTA).

2.1.2 Fault Tree Analysis

Fault Tree Analysis (FTA) was developed for projects where errors are intolerable. It was first conceived in 1961 by H. A Watson of Bell Telephone Laboratories in connection with a US Air Force Contract to study the Minuteman Missile Launch Control System [8]. It was recognized by Dave Haasl of Boeing [9] as a significant system safety analysis tool in 1963 and the first major use was applied by Boeing on the entire Minuteman system for safety evaluation was in 1964. Boeing also began using FTA on the design and evaluation of commercial aircraft in 1966. Later on, Boeing developed a 12-phase fault tree simulation program and a fault tree plotting program on a Calcomp roll plotter.

FTA was fully adopted by the aerospace industry including aircraft and weapons before the 1970's, and was then adopted by the nuclear power industry in 1971. It helped the power industry enhance codes and algorithms; some of the more recognized software codes include: Prepp/Kitt, SETS, FTAP, and COMCAN. In the 1980's, FTA usage started becoming international, primarily via the nuclear power industry; the evaluation algorithms and codes were developed afterwards. It has continually been used on many systems in many countries and is commonly adopted by the robotics and software industry. Since then, FTA became an applicable tool that evaluates complex system. It identifies events that can cause undesired events and investigates accidents to ensure safety, reliability and unavailability. In other words, the FTA not only identifies root cause, but also provides risk assessment.

A fault tree (Figure 2.1) is a visualized model that intuitively displays cause-consequence relationships, fault events, normal events and probabilities. It is a structure by which a particular system failure mode can be expressed in terms of the combination of component failure modes and operator actions. The system failure mode to be considered is determined to be the 'top event' and the fault tree is developed in branches below this particular event, showing its causes. In this way events presented in the tree are continually redefined in terms of more specific events. This development process is terminated when component failure events, termed basic events, are encountered.

An FTA can be carried out by providing information on the basic events and their probabilities, which produces the evaluation qualitatively and quantitatively. The qualitative analysis identifies the combinations of the basic events which cause the top event, i.e. cut sets; the quantitative analysis will result in predictions of the system performance in terms of component level performance data, i.e. probability of failure or frequency of failure [10] [11].

The quantitative analysis incorporates probability, cut sets, and risk importance measures to complete the evaluation.

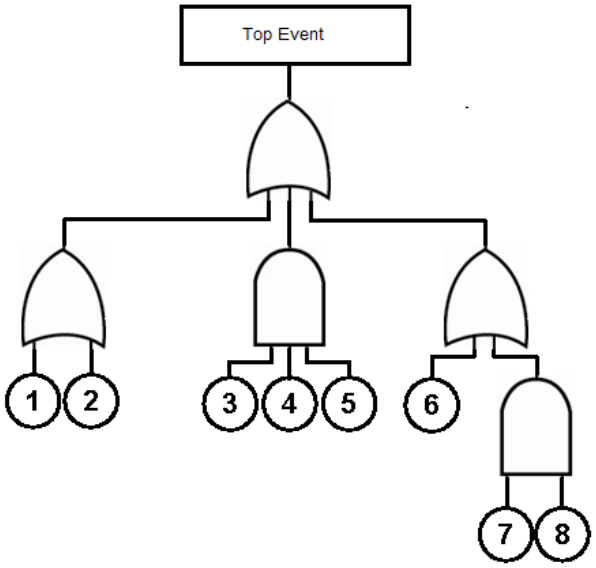


Figure 2.1: A Fault Tree Example

2.1.3 Event Tree Analysis

Event Tree Analysis (ETA) is complimentary to other techniques such as FTA and FMECA (Failure Modes Effect Criticality Analysis) in PSA. Unlike fault tree as a top-down structure for the analysis of a system, an event tree is a bottom-up structure and a "logic method for identifying various possible outcome of a given event which is called the initiating event" [12]. It is applicable to physical systems, with or without human operators and also decision-making and management systems.

An event tree commences with an initiating (or basic) event and works forward in time considering all possible subsequent events until the final consequences are determined – either the system corrects itself or some level or some level of system failure occurs. An event tree can represent the logical order in which the events in a system occur (Figure 2.2).

Fault trees and event trees are used most often in combination to represent a system. Advanced methodologies have been developed for both FTA and ETA [13][14]. The dynamic properties of the system are also taken into consideration in these studies. However, ETA is not the focus in this thesis.

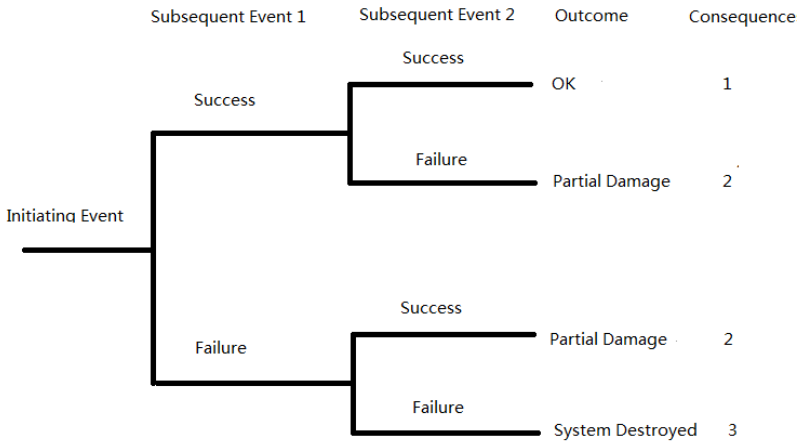


Figure 2.2: An Example of Event Tree Model

2.1.4 Qualitative Analysis

2.1.4.1 Overview

Qualitative analysis is one of the two stages in FTA, which aims to identify the casual relationships between the system components. During qualitative analysis all the possible causes of system failure are identified. Once a fault tree is constructed for a system, it is then necessary to determine the cut sets. A cut set consists of a collection of basic events. If all the basic events in the cut set occur, the top event is guaranteed to occur. For coherent fault trees each possible cause of system failure is called a minimal cut set, which is a combination of component failures that are both necessary and sufficient to cause system failure.

In the case of non-coherent fault trees (introduced in Section 2.3) both component failed states and working states can contribute to system failure. Hence each possible cause of system failure is called a prime implicant set and is a combination of component failure states and component working states that are both necessary and sufficient to fail.

2.1.4.2 Obtaining Minimal Cut Sets

Minimal cut sets are normally obtained by converting a logic expression for the top event into disjunctive normal form. At this point, Boolean algebra laws are used to remove the redundancies in the expression leaving it in the required minimal form. Three operator: OR, AND and NOT are the three basic operations used in Boolean algebra. In a fault tree, OR gate, AND gate and inverter (Or NOT gate) represent the OR, AND and NOT logic, respectively [15].

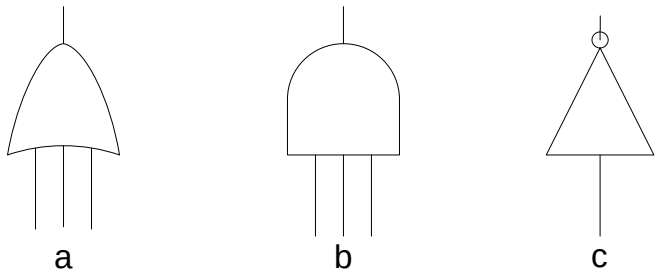


Figure 2.3: OR gate, AND gate and Inverter (or NOT gate)

The OR gate (Figure 2.3a) is a digital logic gate that implements logical disjunction - it behaves according to the truth table (Table 2.1). A HIGH output *1* results if one or both the inputs to the gate are HIGH (1). If neither input is HIGH, a LOW output *0* results. The Boolean expression for the OR operation is: $x = A+B$.

A	B	A+B
0	0	0
0	1	1
1	0	1
1	1	1

Table 2.1: Truth Table defining OR operation

The AND gate (Figure 2.3b) is a digital logic gate that implements logical conjunction - it behaves according to the truth table (Table 2.2). A HIGH output *1* results only if both the inputs to the AND gate are HIGH (1). If neither or only one input to the AND gate is HIGH, a LOW output results. The Boolean expression for the AND operation is $x=A\cdot B$.

A	B	A·B
0	0	0
0	1	0
1	0	0
1	1	1

Table 2.2: Truth Table defining AND operation

An inverter or NOT gate (Figure 2.3c) is a logic gate which implements logical negation. If the variable A is subjected to the NOT operation, the result x can be expressed as: $x=\overline{A}$. The truth table is shown in Table 2.3.

A	$x=\overline{A}$
0	1
1	0

Table 2.3: Truth Table Defining NOT logic

Various Boolean theorems (rules) can help simplifying logic expressions for fault tress. The first group of theorems is given in Figure 2.4. In each theorem, x is a logic variable that can be either 0 or 1. Each theorem is accompanied by a logic-circuit diagram that demonstrates its validity.

Theorem (1) states that if any variable is ANDed with 0, the result must be 0. The AND operation is similar to ordinary multiplication, where anything multiplied by 0 is 0. The output of an AND gate will be 0 whenever any input is 0, regardless of the level on the other input.

Theorem (2) is also obvious by comparison with ordinary multiplication.

Theorem (3) can be proved by trying each case. If $x = 0$, then $0 \cdot 0 = 0$; if $x = 1$, then $1 \cdot 1 = 1$. Thus, $x \cdot x = x$.

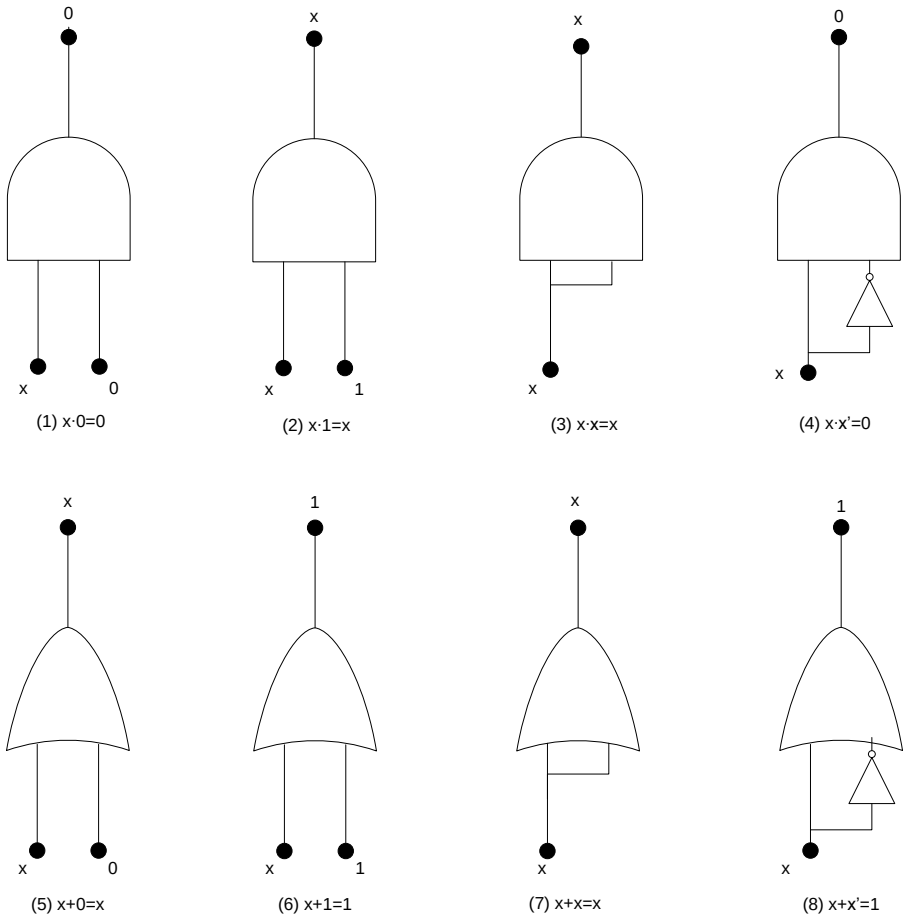


Figure 2.4: Single-variable Theorems

Theorem (4) can be proved in the same manner. However, it can also be reasoned that any time either x or its inverse x' (or $\bar{x}$) must be at the 0 level, and so their AND product always must be 0.

Theorem (5) states that 0 added to anything does not affect its value in OR gate.

Theorem (6) states that if any variable is ORed with 1, the result will always be 1.

Theorem (7) can be proved by checking for both values of x: $0 + 0 = 0$ and $1 + 1 = 1$.

Theorem (8) can be proved similarly, or at any time either x or x' must be at the 1 level so that we are always ORing a 0 and a 1, which always results in 1.

When theorems (1) through (8) are applied, the variable x may actually represent an expression containing more than one variable. The theorems represented below involve more than one variable:

(9) $x + y = y + x$

(10) $x \cdot y = y \cdot x$

(11) $x + (y + z) = (x + y) + z = x + y + z$

(12) $x(yz) = (xy)z = xyz$

(13a) $x(y + z) = xy + xz$

(13b) $(w + x)(y + z) = wy + xy + wz + xz$

(14) $x + xy = x$

(15a) $x + x'y = x + y$

(15b) $x' + xy = x' + y$

Theorem (9) and (10) are called the commutative laws. These laws indicate that the order in which we OR or AND two variables is unimportant; the result is identical.

Theorems (11) and (12) are the associative laws, which state that the variables in an AND expression or OR expression can be grouped differently.

Theorem (13) is the distributive law, which states that an expression can be expanded by multiplying term by term just the same as in ordinary algebra. This theorem also indicates that an expression can be factored. That is, for a sum of two (or more) terms, each of which contains a common variable, the common variable can be factored out just as in ordinary algebra. For example, if we have the expression $A\overline{B}C+\overline{A}\overline{B}\overline{C}$, the $\overline{B}$ variable can be factored as:

$$A\overline{B}C+\overline{A}\overline{B}\overline{C}=\overline{B}(AC+\overline{A}\overline{C})$$

As another example, consider the expression ABC+ABD. Here the two terms have the variables A and B in common, and so $A \cdot B$ can be factored out of both terms. That is,

$$ABC+ABD=AB(C+D)$$

Theorems (9) to (13) are identical to those of ordinary algebra. Theorems (14) and (15), on the other hand, do not have any counterparts in ordinary algebra. Each can be proved be trying all possible cases for x and y. This is illustrated (for theorem 14) by creating an analysis table for the equation $x + xy$ as follows:

x	y	xy	x + xy
0	0	0	0
0	1	0	0
1	0	0	1
1	1	0	1

Table 2.4: Boolean Algebra

The value of the entire expression *(x + xy)* is always the same as *x*.

Theorem (14) can also be proved factoring and using theorem (6) and (2) as follows:

$$x+xy=x(1+y)=x\cdot 1=x$$

In FTA, the top down approach is commonly used to obtain the minimal cut sets and prime implicant sets by developing a Boolean expression for the top-event completely in terms of basic component failures. This approach starts with the top gate and expands each gate by substituting in the inputs that lie directly below it. This process is repeated until the expression has only basic component failures. The Boolean reduction laws introduced above are also applied where possible to simplify the expression. The minimal cut sets of the fault tree in Figure 2.5 can be obtained using the top-down approach as follows.

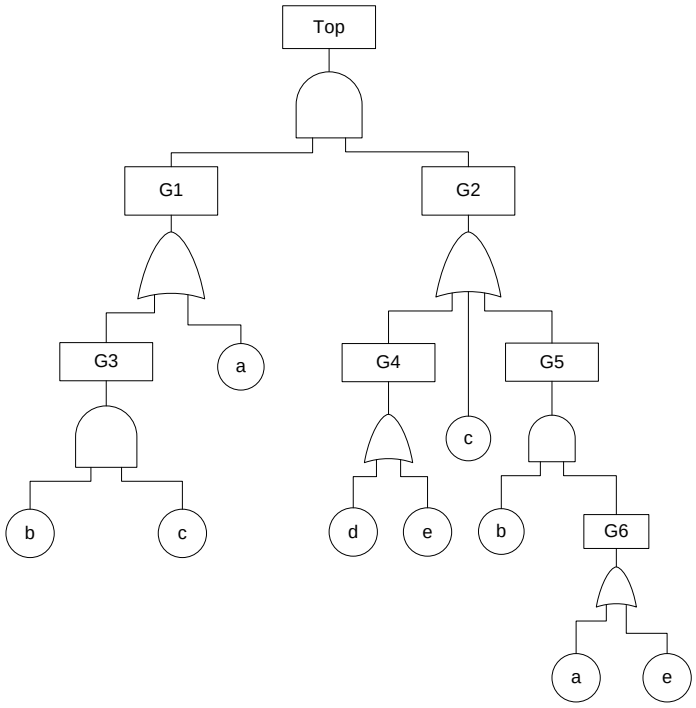


Figure 2.5: Fault Tree Diagram

Starting with the top gate which is an AND gate with two inputs *G1* and *G2* the following expression is obtained:

$$Top=G1 \cdot G2$$

Obtaining expressions for each gate existing in the overall system:

$$G1=G3+a$$

$$G2=G4+c+G5$$

$$G3=b \cdot c$$

$$G4=d+e$$

$$G5=b \cdot G6$$

$$G6=a+e$$

Thus,

$$G5=b\cdot(a+e)$$

$$G1=G3+a=b\cdot c+a$$

$$G2=G4+c+G5=d\cdot e+c+b\cdot(a+e)=d\cdot e+c+b\cdot a+b\cdot e$$

Substitute the expression of *G1* and *G2* into Top:

$$Top=G1\cdot G2=(b\cdot c+a)(d\cdot e+c+b\cdot a+b\cdot e)$$

Expanding this gives the following expression:

$$Top=b\cdot c\cdot d\cdot e+b\cdot c\cdot c+a\cdot b\cdot b\cdot c+b\cdot b\cdot c\cdot e+a\cdot d\cdot e$$

$$+a\cdot c+a\cdot a\cdot b+a\cdot b\cdot e$$

Finally simplifying the expression applying the Boolean reduction laws, the logic expression is obtained for the top event.

$$Top=a\cdot d\cdot e+a\cdot b+a\cdot c+b\cdot c$$

The four minimal cut sets obtained from this example are:

{a,d,e}, {a,b}, {a,c}, {b,c}

2.1.5 Quantitative Analysis

As another stage of FTA, quantitative analysis usually follows qualitative analysis. It involves quantification of the system availability and reliability parameters and analysis of component and/or importance of minimal cut set.

2.1.5.1 Reliability Parameters

A technique is developed to approximate the reliability parameters for a system that consists of several components in [16] because of the complication of quantitative analysis. The calculation is relatively easy and sufficient accuracy can be obtained. The commonly used reliability parameters can be calculated as follows:

The unavailability of a component *i* is:

$$Q_i \approx \frac{\lambda_i}{\lambda_i + \mu_i} \tag{2.1}$$

where λ_i and μ_i are the failure rate and repair rate of the component *i*, respectively. Because λ_i is much smaller than μ_i in value in most cases, the equation can be approximated by:

$$Q_i \approx \frac{\lambda_i}{\mu_i} \tag{2.2}$$

The conditional failure intensity for a cut set *j* at time *t* can be expressed as:

$$\omega_j^*(t) \approx \begin{cases} Q_j^*(t) \times \frac{n}{t} & \text{non-repairable} \\ Q_j^* \times \sum_{i=1}^{n} \mu_i & \text{repairable} \end{cases} \tag{2.3}$$

where *i* is the component *i* in the cut set *j* in (2.3); *n* is the total number of components in the cut set and the superscript "*" indicates that the parameters are for cut sets.

The failure rate for the cut set *j* is:

$$\lambda_j^* = \frac{\omega_j^*}{1-Q_j^*} \tag{2.4}$$

The parameters for a system can be approximated from the parameters of the cut sets for that system as follows:

$$Q_s \approx \sum_{j=1}^{m} Q_j^* \tag{2.5}$$

$$\lambda_s \approx \sum_{j=1}^{m} \lambda_j^* \tag{2.6}$$

$$\omega_s \approx \sum_{j=1}^{m} \omega_j^* \tag{2.7}$$

where *j* indicates the cut set number *j*; the subscript *s* means the system; and *m* is the total number of cut sets in the system.

The unavailability of a system calculated based on the above equations is generally higher than the real system unavailability, which could result in a larger safety margin. However, it should be noted that the discrepancy between the calculated result and the real one can become significant in the following cases:

1. For a repairable component *i*, the unavailability is evaluated at less than twice the mean repair time $1/\mu_i$;
2. For a non-repairable component *i*, the unavailability is evaluated at more than one-tenth the mean time to failure $MTTF = 1/\lambda_i$; and
3. The unavailability of a component is greater than 0.1.

2.1.5.2 Calculating the Top Event Probability

As introduced in [17], the inclusion-exclusion expansion is commonly used to calculate the top event probability. It produces the correct result for trees with repeated events, provided the assumption that basic events are independent.

Consider a fault tree with *n* minimal cut sets

C_i and $i=1,\ldots,n$. The top event exists if at least one of them exists in the overall system:

$$\text{Top}=C_1+C_2+\ldots+C_n=\bigcup_{i=1}^{n} C_i \tag{2.8}$$

The top event probability is calculated as follows:

$$Q_{sys}=P\left(\bigcup_{i=1}^{n} C_i\right)=P(C_1+C_2+\ldots+C_n) \tag{2.9}$$

The result should be expanded according to the inclusion-exclusion method as:

$$Q_{sys}=\sum_{i=1}^{n} P(C_i)-\sum_{i=2}^{n}\sum_{j=1}^{i-1} P\left(C_i \cap C_j\right)+\ldots+(-1)^{n-1} P(C_1 \cap C_2 \cap \ldots \cap C_n) \tag{2.10}$$

To illustrate the calculating process using the method, consider the top event given:

$$Q_{sys}=P(\text{Top})=P(a\cdot b+b\cdot c+a\cdot c)$$

Expanding this using the inclusion-exclusion method:

$$Q_{sys}=q_a\cdot q_b+q_b\cdot q_c+q_a\cdot q_c-q_a\cdot q_b\cdot q_c-q_a\cdot q_b\cdot q_c-q_a\cdot q_b\cdot q_c+q_a\cdot q_b\cdot q_c$$

where q_i represents the unavailability of the component *i*.

For example, suppose $q_a=q_b=q_c=0.03$, the top event probability is:

$$Q_{sys}=(0.03)^2+(0.03)^2+(0.03)^2-(0.03)^3-(0.03)^3-(0.03)^3+(0.03)^3=0.002646$$

The above is the demonstration of calculating the top event probability for coherent fault trees. For non-coherent fault trees, suppose a system with 5 prime implicants include non-coherent event(s) and the Boolean expression obtained from these prime implicants is:

$$T=a\cdot b\cdot d+a\cdot\bar{b}\cdot c+\bar{c}\cdot d\cdot e+a\cdot d\cdot e+a\cdot c\cdot d$$

The system unavailability can be obtained using the method as:

$$Q_{sys}=q_a\cdot q_b\cdot q_d+q_a\cdot p_b\cdot q_c+p_c\cdot q_d\cdot q_e+q_a\cdot q_d\cdot q_e+q_a\cdot q_c\cdot q_d$$

$$-q_a\cdot q_b\cdot q_c\cdot q_d-q_a\cdot q_b\cdot q_d\cdot q_e-q_a\cdot p_b\cdot q_c\cdot q_d-q_a\cdot p_c\cdot q_d\cdot q_e+q_a\cdot q_b\cdot q_c\cdot q_d\cdot q_e$$

2.1.6 Common Cause Failure Analysis

The Common Cause Failures (CCFs) are taken into consideration when performing PSA. A CCF is a condition or an event that causes all the basic events to occur in at least one of the minimal cut sets or prime implicant sets. Even though there are enough redundancies in safety systems in an NPP, these redundancies may lose their ability to protect the plant if there is a CCF. Therefore, the analysis of the CCF is a very important component for PSA.

2.2 Risk Importance Measures

One of the goals for PSA study is to identify the importance of structure, system and components (SSCs). Thus, risk importance measures (RIMs) are computed in PSA to identify the important risk contributors and the important risk sensitivities. Various types of RIMs are calculated, including risk contribution importance, risk reduction importance and

risk increase importance; and they also go by various names such as Birnbaum's Measure, Criticality Importance Factor, Fussell-Vesely Importance, etc.

The RIMs usually depend on two factors: (1) the location of the component in the system; and (2) the reliability of the component in the system. Minimal cut sets or prime implicant sets provided by PSA are one the qualitative ways to examine these RIMs. As the resources, such as man power or cost, are rather limited and have to be directed where they are most efficient, some kind of quantitative measures are needed. That would allow reliability engineers to identify and rank the most important components.

RIMs can be used to evaluate the importance quantitatively on the framework provided by PSA. There are generally three areas of application assigned to RIMs [18]:

1. (Re)Design: optimization of the plant design by adding or removing components;
2. Test and maintenance: optimization of the plant performance by changing the test and maintenance strategy for a given design;
3. Daily configuration control: what will be the effect of taking a component out of service.

2.2.1 Risk Importance Measures for Basic Events

Component failures are modeled in PSA studies as one or more basic events, so the importance of the basic events is used to evaluate the importance of component failures. This means that it is correct to assess a failed event or failed states importance, and not vaguely speak of the component importance [19]. RIMs depend on the risk reference, which means that component importance differs when calculated for different accident sequences.

The eight commonly used RIMs and there mathematical definitions are listed in Table 2.5. The detailed definitions of various RIMs are described in Chapter 3.

For groups of basic events some additional considerations have to be taken. Components can consist of multiple basic events, which could be the different failed states identified for the component. Fussell-Vesely Measure can be readily used for groups of basic events; the sum is just modified to include all the minimal cut sets and prime implicant sets that have some members of the group.

Importance Measures	**Definition**
Birnbaum's Measure (BM)	$G_{BM}=\frac{\partial Q}{\partial q_i}=Q(q_i=1)-Q(q_i=0)$
Criticality Importance Factor (CIF)	$G_{CIF}=\frac{G_{BM}\cdot q_i}{Q}=\frac{\partial Q}{\partial q_i}\cdot\frac{q_i}{Q}$
Improvement Potential (IP)	$G_{IP}=G_{BM}\cdot q_i=G_{CIF}\cdot Q$
Fussell-Vesely Measure (FV)	$G_{FV}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{Q}$
Risk Reduction Worth (RRW)	$G_{RRW}=\frac{Q}{Q(q_i=0)}$
Risk Achievement (RA)	$G_{RA}=Q(q_i=1)-Q$
Risk Achievement Worth (RAW)	$G_{RAW}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{Q\cdot q_i}=\frac{Q(q_i=1)}{Q}$
Conditional Probability (CP)	$G_{CP}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{q_i}=Q(q_i=1)$

Table 2.5: Definitions of Various RIMs

2.2.2 Risk Importance Measures for Failures of Systems and Functions

RIMs can also be used to evaluate the importance of failures of safety functions and systems. Functions appear in fault trees as gates. Systems can be common to several functions and several systems may affect the reliability of the function.

