SYSTEM HAZARD IDENTIFICATION PREDICTION PREVENTION (SHIPP) METHODOLOGY

PREDICTIVE ACCIDENT MODELING APPROACH

SAMITH RATHNAYAKA

SYSTEM HAZARD IDENTIFICATION PREDICTION PREVENTION (SHIPP) METHODOLOGY

PREDICTIVE ACCIDENT MODELING APPROACH

by

SAMITH RATHNAYAKA

A thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

MASTER OF ENGINEERING

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

May 2011

St. John's Newfoundland

ABSTRACT

A process accident occurs as a result of a sequence of events initiated by deviation in the process parameters and/or failure or malfunctioning of one or more components. Many process accidents are controlled and mitigated before they escalate to major events. Unfortunately some do go on to produce catastrophic consequences. As the size and complexity of processing facilities increase, the potential risk posed by accidents is increasing. Operational safety could be improved by giving emphasis to the prevention of incidents, rather than relying on control and mitigative measures. This method is referred to as an "inherently safer approach". To prevent major, though infrequent, event occurrence, it is important to consider accident precursors (symptoms of hazards) such as operational deviations, mishaps, and near misses, in order to prevent abnormal events at source rather than controlling or mitigating them.

The objective of this research is to present a novel methodology known as System Hazards Identification, Prediction and Prevention (SHIPP) for process accident modeling and prevention. In this methodology, a new process accident model with predictive capabilities is developed. The SHIPP is a systematic methodology to identify, evaluate, and model the accident process, thereby predicting and preventing future accidents in a process facility. In this methodology, process hazard accidents are modeled using safety barriers. The model relies on process history, accident precursor information, and accident causation modeling. The fault tree and event tree analysis techniques are used to enhance the accident model and to represent a holistic picture of the cause-consequence mechanism of the accident process. Quantitative analysis has two aspects: updating and

prediction. The model is able to capture the process operational behaviour, and update the accident likelihood using the Bayesian updating mechanism. The predictive model forecasts the probability of a number of abnormal events occurring in the next time interval. Application of this methodology is demonstrated by a case study. The quantitative results demonstrate that the probabilities of abnormal events dramatically change over time as new information is observed, and the adequacy and accuracy of model prediction is better in short term prediction rather than long term prediction.

Through the SHIPP methodology, qualitative and quantitative analyses provide insight to identify critical safety barriers and functions, and determine the likelihood of failure of these measures. Combining management oversight, human factor and engineering analyses, the SHIPP methodology provides a comprehensive, systematic approach to manage a process system risk.

ACKNOWLEDGEMENTS

First and foremost, I would like to express profound gratitude to my supervisors, Dr. Faisal Khan and co-supervisor Dr. Paul Amyotte, for their invaluable support, motivation, immense knowledge, encouragement, supervision and useful suggestions throughout this research work. Their moral support and continuous guidance enabled me to complete my work successfully.

Besides my advisor, I would like to thank Dr. Silvia Vargas for her continues encouragement, insightful comments and important questions. Her knowledge and guidance of technical writing help me to convert my research work to meaningful document.

I would also like to gratefully acknowledge the financial support provided by Natural Sciences and Engineering Research Council (NSERC) through a Strategic Grant.

I thank my fellow lab mates in safety and risk engineering group: Premkumar Thodi, Refaul Ferdous, Nima Khakzad, Mohammad Dadashzadeh, Omid Zadakbar, Alireza Noroozi, Berenice Zakeri and Chandrasekhar Gogo for the stimulating discussions, for the valuable ideas, for the encouragements, for the helps in every means and for all the fun we have had in the last two years. Also I thank my Sri Lankan friends in Memorial University: Awantha Jayasiri, Dilhan Balage, Dilan Amarasinghe, Gayan Gamage, Migara Liyanage, Punayama Jayasinghe and Neel Chandrasekara for supporting and encouraging me in many ways.

I would like to thank my family members, especially my wife, Manoja Munasinghe, my mother and my aunty for supporting and encouraging me to pursue this degree. I thank

them for their love, their support, and their confidence throughout the whole career. As a single mother, my mom, and aunty have always put education as a first priority in my life, and raised me to set high goals for myself. They taught me to value honesty, courage, and humility above all other virtues.