In a way similar to components, when calculating the RIMs for functions or systems the corresponding gate is assumed failed or functioning based on the RIM used. Components represented by the basic events can be common to several functions, so the assumed failure of a gate should not affect basic events, but those are assumed to be at their nominal unavailability level. This is illustrated in Figure 2.6, where Function 1 (darkened) is failed. Systems do not share basic events, since a single component can only belong to a single system. Calculating the importance of functions requires a lot computing power since disabling a function requires recalculation of minimal cut sets. In PSA models with many functions this takes time and needs approximate methods for faster solving.

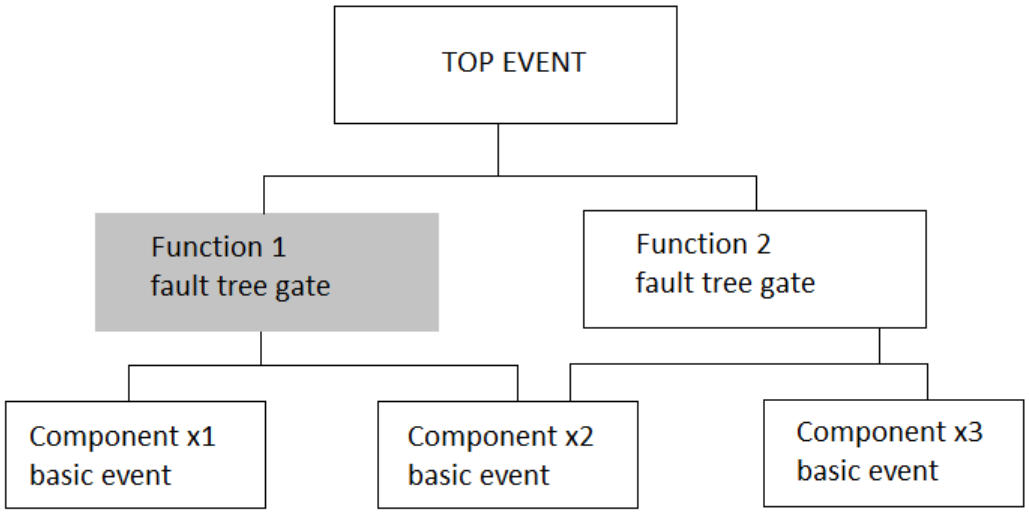


Figure 2.6: Evaluating Functional Importance

2.3 Non-coherent Systems

Fault trees are classified according to their logic function. If during fault tree construction only AND gates and OR gates are used, the resulting fault tree is defined as coherent. If NOT logic is used or directly implied, the resulting fault tree is non-coherent. The indicator x_i is used to show the status of each component

$$x_i = \begin{cases} 1 & \text{if component i has failed} \\ 0 & \text{if component i is working} \end{cases}$$

where $i = 1, 2, \ldots, n$, and n is the number of components in the system.

The logic structure of the fault tree can be expressed by a structure function ϕ.

$$\phi = \begin{cases} 1 & \text{if component } i \text{ has failed} \\ 0 & \text{if component } i \text{ is working} \end{cases}$$

$\phi = \phi(x)$, where $x = (x_1, x_2, \ldots, x_n)$.

According to the requirements of coherency [12], a structure function $\phi(x)$ is coherent if

Each component i is relevant to the system, i.e.

$\phi(0_i, x) \neq \phi(1_i, x)$ for some x_i

$\phi(x)$ is increasing (non-decreasing) for each x_i, i.e.

$\phi(1_i, x) \geq \phi(0_i, x)$ for some x_i

where

$\phi(1_i, x) = \phi(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$

$\phi(0_i, x) = \phi(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$

The second condition means that the system condition does not change or deteriorate as the component deteriorates. If the system is non-coherent for component i, the system is in the failed condition when component i is working; and when component i

fails the system is restored to the non-failed condition. As a consequence of this property, system failure might occur due to the repair of a failed component, or for a failed system the failure of an additional component may give a successful outcome of system performance. The fault tree becomes coherent if the NOT logic can be eliminated from the fault tree structure. It should be noted that because the structure function of non-coherent system is non-monotonic, the cut sets are represented by prime implicant sets because of the complication of the system failure mode.

2.3.1 A Simple Example of Non-coherency

An example is made in [20] and [21]. Consider the example illustrated in Figure 2.7. Cars *A* and *B* are approaching a junction with lights on red, and should stop. Car *C* has the right of way and should proceed through the junction. Event *A*, *B* and *C* are considered:

A: Car *A* fails to stop.

B: Car *B* fails to stop.

C: Car *C* fails to continue.

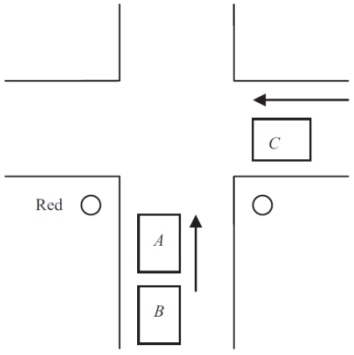


Figure 2.7: Traffic Light System

A collision at the crossroads can happen in two ways:

Car *A* fails to stop and hits car *C* which is moving.

Car *A* stops but car *B* drives into the back of it.

A fault tree representing causes of failure of the collision is shown in Figure 2.8. Working in a bottom-up way, the following logic expression is obtained

$$\text{Top}=A\cdot\overline{C}+\overline{A}\cdot B$$

where '+' is OR and '·' is AND.

Therefore, $\{A\cdot\overline{C}\}$ and $\{\overline{A}\cdot B\}$ are prime implicants, as combinations of component conditions (working or failed) that are necessary and sufficient to cause system failure. This list is incomplete because there is one more failure mode for the system

$\{B\cdot\overline{C}\}$

i.e. if *B* fails to stop and *C* continues across the lights, it does not matter what *A* does – there will be a collision.

Therefore, the full logic expression for the Top event is

$$\text{Top}=A\cdot\overline{C}+\overline{A}\cdot B+B\cdot\overline{C}$$

which can be obtained by applying the consensus law

$$A\cdot X+\overline{A}\cdot Y=A\cdot X+\overline{A}\cdot Y+X\cdot Y$$

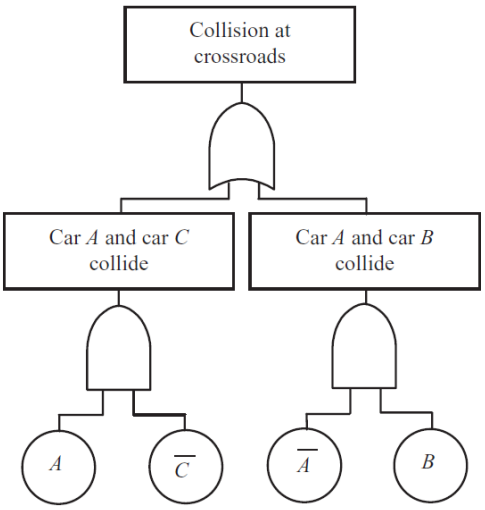


Figure 2.8: Collision Fault Trees

2.3.2 Non-coherent Systems In Real World

While most of the systems in real world have coherent structure, some systems have non-coherent structure due to:

1. The nature of the systems, such as the negative feedback loops and redundant loops [22];
2. The system failure under certain circumstances, such as the Gas Detection Systems presented as a case study in Section 5.2;
3. The bad design of a system, as the occurrence of a non-coherent event, which causes or directly implies the system failure, has a rather high probability.

The maintenance on non-coherent systems is definitely more complicated than those perfectly designed coherent systems. However, the FTA involving non-coherent components/events still needs attention. The accident at the Three Mile Island Unit 2 (TMI-

2) nuclear power plant, for example, shows the fact that non-coherent events may cause severe consequences[23][24][25].

In the night-time hours preceding the accident, the TMI-2 reactor was running at 97 percent of full power, while the companion TMI-1 reactor was shut down for refuelling. The chain of events leading to the partial core meltdown began at 4 a.m. EST on March 28, 1979, in TMI-2's secondary loop, one of the three main water/steam loops in a pressurized water reactor. The layout of TMI-2 is shown in Figure 2.9.

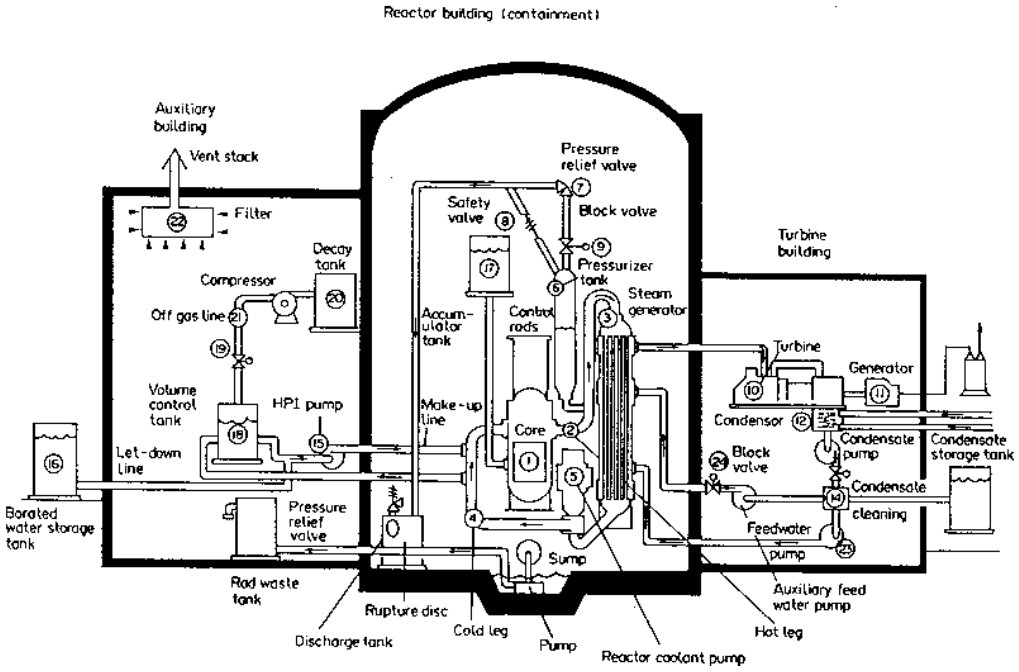


Figure 2.9: Schematic Layout of TMI-2

As a result of mechanical or electrical failure, condensate pump stopped running, followed immediately by the main feedwater pumps. This automatically triggered the turbine to shut down and the reactor to scram: control rods were inserted into the core and fission ceased. However, as the reactor continued to generate decay heat, and steam was no longer being used by the turbine due to the turbine trip, the steam generators no longer removed that heat from the reactor.

Once the secondary feedwater pump system failed, three auxiliary pumps activated automatically. However, because the valves had been closed for routine maintenance, the system was unable to pump any water. The pumps were activated manually eight minutes later, and manually deactivated between 1 and 2 hours later, as per procedure, due to excessive vibration in the pumps.

Due to the loss of heat removal from the primary loop and the failure of the auxiliary system to activate, the primary side pressure began to increase, triggering the pilot-operated relief valve (PORV) at the top of the pressurizer to open automatically. The PORV should have closed again when the excess pressure had been released and electric power to the solenoid of the pilot was automatically cut, but instead the main relief valve stuck open due to a mechanical fault. The open valve permitted coolant water to escape from the primary system, and was the principal mechanical cause of the crisis that followed.

Aside from human factors and emergency system issues in this event, the loss of heat removal from the primary loop, the failure of the auxiliary system were the main causes of the system breakdown; the other event that directly caused the crisis is the mechanical failure on the main relief valve. The event can be illustrated as a fault tree in Figure 2.10.

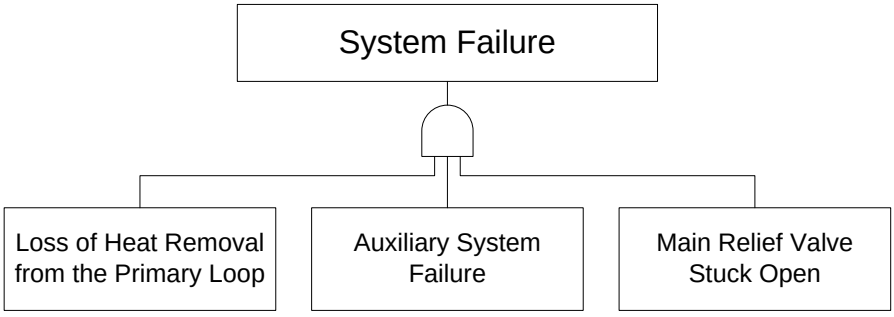


Figure 2.10: TMI-2 Fault Tree 1

Based on the description of the event, several sub-events are considered as follows:

A: Condensate pump stops running;

B: Reactor is shut down;

C: Valves in auxiliary system closed (for maintenance);

D: Main valve of PORV stuck open

The fault tree in Figure 2.10 can be generated based on the sub-events in Figure 2.11:

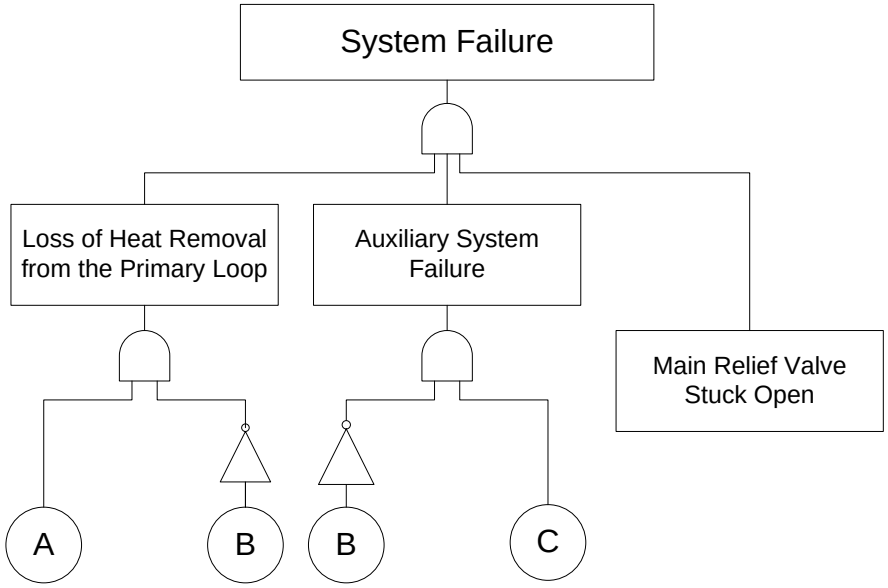


Figure 2.11: TMI-2 Fault Tree 2

And it is minimized into the fault tree in Figure 2.12:

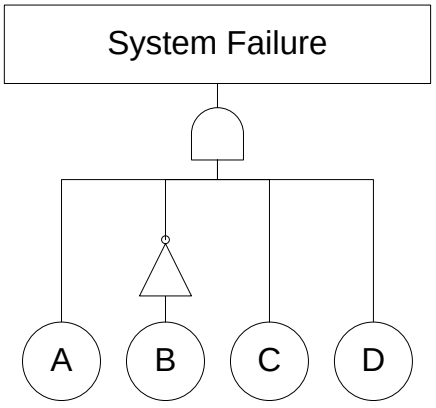


Figure 2.12: TMI-2 Fault Tree 3

Because the reactor was not shut down and still continued to generate heat, the inverse of the event B should be considered in the FTA. This is a typical case of non-

coherent FTA and shows how the system is affected by a non-coherent event ($\overline{B}$: Reactor not shut down). Obviously the coherent events are associated with the mechanical/electrical failure of components, which are the initiating events of the system failure; the non-coherent event is associated with the other faults revealed during the investigation, such as the bad design of the reactor control system's interface, human factor, etc.

In reality, the closure of these valves was a violation of a key NRC rule, according to which the reactor must be shut down if all auxiliary feed pumps are closed for maintenance. This failure was later singled out by NRC officials as a key one, without which the course of events would have been very different.

The accident at the Three Mile Island Unit 2 (TMI-2) nuclear power plant was the most serious in U.S. commercial nuclear power plant operating history, even though it led to no deaths or injuries to plant workers or members of the nearby community [24]. But it brought about sweeping changes involving emergency response planning, reactor operator training, human factors engineering, radiation protection, and many other areas of nuclear power plant operations. It also caused the U.S. Nuclear Regulatory Commission (NRC) to tighten and heighten its regulatory oversight and brought attention to PSA approach in regulatory use, which makes it a watershed event in the history of nuclear industry. Resultant changes in the nuclear power industry and at the NRC had the effect of enhancing safety.

2.3.3 Calculational Tools for Non-coherent Fault Tree Analysis

The System unavailability can be hand calculated by using the method in [9]. When analyzing non-coherent fault trees, the Binary Decision Diagram (BDD) method is usually incorporated to overcome the difficulties in calculation. The BDD method has distinct advantages for quantifying a non-coherent fault tree. The methodology to determine the

prime implicants from the BDD structure is given in [26], and the calculation procedure is given in [27].

In this thesis, the fault trees are constructed using Relex Architect Software (Relex Fault Tree), which helps on calculating the most commonly used RIMs such as Birnbaum's Measure (BM), Criticality Importance Factor (CIF) and Fussell-Vesely Measure (FV). However, the other RIMs cannot be calculated using Relex software. Most of the calculations for various RIMs are done by hands with the help of spreadsheets in Excel.

2.4 Maintenance Engineering

Maintenance is required for almost every complex industrial installation to keep the equipment in adequate condition. An efficient and effective maintenance program plays a key role in reducing costs and improving safety. Different maintenance activities are utilized depending on the type of production process.

At some industrial work, the aims are to repair equipment failures when this occurs; at others effort is taken to prevent failure and/or to minimize equipment downtimes. Thus maintenance is broadly classified to corrective and preventive maintenance; the former comprising activities such as inspection and replacement while the latter concerning fixing or replacing equipment in the event of failure [28]. The classification of maintenance activities is illustrated in Figure 2.13.

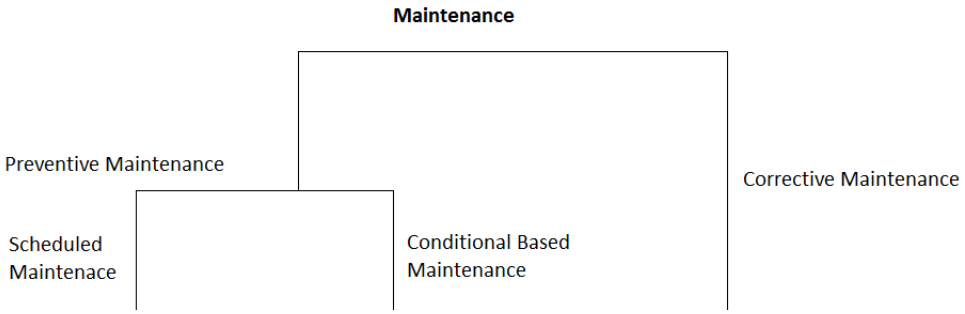


Figure 2.13: Different Types of Maintenance

Test and maintenance methodologies have evolved over the last several decades. Before the 1950s, maintenance was often performed whenever there was a component failure (corrective maintenance) [29]. Gradually, the plant availability, equipment life, plant safety, product quality, and cost were all incorporated into the requirements. Therefore, over time, preventive maintenance was developed [29][30][31] that could be further categorized into two types: Periodic Preventive Maintenance and Condition-Based Predictive Maintenance. The difference between the corrective and preventive maintenance can be shown in Figure 2.14.

Various aspects of maintenance have been investigated in nuclear power industry, where maintenance plays an importance role to reach a high level of performance and safety, which is generally required by NPP owners, regulatory authorities and the public.

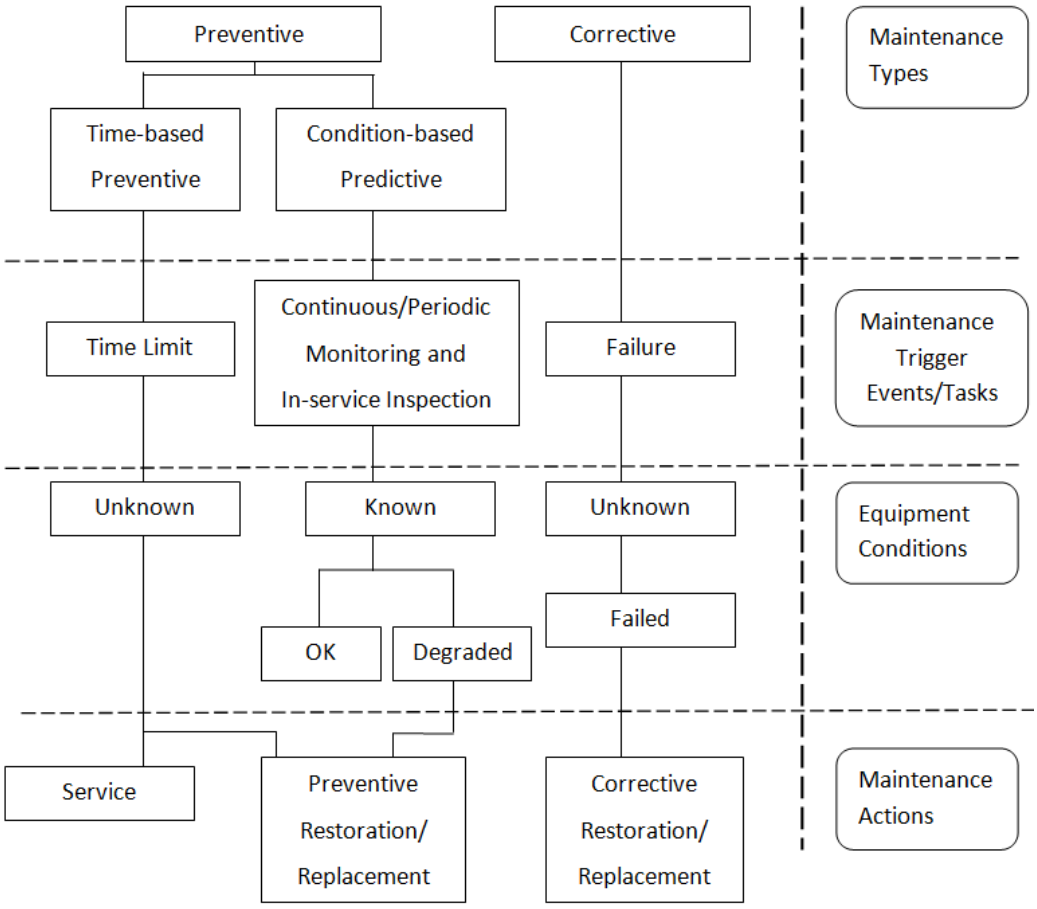


Figure 2.14: Preventive and Corrective Maintenance

Thus, various programs are developed for the purpose of improving the effectiveness of maintenance from both performance and safety view points, such as Reliability Centered Maintenance (RCM) and Risk-informed Maintenance.

2.4.1 Reliability Centered Maintenance

Reliability Centered Maintenance (RCM) is a technique for developing a preventive maintenance (PM) program, which is based on the assumption that the inherent reliability of the equipment is a function of the design and the build quality. RCM is designed to balance the costs and benefits, to obtain the most cost-effective PM program [32].

RCM focuses on the most important functions of the system, while eliminating the inefficient and unnecessary maintenance activities, as the main objective of RCM is to reduce the maintenance cost. The maintainability consideration, which is supposed be considered during the early concept phase of system design, are usually delayed until it is too late to make significant changes. Detailed maintenance strategies should be established before the system is put into operation.

The maintenance tasks considered in the RCM approach are all related to failures and functional degradation. The improvement of a system, which has no effects on the system functions, is outside the scope of RCM, but it should be integrated with the planning of RCM relevant tasks.

The RCM concept was originated within the aircraft industry [33], and then migrated through other industries with high reliability needs such as chemical, offshore oil and gas, etc. By the early 1990's, RCM had made its way to the utility industry via the nuclear industry, and it has proven useful in applications that all share some common characteristics, including systems where reliability is critical and where quantitative data regarding failures are limited.

Generally, the whole RCM analysis is usually carried out as a sequence of activities or steps as follows, while some of the steps are overlapping in time [32]:

1. Study Preparation
2. System Selection and Definition
3. Functional Failure Analysis
4. Critical Item Selection

5. Data Collection and Analysis
6. Failure Mode Effect Criticality Analysis (FMECA)
7. Selection of Maintenance Actions
8. Determination of Maintenance Intervals
9. Preventive Maintenance Comparison Analysis
10. Treatment of Non-Critical Items
11. Implementation
12. In-Service Data Collection and Updating

On the other hand, the whole process is divided into four elements [34]:

1. Planning and Preparation
2. Initial RCM Analysis
3. Implementation of Results
4. Sustaining the Analysis

2.4.2 Risk-informed Maintenance

2.4.2.1 Risk-informed Decision Making Approach

The insights and applications of PSA have made significant improvements to Nuclear Power Plant (NPP) safety, reliability, operational flexibility and economy. [35] Risk-

informed Decision Making (RIDM) integrates insights from deterministic or traditional engineering safety analysis with insights from PSA application process. While much of RIDM experience is from NPP applications, the intent is to offer RIDM to the full range of nuclear facilities such as waste storage.

The RIDM was originally used in nuclear community primarily to identify NPP severe accident vulnerabilities to prioritize mitigating alternatives, and to access operational events. It also had some input to regulatory rule making. However, a primary stimulus came in improving NPP technical specifications by demonstrating the safe and sometimes optimum extensions of allowed outage times and surveillance test intervals.

Success in the area of technical specifications improvement led to applications in the areas of configuration risk analysis and management in a broader sense and to the analyses and optimization of maintenance, both at power and during outages. Numerous safety enhancements were revealed through the application of PSA.

These successes led to additional successful applications, which included further rulemaking, in-service inspection, in-service testing, quality assurance, increasingly flexible technical sections, design, inspection, and regulatory oversight. While many applications received visibility because of their regulatory interfaces, additional applications afforded significant success in areas that were not addressed in the licensing basis, safety case, etc. Emerging applications in several countries are in the area of facility security.

Improved nuclear safety includes improvements to the plant and to its programs and procedures, increased understanding of vulnerabilities, and increased understanding of high risk situations to avoid. Increased plant performance and economy include reduced personal radiation exposure as well as optimized fiscal considerations.