Table of Contents

List of Tables

List of Figures

List of Symbols and Abbreviations

BN	Bayesian Network
DC&EMB	Damage Control and Emergency Management Barrier
DPB	Dispersion Prevention Barrier
EPB	Escalation Prevention Barrier
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Studies
HFB	Human Factor Barrier
HOF	Human and Organizational Factors
ILCI	International Loss Causation Institute
IPB	Ignition Prevention Barrier
MCHE	Main Cryogenic Heat Exchanger
M&OB	Management and Organizational Barrier
MORT	Management and Oversight Risk Tree
PHA	Preliminary Hazard Analysis
RPB	Release Prevention Barrier
SCAT	Systematic Cause Analysis Techniques
SHIPP	System Hazard Identification, Prediction and Prevention

$N_{f,i}$	The number of potential failure events
$N_{f,i}$	The number of potential failure events
y_{t+1}	The number of abnormal events in the next time interval
y	The number of abnormal events
$p(y / data)$	The posterior distribution
$p(y / \lambda)$	Sampling distribution
$p(c_k / data)$	The updated occurrence probability
α	Shape parameter
β	Scale parameter
λ	Rate of occurrence for an abnormal event

List of Appendices

Chapter 1

INTRODUCTION

1.1 Accident Modeling in Process Industry

The process industry is a highly complex technological system containing large quantities of hazardous chemicals. The increasing complexity of system elements such as people, equipment, the operating environment, procedures, software and hardware systems and their interactions are leading to potentially disastrous failure modes. Over the years, notable accidents such as the Bhopal toxic gas release disaster (Eckerman, 2005), the Piper Alpha tragedy (Petrie, 1989), the Nypro factory explosion at Flixborough (Kletz, 2001), BP's Texas city refinery explosion (CSB, 2007), the Imperial sugar refinery dust explosion (CSB, 2009) and most recent BP's Deepwater Horizon offshore drilling rig explosion and oil spill (BP, 2010) are examples of complex process systems failures that led to serious loss of human lives and materials. Not only catastrophic or critical accidents but also events such as incidents and mishaps are financially costly, interrupt the production flow and cause human injuries. Therefore, prevention of these events is of paramount important.

To achieve this goal the engineers must incorporate system safety into the system life cycle. The different hazard and risk management methodologies have been used to establish system safety for the particular processing facility. The overall purpose is to identify the hazards, evaluate them, eliminate or control them and mitigate the residual risk during the phases such as details design and operational stage.

A succinct definition for ***hazard*** is that any source of potential damage, harm or adverse health effects on something or someone under certain conditions at work place. Hazards in process industry can be categorized into three types: (1) occupational hazard, (2) process hazard and (3) external hazard. It is observed that the majority of critical accidents, such as fire, explosion and toxic release, are initiated by flammable and toxic release and process upsets, which are known as process hazards. Therefore, the current work focuses on the process hazard accidents. Process accidents are not usually caused by a single failure or error. They are a result of sequence of events initiated by the deviation of process parameters and/or failures or malfunctioning of one or more components. The accident process usually follows three steps: (1) Initiation (the event where an accident begins), (2) Propagation (the events or events that maintain or expand the accident) and (3) Termination (the events or events where the accidents are stopped or diminished in size) (Crowl and Louvar, 2002). It is important to view an accident as a sequence of event because, in theory, each individual propagating event represents an opportunity to terminate the accident sequence or to lessen the severity of its ultimate outcome. Accident models can help to understand the significance of potential accident sequences associated with a process hazards. This understanding and knowledge lead to identification of ways to prevent or reduce the frequency and severity of consequences of potential process accidents, thus improving the safety of a process facility.

1.1.1 Accident Models

The accident model is a theoretical framework which characterizes how and why an accident occurs and illustrates the relation between causes and consequences. Further,

such models define, structure and summarize all relevant data in a meaningful way. Accident models are important to collect relevant information to study and prevent accident risk and it also helps in safety-critical decision making. The effective use of accident models together with accident investigation methods is capable of analyzing accidents and providing numerical estimation of risk. It also helps to predict and prevent such occurrences in the future.

Traditional accident models use the linear notion of causality to analyze the accident process. A number of accident models and various approaches for accident modeling and analysis have been developed and described in the literature (Heinrich, 1941; Reason, 1990; Rasmussen, 1997; Attwood et al., 2006; Ren et al., 2008; Kujath et al., 2010).