2.4.2.2 The Nuclear Industry's Transition to Risk-informed Regulation

The transition from a prescriptive regulatory structure to a more risk-informed approach of the United States nuclear industry occurred over a 20 yr period in which gradual changes were made in the fundamental regulations and to the approach to nuclear safety and operations. The regulatory changes are continuing even though the number is not huge. The utilities that embraced risk informed operations made dramatic changes in the way they approached operations and outage management. Those utilities that used risk in operations showed dramatic improvement in safety based on Institute of Nuclear Power Operations (INPO) performance indicators. It was also shown that the use of risk did not negatively affect safety performance of the plants compared to standard prescriptive approaches. This was despite having greater flexibility in compliance to regulatory standards and the use of the newly instituted risk-informed reactor oversight process. The development of risk-informed regulation in the US and more details of the implementation strategies in the industry are addressed in [36].

Key factors affecting the successful transition to a more risk-informed approach to regulations and operations are:

- Strong top management support and leadership both at the regulator and the utility;
- Education and training in risk principles and PSA tools for engineers, operators and maintenance staff;
- A slow and steady introduction of risk initiatives in areas that can show value to both the regulator and the industry;
- A transparent regulatory foundation built around a safety goal policy, and

- The development of a strong safety culture at the utility to allow for more independence in safety compliance and risk management.

However, there were several reluctance to use PSA in licensing decisions when WASH-1400 (The Rasmussen Report or the Reactor Safety Study) [12] was published and the process of creating risk-informed regulatory process began in 1970s [36]. The readiness of using risk in technical decision making was questioned because of the certain short comings in the treatment of uncertainties [37]. According to the "Staff Actions Regarding Risk Assessment Review Group Report" in 1979 [38], the regulatory decision should not be solely based on PSA. In addition, the immaturity of PSA approach, the lack of industrial experience, the lack of expertise in methodology in NRC, result in the reluctance to implement PSA in licensing decisions.

In 1979, the TMI accident (introduced in Section 2.3.2) changed the attractiveness of PSA, as the physical damage to the plant and economic damage to the owners was very large which prompt their need to better understand the risk of operation. The actions were taken in response to the event, such as the development of PSA for boiling water reactors (BWR), the development of Industry Degraded Core Rulemaking Program (IDCOR), etc. [36]

The use of PSA for regulatory purposes was growing fast in 1980s. The risk insights were used in the development of many regulations such as the station Blackout Rule and Anticipated Transients without Scram Requirements in the late 1980s, the maintenance rule enable utilities to take advantages of their IPEs in developing risk-informed maintenance programs.

2.4.2.3 Optimized Maintenance through PSA

A research program aimed at making optimum use of maintenance resources was launched in 1990 Electricité de France (EDF). The objective of this was to focus maintenance work on equipment which had a fundamental role in safety program and unit availability and maintenance cost [39]. In this approach, a new maintenance policy is likely to result in an evolution in the reliability and availability of the equipment. The impact of the new policy can be evaluated with PSA in order to achieve full optimization. Such approach is called risk-informed maintenance.

Chapter 3

Extension of Risk Importance Measures to Non-coherent Systems

3.1 Various Risk Importance Measures

One of the major objectives from a PSA is to help focus attention on the most important systems when performing maintenance, namely risk-informed maintenance. This is particularly beneficial when resources are limited in practical applications. To achieve this goal, Risk Importance Measures (RIMs) derived from PSA provides valuable information for risk-informed decision making. Through a RIM, a ranking of the components (or basic events) can be obtained. The components on the top of the list should receive most attention. This is important when resources and limited in order to reduce cost. There are numerous RIMs defined in the open literature, and they have been applied in various applications. In this section, eight commonly used RIMs (Birnbaum's Measure, Criticality Importance Factor, Improvement Potential, Fussell-Vesely Measure, Risk Achievement, Conditional Probability, Risk Achievement Worth and Risk Reduction Worth) are introduced and discussed in detail.

3.1.1 Birnbaum's Measure

Birnbaum's Measure (BM) was introduced with the concept of importance and a probabilistic measure of component reliability in 1969 [50]. It is defined as the ratio of the component unreliability/unavailability to system unreliability/unavailability (denoted by Q_{sys}); and it determines the maximum increase in risk when the given component is failed compared to when it is in a working state. It is also referred to as Partial Derivative (PD) in [18][41].

Mathematically, BM is obtained by partial differentiation of the system unavailability with respect to the probability of failure of the component. However, it has been represented in different forms in different literatures and they are tabulated below.

Mathematical Expression	Description
$I^{BM}(e)=\frac{\partial Pr\{S\}}{\partial Pr\{e\}}=\frac{\partial U_{sys}}{\partial q_e}$ [42]	S – structure function of the system e – given basic event U_{sys} – system unavailability, i.e. Pr {S} q_e – unavailability of the given component *e*
$BI=R(x_i=1)-R(x_i=0)$ [18]	$R(x_i = 1)$ – the increased risk level with basic event *i* assumed to be failed $R(x_i = 0)$ – the decreased risk level with basic event *i* assumed to be working or perfectly reliable
$b_j=O_{j_1}-O_{j_0}$ [43]	O_{j_1} – output of element *j* in failed state O_{j_0} – output of element *j* in functioning state
$I^B_{x_i}=CDF(x_i=1)-CDF(x_i=0)$ [44]	$CDF(x_i = 1)$ – the risk level with particular system is unavailable $CDF(x_i = 0)$ – the risk level with particular system is zero
$G_i(q)=\frac{\partial Q_{sys}(t)}{\partial q_i(t)}$ [21]	$Q_{sys}(t)$ – system unavailability; Pr {System is in a failed state at time *t*} $q_i(t)$ – failure probability of component *i*
$I_B=R_i^+-R_i^-$ [45]	R_i^+ – overall model risk with the probability of basic event *i* set to 1 R_i^- – overall model risk with the probability of basic event *i* set to 0

Table 3.1: Definitions of Birnbaum's Measure

It can be seen in Table 3.1 that the expression of BM can also be defined as the difference between the risk level of the overall when the probability of basic event is set to 1 and the risk level when probability of the basic event is set to 0. Thus the expression can be:

$$G_{BM}=\frac{\partial Q_{sys}}{\partial q_i}=Q(q_i=1)-Q(q_i=0) \tag{3.1}$$

In general, the value of BM represents the sensitivity coefficient of the risk measures to the probability of the given basic event, and provides one way of looking at the defence-in-depth issue in a probabilistic sense [45]. BM does not explicitly indicate how likely the given basic event is to occur as the value of BM is usually independent of the actual unavailability of the given event; it can lead to assigning high importance to events that are very unlikely to occur and difficult to improve.

3.1.2 Criticality Importance Factor

Criticality Importance Factor (CIF) is defined as the probability that the given basic event has occurred, i.e. the failure of the given component is critical to the system. It takes into account the failure probability of the given basic event. Since BM is independent of the actual unavailability of the given event and can lead to assigning high importance to events that are unlikely to occur, CIF is derived from BM as to focus on events that are not only critical to the top event but also are more likely to occur.

The mathematical definition of CIF is:

$$G_{CIF}=\frac{G_{BM}\cdot q_i}{Q_{sys}}=\frac{Q(q_i=1)-Q(q_i=0)}{Q_{sys}}\cdot q_i=\frac{\partial Q_{sys}}{\partial q_i}\cdot\frac{q_i}{Q_{sys}} \tag{3.2}$$

It is also referred to as Criticality Measure [42][46], Criticality Importance[18], or Fractional Contribution [47], in different studies.

3.1.3 Improvement Potential

Improvement Potential (IP) measures how much the system reliability increases if the given basic event was replaced by a perfect component, i.e. a component in a working state [42][48][49]. It is also referred to as Risk Reduction [18][50]. The mathematical definition of IP is based on BM and CIF:

$$G_{IP}=G_{BM}\cdot q_i=G_{CIF}\cdot Q_{sys} \tag{3.3}$$

Since the unavailability of the overall system Q_{sys} is constant, IP has the same functions when ranking the importance of basic events or components.

3.1.4 Fussell-Vesely Measure

Fussell-Vesely Measure (FV) is defined as the probability that a given basic event has contributed to the basic risk level, assuming the system has failed. Mathematically, FV is the ratio of the probability of any cut set or prime implicant set containing the given event and the probability of the top event, i.e. the system unavailability. Thus, it assesses the contribution of the group in such a way that, any combination (Minimal Cut Sets, Prime Implicant Sets) that has a contribution from any one member of the group is included. It is commonly used as a risk reduction indicator.

FV has been represented in multiple forms by different literatures are presented in Table 3.2.

Mathematical Expression	Description
$I_i=1-\frac{F(0)}{F}$ [51]	F(0) – risk level supposing that the unavailability associated with the basic event i is zero F – Basic event level
$FV=\frac{\{CDF(base)-CDF(x_i=0)\}}{CDF(base)}$ [44]	CDF(base) – the time averaged CDF $CDF(x_i = 0)$ – the risk level when particular system unavailability is zero
$FV=\frac{R(base)-R(x_i=0)}{R(base)}$ [18]	R(base) – the present risk level $R(x_i = 0)$ – the decreased risk level with the basic event optimized or assumed to be perfectly reliable
$FV_i=\frac{R_0-R_i^-}{R_0}=1-\frac{R_i^-}{R_0}$ [45]	R_0 – base (reference) case overall model risk R_i^- – overall model risk with the probability of basic event *i* set to 0
$I_{FV}=\frac{Pr\{\bigcup_{k=1;i\in C_k}^{n_p} C_k\}}{Q_{sys}(t)}$ [21]	n_p – total number of minimal cut sets or prime implicant sets C_k – minimal cut set *k* for coherent systems/prime implicant set *k* for non-coherent systems Q_{sys} - system unavailability; Pr {System is in a failed state at time *t*}
$f_j=\frac{O-O_{j0}}{O}=1-\frac{1}{r_j}$ [43]	O_{j0} – output of element *j* in failed state O – output performance measure r_j – performance reduction work

Table 3.2: Definitions of Fussell-Vesely Measure

Since the risk equation can be represented in a linear equation:

$$R(X_i)=aX_i+b,$$

where *b* represents the base risk for a perfectly reliable component, FV can be expressed as:

$$FV = \frac{aX_i(base)}{aX_i(base)+b}$$

As a basis of risk significance (RS), the above equation can be rewritten as:

$$FV = \frac{ax_i(base)}{ax_i(base)+b} \approx \frac{a}{b} x_i, \text{ when } ax_i \ll b.$$

This equation indicates that FV is proportional to x_i, which is the unavailability of component *i* [18].

Although FV assesses the contribution of the group of basic events in such a way that any minimal cut set or prime implicant set that has a contribution from any one member of the group is included, it is not additive. Since FV is simply a ratio of contributors and does not involve assessing changes, it is an appropriate measure of group importance [45].

In this thesis, the expression of FV is written as:

$$G_{FV} = \frac{\Pr\{\bigcup_{k|i\in k} C_k\}}{Q_{sys}} \tag{3.4}$$

FV is frequently adopted instead of CIF which can also be defined as the probability that a given basic event is contributing to the basic risk level. Although they are not equivalent to each other, they give similar results [51].

3.1.5 Risk Achievement

Risk Achievement (RA) measures the increase in risk of system failure if a given component fails. The expression is given in [18]:

$$RA=R(x_i=1)-R(base) \tag{3.5}$$

where $R(x_i = 1)$ denotes the increase risk level without basic event x_i or with basic event x_i assumed failed and $R(base)$ represents the present risk level.

In this thesis, the expression of RA is written as:

$$G_{RA}=Q(q_i=1)-Q_{sys} \tag{3.6}$$

where $Q(q_i=1)$ denotes the system unavailability with event i assumed occurred.

3.1.6 Conditional Probability

Conditional Probability (CP) gives the value of the change in system unreliability (or risk) that involves the failure of the given basic event. The expression is given in [52]:

$$I^{CP}(e)=Pr\{S|e\}=\frac{Pr\{S\cap e\}}{Pr\{e\}}=\frac{Pr\{S\cap e\}}{q_e} \tag{3.7}$$

In this thesis, the expression of CP is written as:

$$G_{CP} = \frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{q_i} = Q(q_i = 1) \tag{3.8}$$

3.1.7 Risk Achievement Worth

Risk Achievement Worth (RAW) is most commonly used as a measure of safety consideration and a risk achievement indicator. It is defined as the 'worth' of the given basic event in 'achieving' the present level of risk, and indicates the importance of maintaining the current level of reliability with respect to the failed event associated to corresponding components.

Using the same linear approximation described above for FV, RAW can be written as:

$$\text{RAW} = \frac{a+b}{aX_i(\text{base})+b} \approx \frac{a}{b} + 1, \text{ when } aX_i(base) \ll b \tag{3.9}$$

The expression has shown that unlike FV, RAW does not represent the component itself as it seen to independent of the unavailability of the given basic event. Table 3.3 shows the variations of the definitions of RAW.

Mathematical Expression	Description
$A_i = \frac{F(1)}{F}$ [51]	F(1) – the risk level supposing that the unavailability associated with the basic event *i* is set to 1 F – basic event level
$RAW = \frac{CDF(x_i=1)}{CDF(base)}$ [44]	CDF(x_i = 1) – the risk level when particular system is unavailable CDF(base) – the time averaged CDF
$RAW = \frac{R(x_i=1)}{R(base)}$ [18]	R(x_i = 1) – the increased risk level without basic event x_i or with basic event x_i assumed failed R(base) – the present risk level
$a_i = \frac{R_i^+}{R_0}$ [45]	R_0 – base (reference) case overall model risk R_i^- – overall model risk with the probability of basic event *i* set to 0
$I^{RAW}(e) = \frac{Pr\{S \mid e\}}{Pr\{S\}} = \frac{Pr\{S \cap e\}}{U_{sys} q_e}$ [42]	S – structure function of the system e – given basic event U_{sys} – system unavailability, i.e. $Pr\{S\}$ q_e – unavailability of the given component *e*
$a_j = \frac{O_{j_1}}{O}$ [42]	O_{j_1} – output of element *j* in failed state O – output performance measure

Table 3.3: Definitions of Risk Achievement Worth

RAW is also called Risk Increase Factor as it measures the increase in system unreliability assuming the worst case of the failure of the given component [53]. It has been applied to systems made up of binary elements (i.e. elements that can be in either failed or working state) [43]. In this thesis, the expression of RAW is written as:

$$G_{RAW} = \frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{Q_{sys} \cdot q_i} = \frac{Q(q_i = 1)}{Q_{sys}} \tag{3.10}$$

3.1.8 Risk Reduction Worth

Risk Reduction Worth (RRW) measures the maximum decrease of the risk (system unavailability) by the improvement of the element associated with the given basic event considered [18][42][43]. In a different definition, RRW yields the ratio of the basic case model risk to the risk with the probability of the basic event set to be 0, i.e. the basic event does not happen; and it represents the maximum decrease in risk for an improvement to the element associated with the basic event [45]. For all intents and purposes, both of the above definitions are accurate to describe RRW. It can be used to select components that are the best candidates for efforts leading to improving system reliability [42]; and it has been applied to systems made of up of binary elements (i.e. elements that can be in either failed or working state) [43]. Table 3.4 shows the variations of the definitions of RRW.

Mathematical Expression	Description
$R_i = \frac{F}{F(0)}$ [51]	F(0) – risk level supposing that the unavailability associated with the basic event i is zero F – basic event level
$RRW = \frac{CDF(base)}{CDF(x_i=0)}$ [44]	CDF(base) – the time averaged CDF $CDF(x_i = 0)$ – the risk level when particular system unavailability is zero
$RRW = \frac{R(base)}{R(x_i=0)}$ [18]	R(base) – the present risk level $R(x_i = 0)$ – the decreased risk level with the basic event optimized or assumed to be perfectly reliable
$r_i = \frac{R_0}{R_i^-}$ [45]	R_i^+ – overall model risk with the probability of basic event *i* set to 1 R_0 – base (reference) case overall model risk
$I^{RRW}(e) = \frac{Pr\{S\}}{Pr\{S \mid e\}} = \frac{U_{sys}(1-q_e)}{Pr\{S \cap e\}}$ [42]	S – structure function of the system e – given basic event U_{sys} – system unavailability, i.e. $Pr\{S\}$ q_e – unavailability of the given component *e*
$r_j = \frac{O}{O_{j_0}}$ [43]	O_{j_0} – output of element *j* in functioning state O – output performance measure

Table 3.4: Definitions of Risk Reduction Worth

In this thesis, the expression of RRW is written as:

$$G_{RRW} = \frac{Q_{sys}}{Q(q_i=0)} \tag{3.11}$$

where $Q(q_i=0)$ denotes the system unavailability with event *i* assumed not occurred.

3.2 Extension of Various Risk Importance Measures to Non-coherent Systems

Whether the fault tree is coherent or non-coherent is important to determine during FTA when coordinating maintenance activities. The non-coherency of the events/components in a fault tree varies the maintenance sequence and priority. Although this field has received much attention over the past 35 years, the majority of measures have been developed specifically for the analysis of coherent systems, and therefore have ranked component failures. Importance analysis of non-coherent systems is rather limited; it is generally inaccurate and misleading because importance is approximated using the measures developed for the analysis of coherent systems.

3.2.1 The Extension of Birnbaum's Measure to Non-coherent Systems

In FTA, the probability of the top event in a coherent fault tree is a function of the probabilities of the occurred basic events. In a non-coherent fault tree however, the probability of the top event is a function of the probability of some basic events not occurring, which complicates the evaluation of RIMs.

As introduced before, BM is defined as probability that component is critical to system failure. It is the fundamental probabilistic measure of importance and a central of many other measures such as CIF and IP.

In [21][54], BM for non-coherent fault trees is failure critical when the given basic event is coherent to the occurrence of the top event; and is repair critical when the negation of the given basic event is coherent to the occurrence of the top event, i.e. the component is non-coherent to the overall system. This is because not only the occurrence of a basic event but also the non-occurrence of the basic event can result in the occurrence of the top event in a fault tree. These two criticalities should be considered separately when analyzing a system because the given component can exist in only 1 state at any time. Thus the expression of BM, $G_{BM}=Q(q_i=1)-Q(q_i=0)$, is not applicable when extending to non-coherent systems because if BM of component *i* was written as $Q(q_i=1)-Q(q_i=0)$, BM of its negation $\bar{i}$ is $Q(q_i=0)-Q(q_i=1)$, which is meaningless in ranking. On the other hand, BM is also calculated from the system unavailability function, $Q_{sys}(i)$, which is obtained using the exclusion-inclusion principle and Boolean reduction laws. G_{BM} can be expressed as:

$$G_{BM}=\frac{\partial Q_{sys}}{\partial q_i} \tag{3.12}$$

As Component *i* is failure critical if the system is working, but the system fails if the component fails. Thus the probability that component is failure critical is the probability that the system is in a working state such that the failure of the component causes at least 1 prime-implicant set containing event to occur. This probability is calculated by obtaining the probability that at least 1 prime-implicant set containing event exists and then dividing this probability by the unavailability of component *i*. [48]

To calculate this probability, the system unavailability can be re-written using 3 distinct terms:

$$Q_{sys} = i \cdot A + \bar{i} \cdot B + C \tag{3.13}$$

The three terms represent, respectively,

- those products involving the failure of the given component,
- those products involving the repair of the given component,
- those products for which component is irrelevant.

Thus the probability that the given component is failure critical is:

$$G_i^{BM}\left(\underline{q}\right) = \frac{\Pr\{i \cdot A\}}{q_i} = \Pr\{A\} \tag{3.14}$$

Similarly, the probability that component *i* is repair critical is the probability that the system is in a working state such that the repair of component *i* causes at least 1 prime-implicant set containing event $\bar{i}$ to occur. This is calculated by obtaining the probability that at least 1 prime implicant set containing event $\bar{i}$ exists and then dividing this probability by the availability of component *i*.

$$G_i^{BM}\left(\underline{p}\right) = \frac{\Pr\{\bar{i} \cdot B\}}{p_i} = \Pr\{B\} \tag{3.15}$$

Therefore, the failure and repair criticalities can be calculated separately by differentiating the system unavailability Q_{sys} with respect to q_i and p_i, respectively:

$$G_i^{BM}\left(\underline{q}\right) = \frac{\partial Q_{sys}}{\partial q_i} \tag{3.16}$$

$$G_i^{BM}\left(\underline{p}\right) = \frac{\partial Q_{sys}}{\partial p_i} \tag{3.17}$$

3.2.2 The Extension of Criticality Importance Factor to Non-coherent Systems

The Component Importance Factor (CIF) is defined as: the probability that a component is critical to the system and has failed, weighted by the system unavailability. It is one of the most importance RIMs that has been developed from BM. When analyzing a non-coherent fault tree, then component failure and component repair can cause system failure; thus the expression for failure importance and repair importance must be obtained. [21]

Because CIF is defined based on BM, the failure criticality and repair criticality can be written separately as:

$$G_i^{CIF}\left(\underline{q}\right) = \frac{G_i^{BM}\left(\underline{q}\right)\cdot q_i}{Q_{sys}} \tag{3.18}$$

$$G_i^{CIF}\left(\underline{p}\right) = \frac{G_i^{BM}\left(\underline{p}\right)\cdot p_i}{Q_{sys}} \tag{3.19}$$

3.2.3 The Extension of Improvement Potential to Non-coherent Systems

The Improvement Potential (IP) represents how much the system reliability increases if the given basic event is replaced by a component in a working state. Mathematically, it is the product of BM and the given basic event probability, or the product of CIF and the system unavailability. And because the system unavailability remains constant, IP and CIF function identically in ranking for maintenance priority of components. Thus the extension of IP to non-coherent systems is similar to CIF, which consists of failure and repair criticality and they are written separately as:

$$G_i^{IP}\left(\underline{q}\right) = G_i^{BM}\left(\underline{q}\right) \cdot q_i \tag{3.20}$$

$$G_i^{IP}\left(\underline{p}\right) = G_i^{BM}\left(\underline{p}\right) \cdot p_i \tag{3.21}$$

3.2.4 The Extension of Fussell-Vesely Measure to Non-coherent Systems

The Fussell-Vesely measure (FV) of component importance [16] is concerned with component failures contributing to the occurrence of the top event. As introduced before, FV is defined as the probability that a minimal cut set containing the basic event *i* causes the top event. This definition is used in coherent system, or can be used as the FV failure importance:

$$G_i^{FV}\left(\underline{q}\right) = \frac{\Pr\{\bigcup_{k|i\in k} C_k\}}{Q_{sys}} \tag{3.22}$$

And the FV repair importance can be defined as the prime implicant set(s) containing the negation of the basic event *i*, it can be written as:

$$G_i^{FV}\left(\underline{p}\right) = \frac{\Pr\{\bigcup_{k|\bar{i}\in k} C_k\}}{Q_{sys}} \tag{3.23}$$

3.2.5 The Extension of Risk Achievement to Non-coherent Systems

The Risk Achievement (RA) is defined as the increase in risk of system failure if a given component fails. According to the definition, RA is a measure based on the assumption of the given event already occurred. However, when dealing with the non-coherent event, which the event itself is also coherent to the top event, i.e. i and its negation $\bar{i}$ both exist in the function of the top event, the computation of RA is more complicated. Since a given event can exit in only 1 state at any time, when the probability of the event is set to be 1 ($q_i = 1$), the negation is set to be 0 ($p_i = 0$) and vice versa. The RA failure importance is written as:

$$G_i^{RA}\left(\underline{q}\right) = Q_{sys}(q_i=1, p_i=0) - Q_{sys} \tag{3.24}$$

And the RA repair importance can be written as:

$$G_i^{RA}\left(\underline{p}\right) = Q_{sys}(p_i=1, q_i=0) - Q_{sys} \tag{3.25}$$

To check the feasibility of the extension, consider the non-coherent system used in [55] and [20], the Boolean expression for the top event is:

$$T=a\cdot b+a\cdot c+b\cdot \bar{c}$$

The system unavailability is:

$$Q_{sys}=q_a\cdot q_b+q_a\cdot q_c+q_b\cdot p_c-q_a\cdot q_b\cdot q_c-q_a\cdot q_b\cdot p_c$$

The proposed extension can be used to calculate the failure and repair importance of any event. The failure and repair importance of RA for each of the event are calculated from (3.24) and (3.25):

$$G_a^{RA}\left(\underline{q}\right)=q_c+q_b\cdot p_c-Q_{sys}$$

$$G_b^{RA}\left(\underline{q}\right)=p_c+q_a\cdot q_c-Q_{sys}$$

$$G_c^{RA}\left(\underline{q}\right)=q_a-Q_{sys}$$

$$G_c^{RA}\left(\underline{p}\right)=q_b-Q_{sys}$$

The component unavailabilities assigned in [55] are:

$$q_a=9.90099\times10^{-3}$$

$$q_b = 3.84615 \times 10^{-2}$$

$$q_c = 1.52534 \times 10^{-1}$$

$$p_c = 0.847466$$

The system unavailability Q_{sys} remains constant at 0.034105. The results of RA measure for the four events are:

Event	RA	Ranking
a	0.01510238	2
b	0.94687177	1
c	-0.02812487	4
$\bar{c}$	0.00043564	3

Table 3.5: The Result Obtained from the Example

The exhaustive tabular approach [54] can be used to check the feasibility of RA measure:

Consider a system with *n* components; the system state can then be expressed in terms of the component states. It is possible to determine whether a component is critical to system failure, given the states of the remaining *n-1* components. There are 2^{n-1} possible states of the other *n-1* components. By identifying the critical situations for component *i* and summing their probabilities of occurrence, one can calculate the probability that component *i* is critical to system failure. Thus, Table 3.6 identifies the critical states for each of the three components. Table 3.7 records the sum of the critical situations for each event, the

probability that each event is critical to system failure, and the ranking that each component receives.

State of a	State of b	Is c critical?	State of a	State of c	Is b critical?	State of b	State of c	Is a critical?
W	W	No	W	W	Yes (F)	W	W	No
W	F	Yes (R)	W	F	No	W	F	Yes (F)
F	W	Yes (F)	F	W	Yes (F)	F	W	No
F	F	No	F	F	No	F	F	Yes (F)

W = working

F = failed

Table 3.6: Possible and Critical States for the Events

Event	Sum of Critical Situation	Expected Results	Rank
a	$p_b \cdot q_c + q_b \cdot q_c = q_c$	1.52534×10^{-2}	2
b	$p_a \cdot p_c + q_a \cdot p_c = p_c$	0.84747	1
c	$q_a \cdot p_b$	0.00952	4
$\bar{c}$	$p_a \cdot q_b$	0.03808	3

Table 3.7: Expected Results

The ranking result obtained using the tabular approach is the same as the result obtained using the proposed equations.

3.2.6 The Extension of Conditional Probability to Non-coherent Systems

The Conditional Probability (CP) gives the value of the change in system unreliability (or risk) that involves the failure of the given basic event, i.e. the system unavailability with the given event assumed to be occurred.

Mathematically, CP has the same function with RA as the original system unavailability Q_{sys} remains constant. Thus the failure importance and repair importance of CP can be written according to the extension of RA:

$$G_i^{CP}\left(\underline{q}\right) = Q_{sys}(q_i=1, p_i=0) \tag{3.26}$$

$$G_i^{CP}\left(\underline{p}\right) = Q_{sys}(p_i=1, q_i=0) \tag{3.27}$$

The feasibility of this extension can be proved using the method in section 3.2.5.

3.2.7 The Extension of Risk Achievement Worth to Non-coherent Systems

In the mathematical definition of Risk Achievement Worth (RAW), the numerator is identical to CP while the denominator is simply Q_{sys}. As Q_{sys} remains constant, the failure importance and repair importance of RAW can be written according to the extension of CP:

$$G_i^{RAW}\left(\underline{q}\right) = \frac{Q_{sys}(q_i=1,\ p_i=0)}{Q_{sys}} \tag{3.28}$$

$$G_i^{RAW}\left(\underline{p}\right) = \frac{Q_{sys}(p_i=1,\ q_i=0)}{Q_{sys}} \tag{3.29}$$

The feasibility of this extension can be proved using the method in section 3.2.5.

3.2.8 The Extension of Risk Reduction Worth to Non-coherent Systems

The Risk Reduction Worth (RRW) yields the ratio of the system unavailability to the risk with the probability of the basic event set to 0. Based on the mathematical definition of RRW for coherent systems:

$$G_{RRW}=\frac{Q_{sys}}{Q(q_i=0)} \tag{3.30}$$

where $Q(q_i=0)=Q_{sys}\text{-}Pr\{\bigcup_{k\,|\,i\in k} C_k\}$,

Thus RRW can be also defined as:

$$G_{RRW}=\frac{Q_{sys}}{Q_{sys}\text{-}Pr\{\bigcup_{k\,|\,i\in k} C_k\}} \tag{3.31}$$

And since $G_i^{FV}\left(\underline{q}\right)=\frac{\Pr\{U_{k|i\in k}C_k\}}{Q_{sys}}$, $G_{RRW}=\frac{Q_{sys}}{Q_{sys}-\Pr\{U_{k|i\in k}C_k\}}=\frac{Q_{sys}}{Q_{sys}-FV\cdot Q_{sys}}=\frac{1}{1-FV}$, which is why both RRW and FV are referred to as risk reduction indicator. In this case, the failure and repair criticality of RRW can be written respectively as:

$$G_i^{RRW}\left(\underline{q}\right)=\frac{Q_{sys}}{Q_{sys}-\Pr\{U_{k|i\in k}C_k\}} \tag{3.32}$$

$$G_i^{RRW}\left(\underline{p}\right)=\frac{Q_{sys}}{Q_{sys}-\Pr\{U_{k|\bar{i}\in k}C_k\}} \tag{3.33}$$

However, equation (3.32) and (3.33) have avoided the condition that if the probability of the given event is set to be 0, its negation should be set to 1 as one component can exist in only 1 state at any time. According to (3.11), the failure and repair criticality of RRW can be defined as:

$$G_i^{RRW}\left(\underline{q}\right)=\frac{U_{sys}}{Q_{sys}(q_i=0,\,p_i=1)} \tag{3.34}$$

$$G_i^{RRW}\left(\underline{p}\right)=\frac{U_{sys}}{Q_{sys}(p_i=0,\,q_i=1)} \tag{3.35}$$

The definition given in (3.34) and (3.35) obviously distinguishes RRW from FV in the evaluation for non-coherent systems, and also makes the evaluation of RRW more complicated for non-coherent FTA.

Chapter 4

Categorization of Various Risk Importance Measures

4.1 Overview

Risk Importance Measures (RIMs) provide information that can be extracted from PSA. Components within a system can be ranked with respect to each specific criterion defined by each RIM, while rankings given by RIMs can be used to aid decision-making in PSA. The process is called risk-informed maintenance when they are implemented in maintenance activities. Important components that appear on the top of the list generally receive the most attention. This is extremely important in order to achieve the maximum benefit with limited resources.

Maintenance are generally classified into two major categories—corrective maintenance and preventive maintenance [41]. Corrective maintenance is performed when there is a component or system failure. This is not always preferred and more proactive actions are desired. Therefore, time-based periodic preventive maintenance and condition-based predictive maintenance are desired. For both types of maintenance, resources are often limited in real applications due to budget restriction or lead time required for component

enquiry. The objective of risk-informed maintenance is to direct the maintenance effort towards the area that deserves the most attention.

On the other hand, RIMs can be classified into two major categories: risk significant measures and safety significant measures. Among the most popular RIMs introduced/used in numerous literatures, CIF, FV and RRW belong to the risk significant measures, while BM, RA and RAW are used as safety significant measures. This section will use one representative from each category, the CIF for risk significant measures and the RAW for safety significant measures, to investigate their applications in risk-informed maintenance.

Although most engineering systems are coherent, some do present the non-coherent feature. In a non-coherent system, if a component functions, the overall system fails. On the other hand, if the same component fails, the overall system actually resides in a better state. This contradicts common sense. However, it does happen due to various reasons, either poor design or the nature of the system. There have been many examples of non-coherent systems and the most comprehensive list can be found in [56]. Results applicable for coherent systems cannot always be extended to non-coherent systems [57]. This section investigates whether the conclusion regarding risk-informed maintenance for coherent systems are applicable to non-coherent systems [58].

4.2 Risk Significance and Safety Significance

The ranking of structures, systems and components (SSCs) with respect to risk significance (RS) and safety significance (SS) is one of the principal activities in PSA. Risk

significance and safety significance are regarded as complementary ways of identifying the role of SSCs in determining risks.

There are 8 Risk Importance Measures (RIMs) introduced in Chapter 3. In order to apply them correctly, it is important to understand the fundamental meaning and identify the applicable area(s) for them. In the area of risk-informed maintenance, if one importance measure that provides insights for corrective maintenance is used for preventive maintenance, resources may be misplaced. This section investigates this issue by classifying the risk importance measures into two major categories—risk significant measures and safety significant measures. Two representatives from each category, CIF as a representative for risk significant measures and RAW as a representative for safety significant measures, are discussed in detail below. Simple series systems and parallel systems are used to demonstrate the basic ideas first. A more complicated system with a repeated basic event(s) in the minimal cut sets or prime implicant sets follows. If all of them occur, the top event occurs.

4.2.1 Risk Significance

Risk significance is easier to define and understand in an operational sense. An individual SSC can be identified as being risk-significant if it were demonstrated that its failure or unavailability contributes significantly to measures of risk [59].

Risk significant measures represent which component most likely caused a system failure. This section uses a simple series system to clarify this idea, while CIF is used as a

representative of risk significant measures since it is one of the most widely used RIMs. The definition of CIF was presented in Section 3.1.2.

The CIF of component *i* in a system is defined as

$$G_{CIF}(i)=\frac{Q(q_i=1)-Q(q_i=0)}{Q_{sys}}\cdot q_i \tag{4.1}$$

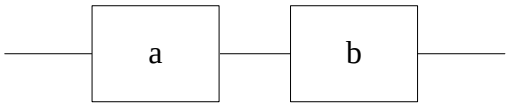


Figure 4.1: A Simple Series System

Figure 4.1 shows two components, *a* and *b*, connected in series. If any one of the components fails, the system will fail. The question is which component is most likely to fail first so as to result in a system failure. The answer can be obtained through the CIF of these two components. The component that has a higher CIF should be the one that needs to be checked first. This is proved as follows.

$$Q_{sys}=q_a+q_b-q_a\cdot q_b \tag{4.2}$$

Based on (4.1),

$$G_{CIF}(a)=\frac{q_a-q_a\cdot q_b}{q_a+q_b-q_a\cdot q_b} \tag{4.3}$$

$$G_{CIF}(b)=\frac{q_b-q_a\cdot q_b}{q_a+q_b-q_a\cdot q_b} \tag{4.4}$$

From (4.3) and (4.4), it can be obtained that if $q_a<q_b$, then $G_{CIF}(a)<G_{CIF}(b)$, and vice versa. This implies that if the CIF of component *a* is smaller than that of component *b*, the latter is most likely to fail first so as to result in a system failure.

To demonstrate the use of risk significant measure in a complex system, suppose a system has two cut sets, {*a, b*} and {*a, c*}. Figure 4.2 shows the corresponding fault tree of this system. The CIFs of the three components are calculated as follows, by assuming $q_a<q_b<q_c$.

$$G_{CIF}(a)=1 \tag{4.6}$$

$$G_{CIF}(b)=\frac{q_a\cdot q_b-q_a\cdot q_b\cdot q_c}{q_a\cdot q_b+q_a\cdot q_c-q_a\cdot q_b\cdot q_c} \tag{4.7}$$

$$G_{CIF}(c)=\frac{q_a\cdot q_c-q_a\cdot q_b\cdot q_c}{q_a\cdot q_b+q_a\cdot q_c-q_a\cdot q_b\cdot q_c} \tag{4.8}$$

It can be shown from (4.6)-(4.8) that

$$G_{CIF}(a)>G_{CIF}(c)>G_{CIF}(b)$$

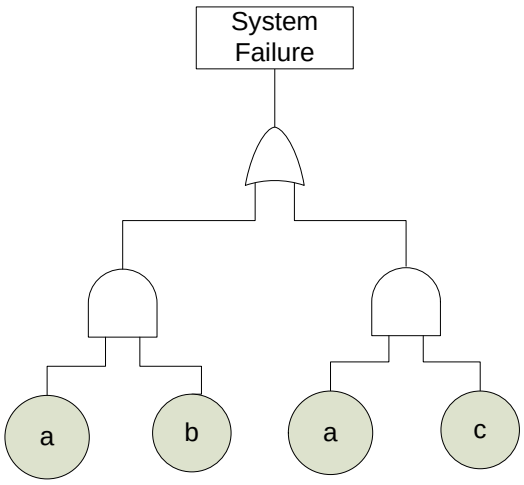


Figure 4.2: A Complex System

The result implies that when the system fail, the first component that needs to be checked is component *a*, followed by component *c* and *b*. This makes common sense because component *a* appears in both of the cut sets. Since component *c* has a higher unavailability than component *b*, it is more likely to also have failed and needs to be checked next. It should be noted that the ranking of criticality importance factor is not always compliant with component unavailability, as opposed to the statements in [18]. In this case, although component *a* has the lowest unavailability, it ranks high in terms of its CIF. This is due to the configuration of the system and the position that component *a* takes in the system.

4.2.2 Safety Significance

Safety significance is conceptually considered as being related to the level of prevention required for the SSCs in the system. The safety significant SSCs are captured by identifying the levels of "defence-in-depth" of the SSCs. The term "defence-in-depth", which is widely used in the nuclear industry, is used here to represent how well the overall

system is protected against the failure of a single component. The lower is the "defence-in-depth" for a component; the higher is the effect of the component failure on the overall system availability.

Safety significant measures represent the level of "defence-in-depth" of a system with respect to the failure of a component in the system. Thus the information provided by safety significant measures can be used to guide preventive maintenance, which is performed before the system has failed. The goal is to increase the level of defence-in-depth against the failure of a component, either by shortening the inspection interval, or adding another layer of redundancy, etc. This section uses a simple parallel system to clarify this idea. Series systems are not considered since there is no defence-in-depth in a series system because any component failure will result in a system failure in a series system. RAW is used as a representative of safety significant measures. The definition of RAW was presented in Chapter 3. The RAW for component *i* in a system is defined as

$$G_{RAW}(i) = \frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{Q_{sys} \cdot q_i} = \frac{Q(q_i=1)}{Q_{sys}} \tag{4.9}$$

Figure 4.3 shows two components, *a* and *b*, connected in parallel.

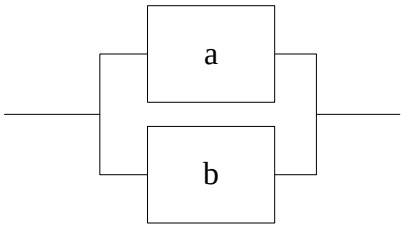


Figure 4.3: A Simple Parallel System

The system will not fail when only one component fails. The question is which component failure will put the system in a more dangerous position. The answer can be obtained through the RAW. The component with the higher RAW has a lower level of defense-in-depth and its failure affects the system unavailability more severely. When performing preventive maintenance, more resources should be allocated to improve the level of defence-in-depth of that component. This is proved as follows.

$$G_{RAW}(a)=\frac{1}{q_a} \tag{4.10}$$

$$G_{RAW}(b)=\frac{1}{q_b} \tag{4.11}$$

where q_a is the unavailability of component *a*, and q_b is the unavailability of component *b*. Based on Equation (4.8) and (4.9), it can be obtained that if $q_a<q_b$, then, *RAW(a) > RAW(b)* and vice versa. This implies that if the RAW of component *a* is higher, it has a lower level of defence-in-depth, which means more resources should be allocated to it during the preventive maintenance activities.

To demonstrate the use of safety significant measures in a complex system, consider the complex system introduced in Section 4.2.1. The fault tree diagram is shown in Figure 4.2. The RAWs of all components in the system are calculated as follows:

$$G_{RAW}(a)=\frac{q_b+q_c-q_b\cdot q_c}{q_a\cdot q_b+q_a\cdot q_c-q_a\cdot q_b\cdot q_c} \tag{12}$$

$$G_{RAW}(b)=\frac{q_a}{q_a\cdot q_b+q_a\cdot q_c-q_a\cdot q_b\cdot q_c} \tag{13}$$

$$G_{RAW}(c) = \frac{q_a}{q_a \cdot q_b + q_a \cdot q_c - q_a \cdot q_b \cdot q_c} \quad (14)$$

The results can be interpreted as follows: suppose component *a* fails, the fault tree of the system shown in Figure 4.2 is simplified (Figure 4.4). The unavailability of the system in Figure 4.4 is exactly the numerator of $G_{RAW}(a)$.

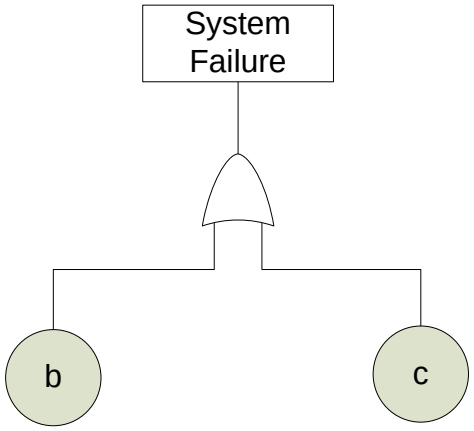


Figure 4.4: System Fault Tree with Component *a* Assumed Failed

Similarly, suppose component *b* fails, the fault tree of the system in Figure 4.2 becomes Figure 4.5.

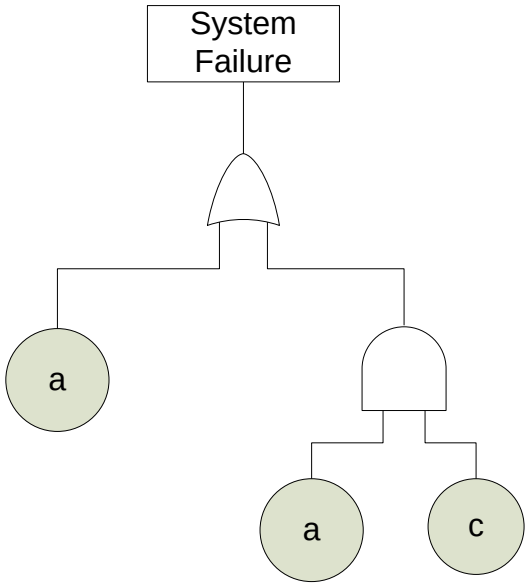


Figure 4.5: System Fault Tree with Component *b* Assumed Failed

The fault tree in Figure 4.5 is not minimized. Therefore, it is further reduced to Figure 4.6 to obtain the minimal cut set(s). In this case, the result is very simple as the simplified figure only contains component *a*.

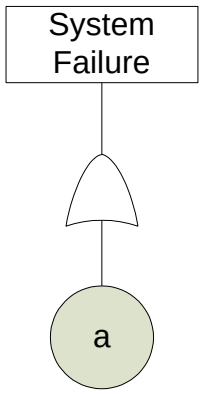


Figure 4.6: Final System Fault Tree with component *b* assumed failed

The unavailability of the system in Figure 4.6 is exactly the numerator of *RAW(b),* Similar results can be obtained for component *c*. If the unavailability of the system in Figure

4.4 is higher than that of the system shown in Figure 4.6, which is most probably the case, component *a* has the worst defence-in-depth and *RAW(a)* ranks the highest. Component *b* and *c* have the same level of defence-in-depth. Thus they have the same RAW, i.e. *RAW(b)* = *RAW(c)*. When performing preventive maintenance before the system fails, these results should be taken into consideration. Resources should first be allocated to increase the level of defence against the failure of component *a*.

4.3 Classification of Risk Importance Measures for Risk-informed Maintenance

Besides CIF and RAW, there were six important risk importance measures (RIMs) presented in Chapter 3. The purpose of this section is to classify them into different categories. The definition of various RIMs was presented in section 3 and the mathematical expressions are shown in Table 4.1.

RIM	**Definition**
Birnbaum's Measure (BM)	$G_{BM}=\frac{\partial Q_{sys}}{\partial q_i}=Q(q_i=1)-Q(q_i=0)$
Criticality Importance Factor (CIF)	$G_{CIF}=\frac{G_{BM}\cdot q_i}{Q_{sys}}=\frac{Q(q_i=1)-Q(q_i=0)}{Q_{sys}}\cdot q_i=\frac{\partial Q_{sys}}{\partial q_i}\cdot\frac{q_i}{Q_{sys}}$
Improvement Potential (IP)	$G_{IP}=G_{BM}\cdot q_i=G_{CIF}\cdot Q_{sys}$
Fussell-Vesely Measure (FV)	$G_{FV}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{Q_{sys}}$
Risk Achievement (RA)	$G_{RA}=Q(q_i=1)-Q_{sys}$
Conditional Probability (CP)	$G_{CP}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{q_i}=Q(q_i=1)$
Risk Achievement Worth (RAW)	$G_{RAW}=\frac{\Pr\{\bigcup_{k\mid i\in k} C_k\}}{Q_{sys}\cdot q_i}=\frac{Q(q_i=1)}{Q_{sys}}$
Risk Reduction Worth (RRW)	$G_{RRW}=\frac{Q_{sys}}{Q(q_i=0)}$

Table 4.1: The Definition of Various RIMs

Following the analysis described in Section 4.2, the eight RIMs are used in both parallel systems; the results are shown in Table 4.2 and Table 4.3. The analysis on a complex system is shown in Table 4.4.

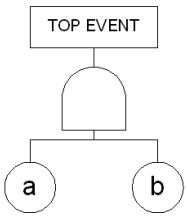
Fault Tree	RIM	Results	Ranking
Assumption: $q_a < q_b$ 	BM	$G_{BM}(a)=q_b$ $G_{BM}(b)=q_a$	$G_{BM}(a)>G_{BM}(b)$
	CIF	$G_{CIF}(a)=\frac{q_a \cdot q_b}{Q}$ $G_{CIF}(b)=\frac{q_a \cdot q_b}{Q}$	$G_{CIF}(a)=G_{CIF}(b)$
	IP	$G_{IP}(a)=q_a \cdot q_b$ $G_{IP}(b)=q_a \cdot q_b$	$G_{IP}(a)=G_{IP}(b)$
	FV	$G_{FV}(a)=\frac{q_a \cdot q_b}{Q}$ $G_{FV}(b)=\frac{q_a \cdot q_b}{Q}$	$G_{FV}(a)=G_{FV}(b)$
	RRW	N/A	N/A
	RA	$G_{RA}(a)=q_b-Q$ $G_{RA}(b)=q_a-Q$	$G_{RA}(a)>G_{RA}(b)$
	RAW	$G_{RAW}(a)=\frac{q_b}{Q}$ $G_{RAW}(b)=\frac{q_a}{Q}$	$G_{RAW}(a)>G_{RAW}(b)$
	CP	$G_{CP}(a)=q_b$ $G_{CP}(b)=q_a$	$G_{CP}(a)>G_{CP}(b)$

Table 4.2: Various RIMs on a Parallel System

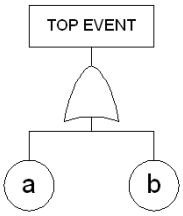
Fault Tree	RIMs	Results	Ranking
Assumption: $q_a < q_b$ 	BM	$G_{BM}(a)=1-q_b$ $G_{BM}(b)=1-q_a$	$G_{BM}(b)>G_{BM}(a)$
	CIF	$G_{CIF}(a)=\frac{q_a\cdot(1-q_b)}{Q}$ $G_{CIF}(b)=\frac{q_b\cdot(1-q_a)}{Q}$	$G_{CIF}(b)>G_{CIF}(a)$
	IP	$G_{IP}(a)=q_a\cdot(1-q_b)$ $G_{IP}(b)=q_b\cdot(1-q_a)$	$G_{IP}(b)>G_{IP}(a)$
	FV	$G_{FV}(a)=\frac{q_a}{Q}$ $G_{FV}(b)=\frac{q_b}{Q}$	$G_{FV}(b)>G_{FV}(a)$
	RRW	$G_{RRW}(a)=\frac{Q}{q_b}$ $G_{RRW}(b)=\frac{Q}{q_a}$	$G_{RRW}(b)>G_{RRW}(a)$
	RA	$G_{RA}(a)=0-Q$ $G_{RA}(b)=0-Q$	$G_{RA}(a)=G_{RA}(b)$
	RAW	$G_{RAW}(a)=\frac{1}{Q}$ $G_{RAW}(b)=\frac{1}{Q}$	$G_{RAW}(a)=G_{RAW}(b)$
	CP	$G_{CP}(a)=1$ $G_{CP}(b)=1$	$G_{CP}(a)=G_{CP}(b)$

Table 4.3: Various RIMs on a Series System

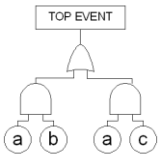
Fault Tree	RIMs	Results	Ranking
Assumption: $q_a<q_b<q_c$ 	BM	$G_{BM}(a)=q_b+q_c-q_b\cdot q_c$ $G_{BM}(b)=q_a-q_a q_c=q_a(1-q_c)$ $G_{BM}(c)=q_a-q_a q_b=q_a(1-q_b)$	$G_{BM}(a)>G_{BM}(c)>G_{BM}(b)$
	CIF	$G_{CIF}(a)=\frac{q_a\cdot(q_b+q_c-q_b\cdot q_c)}{Q}=1$ $G_{CIF}(b)=\frac{q_a\cdot q_b-q_a\cdot q_b\cdot q_c}{Q}$ $G_{CIF}(c)=\frac{q_a\cdot q_c-q_a\cdot q_b\cdot q_c}{Q}$	$G_{CIF}(a)>G_{CIF}(c)>G_{CIF}(b)$
	IP	$G_{IP}(a)=q_a\cdot q_b+q_a\cdot q_c-q_a\cdot q_b\cdot q_c$ $G_{IP}(b)=q_a\cdot q_b-q_a\cdot q_b\cdot q_c$ $G_{IP}(c)=q_a\cdot q_c-q_a\cdot q_b\cdot q_c$	$G_{IP}(a)>G_{IP}(c)>G_{IP}(b)$
	FV	$G_{FV}(a)=\frac{q_a(q_b+q_c)}{Q}$ $G_{FV}(b)=\frac{q_a\cdot q_b}{Q}$ $G_{FV}(c)=\frac{q_a\cdot q_c}{Q}$	$G_{FV}(a)>G_{FV}(c)>G_{FV}(b)$
	RRW	$G_{RRW}(a)=\infty$ $G_{RRW}(b)=\frac{Q}{q_a\cdot q_c}$ $G_{RRW}(c)=\frac{Q}{q_a\cdot q_b}$	$G_{RRW}(a)>G_{RRW}(c)>G_{RRW}(b)$
	RA	$G_{RA}(a)=q_b+q_c-q_b\cdot q_c-Q$ $G_{RA}(b)=q_a-Q$ $G_{RA}(c)=q_a-Q$	$G_{RA}(c)=G_{RA}(b)>G_{RA}(a)$ *if* $q_a>q_b+q_c$ $G_{RA}(a)>G_{RA}(c)=G_{RA}(b)$ *if* $q_a<q_b+q_c$
	RAW	$G_{RAW}(a)=\frac{q_b+q_c}{Q}$ $G_{RAW}(b)=\frac{q_a}{Q}$ $G_{RAW}(c)=\frac{q_a}{Q}$	$G_{RAW}(c)=G_{RAW}(b)>G_{RAW}(a)$ *if* $q_a>q_b+q_c$ $G_{RAW}(a)>G_{RAW}(c)=G_{RAW}(b)$ *if* $q_a<q_b+q_c$
	CP	$G_{CP}(a)=q_b+q_c$ $G_{CP}(b)=q_a$ $G_{CP}(c)=q_a$	$G_{CP}(c)=G_{CP}(b)>G_{CP}(a)$ *if* $q_a>q_b+q_c$ $G_{CP}(a)>G_{CP}(c)=G_{CP}(b)$ *if* $q_a<q_b+q_c$

Table 4.4: Comparison of Different RIMs on a Complex System

The ranking results for CIF, IP, FV and RRW are identical. It can be seen that these measures are not very applicable in parallel systems. All four RIMs have common ground in a series system in that the component which has higher unavailability ranks higher than those with lower unavailability. This has categorized them as risk significant measures as they represent which component most likely caused a system failure. They also provide information to guide corrective maintenance. This also explains why they cannot be used in a parallel system, because all the components are failed if the system was assumed to be failed.

The result of CIF shows that the ranking of risk significance is not always compliant with component unavailability, but also depends on the configuration of the system fault tree and the position that the component takes in the system. The result of IP is always the same as CIF because the unavailability of the system Q is constant. As of FV, the ranking result is identical to those of CIF and IP as well. However, since FV only compares the importance between different minimal cut sets, the data results are slightly different as FV does not subtract the redundancy in the numerator. The RRW also gives same ranking results as the other three. However, if one basic event /component existed in every minimal cut set, its RRW tends to be positively infinitive, i.e. the more cut sets it appears to belong to, the smaller the denominator of the RRW, and the greater the RRW value.

As RA includes the assumption of the failure of the give component ($q_i=1$), it can be a reference of the measure of defence-in-depth. The RAW, CP shows identical results as RA, which means they all represent the level of defence-in-depth of a system with respect to the unavailability of a component in the system. This has concluded that all three (RA, RAW, CP) can be considered safety significant measures which are applicable for preventive

maintenance. On the other hand, BM is also considered a safety significant measure because mathematically, it is independent of the unavailability of the given component. Unlike the other safety significant measures, BM gives different values for components with same situations in series.

The eight importance measures can be categorized with respect to risk significance and safety significance and they are shown in the table below.