The sequential nature of causality was first adopted for accident modeling by Heinrich (1941) who introduced the "Domino Theory", in which an accident is described as a chain of independent conditions or events that occurs in a particular order terminating at an injury. This model indicated that an accident can be prevented by removing any single factor from the accident sequence or through the reduction of these factors. The International Loss Control Institute has modified the "Domino Theory", developing a loss causation model (ILCI model) to evaluate how unsafe acts and conditions are initiated (Bird and Germain, 1996). The analysis begins with loss to people, property, and the environment and steps back through the sequential events that contribute to loss independently. Further, in the ILCI model, the immediate and root causes that lead to an accident are described as management deficiencies, personal and job factors and substandard acts and conditions. Further, these models explain the accident causation as a one-dimensional sequence of events and do not take into account multiple causality of the

accident process (Kjellen, 2000). Reason (1990) proposed the "Swiss cheese" model to demonstrate how human and organizational failures influence the accident process independently, taking multi-causality of the accident into consideration. Svenson's (1991) "Accident Evolution and Barrier function (AEB)" model represents the development of accidents as a sequence of events belonging either to a human/organizational system or a technical system. This type of model is commonly known as an epidemiological accident model. The main feature of this type of model is the barrier that could prevent the unexpected consequences from occurring; whereby the development of an accident process could be prevented. Attwood et al. (2006) developed a holistic, quantitative model to predict occupational accident frequency in the offshore oil and gas industry. This model has both qualitative and quantitative capabilities. Three layers; the direct layer, the corporate support layer and the external layer were introduced considering factors that lead to occupational accidents in the offshore environment. In this model, the reliability concept was used to evaluate the probability of an occupational accident under various scenarios in an asset's development cycle. The prediction capability of this model offers insight into safety improvement efforts in the offshore oil and gas industry. Ren et al. (2008) developed a methodology to model the causal relationships of offshore safety assessment focusing on human and organizational factors (HOF). The model addresses latent failures within the causal sequence of events. Similar to Swiss cheese modeling approach, five levels; root causes level, trigger event level, incidents level, accident level and consequences level were placed in sequential order to depict accident due to HOF. The model adopts the Bayesian network that is able to provide graphical representation of cause-consequence relationship and to calculate numerical values of occurrence

likelihood for each failure event. Kujath et al. (2010) has proposed a conceptual process accident model prioritizing the prevention of process accidents in an offshore environment. This model is developed using features of both sequential and epidemiological models. In this model, hydrocarbon release accidents were modeled using the safety barrier concept.

Existing accident models have their own capabilities and limitations. They vary in the areas of their application, purpose, and focus. The distinctions between the existing accident models do not imply that one is unequivocally better than others.

1.1.2 Accident Precursors Information in Process Industry

Most accidents are preceded by deviations in the normal operational process. Furthermore, many deviations are present that are not covered by current pro-active safety indicators. These deviations are characterized by a high likelihood and low perceived safety related consequences (defined as precursors) and re-occur in the operational process of the organization prior to an accident. However, these events are sometimes omitted or unnoticed by operators due to the under estimation of their adverse effects. In this work, the accident precursors (abnormal events) are classified as: (1) safe, (2) near miss, (3) mishap, (4) incident and (5) accident, considering the probabilities and degree of severities. In order to find these deviations in a real life operation and to find their underlying causes, the concepts of re-occurring deviation and operational process have to be explained in more detail.

1.2 Motivation of Research

The comprehensive study of how accidents evolve from the initiating events to their propagating effects and final consequences is vital for integrating safety into systems for accident prevention. In this aspect, accident models play an important role in accident analysis and risk management. However, the literature indicates that existing accident modeling approaches have certain limitations when modeling the accident process in order to prevent the accidents. Each accident model has its own characteristics as to the types of "causal factors" that it highlights.

In the process industry, major accidents are often initiated through errors induced by process, mechanical and operational hazards. Many traditional accident models were developed mainly focusing on human, organizational and management factors. Thus, the models focusing on process hazards are scarce. Other models have adopted a descriptive approach to analyze an accident, but they are not able to offer a predictive model which helps to guide safety related decisions. Also, available models are not able to accommodate modeling of multiple risk factors considered in process systems where interaction and inter-relationship of system elements are complex and non-linear. The literature also describes that some models have adopted a quantitative approach using historical statistics to study the existing relationship between causal factors. However, these models are unable to update the risk during the life of the process. Further limitation of quantification of existing method, models such as Management and Oversight Risk Tree (MORT), is highly complex and it is difficult to provide quantified results.

Information on accident precursors such as near miss, mishaps, incidents and accidents often termed as accident precursors are ignored, leaving worth of information behind. The

available accident models were not able to make use of this information. This information can be used in systematic manner to better learn the health of the process industry. It helps to assess the accident likelihood in the given facility, and thus, suitable preventive measurements could be taken against such occurrence.