RIM	Risk Significance	Safety Significance
BM	○	●
CIF	●	○
IP	●	○
FV	●	○
CP	○	●
RAW	○	●
RRW	●	○
RA	○	●

Table 4.5: The Categorization of Various RIMs with respect to Risk and Safety Significance

4.4 The Application of RIMs in Non-coherent Systems

Extra attention should be brought to the use of extended RIMs on non-coherent systems. The extensions are presented in Section 3.2 and they are listed in Table 4.6.

RIM	**Extension to Non-coherent Systems**
Birnbaum's Measure (BM)	$G_i^{BM}(\underline{q}) = \frac{\partial Q_{sys}}{\partial q_i}$ $G_i^{BM}(\underline{p}) = \frac{\partial Q_{sys}}{\partial p_i}$
Criticality Importance Factor (CIF)	$G_i^{CIF}(\underline{q}) = \frac{G_i^{BM}(\underline{q}) \cdot q_i}{Q_{sys}}$ $G_i^{CIF}(\underline{p}) = \frac{G_i^{BM}(\underline{p}) \cdot p_i}{Q_{sys}}$
Improvement Potential (IP)	$G_i^{IP}(\underline{q}) = G_i^{BM}(\underline{q}) \cdot q_i$ $G_i^{IP}(\underline{p}) = G_i^{BM}(\underline{p}) \cdot p_i$
Fussell-Vesely Measure (FV)	$G_i^{FV}(\underline{q}) = \frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{Q_{sys}}$ $G_i^{FV}(\underline{p}) = \frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{Q_{sys}}$
Risk Achievement (RA)	$G_i^{RA}(\underline{q}) = Q_{sys}(q_i=1, p_i=0) - Q_{sys}$ $G_i^{RA}(\underline{p}) = Q_{sys}(p_i=1, q_i=0) - Q_{sys}$
Conditional Probability (CP)	$G_i^{CP}(\underline{q}) = Q_{sys}(q_i=1, p_i=0)$ $G_i^{CP}(\underline{p}) = Q_{sys}(p_i=1, q_i=0)$
Risk Achievement Worth (RAW)	$G_i^{RAW}(\underline{q}) = \frac{Q_{sys}(q_i=1,\ p_i=0)}{Q_{sys}}$ $G_i^{RAW}(\underline{p}) = \frac{Q_{sys}(p_i=1, q_i=0)}{Q_{sys}}$
Risk Reduction Worth (RRW)	$G_i^{RRW}(\underline{q}) = \frac{Q_{sys}}{Q_{sys}(q_i=0,\ p_i=1)}$ $G_i^{RRW}(\underline{p}) = \frac{Q_{sys}}{Q_{sys}(p_i=0, q_i=1)}$

Table 4.6: The Extended RIMs to Non-coherent Systems

Consider a non-coherent system with two prime implicant sets: {a, c} and {b, $\bar{c}$}. The fault tree of this system is show in Figure 4.7. The system unavailability

$Q_{sys}=q_a \cdot q_c+q_b \cdot p_c$

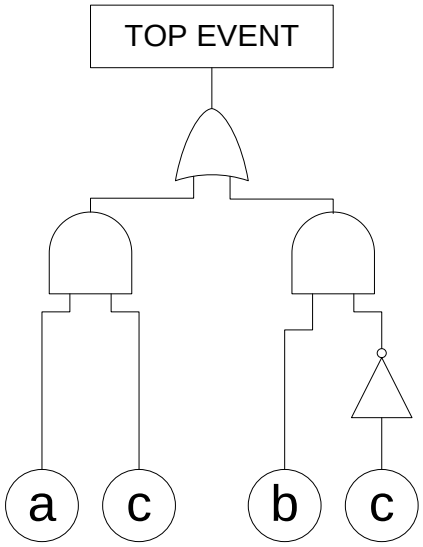


Figure 4.7: Non-coherent Fault Tree 1

To demonstrate the use of risk significant RIMs in a non-coherent system, assume $q_a=0.1$, $q_b=0.2$, and $q_c=0.3$. It should be noted these numbers are not realistic and they are used for demonstration purposes only. Based on the mathematical definition of CIF,

$$G_a^{CIF}\left(\underline{q}\right) = \frac{G_i^{BM}\left(\underline{q}\right)\cdot q_a}{Q_{sys}} \tag{4.15}$$

$$G_b^{CIF}\left(\underline{q}\right) = \frac{G_i^{BM}\left(\underline{q}\right)\cdot q_b}{Q_{sys}} \tag{4.16}$$

$$G_c^{CIF}\left(\underline{q}\right) = \frac{G_i^{BM}\left(\underline{q}\right)\cdot q_c}{Q_{sys}} \tag{4.17}$$

$$G_c^{CIF}\left(\underline{p}\right) = \frac{G_i^{BM}\left(\underline{p}\right)\cdot p_c}{Q_{sys}} \tag{4.18}$$

Since

$$G_a^{BM}\left(\underline{q}\right)=\frac{\partial Q_{sys}}{\partial q_i}=q_c$$

$$G_b^{BM}\left(\underline{q}\right)=\frac{\partial Q_{sys}}{\partial q_i}=p_c$$

$$G_c^{BM}\left(\underline{q}\right)=\frac{\partial Q_{sys}}{\partial q_i}=q_a$$

$$G_c^{BM}\left(\underline{p}\right)=\frac{\partial Q_{sys}}{\partial p_i}=q_b$$

Then

$$G_a^{CIF}\left(\underline{q}\right)=0.176$$

$$G_b^{CIF}\left(\underline{q}\right)=0.824$$

$$G_c^{CIF}\left(\underline{q}\right)=0.176$$

$$G_c^{CIF}\left(\underline{p}\right)=0.824$$

It can be seen that the CIF for component *b* and the repair importance of CIF for component *c* are equivalent and rank the highest. This is expected because when the system fails, it is more likely that the prime implicant $\{b, \bar{c}\}$ has occurred. Thus, when system failure occurs, the first step should be checking whether component *c* is functioning and component *b* has failed. If this is the case, component *b* should be repaired. This should restore the system to a working state.

Using RAW as the safety significant RIM on the same non-coherent system example,

$$G_a^{RAW}\left(\underline{q}\right)=\frac{Q_{sys}(q_a=1)}{Q_{sys}}=1.765 \qquad (4.19)$$

$$G_b^{RAW}\left(\underline{q}\right) = \frac{Q_{sys}(q_b=1)}{Q_{sys}} = 4.118 \tag{4.20}$$

$$G_c^{RAW}\left(\underline{q}\right) = \frac{Q_{sys}(q_c=1,\ p_c=0)}{Q_{sys}} = 0.588 \tag{4.21}$$

$$G_c^{RAW}\left(\underline{p}\right) = \frac{Q_{sys}(p_c=1,q_c=0)}{U_{sys}} = 1.176 \tag{4.22}$$

Therefore,

$$G_b^{RAW}\left(\underline{q}\right) > G_a^{RAW}\left(\underline{q}\right) > G_c^{RAW}\left(\underline{p}\right) > G_c^{RAW}\left(\underline{q}\right)$$

This result shows that the system has the lowest defence-in-depth against failure of component *b*, then *a*, then the repair of component *c*, then the failure of component *c*. To visualize this, assume component *b* fails, the system fault tree becomes as shown in Figure 4.8.

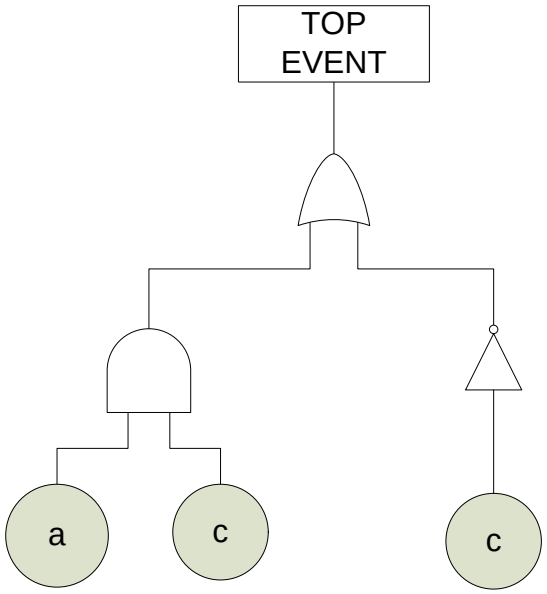


Figure 4.8: System Fault Tree when component *b* fails

For this fault tree, when component *a* fails, the system fails regardless whether component *c* is failed or working. Therefore, the fault tree can be further simplified to Figure 4.9.

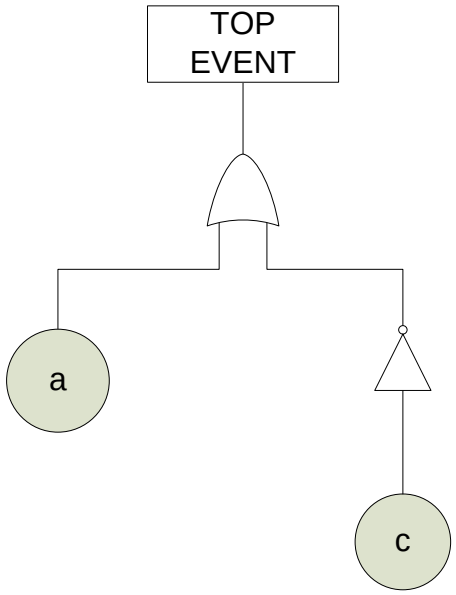


Figure 4.9: Simplified Fault Tree for Figure 4.8

The unavailability of this system is

$$Q(q_b=1)=q_a+p_c-q_a \cdot p_c=0.73$$

Similarly, when component *a* fails, the system fault tree becomes as shown in Figure 4.10.

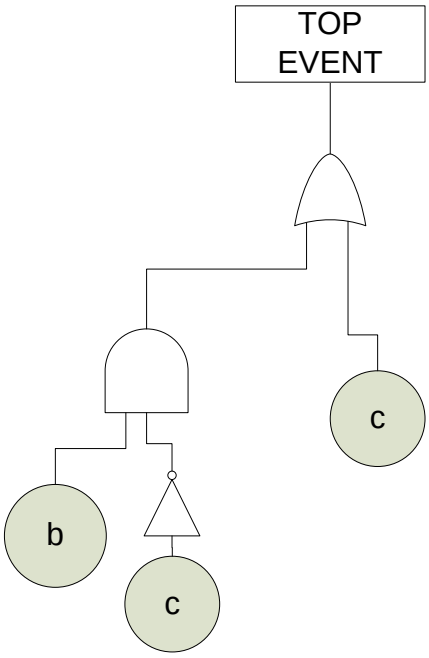


Figure 4.10: System Fault Tree Assuming Component *a* Fails

This fault tree can be further simplified to Figure 4.11.

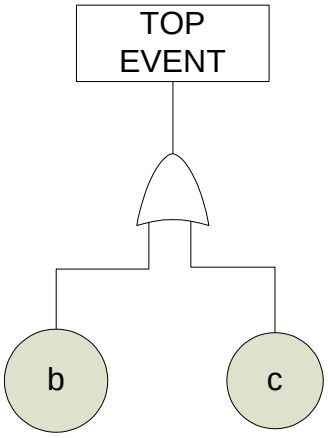


Figure 4.11: Simplified Fault Tree for Figure 4.10

The unavailability of this system is

$$Q(q_a=1)=q_b+q_c-q_b \cdot q_c=0.44$$

When component *c* works, the system fault tree is shown in Figure 4.12. This fault tree can be further simplified to Figure 4.13.

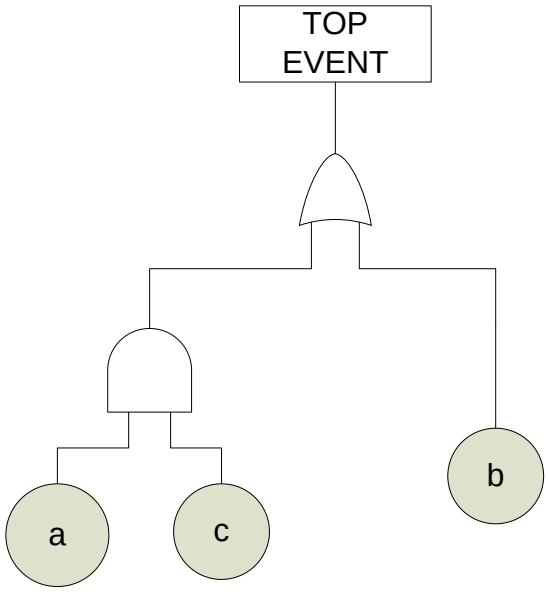


Figure 4.12: System Fault Tree Assuming Component *c* Works

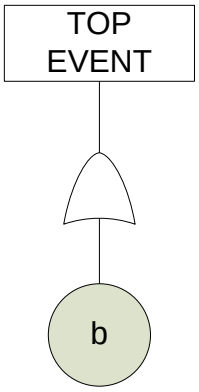


Figure 4.13: Simplified Fault Tree for Figure 4.12

When component *c* works, the prime implicant set {*a,c*} will not occur. The unavailability of this system is

$$Q(p_c=1)=q_b=0.2$$

When component *c* fails, the system fault tree is shown in Figure 4.14. This fault tree can be further simplified to Figure 4.15.

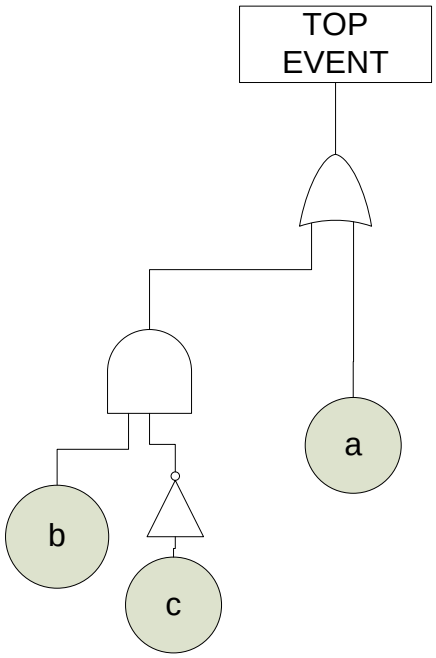


Figure 4.14: System Fault Tree Assuming Component *c* Fails

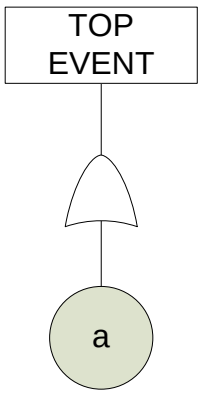


Figure 4.15: Simplified Fault Tree for Figure 4.14

The unavailability of this system is

$$Q(q_c=1)=q_a=0.1$$

As can be seen, As can be seen, $Q(q_c=1)>Q(q_a=1)>Q(p_c=1)>Q(q_c=1)$, This means the system has higher to lower defence-in-depth in the order of assuming $q_c=1$, $p_c=1$, $q_a=1$, $q_b=1$. Using the same method to demonstrate the use of other RIMs on the same system, the results are shown in Table 4.7. To generalize the results, the probability of $\bar{c}$ (p_c) are assumed to be much greater than the probability of event a, b and c.

Prime implicant sets: {a, c} {b, $\bar{c}$ }

RIM	**Results**	**Notes**
BM	$G_{BM}(a)=q_c$ $G_{BM}(b)=p_c$ $G_{BM}(c)=q_a$ $G_{BM}(\bar{c})=q_b$	
CIF	$G_{CIF}(a)=\frac{q_a \cdot q_c}{Q}$ $G_{CIF}(b)=\frac{q_b \cdot p_c}{Q}$ $G_{CIF}(c)=\frac{q_a \cdot q_c}{Q}$ $G_{CIF}(\bar{c})=\frac{q_b \cdot p_c}{Q}$	$G_{CIF}(a)=G_{CIF}(c)$, $G_{CIF}(b)=G_{CIF}(\bar{c})$
IP	$G_{IP}(a)=q_a \cdot q_c$ $G_{IP}(b)=q_b \cdot p_c$ $G_{IP}(c)=q_a \cdot q_c$ $G_{CIP}(\bar{c})=q_b \cdot p_c$	The ranking results should be identical to CIF since Q_{sys} is constant.

FV	$G_{FV}(a)=\frac{q_a \cdot q_c}{Q}$ $G_{FV}(b)=\frac{q_b \cdot p_c}{Q}$ $G_{FV}(c)=\frac{q_a \cdot q_c}{Q}$ $G_{FV}(\bar{c})=\frac{q_b \cdot p_c}{Q}$	The data calculated should be identical to CIF, so is the ranking results.
RA	$G_{RA}(a)=q_c+q_b \cdot p_c-Q$ $G_{RA}(b)=q_a \cdot q_c+p_c-Q$ $G_{RA}(c)=q_a-Q$ as when $q_c=0,\ p_c=0$ $G_{RA}(\bar{c})=q_b-Q$ as when $p_c=0,\ q_c=0$	It can only be concluded that c and $\bar{c}$ depend on the unavailability of a and b, the ranking of a and b according to RA cannot be generalized through the equations.
CP	$G_{CP}=\frac{\Pr\{\bigcup_{k \mid i \in k} C_k\}}{q_i}=Q(q_i=1)$	
RAW	$G_{RAW}(a)=\frac{q_c+q_b \cdot p_c}{Q}$ $G_{RAW}(b)=\frac{q_a \cdot q_c+p_c}{Q}$ $G_{RAW}(c)=\frac{q_a}{Q}$ $G_{RAW}(\bar{c})=\frac{q_b}{Q}$	
RRW	$G_{RRW}(a)=\frac{Q}{q_b \cdot p_c}$ $G_{RRW}(b)=\frac{Q}{q_a \cdot q_c}$ $G_{RRW}(c)=\frac{Q}{q_b}$ as when $q_c=0,\ p_c=1$ $G_{RRW}(\bar{c})=\frac{Q}{q_a}$ as when $p_c=0,\ q_c=1$	$G_{RRW}(b)>G_{RRW}(\bar{c})$, $G_{RRW}(a)>G_{RRW}(c)$

Table 4.7: Demonstration of various RIMs on the Non-coherent System

The demonstrated results have shown that CIF, IP and FV, which are categorized as risk significant measures, have identical results in a non-coherent system. CIF and IP have somewhat the same meaning as Q_{sys} is constant. Unlike FV, CIF and IP are not solely comparing the importance between different minimal cut sets or prime implicant sets. This may result in some slight differences in more complicated systems. However, due to the result, we can say all of the three have

ranked components with respect to risk significance in non-coherent systems because $\{b, \bar{c}\}$ is usually more likely to occur than $\{a, c\}$ in a failed system.

The ranking results for RRW are different from CIF, IP and FV in a non-coherent system. The result shows that the RRW in a given component depends on those events exist in the prime implicant set(s) which include the negation of the given component, but not the negation of the given component itself. For example, in a non-coherent system in Figure 4.16:

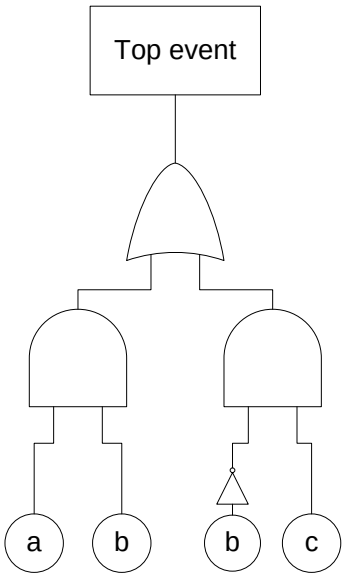


Figure 4.16: Non-coherent Fault Tree 2

The RRW of component b is $\frac{Q_{sys}}{q_c}$, which depend on the component c as c belongs to prime implicant set $\{\bar{b}, c\}$ which consists of c and the negation of b; the RRW of $\bar{b}$ is $\frac{Q_{sys}}{q_a}$, which is dependent of component a as a belongs to $\{a, b\}$ which includes the inverse of $\bar{b}$. This means unlike the other risk significant measures, RRW

is not relevant to the unavailability of the given component itself. Thus in the real non-coherent systems, FV, CIF and IP are more applicable.

The non-coherency of components makes the system more complicated. For example, when a measure includes an assumption of component failure, its negation should be assumed working (when $q_c=1$, $p_c=0$). It is still possible to use RA to measure safety significance in non-coherent system as it always includes the assumption of component failure ($q_c=1$. However, the expression of RAW, $\frac{Pr\{\bigcup_{k|i\in k} C_k\}}{Q_{sys}\cdot q_i}$, is not applicable for non-coherent systems due to the uncertainty of non-coherent components. The other expression of RAW, $\frac{Q(q_i=1)}{Q_{sys}}$, should be applied when dealing with the non-coherent components; while CP goes with $Q(q_i=1)$ as well due to the same reason. This makes RA, RAW and CP provide same ranking results in non-coherent systems.

The results of BM and RA for the non-coherent system are compared in Table 4.8:

BM	RA
$G_{BM}(a)=q_c$ $G_{BM}(b)=p_c$ $G_{BM}(c)=q_a$ $G_{BM}(\bar{c})=q_b$	$G_{RA}(a)=q_c+q_b\cdot p_c-Q$ $G_{RA}(b)=q_a\cdot q_c+p_c-Q$ $G_{RA}(c)=q_a-Q$ $G_{RA}(\bar{c})=q_b-Q$

Table 4.8: The Comparison of Results of BM and RA for the Non-coherent System

BM can still be considered a safety significant measure as it is totally independent of the unavailability of the given component. However, because BM is the partial derivative of the given component, it considers the negation of a

component (the non-coherent component) as an independent component. If BM of component i was written as $Q(q_i=1)-Q(q_i=0)$, BM of its negation is $Q(q_i=0)-Q(q_i=1)$ - which is meaningless in ranking. As a result, RA, RAW and CP are more applicable and provide useful information with respect to safety significance in non-coherent systems.

Chapter 5

Case Studies

5.1 The Application of Non-coherent Fault Tree Analysis on a Steam Generator Level Control System

5.1.1 Steam Generator Level Control System

In a typical CANDU Nuclear Power Plant (NPP), the Steam Generator Level Control System (SGLCS) adjusts the feedwater flow in response to changes of inventory of light water in the steam generators. The diagram in Figure 5.1 [60] shows the main pieces of equipment typical for a CANDU High Pressure Feedwater system, which also shows a typical set of steam generator level control valves along with steam generator feed pumps. The level in each steam generator is controlled individually. Because of safety, range of control and maintenance considerations, each steam generator has a set of several control valves for feedwater connected in parallel.

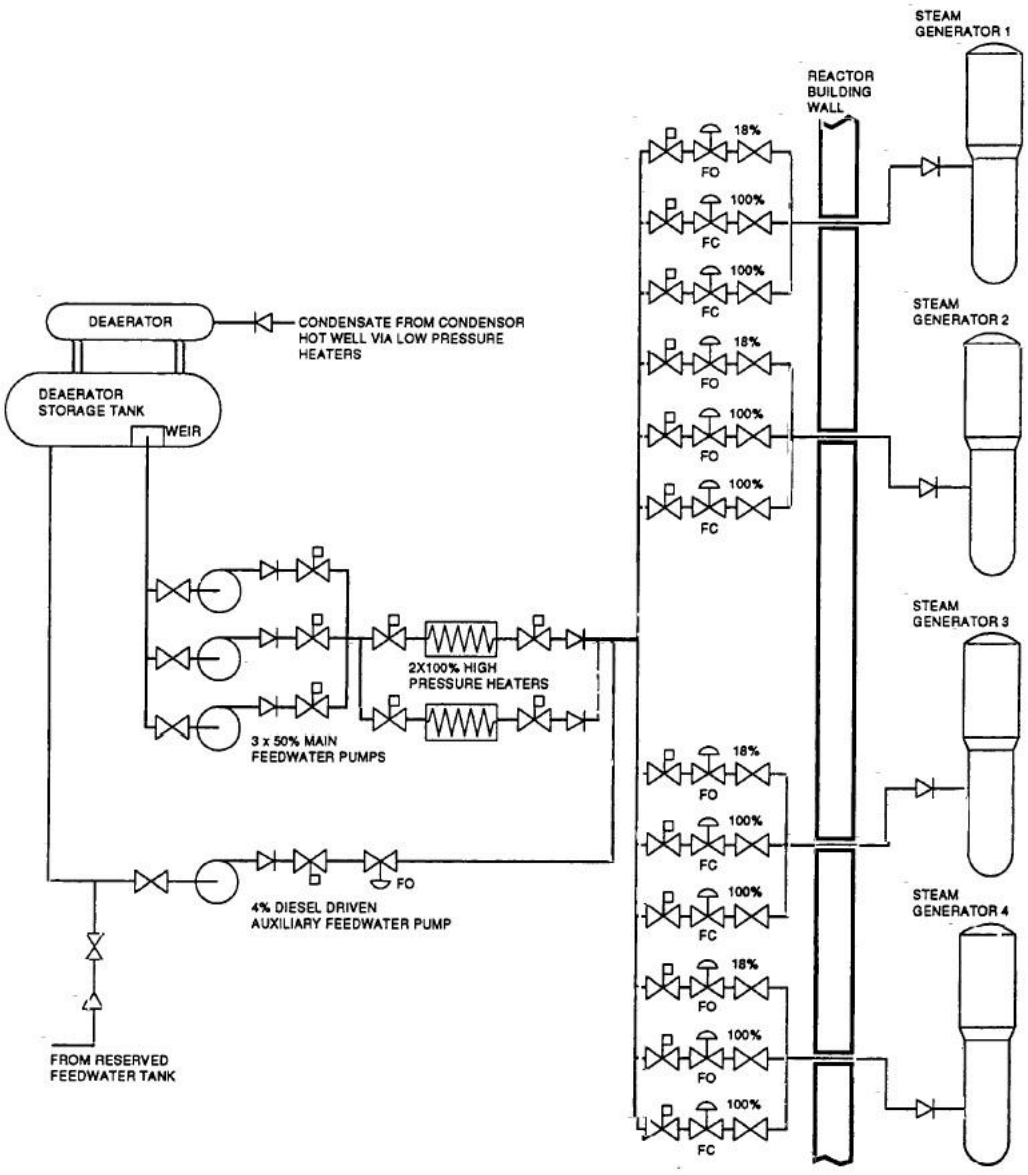


Figure 5.1: Steam Generator Feed Pumps and Level Control Valves

5.1.2 Demonstration of Non-coherent Fault Tree Analysis on the SGLCS

Under low power conditions, or if the flow measurements are not available, the SGLCS can be operated as a single element controller (Figure 5.2). In the case of One Element Level Control, the set point is the desired steam generator level, which is compared

with the measured level. The level error is computed as the difference between the level set-point and the actual (measured) level. The resultant controller signal is fed to the feedwater control valve's actuator, which alter the valve opening and hence the flow of feedwater to the steam generator [50].

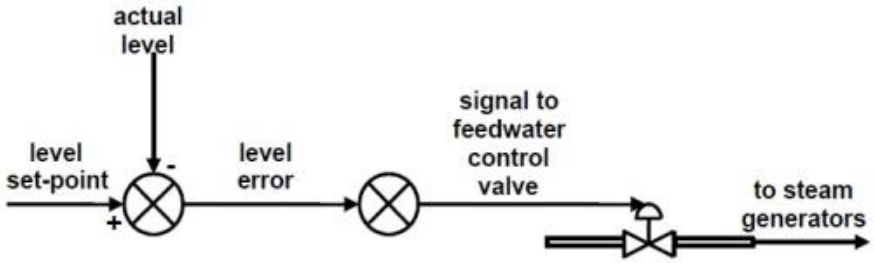


Figure 5.2: One Element Control of SGLCS

In order to analyze the level control system, we developed a simplified level control system which was developed, only includes pump, vessel, sensor, controller and valves (Figure 5.3).

In this system, liquid is fed to the vessel by the pump and the inlet flow is controlled by the inlet valve. A level sensor is used to measure the level of the liquid. If the liquid level exceeds a specified level, a signal "liquid level in the vessel is high" will be sent by the sensor. Upon receiving the signal, the level controller will send a command to the inlet control valve to reduce the input flow. The outlet valve constantly outflows the liquid from the vessel.

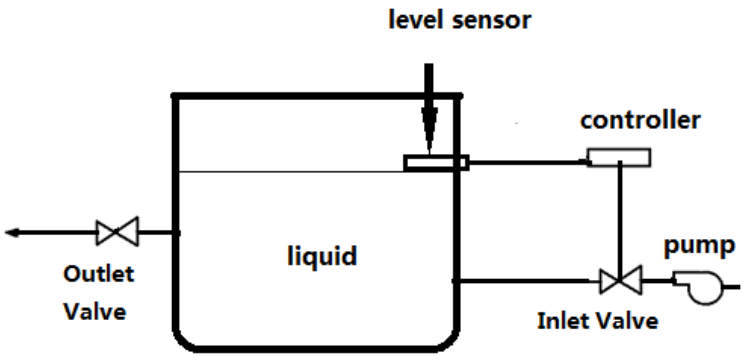


Figure 5.3: Simplified Level Control System

Assuming:

i. The outlet valve is stuck closed and fails to let the liquid outflow from the vessel (event *A*) and the level sensor generates a spurious signal indicating that the liquid level is low (event *B*);

ii. The outlet valve is stuck closed and fails to let the liquid outflow from the vessel (event *A*) and the level controller fails to respond to the signal from the level sensor (event *C*);

iii. The level sensor generates a spurious signal indicating that the liquid level in the vessel is low (event *B*) and the level sensor controller responds correctly to the signal from the level sensor (event $\overline{C}$).

These failure modes are assumed to be the only prime implicants of this system. The three prime implicant sets are: {*A, B*}, {*A, C*} and {*B,* $\overline{C}$}. Figure 5.4 shows the fault tree model of this system.

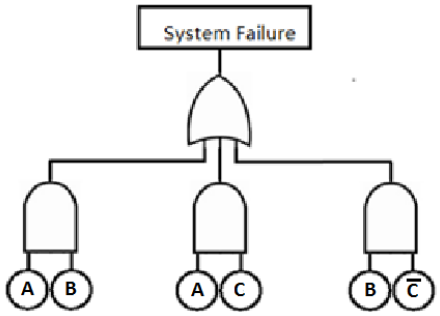


Figure 5.4: Example System Structure in Fault Tree

The Boolean expression obtained from the prime implicants is:

$$T = AB + AC + B\overline{C}$$

Because the availability of the component C ($q_{\overline{C}}$ or p_C) has the greatest value among the four in most cases, six situations should be considered during our analysis; thus six sets of component failure parameters (Table 5.1) are designed and used to measure the importance of the components in the system. The data set to the components however, are not realistic and only made up for demonstration in this case.

e	set 1		set 2	
	q_e	p_e	q_e	p_e
A	5.00E-04	1.00E+00	1.00E-04	1.00E+00
B	1.00E-04	1.00E+00	5.00E-04	1.00E+00
C	9.00E-04	9.99E-01	9.00E-04	9.99E-01
$\overline{C}$	9.99E-01	9.00E-04	9.99E-01	9.00E-04
e	set 3		set 4	
	q_e	p_e	q_e	p_e
A	9.00E-04	9.99E-01	9.00E-04	9.99E-01
B	5.00E-04	1.00E+00	1.00E-04	1.00E+00
C	1.00E-04	1.00E+00	5.00E-04	1.00E+00
$\overline{C}$	1.00E+00	1.00E-04	1.00E+00	5.00E-04
e	set 5		set 6	
	q_e	p_e	q_e	p_e
A	1.00E-04	1.00E+00	5.00E-04	1.00E+00
B	9.00E-04	9.99E-01	9.00E-04	9.99E-01
C	5.00E-04	1.00E+00	1.00E-04	1.00E+00
$\overline{C}$	1.00E+00	5.00E-04	1.00E+00	1.00E-04

Table 5.1: Failure/Repair Parameters of the Example System

The relation among the component unavailability for these six sets of data is shown below:

1. $q_{\overline{C}} > q_C > q_A > q_B$
2. $q_{\overline{C}} > q_C > q_B > q_A$
3. $q_{\overline{C}} > q_A > q_B > q_C$
4. $q_{\overline{C}} > q_A > q_C > q_B$
5. $q_{\overline{C}} > q_B > q_C > q_A$
6. $q_{\overline{C}} > q_B > q_A > q_C$

The risk importance measures (RIMs) of components for the six sets of data are calculated based on the mathematical models introduced in Section 3, and ranked accordingly in Table 5.2-5.13. The calculations are done by hands and Excel as this is a simple non-coherent system. Table 5.2-5.7 shows the results calculated for data sets 1~6 accordingly with respect to risk significance. Table 5.8-5.13 shows the results calculated for data sets 1-6 accordingly with respect to safety significance.

e	q	FV	CIF	IP	RRW
A	5.000E-04	4.484E-03	4.484E-03	4.500E-07	1.005E+00
B	1.000E-04	9.955E-01	9.955E-01	9.991E-05	2.230E+02
C	9.000E-04	4.483E-03	4.483E-03	4.500E-07	1.004E+00
$\overline{C}$	9.991E-01	9.950E-01	9.950E-01	9.986E-05	2.007E-01
ranking	$\overline{C}$>C>A>B	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>A>C>$\overline{C}$
sequential order for maintenance	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→A→C→$\overline{C}$

Table 5.2: Measure and Ranking of Importance with Respect to RS Using Parameter Set 1

e	q	FV	CIF	IP	RRW
A	1.000E-04	1.801E-04	1.801E-04	9.000E-08	1.000E+00
B	5.000E-04	9.998E-01	9.998E-01	4.996E-04	5.552E+03
C	9.000E-04	1.800E-04	1.800E-04	8.996E-08	9.993E-01
$\overline{C}$	9.991E-01	9.997E-01	9.997E-01	4.995E-04	4.996E+00
ranking	$\overline{C}$>C>B>A	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>A>$\overline{C}$>C
sequential order for maintenance	N/A	B→$\overline{C}$→A>C	B→$\overline{C}$→A>C	B→$\overline{C}$→A→C	B→A→$\overline{C}$→C

Table 5.3: Measure and Ranking of Importance with Respect to RS Using Parameter Set 2

e	q	FV	CIF	IP	RRW
A	9.000E-04	1.800E-04	1.800E-04	9.000E-08	1.000E+00
B	5.000E-04	9.998E-01	9.998E-01	5.000E-04	5.556E+03
C	1.000E-04	1.799E-04	1.799E-04	8.996E-08	1.000E+00
$\overline{C}$	9.999E-01	9.989E-01	9.989E-01	4.995E-04	5.556E-01
ranking	$\overline{C}$>A>B>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>A>C>$\overline{C}$
sequential order for maintenance	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→A→C→$\overline{C}$

Table 5.4: Measure and Ranking of Importance with Respect to RS Using Parameter Set 3

e	q	FV	CIF	IP	RRW
A	9.000E-04	4.482E-03	4.482E-03	4.500E-07	1.005E+00
B	1.000E-04	9.955E-01	9.955E-01	9.995E-05	2.231E+02
C	5.000E-04	4.482E-03	4.482E-03	4.500E-07	1.004E+00
$\overline{C}$	9.995E-01	9.946E-01	9.946E-01	9.986E-05	1.116E-01
ranking	$\overline{C}$>A>C>B	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>A>C>$\overline{C}$
sequential order for maintenance	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→A→C→$\overline{C}$

Table 5.5: Measure and Ranking of Importance with Respect to RS Using Parameter Set 4

e	q	FV	CIF	IP	RRW
A	1.000E-04	5.558E-05	5.558E-05	5.000E-08	1.000E+00
B	9.000E-04	9.999E-01	9.999E-01	8.996E-04	1.799E+04
C	5.000E-04	5.553E-05	5.553E-05	4.996E-08	9.996E-01
$\overline{C}$	9.995E-01	9.998E-01	9.998E-01	8.995E-04	8.996E+00
ranking	$\overline{C}$>B>C>A	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>A>C>$\overline{C}$
sequential order for maintenance	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→A→C→$\overline{C}$

Table 5.6: Measure and Ranking of Importance with Respect to RS Using Parameter Set 5

e	q	FV	CIF	IP	RRW
A	5.000E-04	5.556E-05	5.556E-05	5.000E-08	1.000E+00
B	9.000E-04	9.999E-01	9.999E-01	8.999E-04	1.800E+04
C	1.000E-04	5.551E-05	5.551E-05	4.996E-08	1.000E+00
$\overline{C}$	9.999E-01	9.994E-01	9.994E-01	8.995E-04	1.800E+00
ranking	$\overline{C}$>B>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C
sequential order for maintenance	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C

Table 5.7: Measure and Ranking of Importance with Respect to RS Using Parameter Set 3

e	q	BM	RAW	CP	RA
A	5.000E-04	9.000E-04	9.963E+00	9.999E-04	8.996E-04
B	1.000E-04	9.991E-01	9.955E+03	9.991E-01	9.990E-01
C	9.000E-04	5.000E-04	4.982E+00	5.000E-04	3.996E-04
$\overline{C}$	9.991E-01	9.995E-05	1.996E+00	2.004E-04	1.000E-04
ranking	$\overline{C}$>C>A>B	B>A>C>$\overline{C}$	B>A>C>$\overline{C}$	B>A>C>$\overline{C}$	B>A>C>$\overline{C}$
maintenance Priority	N/A	B→A→C→$\overline{C}$	B→A→C→$\overline{C}$	B→A→C→$\overline{C}$	B→A→C→$\overline{C}$

Table 5.8: Measure and Ranking of Importance with Respect to SS Using Parameter Set 1

e	q	BM	RAW	CP	RA
A	1.000E-04	9.000E-04	2.801E+00	1.400E-03	8.999E-04
B	5.000E-04	9.991E-01	2.000E+03	9.991E-01	9.986E-01
C	9.000E-04	9.995E-05	2.001E-01	1.000E-04	-3.996E-04
$\overline{C}$	9.991E-01	5.000E-04	2.001E+00	9.996E-04	5.000E-04
ranking	$\overline{C}$>C>B>A	B>A>$\overline{C}$>C	B>A>$\overline{C}$>C	B>A>$\overline{C}$>C	B>A>$\overline{C}$>C
maintenance Priority	N/A	B→A→$\overline{C}$→C	B→A→$\overline{C}$→C	B→A→$\overline{C}$→C	B→A→$\overline{C}$→C

Table 5.9: Measure and Ranking of Importance with Respect to SS Using Parameter Set 2

e	q	BM	RAW	CP	RA
A	9.000E-04	1.000E-04	1.200E+00	6.000E-04	9.991E-05
B	5.000E-04	9.999E-01	2.000E+03	9.999E-01	9.994E-01
C	1.000E-04	8.996E-04	1.800E+00	9.000E-04	4.000E-04
$\overline{C}$	9.999E-01	4.996E-04	2.000E+00	1.000E-03	5.000E-04
ranking	$\overline{C}$>A>B>C	B>C>$\overline{C}$>A	B>$\overline{C}$>C>A	B>$\overline{C}$>C>A	B>$\overline{C}$>C>A
maintenance Priority	N/A	B→C→$\overline{C}$→A	B→$\overline{C}$→C→A	B→$\overline{C}$→C→A	B→$\overline{C}$→C→A

Table 5.10: Measure and Ranking of Importance with Respect to SS Using Parameter Set 3

e	q	BM	RAW	CP	RA
A	9.000E-04	5.000E-04	5.976E+00	6.000E-04	4.996E-04
B	1.000E-04	9.995E-01	9.955E+03	9.995E-01	9.994E-01
C	5.000E-04	8.999E-04	8.964E+00	9.000E-04	7.996E-04
$\overline{C}$	9.995E-01	9.991E-05	1.996E+00	2.004E-04	1.000E-04
ranking	$\overline{C}$>A>C>B	B>C>A>$\overline{C}$	B>C>A>$\overline{C}$	B>C>A>$\overline{C}$	B>C>A>$\overline{C}$
maintenance Priority	N/A	B→C→A→$\overline{C}$	B→C→A→$\overline{C}$	B→C→A→$\overline{C}$	B→C→A→$\overline{C}$

Table 5.11: Measure and Ranking of Importance with Respect to SS Using Parameter Set 4

e	q	BM	RAW	CP	RA
A	1.000E-04	5.000E-04	1.556E+00	1.400E-03	5.000E-04
B	9.000E-04	9.995E-01	1.111E+03	9.995E-01	9.986E-01
C	5.000E-04	9.991E-05	1.112E-01	1.000E-04	-7.996E-04
$\overline{C}$	9.995E-01	8.999E-04	2.000E+00	1.800E-03	9.000E-04
ranking	$\overline{C}$>B>C>A	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C	B>$\overline{C}$>A>C
maintenance Priority	N/A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C

Table 5.12: Measure and Ranking of Importance with Respect to SS Using Parameter Set 5

e	q	BM	RAW	CP	RA
A	5.000E-04	1.000E-04	1.111E+00	9.999E-04	9.995E-05
B	9.000E-04	9.999E-01	1.111E+03	9.999E-01	9.990E-01
C	1.000E-04	4.996E-04	5.556E-01	5.000E-04	-4.000E-04
$\overline{C}$	9.999E-01	8.996E-04	2.000E+00	1.800E-03	9.000E-04
ranking	$\overline{C}$>B>A>C	B>$\overline{C}$>C>A	B>$\overline{C}$>A>C	B>$\overline{C}$'>A>C	B>$\overline{C}$>A>C
maintenance Priority	N/A	B→$\overline{C}$→C→A	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C	B→$\overline{C}$→A→C

Table 5.13: Measure and Ranking of Importance with Respect to SS Using Parameter Set 6

The ranking of various RIMs are given in the second last row of Table 5.2-5.13; the last row has shown the sequential order of maintenance according to the ranking. With respect to the risk significance, the sequential orders of maintenance are as same as the rankings; for safety significance, the maintenance priority is identical to the rankings.

Most of the ranking results from Table 5.2-5.13 have shown that component B should be paid the most attention which is reasonable because component B not only co-exists in a same cut set with component A, but also in a same prime implicant set with $\overline{C}$ which has the greatest value of probability. Based on the real system, the vulnerability of level sensor (related to component B) requires most attention.

Thus for the non-coherent system, CIF, FV and IP provide the same ranking for all six data sets. As an informative risk significant measure for coherent systems, RRW cannot

show a consistent and informative result in non-coherent systems, as the RRW of a non-coherent event depends on the probabilities of the other events which belong to the prime implicant sets that includes the negation of the non-coherent event; and is totally independent of the probability of the given non-coherent event/components. As a result, although CIF, FV, IP and RRW measures risk significance for coherent systems, CIF, FV and IP are the more applicable than RRW as risk significant measures which provide useful information for maintenance in non-coherent systems.

RA, RAW and CP provide the same ranking results and the results also vary according to different data sets, whereas BM shows different ranking results. Even though BM can be considered as a safety significant measures as it is totally independent of the unavailability of the component, it shows meaningless ranking due to its definition. As a result, RA, RAW and CP are more applicable as safety significant measures which provide useful information for maintenance in non-coherent systems.

On the other hand, the analysis has shown that the non-coherent components cannot be deliberately set to be 'failed' during maintenance activities. The coherent components existing in the same minimal cut sets and prime implicant sets with the non-coherent component should draw more attention than the non-coherent component itself, although the non-coherent components usually ranks higher because the availability is always higher than the unavailability of one component.

5.2 The Application of Non-coherent Fault Tree Analysis on a Gas Detection System

5.2.1 Gas Detection System

Analyzing a multitasking system is the one of the best ways to illustrate the use of NOT logic, because it has been demonstrated that there needs to be a convincing reason for their inclusion [27]. In this case the outcomes of the system performance can produce combinations of some tasks being performed whilst others have failed. The causes of each system outcome cannot be identified correctly without accounting for the parts of the system which have worked. A Simplified Gas Detection System (GDS) has been used in [51] and [44] and shown in Figure 5.5.

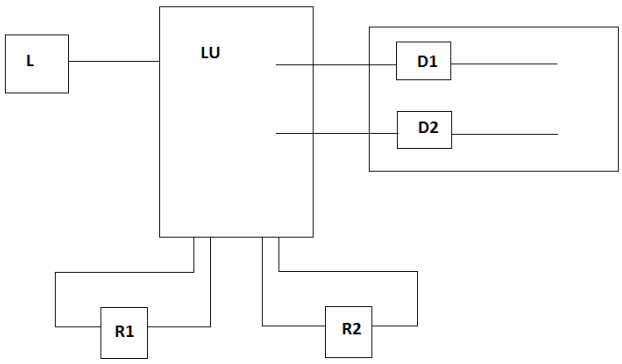


Figure 5.5: Simplified Gas Detection System

In this system, two gas sensors are denoted by *D1* and *D2*; both of them are used to detect a leakage of gas in a confined space. The signals from these detectors are fed along individual cables back to the computer logic control unit (*LU*). On receiving a signal which represents a gas leak from either detector the system has three functions:

(a) Process shut-down (isolation)—by de-energizing relay *R1*;

(b) Inform the operator of the leak by lamp/siren labeled *L*;

(c) Remove the power supply (potential ignition sources) to the affected area by de-energizing relay *R2*.

All the three tasks should be completed or the system will be considered to fail by giving a leak condition. The fault tree diagram for the top event is shown in Figure 5.6.

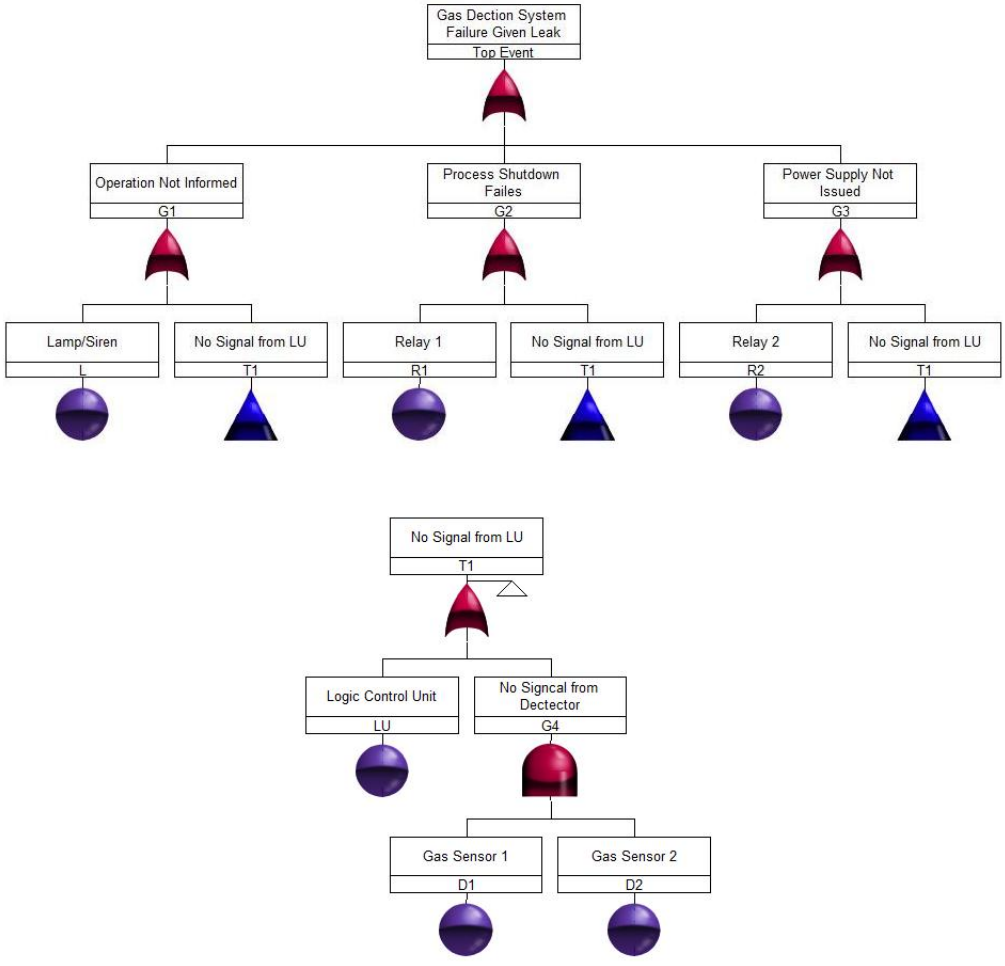


Figure 5.6: Fault Tree for Gas Detection System

5.2.2 Demonstration of Non-coherent Fault Tree Analysis on the GDS

Boolean analysis of this fault tree gives minimal cut sets: *L, R1, R2, LU, D1D2*. However, the overall system seems to be coherent. It can only be considered non-coherent in certain circumstances. Because gate at the top of the fault tree is an OR gate, any occurrence of the three tasks (represented by *G1*, *G2* and *G3*) can cause the top event, there are 7 (2^3-1) outcomes of the system failure, which is shown in Table 5.14.

Gate	G1	G2	G3
Outcome	Operator Informed	Process Shutdown	Power Isolation
1	W	W	F
2	W	F	W
3	W	F	F
4	F	W	W
5	F	W	F
6	F	F	W
7	F	F	F

W: Subsystem at working state
F: Subsystem fails

Table 5.14: Gas Detection System Outcome

Even though they all cause the top event, the seven outcomes have different severity between each other. However, the possibility of outcome 3 is rather small as it indicates that the operator thinks everything is fine but the process has not shut down, nor has the power been isolated. Because the quantification of the fault tree will substantially overestimate the probability of the outcome 3, the functioning part of the system is taken into consideration. Thus the NOT gate should be used in the proper assessment.

This situation can be illustrated in a non-coherent fault tree in Figure 5.7.

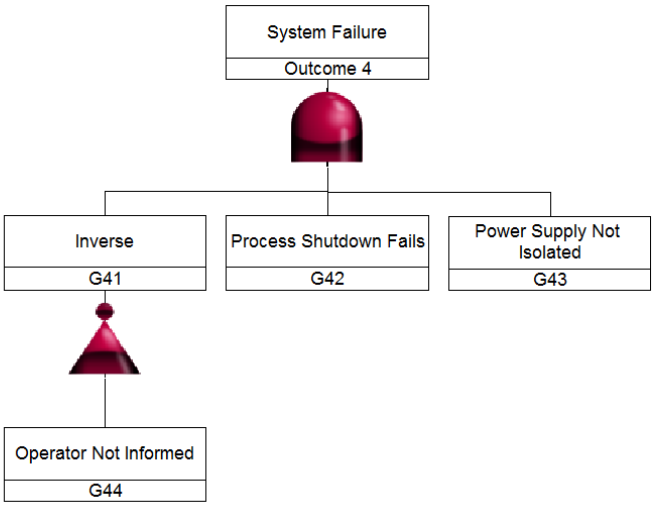


Figure 5.7: Non-coherent Fault Tree Diagram for Outcome 4

Incorporating the logic function and Boolean theorem into the non-coherent system, given the logic equation for each of the gates is given as:

$$G1=\overline{\bar{L}+LU+D1\cdot D2}=\bar{L}\cdot\overline{LU}\cdot(\overline{D1}+\overline{D2})=\bar{L}\cdot\overline{LU}\cdot\overline{D1}+\bar{L}\cdot\overline{LU}\cdot\overline{D2}$$

$$G2=R1+LU+D1\cdot D2$$

$$G3=R2+LU+D1\cdot D2$$

$$Top=G1\cdot G2\cdot G3=(\bar{L}\cdot\overline{LU}\cdot\overline{D1}+\bar{L}\cdot\overline{LU}\cdot\overline{D2})\cdot(R1+LU+D1\cdot D2)\cdot(R2+LU+D1\cdot D2)$$

$$=\bar{L}\cdot\overline{LU}\cdot R1\cdot R2\cdot\overline{D1}+\bar{L}\cdot\overline{LU}\cdot R1\cdot R2\cdot\overline{D2}$$

Thus, the fault tree for this particular failure mode has two prime implicant sets: $\{\bar{L}\cdot\overline{LU}\cdot R1\cdot R2\cdot\overline{D1}\}$ and $\{\bar{L}\cdot\overline{LU}\cdot R1\cdot R2\cdot\overline{D2}\}$. The simplified fault tree which took the outcome 4 as the top event is shown in Figure 5.8.