1.3 Objectives of Research

The main objective of this research is to develop methodology that can be used to define, illustrate, analyze and improve system safety in the operational phase of process facility through accident modeling and prediction.

Based on this main objective, the following sub-objectives are developed for this work:

- To fill the knowledge gap of accident process models that have been developed focusing on process hazard accidents.
- To develop the accident process model in terms of safety barriers rather than causal factors that is capable of capturing multi-causality of accident and providing holistic view of cause-consequence mechanism.
- To develop the update mechanism to reduce the uncertainty of the probabilistic quantification by using real plant abnormal event data (accident precursor data).
- To develop predictive model by using probabilistic approach which can predict the future likelihood of the accident (number of event occurring in the next time interval). And, further, results are able to update and learn the system behavior dynamically whenever new information is observed in the system.
- To carry out a case study to test and verify the method.

Towards these objectives, the System Hazard Identification, Prediction and Prevention (SHIPP) methodology is proposed to identify process hazards, evaluate them, and model the accident sequences by means of predicting and preventing their occurrences.

1.4 Thesis Structure

The thesis comprises of six chapters. The first chapter is a brief introduction on the concept of accident modeling and prevention in process industries followed by the motivations and objectives of this research. Chapter 2 gives a broad overview on the development of accident models over the years and their significance, capabilities and limitations in the process industry safety assessment. Further, this chapter evaluates selected accident models using the several important characteristics as the literature review of this thesis. Chapter 3 gives a detailed description of the development of predictive accident modeling approach so called SHIPP methodology (System Hazard Identification, Prediction and Prevention). This includes description of methodology and steps of development of: (1) accident model, (2) generic event tree and fault tree, (3) updating mechanism and (4) predictive model. Chapter 4 presents the results of a case study conducted on a gas processing facility to validate the SHIPP methodology. This chapter illustrates accident model development and cause-consequence analysis. The updated results demonstrate that the probabilities of abnormal events dramatically change over time as new information is observed. Further this chapter discussed two different predictive models to estimate the number of abnormal event and expected time to the next abnormal event occurrence. The quantification is performed in two ways: deterministically and probabilistically. Chapter 5 demonstrates application of the SHIPP

methodology to an LNG processing facility. External validation method was used to assess the predictive model results through regression of real data gathered from the LNG facility examined. Chapter 6 concludes the study by a brief summary, conclusion and future scope of research in this area.

Chapter 2

LITERATURE REVIEW

System safety assessment is an integral part the life cycle of a project, engineering design, program, or activity either required by local or international regulation or carried out by individual(s) within particular industry. The overall purpose is to identify hazards, prevent or control them, and mitigate the residual risk. It is necessary to combine management oversight and engineering analyses to develop a systematic and comprehensive process to adequately manage the system risk (Bahr, 1997). The system safety process should be able to apply to the entire system and the primary objective is accident prevention. It could be achieved by identifying, assessing, and eliminating or controlling safety-related hazards, to acceptable levels. It is important that realistic prediction is essential of accident prevention. However, lack of concentration of accident prediction has been devoted of existing safety processes. A hazard is a condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event. Risk is an expression of the impact of an undesired event in terms of event severity and event likelihood. Therefore, throughout this process, hazards are identified, risks analyzed, assessed, prioritized, and results documented for decision-making. The continuous loop process provides for validation of decisions and evaluation for desired results and/or the need for further action. Several textbook and researchers have described the safety and risk assessment process (Turney and Pitblado, 1996; CCPS, 2008; Mannan, 2005). Typically, the system safety process comprised set of steps that provides guidelines to obtain system safety.

However, none of system safety process has been adopted accident models to identify and analysis the hazards. Accident models play a vital role in safety assessment. The accident model is a theoretical framework which characterizes what, how and why an accident occurs and illustrates the relation between causes and consequences. Further, such models define, structure, and summarize all relevant data in a meaningful way. The effective use of accident models together with accident investigation methods is capable of analyzing accidents and providing numerical estimation of causes and consequences. It also helps to predict and prevent such occurrences in the future.

Since the early 1930s, a number of accident models and various approaches for accident modeling and analysis have been developed and described in literature (Heinrich, 1941; Reason, 1990; Bird and Germain, 1996; Rasmussen, 1997; Attwood et. al., 2006; Ren, et al., 2008; Kujath et al., 2010). Accident models have its own characteristics according to their focus (causal factors), area of application and purpose. General classification and evaluation of the accident models can also be found in literature, and related works have been done by Benner (1978), Hollanagel (2004), Lehto and Salvendy (1991), Skelt (2004), and Katsakiori et al., (2009).