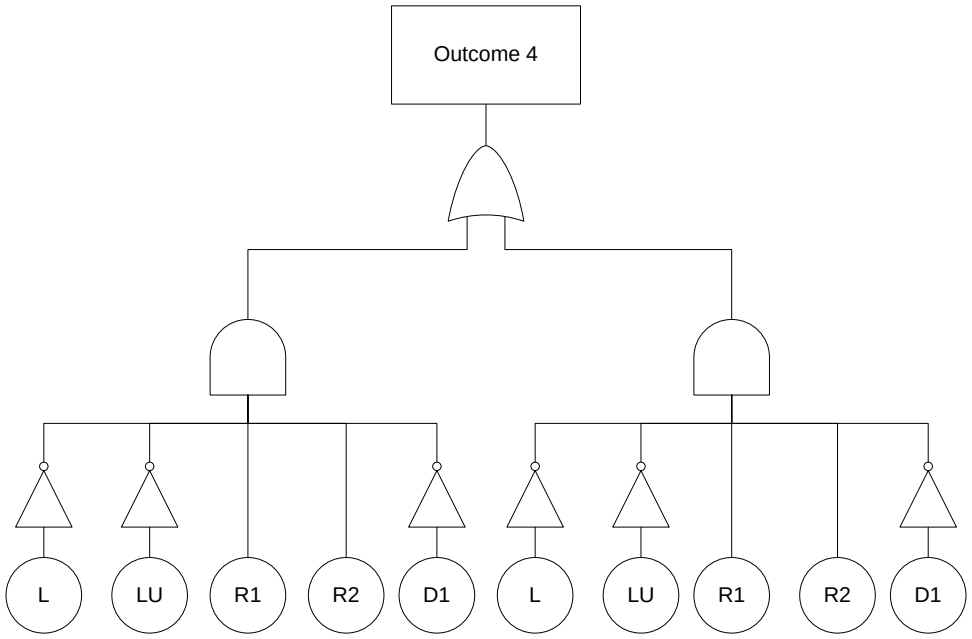


Figure 5.8: Simplified Fault Tree for Outcome 4

The unavailability if the system is:

$$Q_{sys} = p_L \cdot p_{LU} \cdot q_{R1} \cdot q_{R2} \cdot p_{D1} + p_L \cdot p_{LU} \cdot q_{R1} \cdot q_{R2} \cdot p_{D2} - p_L \cdot p_{LU} \cdot q_{R1} \cdot q_{R2} \cdot p_{D1} \cdot p_{D2}$$

To illustrate the method used to analyze component importance, the data assigned to each component in [54] can be used in here:

Component *i*	q_i	p_i
L	0.01	0.99
LU	0.04	0.96
R1	0.06	0.94
R2	0.06	0.94
D1	0.02	0.98
D2	0.02	0.98

Table 5.15: Component Availability/Unavailability Values for GDS

There are six events that need to be focused on according to the fault tree in Figure 5.8: $\overline{L}$, $\overline{LU}$, R1, R2, $\overline{D1}$, $\overline{D2}$. In this case, the failure criticality of R1 and R2 are concerned while the repair criticality of component L, LU, D1 and D2 are concerned. The importance of each event can be calculated with respect to various RIMs. The results are calculated in a spread sheet of Excel and shown in Table 5.16.

e	BM	RA	CP	RAW
$\overline{L}$	0.003454618	3.45462E-05	0.003454618	1.01010101
$\overline{LU}$	0.003562574	0.000142503	0.003562574	1.041666667
R1	0.05700119	0.053581119	0.05700119	16.66666667
R2	0.05700119	0.053581119	0.05700119	16.66666667
$\overline{D1}$	6.84288E-05	1.36858E-06	0.00342144	1.00040016
$\overline{D2}$	6.84288E-05	1.36858E-06	0.00342144	1.00040016
Ranking	R1=R2>$\overline{LU}$>$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2>$\overline{LU}$>$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2>$\overline{LU}$>$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2>$\overline{LU}$>$\overline{L}$>$\overline{D1}$=$\overline{D2}$
e	CIF	IP	FV	RRW
$\overline{L}$	1	0.003420071	1	∞
$\overline{LU}$	1	0.003420071	1	∞
R1	1	0.003420071	1	∞
R2	1	0.003420071	1	∞
$\overline{D1}$	0.019607843	6.70602E-05	0.003353011	1.02
$\overline{D2}$	0.019607843	6.70602E-05	0.003353011	1.02
Ranking	R1=R2=$\overline{LU}$=$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2=$\overline{LU}$=$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2=$\overline{LU}$=$\overline{L}$>$\overline{D1}$=$\overline{D2}$	R1=R2=$\overline{LU}$=$\overline{L}$>$\overline{D1}$=$\overline{D2}$

Table 5.16: Measures and Rankings of Component Importance for GDS

The results have reflected the categorization of various RIMs as the risk significant measures (CIF, IP, FV and RRW) record the same results of ranking while safety significant measures (BM, RA, CP and RAW) have recorded the same results of ranking as well.

According to the safety significant measures, coherent event R1 and R2 are ranked highest. From this ranking, R1 and R2 should be put into the highest maintenance priority than the other components and preventive maintenance activity should be taken to increase the availability of R1 and R2 in order to reduce the likelihood of system failure.

Components LU and L were ranked 2nd and 3rd highest, while both of them are non-coherent. Thus they can only be repair critical. However, it is not appropriate to reduce the availability of components that can be repair critical during maintenance activities. The probability of existence of the necessary and sufficient conditions for the component to be repair critical should be minimized. D1 and D2 are always ranked behind the other components as they do not appear in both prime implicant sets.

The repair of a component which can be repair critical needs to be done when it is not repair critical. The ranking results have reflected the fact that during the maintenance on the non-coherent system, the other failure critical components should be repaired prior to the repair critical components i.e. the non-coherent components.

Because components L, LU, R1 and R2 have the same status in the fault tree, they have the same value of importance according to the rankings provided by risk significant measures, which is not informative for maintenance activity.

5.3 The Application of Non-coherent Fault Tree Analysis on the Automatic Power Control System

An Automatic Power Control System (APCS) of the experimental nuclear reactor of Tsinghua University is introduced in [61]. The flowsheet of APCS is shown in Figure 5.9. This system helps keep the reactor power to the demanded value by adjustment. The system contains two negative feedback loops while one of them is in the standby mode. In the flowsheet diagram, the arrowhead indicates the pass direction of the signal or control.

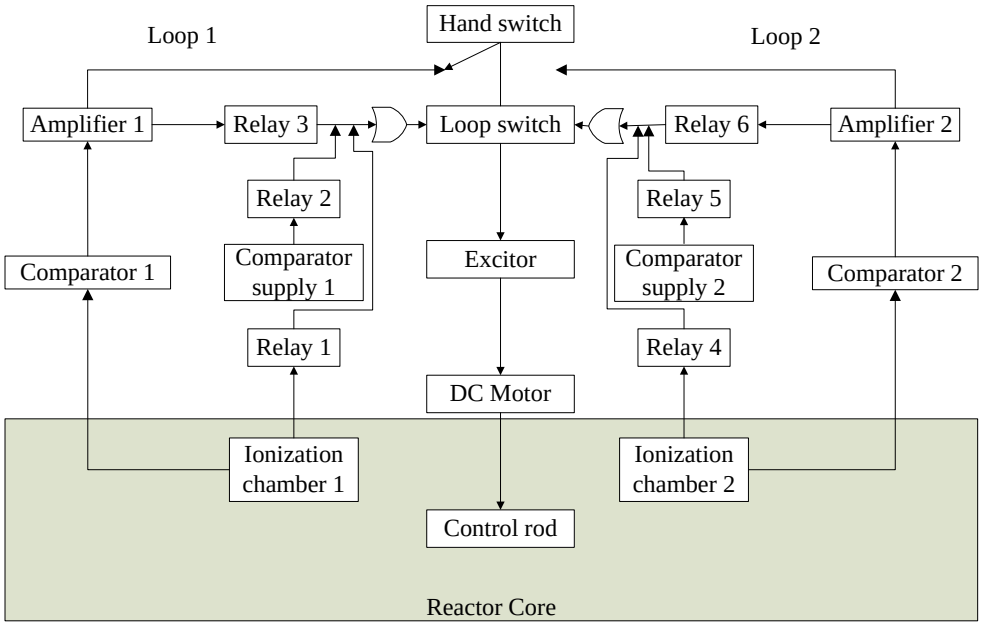
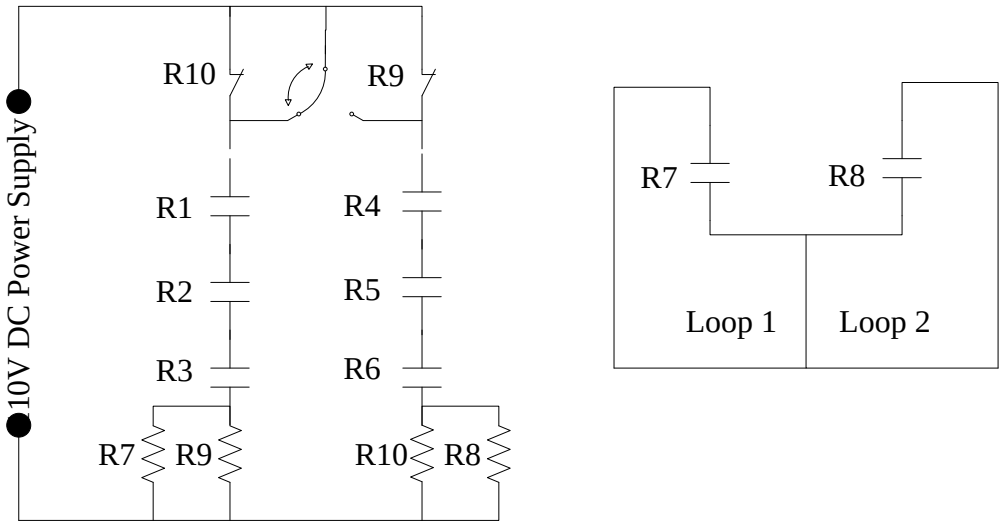


Figure 5.9: The Flowsheet of APCS

An electric current I is given to the comparator from the ionization chamber, where I is compared to the standard electric current I_0 set according to the power value demanded. The difference between the two is sent the amplifier before passing through the loop switch

to the exciter. It is sent to the DC motor after the amplification. The reactor power is adjusted by the DC motor as it lifts and drops the control rod.

The two loops are performed independently. Each loop contains one ionization chamber to measure the reactor power, one comparator to compare this value to the demanded value, and one amplifier to magnify the control current. When any one of these components fail, their corresponding relays will open up, so that the control can be automatically switched to the other loop. The switching mechanism is shown in Figure 5.10. More detailed explanation on how this system functions is found in [61].



R=Relay

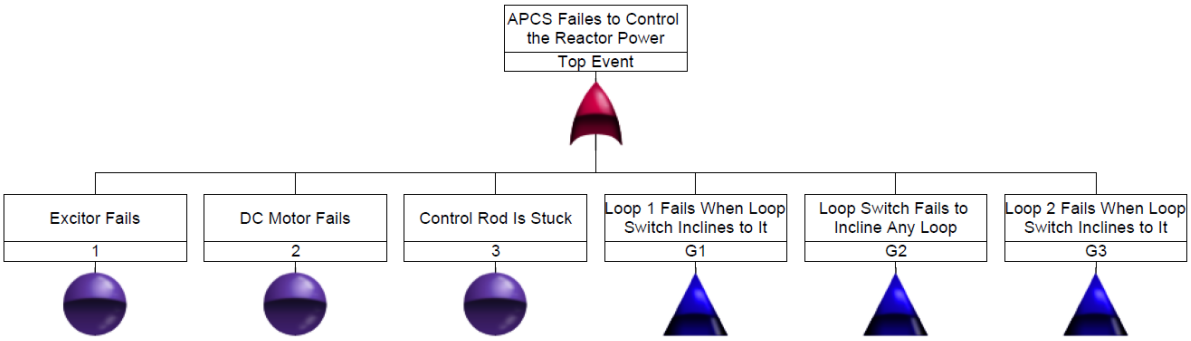
H=Hand Switch

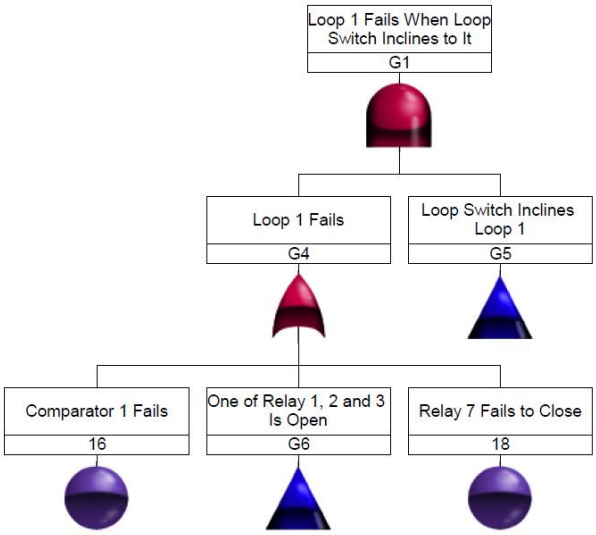
Figure 5.10: The Loop Switch of APCS

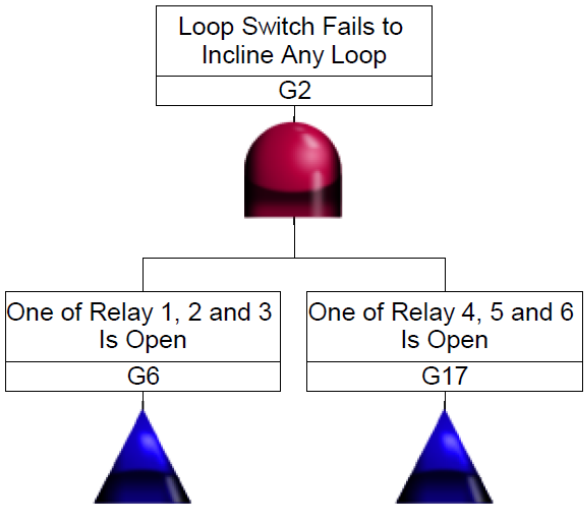
There are four assumptions made for the sake of simplification in FTA:

1. Loop 1 has the priority to be closed first, i.e. if relay 1-3 are closed, the loop switch inclines to loop 1, which means that relay 9 is open and relay 10 is closed. This assumption is the real situation when the hand switch is turned to loop 1.
2. Relay 9 and 10 are 100% reliable (unavailability set to 0).
3. The failure mode of relays are "failed to close".
4. The 100V DC supply is 100% reliable.

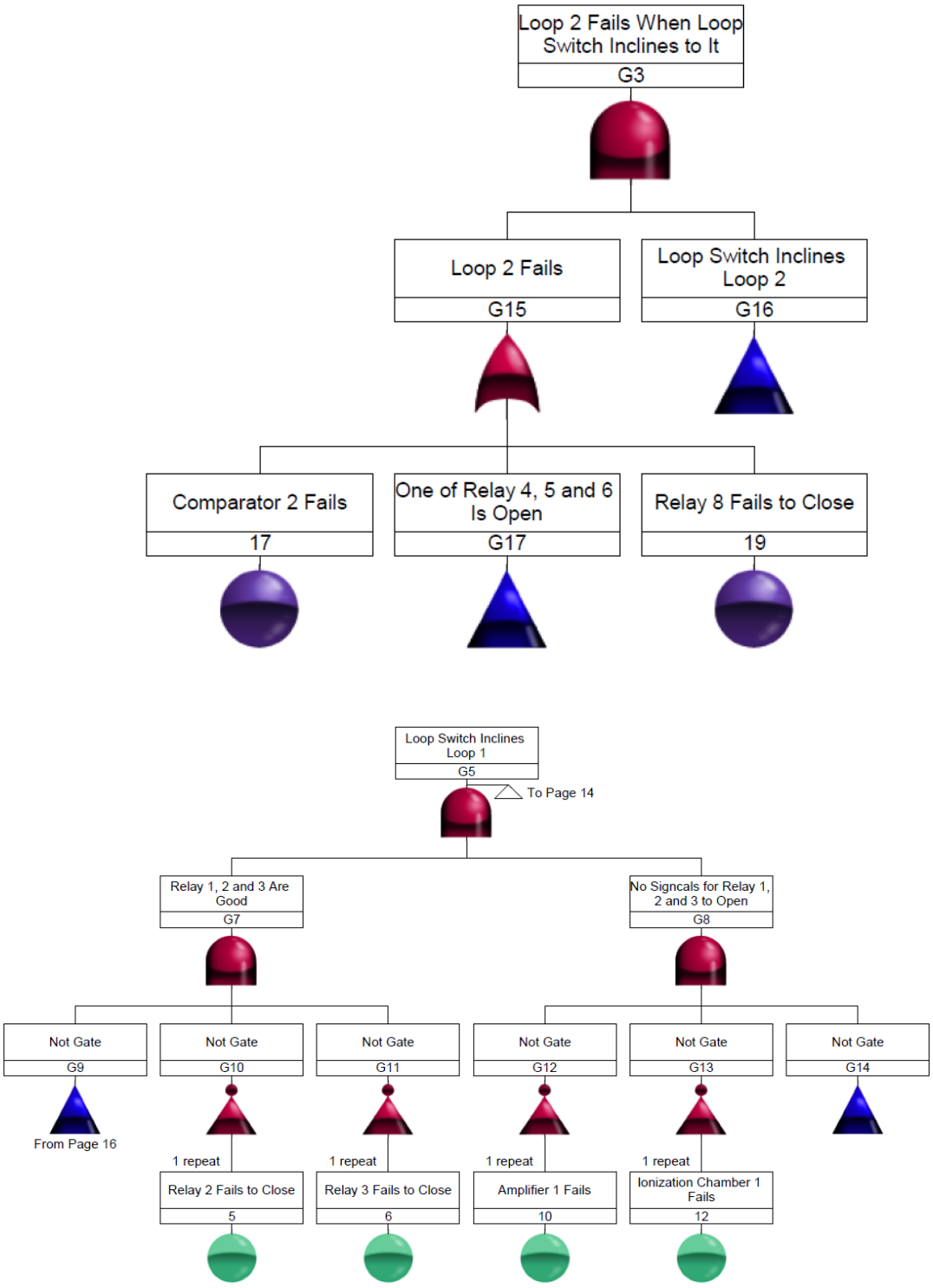
Base on the assumptions, the fault tree for APCS can be illustrated in RELEX Studio with the data input. The fault tree is shown in Figure 5.11. The basic events are shown in Table 5.17.



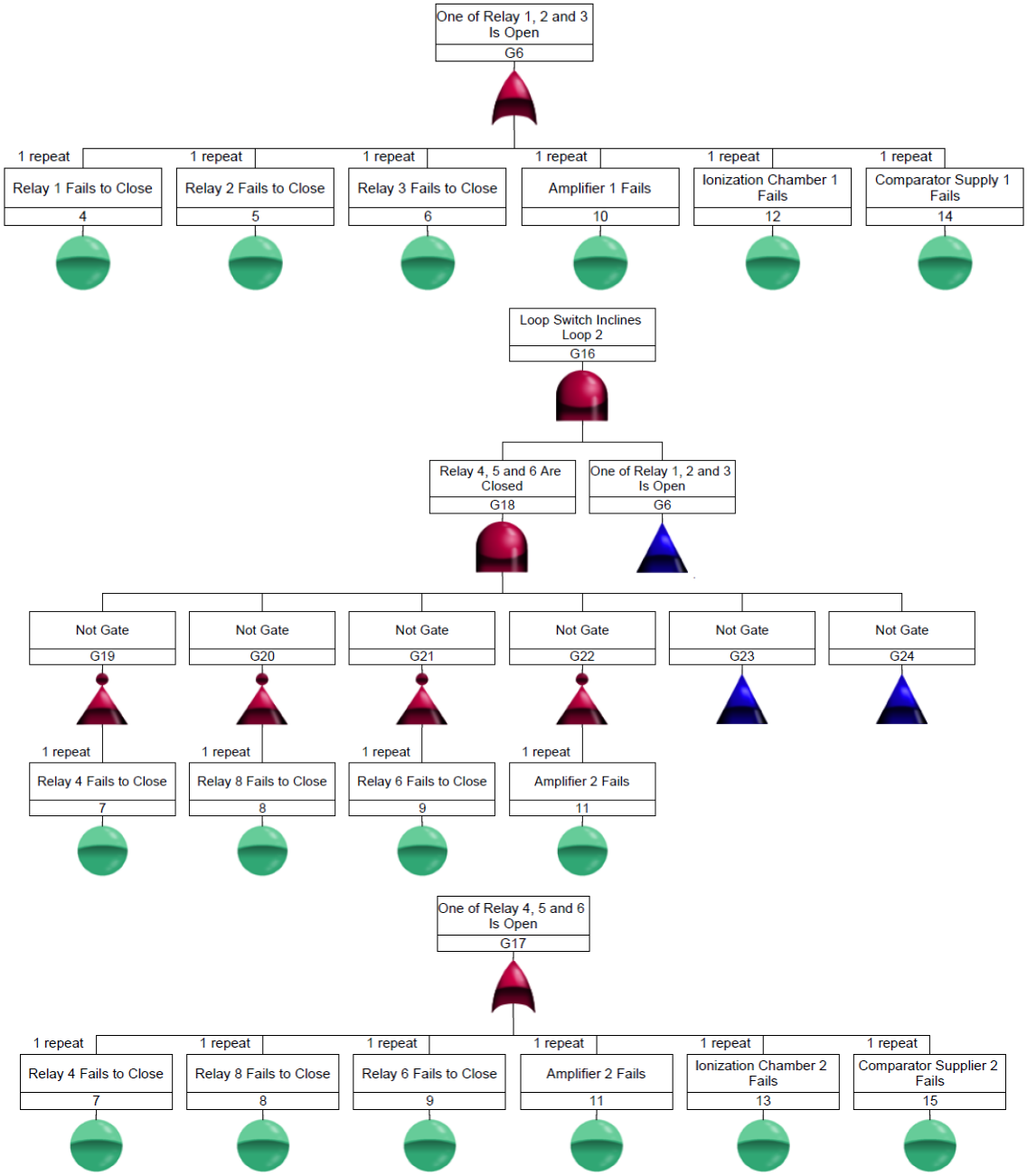




(Continued Next Page)



(Continued Next Page)



(Continued Next Page)

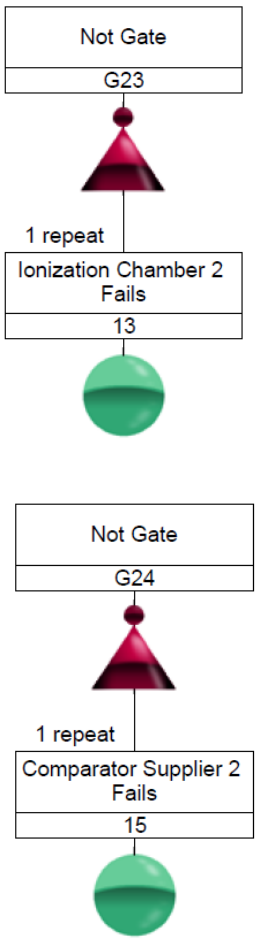


Figure 5.11: Fault Tree of the APCS

e	Description	$q_i(10^{-4})$
1	Excitor fails	20
2	DC motor fails	9.99
3	Control rod is stuck	9.99
4	Relay 1 fails to close	9.99
5	Relay 2 fails to close	9.99
6	Relay 3 fails to close	9.99
7	Relay 4 fails to close	9.99
8	Relay 5 fails to close	9.99
9	Relay 6 fails to close	9.99
10	Amplifier 1 fails	99
11	Amplifier 2 fails	99
12	Ionization chamber 1 fails	196
13	Ionization chamber 2 fails	196
14	Comparator supply 1 fails	9.99
15	Comparator supply 2 fails	9.99
16	Comparator 1 fails	4
17	Comparator 2 fails	4
18	Relay 7 fails to close	9.99
19	Relay 8 fails to close	9.99

Table 5.17: Basic Events and Their Unavailabilities

Because the system involves NOT logic in the fault tree, it is considered non-coherent in fault tree analysis. Based on the fault tree analysis in [61], this system contains 52 prime implicant sets as follows: {1}, {2}, {3}, {4, 7}, {4, 8}, {4, 9}, {4, 11}, {4, 13}, {4, 15}, {4, 17}, {4, 19}, {5, 7}, {5, 8}, {5, 9}, {5, 11}, {5, 13}, {5, 15}, {5, 17}, {5, 19}, {6, 7}, {6, 8}, {6, 9}, {6, 11}, {6, 13}, {6, 17}, {6, 19}, {10, 7}, {10, 8}, {10, 9}, {10, 11}, {10, 13}, {10, 15}, {10, 17}, {10, 19}, {12, 7}, {12, 8}, {12, 9}, {12, 11}, {12, 13}, {12, 15}, {12, 17}, {12, 19}, {14, 7}, {14, 8}, {14, 9}, {14, 11}, {14, 13}, {14, 15}, {14, 17}, {14, 19}, { $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{10}$, $\overline{12}$, $\overline{14}$, 16}, { $\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{10}$, $\overline{12}$, $\overline{14}$, 18}.

The unavailability of the system calculated using the method in [62] is

$$Q_{sys}=6.5\times10^{-3}$$

Although there are 19 coherent events existing in the fault tree, six of them ($\overline{4}$, $\overline{5}$, $\overline{6}$, $\overline{10}$, $\overline{12}$, $\overline{14}$) are non-coherent. Thus there are 25 events that needs to be considered in calculation and ranking according to various RIMs. The calculation of BM and FV can be done with RELEX Studio with the non-coherent events set to independent. However, because the software does not involve the assessment with the other measures, the calculation is also done with the help of Excel.

The calculated results are shown in Table 5.18. The rankings provided by various RIMs of all the events are listed in order to show the sequential order of maintenance; they are listed with respect to risk significant measures and safety significant measures in Table 5.19 and Table 5.20, respectively.

It should be noted that the negative values of RA is due to the subtraction of the system unavailability; it does not affect the ranking results.