Process accidents result from a sequence of events initiated by deviation of process parameters, failures or malfunctioning of one or more components. Lehto and Salvendy (1991) systematically evaluated accident causation models and categorized accident model in four types: general models of the accident process, models of human error and unsafe behaviour, models of mechanic of human injury and application techniques. Linearity among the causal factors for the accident is the main aspect of general process accident models. This group is further categorized into four sub groups; sequential,

epidemiological, energy transfer and system model. These models describe the accident process dynamic focusing on causal factors such as human, product, task or environment. Hollnagel (2004) presented and discussed the need of accident models including accident barriers and a theoretical framework for characterizing how and why accidents occur. Based on search principle and analysis goal, Hollnagel (2004) distinguished accident models into three different types: sequential, epidemiological and systematic. Kjellen (2000) discussed five accident model types considering the design of modern Safety, Health and the Environment (SHE) information system. Kjellen's models are logical tree and casual sequence model (classified as general model by Lehto and Hollnagel). The other three models are process, energy and human processing information (similar term used by Lehto to describe the models focusing on the flow of information through a person while performing the task). Kjellen did not use the term "epidemiological model" directly, but the energy model has been identified as a kind of epidemiological model. Most recently, Katsakiori et al. (2009) divided accident models into three categories: sequential, human information processing and systematic (similar to terms used by Hollnagel and Lehto). Attwood et al (2006) compiled the accident models that focus on occupational accident in the offshore oil and gas sector.

The key accident causation models were selected to conduct this study and are discussed in the subsequent sections.

Heinrich's Domino Model

The sequential aspect of accident occurring was first used by Heinrich (1941) and thus "Domino Theory" was introduced. This theory describes an accident as a natural culmination of a serious of events or circumstances, which invariably occur in specific

logical order. Ancestry and social environment, fault of person, unsafe act and/or mechanical or physical hazard that leads to an accident were identified and placed in sequential order. The last block of the Domino model is injury, which is caused by the action of a preceding factor. The unsafe act and condition is the central factor or main link in the accident sequence and the removal of this factor makes propagation of hazardous events ineffective. The main contribution of Domino theory is that the accident can be prevented if this series is interpreted by elimination of one or more domino blocks. However, this model implies that the accident is the result of a single cause. But in reality, the accident is occurring due to the multiple causes. Therefore, this model was unable to represent multiple causality of the accident.

Loss Causation Model

Bird (1974) updated the Domino theory proposing loss causation model or International Loss Causation Institute (ILCI) model. In this model, management factor replaces ancestry, social environment and fault of person. Greater emphasis is placed on loss that includes harm to people, property, environment and progress. The term "accident" is replaced with "incident" to represent all possible event scenarios such as near misses and mishaps. In the loss causation model, there are five sequential blocks identified and placed in sequential manner. The model starts with lack of control followed by basic causes, immediate causes, incident and loss as shown in Figure 2.1.

Although Bird (1974) used same sequential approach as Domino theory, it is different from the Domino theory in terms of causal factors that each models are highlighted. In Domino theory, unsafe acts and conditions are only symptoms of deeper problem (Bird and Germain, 1996).

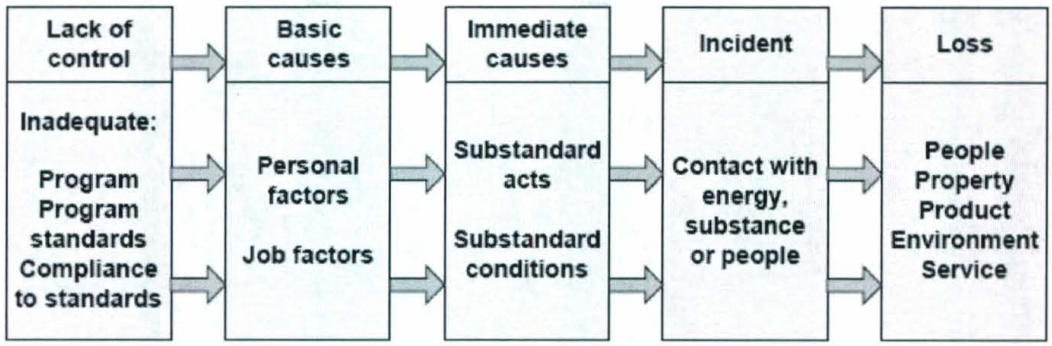

Figure 2.1: The ILCI or loss causation model (Bird and Germain, 1996)

Management and organizational factors were emphasized in the loss causation model to minimize losses. Through this type of modeling approach, the information flows to the upper management to make the decision to stop the reoccurrence at any level in the chain (Kujath, 2010). However, Domino and Loss Causation model have no clear distinction between the observable facts about accident sequences and uncertain causal relationship at personal, organizational and management levels (Kjellen, 2000).