Event		RIMs							
#	Description	BM	CIF	IP	FV	RA	CP	RAW	RRW
1	Excitor fails	9.97E-01	3.07E-01	1.99E-03	3.08E-01	9.94E-01	1.00E+00	1.54E+02	9.39E-03
2	DC motor fails	9.98E-01	1.53E-01	9.97E-04	1.54E-01	9.94E-01	1.00E+00	1.54E+02	7.68E-03
3	Control rod is stuck	9.98E-01	1.53E-01	9.97E-04	1.54E-01	9.94E-01	1.00E+00	1.54E+02	7.68E-03
4	Relay 1 fails to close	3.34E-02	5.13E-03	3.33E-05	5.36E-03	2.84E-02	3.49E-02	5.37E+00	6.54E-03
$\bar{4}$	Relay 1 close as required	1.31E-03	2.01E-01	1.30E-03	2.08E-01	-6.11E-03	3.87E-04	5.96E-02	8.21E-03
5	Relay 2 fails to close	3.34E-02	5.13E-03	3.33E-05	5.36E-03	2.84E-02	3.49E-02	5.37E+00	6.54E-03
$\bar{5}$	Relay 2 close as required	1.31E-03	2.01E-01	1.30E-03	2.08E-01	-6.11E-03	3.87E-04	5.96E-02	8.21E-03
6	Relay 3 fails to close	3.34E-02	5.13E-03	3.33E-05	5.36E-03	2.84E-02	3.49E-02	5.37E+00	6.54E-03
$\bar{6}$	Relay 3 close as required	1.31E-03	2.01E-01	1.30E-03	2.08E-01	-6.11E-03	3.87E-04	5.96E-02	8.21E-03
7	Relay 4 fails to close	3.21E-02	4.93E-03	3.20E-05	1.59E-01	2.70E-02	3.35E-02	5.15E+00	7.72E-03
8	Relay 5 fails to close	3.21E-02	4.93E-03	3.20E-05	1.59E-01	2.70E-02	3.35E-02	5.15E+00	7.72E-03
9	Relay 6 fails to close	3.21E-02	4.93E-03	3.20E-05	1.59E-01	2.70E-02	3.35E-02	5.15E+00	7.72E-03
10	Amplifier 1 fails	3.37E-02	5.13E-02	3.33E-04	5.31E-02	2.84E-02	3.49E-02	5.37E+00	6.86E-03
$\bar{10}$	Amplifier 1 works	1.32E-03	2.01E-01	1.30E-03	2.08E-01	-6.11E-03	3.90E-04	6.00E-02	8.21E-03
11	Amplifier 2 fails	3.23E-02	4.93E-02	3.20E-04	2.12E-02	2.70E-02	3.35E-02	5.15E+00	6.64E-03
12	Ionization chamber 1 fails	3.40E-02	1.03E-01	6.67E-04	1.05E-01	2.84E-02	3.49E-02	5.37E+00	7.26E-03
$\bar{12}$	Ionization chamber 1 works	1.33E-03	2.01E-01	1.30E-03	2.08E-01	-6.10E-03	3.97E-04	6.10E-02	8.21E-03
13	Ionization chamber 2 fails	3.27E-02	9.85E-02	6.41E-04	1.01E-01	2.70E-02	3.35E-02	5.15E+00	7.23E-03
14	Comparator supply 1 fails	3.34E-02	5.13E-03	3.33E-05	5.36E-03	2.84E-02	3.49E-02	5.37E+00	6.54E-03
$\bar{14}$	Comparator supply 1 works	1.31E-03	2.01E-01	1.30E-03	2.08E-01	-6.11E-03	3.87E-04	5.96E-02	8.21E-03
15	Comparator supply 2 fails	3.21E-02	4.93E-03	3.20E-05	1.58E-01	2.70E-02	3.35E-02	5.15E+00	7.72E-03
16	Comparator 1 fails	9.65E-01	5.94E-02	3.86E-04	2.08E-01	9.60E-01	9.67E-01	1.49E+02	8.21E-03
17	Comparator 2 fails	3.20E-02	1.97E-03	1.28E-05	1.45E-03	2.70E-02	3.35E-02	5.15E+00	6.51E-03
18	Relay 7 fails to closed	9.66E-01	1.48E-01	9.65E-04	2.08E-01	9.60E-01	9.67E-01	1.49E+02	8.21E-03
19	Relay 8 fails to closed	3.21E-02	4.93E-03	3.20E-05	1.59E-01	2.70E-02	3.35E-02	5.15E+00	7.72E-03

Table 5.18: RIMs for basic events in APCS

Event		CIF	IP	Ranking
1	Excitor fails	3.07E-01	1.99E-03	1
$\overline{4}$	Relay 1 closed as required	2.01E-01	1.30E-03	2
$\overline{5}$	Relay 2 closed as required	2.01E-01	1.30E-03	
$\overline{6}$	Relay 3 closed as required	2.01E-01	1.30E-03	
$\overline{10}$	Amplifier 1 works	2.01E-01	1.30E-03	
$\overline{12}$	Ionization chamber 1 works	2.01E-01	1.30E-03	
$\overline{14}$	Comparator supply 1 works	2.01E-01	1.30E-03	
2	DC motor fails	1.53E-01	9.97E-04	3
3	Control rod is stuck	1.53E-01	9.97E-04	
18	Relay 7 fails to closed	1.48E-01	9.65E-04	4
12	Ionization chamber 1 fails	1.03E-01	6.67E-04	5
13	Ionization chamber 2 fails	9.85E-02	6.41E-04	6
16	Comparator 1 fails	5.94E-02	3.86E-04	7
10	Amplifier 1 fails	5.13E-02	3.33E-04	8
11	Amplifier 2 fails	4.93E-02	3.20E-04	9
4	Relay 1 fails to close	5.13E-03	3.33E-05	10
5	Relay 2 fails to close	5.13E-03	3.33E-05	
6	Relay 3 fails to close	5.13E-03	3.33E-05	
14	Comparator supply 1 fails	5.13E-03	3.33E-05	
7	Relay 4 fails to close	4.93E-03	3.20E-05	11
8	Relay 5 fails to close	4.93E-03	3.20E-05	
9	Relay 6 fails to close	4.93E-03	3.20E-05	
15	Comparator supply 2 fails	4.93E-03	3.20E-05	
19	Relay 8 fails to closed	4.93E-03	3.20E-05	
17	Comparator 2 fails	1.97E-03	1.28E-05	12

Event		FV	RRW	Ranking
1	Excitor fails	3.08E-01	9.39E-03	1
$\overline{4}$	Relay 1 closed as required	2.08E-01	8.21E-03	2
$\overline{5}$	Relay 2 closed as required	2.08E-01	8.21E-03	
$\overline{6}$	Relay 3 closed as required	2.08E-01	8.21E-03	
$\overline{10}$	Amplifier 1 works	2.08E-01	8.21E-03	
$\overline{12}$	Ionization chamber 1 works	2.08E-01	8.21E-03	
$\overline{14}$	Comparator supply 1 works	2.08E-01	8.21E-03	
16	Comparator 1 fails	2.08E-01	8.21E-03	
18	Relay 7 fails to closed	2.08E-01	8.21E-03	
7	Relay 4 fails to close	1.59E-01	7.72E-03	3
8	Relay 5 fails to close	1.59E-01	7.72E-03	
9	Relay 6 fails to close	1.59E-01	7.72E-03	
19	Relay 8 fails to closed	1.59E-01	7.72E-03	
15	Comparator supply 2 fails	1.58E-01	7.72E-03	
2	DC motor fails	1.54E-01	7.68E-03	
3	Control rod is stuck	1.54E-01	7.68E-03	
12	Ionization chamber 1 fails	1.05E-01	7.26E-03	4
13	Ionization chamber 2 fails	1.01E-01	7.23E-03	5
10	Amplifier 1 fails	5.31E-02	6.86E-03	6
11	Amplifier 2 fails	2.12E-02	6.64E-03	7
4	Relay 1 fails to close	5.36E-03	6.54E-03	8
5	Relay 2 fails to close	5.36E-03	6.54E-03	
6	Relay 3 fails to close	5.36E-03	6.54E-03	
14	Comparator supply 1 fails	5.36E-03	6.54E-03	
17	Comparator 2 fails	1.45E-03	6.51E-03	9

Table 5.19: Importance Rankings Provided by Risk Significant Measures

Event		BM	Ranking
2	DC motor fails	9.98E-01	1
3	Control rod is stuck	9.98E-01	
1	Excitor fails	9.97E-01	2
18	Relay 7 fails to closed	9.66E-01	3
16	Comparator 1 fails	9.65E-01	4
12	Ionization chamber 1 fails	3.40E-02	5
10	Amplifier 1 fails	3.37E-02	6
4	Relay 1 fails to close	3.34E-02	7
5	Relay 2 fails to close	3.34E-02	
6	Relay 3 fails to close	3.34E-02	
14	Comparator supply 1 fails	3.34E-02	
13	Ionization chamber 2 fails	3.27E-02	8
11	Amplifier 2 fails	3.23E-02	9
7	Relay 4 fails to close	3.21E-02	10
8	Relay 5 fails to close	3.21E-02	
9	Relay 6 fails to close	3.21E-02	
15	Comparator supply 2 fails	3.21E-02	
19	Relay 8 fails to closed	3.21E-02	
17	Comparator 2 fails	3.20E-02	11
$\bar{12}$	Ionization chamber 1 works	1.33E-03	12
$\bar{10}$	Amplifier 1 works	1.32E-03	13
$\bar{4}$	Relay 1 closed as required	1.31E-03	14
$\bar{5}$	Relay 2 closed as required	1.31E-03	
$\bar{6}$	Relay 3 closed as required	1.31E-03	
$\bar{14}$	Comparator supply 1 works	1.31E-03	

Event		RA	CP	RAW	Ranking
1	Excitor fails	9.94E-01	1.00E+00	1.54E+02	1
2	DC motor fails	9.94E-01	1.00E+00	1.54E+02	
3	Control rod is stuck	9.94E-01	1.00E+00	1.54E+02	
16	Comparator 1 fails	9.60E-01	9.67E-01	1.49E+02	2
18	Relay 7 fails to closed	9.60E-01	9.67E-01	1.49E+02	
4	Relay 1 fails to close	2.84E-02	3.49E-02	5.37E+00	3
5	Relay 2 fails to close	2.84E-02	3.49E-02	5.37E+00	
6	Relay 3 fails to close	2.84E-02	3.49E-02	5.37E+00	
10	Amplifier 1 fails	2.84E-02	3.49E-02	5.37E+00	
12	Ionization chamber 1 fails	2.84E-02	3.49E-02	5.37E+00	
14	Comparator supply 1 fails	2.84E-02	3.49E-02	5.37E+00	
7	Relay 4 fails to close	2.70E-02	3.35E-02	5.15E+00	4
8	Relay 5 fails to close	2.70E-02	3.35E-02	5.15E+00	
9	Relay 6 fails to close	2.70E-02	3.35E-02	5.15E+00	
11	Amplifier 2 fails	2.70E-02	3.35E-02	5.15E+00	
13	Ionization chamber 2 fails	2.70E-02	3.35E-02	5.15E+00	
15	Comparator supply 2 fails	2.70E-02	3.35E-02	5.15E+00	
17	Comparator 2 fails	2.70E-02	3.35E-02	5.15E+00	
19	Relay 8 fails to closed	2.70E-02	3.35E-02	5.15E+00	
$\bar{12}$	Ionization chamber 1 works	-6.10E-03	3.97E-04	6.10E-02	5
$\bar{10}$	Amplifier 1 works	-6.11E-03	3.90E-04	6.00E-02	6
$\bar{4}$	Relay 1 closed as required	-6.11E-03	3.87E-04	5.96E-02	7
$\bar{5}$	Relay 2 closed as required	-6.11E-03	3.87E-04	5.96E-02	
$\bar{6}$	Relay 3 closed as required	-6.11E-03	3.87E-04	5.96E-02	
$\bar{14}$	Comparator supply 1 works	-6.11E-03	3.87E-04	5.96E-02	

Table 5.20: Importance Rankings Provided by Safety Significant Measures

Table 5.19 shows that CIF and IP provide the same rankings while the rankings provided by FV and RRW are identical. Both rankings put Event 1 to top priority as it not only corresponds with the top event directly but also has a relatively high unavailability comparing to Event 2 and 3 which are in the same status in the fault tree with Event 1. This has reflected that risk significant measures are more influenced by the basic event probabilities than safety significant measures. The two are somewhat different as they FV and RRW tend to compare the importance of minimal cut sets or prime implicant sets. For example, Event 16 and 18 has the same priority with the 6 non-coherent events as they exist in the same prime implicant sets with them.

The rankings provided by risk significant measures all put the 6 non-coherent events on the second place, which means relay 1, 2, 3, amplifier 1, Ionization Chamber 1 and Comparator Supply 1 should be checked to know whether or not the system failure is caused by the component at working state. For the sake of corrective maintenance, each of them should be simulated as failed before checking on the other components.

The safety significant measures RA, CP and RAW give identical ranking results in Table 5.20. It can be seen that the Event 1, 2 and 3 have the highest ranking, thus the lowest defense-in-depth. Every effort should be made to avoid failure of the excitor or the DC motor to fail, or the control rod may be stuck.

All the safety significant measures put the non-coherent basic events at the bottom of the list. This is expected since when the corresponding components function, the system performs the best. However, the ranking provided by BM is different due to the nature of BM itself, which is not appropriate for the sake of preventive maintenance. For example, according to the ranking provided by BM, the excitor should be checked after the DC motor and control rod, while the excitor has a higher failure probability than the other two.

The ranking results given by RA, CP and RAW have generated an optimum sequence for preventive maintenance. The ranking has reflected that Event 1, 2 and 3 are at the top priority as any of them is associated with the top event. Event 16 and 18 are at second place before all the non-coherent events as they exist in the same prime implicant sets with the non-coherent events which often have relatively high probabilities.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The PSA methodology in the application of risk-informed maintenance is proposed in this thesis. The risk importance measures (RIMs) derived from FTA are utilized to provide sufficient information about existing and potential weak links of the overall system so that appropriate maintenance decisions can be made.

The importance analysis of non-coherent systems is rather limited as the majority of RIMs that have been developed can only be used to analyze the coherent fault trees. In this thesis, various RIMs (Birnbaum's Measure, Criticality Importance Factor, Improvement Potential, Fussell-Vesely Measure, Risk Achievement, Conditional Probability, Risk Achievement Worth and Risk Reduction Worth) are investigated and extended to non-coherent forms. The feasibility of the extension are proved and presented throughout the analysis and applications.

On the other hand, RIMs are classified with respect to risk significance and safety significance, which serve for corrective and preventive maintenance, respectively.

As stated, different maintenance strategies have different purposes and advantages. Compared to corrective maintenance, preventive maintenance may not be as practical to be conducted in slow-aged systems; whereas it is the other way around in a system with high

failure rate. However, in the application of FTA in non-coherent systems, preventive maintenance seems to be more reasonable choice, which has been reflected by the results from the theoretical analysis.

6.2 Future Work

FTA is only a part of PSA techniques in risk-informed maintenance. To gain insights into the dependence of subsystems within the safety systems, common cause failure (CCF), human reliability, uncertainty analysis and many other techniques should be used in the overall framework. In this thesis, RIMs are categorized with respect to risk and safety significance. However, they need to be specifically categorized into different types of maintenance tasks or different phases of maintenance activities, through further investigation.

The uncertainty in probability of the basic event makes it difficult to rank the SSCs with respect to risk and safety significance. Even though the uncertainty has relatively small effects on the applications that requires categorization of SSCs [19], it should be considered as a factor in the integrated decision making process, particularly when the uncertainty is relatively larger.

As stated, FTAs in the application of non-coherent systems are rather limited, and there are difficulties in analyzing the complex fault trees generated by large projects. The sequence provided by RIMs for non-coherent systems may not be the best option in practice because it only considers the mathematical characteristics of elements, but not their practical diagnosis and repair conditions, which is why different information from operations should be taken into consideration as well. Although the state-of-the-art software programs such as FTAP has relatively ideal algorithm to aid the calculation of prime implicant sets [63], most

of the RIMs for non-coherent systems cannot be assessed with computers. A computer aided method needs to be developed in the future for the importance analysis in the application of non-coherent systems.

Bibliography

[1] I.B.Wall, J.J.Haugh, and D.H.Worlege, "Recent Applications of PSA for Managing Nuclear Power Plant Safety", *Progress In Nuclear Energy*, vol. 39, pp. 367-425, 2001.

[2] F.R.Farmer, Siting Criteria – A New Approach, Symposium On the Containment and Siting of Nuclear Power Reactors, *International Atomic Energy Agency*, Vienna, Austria, 1967.

[3] I.B.Wall, Probabilistic Assessment of Risk for Reactor Design and Siting, *Trans. of American Nuclear Society*, 1969.

[4] H.J.Otway and R.C.Erdmann, Reactor Siting and Design from a Risk Viewpoint, *Nuclear Engineering & Design*, pp. 365-376, 1970.

[5] L.Lu and J.Jiang, "Probabilistic Safety Assessment for Instrumentation and Control Systems In Nuclear Power Plants: An Overview", *Nuclear Science and Technology*, vol. 41, pp. 323-330, 2004.

[6] H.D.Brewer and K.S.Canady, "Probabilistic Safety Assessment for the Maintenance Rule at Duke Power Company", *Reliability Engineering and System Safety*, pp. 243-249, 1999.

[7] Nuclear Regulatory Commission, 10 CFR 50: Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Federal Register 56 FR 31306, 1991.

[8] Bell Telephone Lab, Launch Control Safety Study, Selection VII, vol. 1, Bell Telephone Labs, Murray Hill, NJ USA, 1961.

[9] T.Inagaki and E.J.Henley, "Probabilistic Evaluation of Prime Implicants and Top Events for Non-coherent Systems", *IEEE Trans. Rel.*, vol. R-29, pp. 361-367, 1980.

[10] J.D.Andrews and T.R.Moss, Reliability and Risk Assessment, 2nd Ed, *ASME*, 2002.

[11] E.J.Henley and H.Kumamoto, Probabilistic Risk Management, *IEEE Press*, 1991.

[12] Nuclear Regulatory Commission, Reactor Safety Study – An Assessment of Accident Risks In US Nuclear Power Plants, WASH-1400 (NUREG-75/014), 1975.

[13] R.M.Sinnamon and J.D.Andrews, "Improved Efficiency In Qualitative Fault Tree Analysis", *Quality and Reliability Engineering International*, vol. 13, pp. 293-298, 1997.

[14] J.D.Andrews and S.J.Dunnett, "Event-tree Analysis Using Binary Decision Diagrams", *IEEE Transactions On Reliability*, vol. 49, pp. 230-237, 2000.

[15] R.J.Tocci, N.S.Widmer, and G.L.Moss, Digital Systems: Principles and Applications, 10th Ed, Pearson Education, Inc. 2007.

[16] J. Fussell, "How to Hand Calculate System Reliability Characteristics", *IEEE Trans. Rel.*, Vol. R-24, pp. 169-174, 1975.

[17] S.Beeson, "Non-coherent Fault Tree Analysis", Doctoral Thesis, Loughborough University, UK, 2002.

[18] M.Van der Borst and H.Schoonakker, "An Overview of PSA Importance Measures", *Reliability Engineering and System Safety*, vol. 72, pp. 241-245, 2001.

[19] W.E.Vesely, "Letter to the Editor: Supplemental Viewpoints on the Use of Importance Measures In Risk-Informed Regulatory Applications", *Reliability Engineering & System Safety, Reliability Engineering & System Safety*, vol. 60, pp. 257-259, 1998.

[20] J.D.Andrews, "To Not or Not to Not", *In Proc. Int. System Safety Conf.*, Sept., pp. 267-275, 2000.

[21] S.Beeson and J.D.Andrews, "Importance Measures for Non-coherent-system Analysis", *IEEE Transactions on Reliability*, Vol. 52, pp301-310, 2003.

[22] T.L.Chu and G.Apostolakis, "Methods for Probabilistic Analysis of Noncoherent Fault Trees", IEEE Trans. Reliability, vol. R-29, pp. 354-360, 1980.

[23] C.J.Walsh, "Resource Mobilization and Citizen Protest In Communities Around Three Mile Island", Social Problems, vol. 29, No. 1, pp. 1-21, 1981.

[24] Nuclear Regulatory Commission, Fact Sheet On the Three Mile Island Accident, Retrieved 2008.

[25] J.S.Walker, Three Mile Island: A Nuclear Crisis In Historical Perspective. Berkeley: University of California Press, 2004.

[26] Group Aralia, "Computation of Prime Implicants of a Fault Tree within Aralia", *Proceedings of the European Safety and Reliability Association Conference*, pp. 190-202, 1995.

[27] J.D.Andrews, "The Use of Not Logic In Fault Tree Analysis", *Qual. Reliab. Engng. Int. 2001*, vol.17, pp. 143-150, 2001.

[28] C.G.Vassiliadis and E.N.Pistikopiulos, "Maintenance Scheduling and Process Optimization Under Uncertainty", *Computers and Chemical Engineering 25*, pp. 217-136, 2000.

[29] S.Nakajima and B.S.Blanchard, TPM Development Program: Implementing Total Productive Maintenance, *Cambridge: Productivity Press*, 1989.

[30] B.S.Dhillion, Engineering Maintenance: A Modern Approach, *New York: CRC Press*, 2002.

[31] J.Moubray, Reliability Centred Maintenance, 2nd Edition, *Oxford: Butterworth Hernemann*, 1997.

[32] M.Rausand, "Reliability Centered Maintenance", *Reliability Engineering and System Safety 60*, pp. 121-132, 1998.

[33] F.S.Nowlan and H.F.Heap, "Reliability-Centred Maintenance, Report Number AD-A066579", United States Department of Defense, 1978.

[34] G.Abdul-Nour, H.Beaudoin, P.Ouellet, R.Rochette, and S.Lambert, "A Reliability Based Maintenance Policy: A Case Study, Computers and Industrial Engineering", vol. 35, Issue: 3-4, pp. 591-594, 1998.

[35] M.Reinhart, "Risk-informed Decision Making: A Key In Advanced Safety Assessment", *International Atomic Energy Agency, Proceedings of ICAPP*, Nice, France, 2007.

[36] A.C.Kadak and T.Matsuo, "The Nuclear Industry's Transition to Risk-informed Regulation and Operation In the United States", *Reliability Engineering and System Safety 92,* pp.609-618, 2007.

[37] Nuclear Regulatory Commission, Risk Assessment Review Group Report, NUREG CR-0400, 1978.

[38] Nuclear Regulatory Commission, Requirements Memorandom, Staff Actions Regarding Risk Assessment Review Group Report, 1979.

[39] P.Mauger and A.D.Chambardel, "Optimizing Maintenance through Probabilistic Safety Assessment In Order to Improve Safety", *Proc. of the International Conference On Advances In Operational Safety of Nuclear Power Plants*, IAEA-CN-61/30, 1995.

[40] Z.W.Birnbaum, "On the Importance of Different Components In a Multi-component System" Multivariate Analysis II, PR Krishnaiah, Academic Press, 1969.

[41] E.Borgonovo and G.E.Apostolakis, "A New Importance Measure for Risk-informed Decision Making", *Reliability Engineering and System Safety*, vol. 72, pp. 193-212, 2001.

[42] L.Xing, "Maintenance-Oriented Fault Tree Analysis of Component Importance," *Reliability and Maintainability Annual Symposium*, pp. 26-29, 2004.

[43] G.Levitin, L.Podofillini, and E.Zio, "Generalized Importance Measures for Multi-state Elements Based On Performance Level Restrictions", *Reliability Engineering and Safety Systems*, vol. 82, pp. 287-98, 2003.

[44] G.Vinod, H.S.Kushwaha, A.K.Verma, and A.Srividya, "Importance Measures In Ranking Piping Components for Risk Informed In-service Inspection", *Reliability Engineering and Safety Systems*, vol. 80, pp. 107-13, 2003.

[45] M.C.Cheok, G.W.Parry, and R.R.Sherry, "Use of Importance Measures In Risk-informed Regulatory Applications", *Reliability Engineering and System Safety*, vol. 60, pp. 213-26, 1998.

[46] R.M.Sinnamon and J.D.Andrews, "Improved Accuracy In Quantitative Fault Tress Analysis", *Quality and Reliability Engineering International*, vol. 13, pp. 285-292, 1997.

[47] I.C.Gauld and J.C.Ryman, Nuclide Importance to Criticality Safety, Decay Heating, and Source Terms Related to Transport and Interim Storage of High-Burnup LWR Fuel, *NUREG/CR-6700*, 2000.

[48] S.Eisinger, E.Sutter, and A.B.Huseby, "Component Importance Measures In Complex Systems", *European Safety and Reliability Conference – Safety and Reliability for Managing Risk*, vol.1, pp. 679-685, 2006.

[49] T.Aven and T.E.Nkland, "On the Use of Uncertainty Importance Measures In Reliability and Risk Analysis", *Reliability Engineering and System Safety* 2007, vol. 95, pp. 127-133, 2007.

[50] W.E.Vesely, M.Belhadj and J.T.Rezos, "PRA Importance Measures for Maintenance Prioritization Applications", *Reliability Engineering and Systems Safety*, Vol. 43, pp. 307-318, 1994.

[51] S.Martorell, V.Serradell, and G.Verdu, "Safety-related Equipment Prioritization for Reliability Centered Maintenance Purposes Based On a plant Specific Level 1 PSA", *Reliability Engineering and System Safety*, vol. 52, pp. 35-44, 1996.

[52] A.Papoulis, Probability, Random Variables, and Stochastic Process, 3rd Edition, McGraw-Hill Series In Electrical Engineering, 1991.

[53] S.Koukhar and B.Vinnikov, "Application of PSA Methodology for Optimization of Repairs, Maintenance and Tests Modes of the Equipment of NPPs with RBMK Types Reactors", *Societe Francaise d'Energie Nucleaire* -

International Congress on Advances in Nuclear Power Plants - ICAPP 2007, "The Nuclear Renaissance at Work", vol. 4, pp. 2605-2609, 2008.

[54] S.Beeson and J.D.Andrews, "Birnbaum's Measure of Component Importance for Non-coherent Systems", *IEEE Transactions on Reliability*, vol. 52, pp. 213-219.

[55] P.S.Jackson, "On the s-Importance of Elements and Prime Implicants of Non-Coherent Systems," *IEEE Transactions On Reliability*, vol. 52, 2003.

[56] S.Contini, G.G.M. Cojazzi, and G.Renda, "On the Use of Non-coherent Fault Trees In Safety and Security Studies", *Reliability Engineering and System Safety*, vol. 93, pp. 1886-1895, 2008.

[57] L.Lu and J.Jiang, "Joint Failure Importance for Noncoherent Fault Trees", *IEEE Transactions on Reliability*, vol. 56, pp. 435-443, 2007.

[58] R.Billinton and R.N.Allan, Reliability Evaluation of Engineering Systems: Concepts and Techniques, New York: Plenum Press, 1992.

[59] M.C.Cheok, G.W.Parry, and R.R.Sherry, "Use of Importance Measures In Risk-informed Regulatory Applications", *Reliability Engineering and System Safety*, Issue. 60, pp. 213-226, 1998.

[60] G.Bereznai, "Nuclear Power Plant Systems and Operation Lecture" Notes, Revision 4, 2005, University of Ontario Institute of Technology, 2005

[61] Q.Zhang and Q.Mei, "Reliability Analysis for a Real Non-coherent System", *IEEE Transactions On Reliability*, vol. 36, pp. 436-439, 1987.

[62] Q.Zhang, "Some Theorem and Calculation Methods of the System Reliability and Their Applications In Reactor Systems". MS Thesis, In Chinese, Institute of Nuclear Energy Technology Tsinghua University, 1984.

[63] R.R.Willie, Computer-aided Fault Tree Aided Analysis, Operations Research Centre, University of California, 1978.

VITA

Name	Ye Tao
Place of Birth	Jiangsu, China
Year of Birth	1984
Post-secondary Education and Degrees	University of Windsor Windsor, ON, Canada 2003-2007 B.A.Sc
Related Work Experience	Teaching Assistant/Research Assistant University of Ontario Institute of Technology Oshawa, ON, Canada 2008-2010
	Intern- Engineer Volkswagen Co. – Product Engineering Division Shanghai, China 2005-2006

Publications:

Ye Tao and Lixuan Lu (2010). *Risk Importance Measures for Maintenance in Non-coherent Systems*. In Proceedings of the 2010. Proceedings of the 18th International Conference on Nuclear Engineering, ICONE18, May 17-21, Xi'an China.

Dan Zhang, Qi Shi and Ye Tao (2009). *Novel Design of Polysilicon Microphone with Corrugated Diaphragm*. In Proceedings of the 2009 ASME International Mechanical Engineering Congress Exposition, IMECE2009, November 13-19, 2009, Lake Buena Vista, Florida, USA.