Keltz Model

Keltz (1988) proposed a model oriented methodology for accident investigation. This methodology uses the concept of accident causation chain in which an accident is placed at top and the sequence of leading events and causes are developed beneath it (Figure 2.2). The strength of this approach is recommendations for accident prevention and mitigation as it focuses on inherent safer design by the layer of avoiding the hazard. The preventive recommendations comprised three aspects or layers: (1) immediate technical recommendations, (2) avoiding the hazard and (3) improving the management system. The model suggested possible technical, human and management preventive strategies.

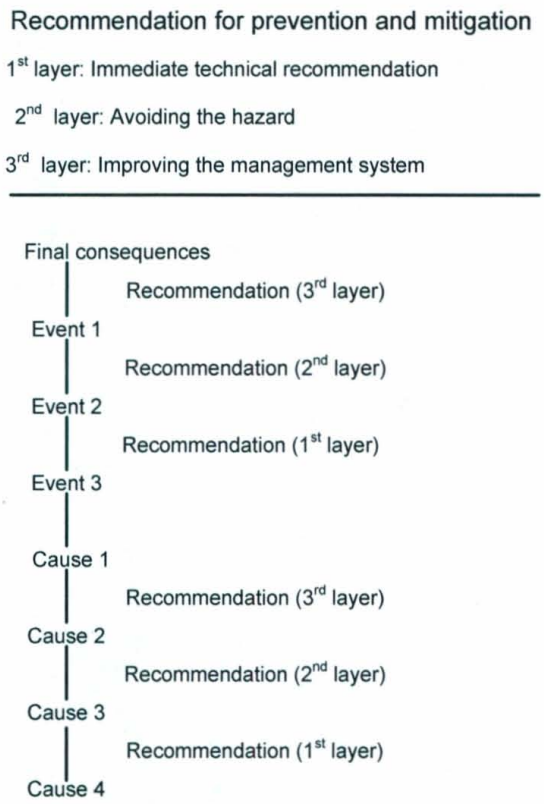

Figure 2.2: Keltz model of accident process (Khan and Abbasi, 1999)

Management Oversight and Risk Tree (MORT)

The MORT model was developed by Johnson in 1973 to analyze the system and identify the relationship between the management and organizational factors and plant operations (Johnson, 1980; Bhar, 1997). MORT gives an idealized safety system represented as a logic tree, which contains specific control and general management factors. The top event of the logic tree is injury, damage or system loss. Evaluating control and management factors are used to identify the causal factors leading to the top event (Skelt, 2004). MORT provides a large graphical checklist to help investigating the facts and looking for

evidence. It permits a large number of problems to be identified, and it prompts the investigator to look for direct causes and for causal contribution at the management and organizational levels.

Swiss cheese Model

Reason (1990) proposed the Swiss cheese model to demonstrate how human and organizational failures influence the accident process independently taking multi causality of accident into consideration. The Swiss cheese model is used in many industries, especially aviation industry, to prevent accidents due to human errors. In the Swiss cheese model, four successive cheese slices are placed on sequential manner representing safety barriers relevant to particular hazards, and the holes represent the latent errors. The cheese slices behave as the defensive barriers against the accidents or incidents, and the holes are subjected to change according to the failure types. When the holes are lined up all barriers failed; hence an accident will occur. The holes in the first slice represent the latent failures, such as poor designs, lack of supervision, undetected manufacturing defects, defect or maintenance failures, lack of training and poor work procedures. Unsafe acts are mostly situated in the last slices, while latent conditions are the holes throughout the cheese.

Daryl's Occupational Accident Model

Attwood et al. (2006) proposed an accident model to predict the accident frequency and associated cost of occupational accidents in the offshore oil and gas industry. Factors affecting occupational accidents in oil and gas industries were identified and their interrelationship determined to formulate this model. According to their hierarchical

effect in the accident, the factors are divided into three layers: external, corporate and direct.

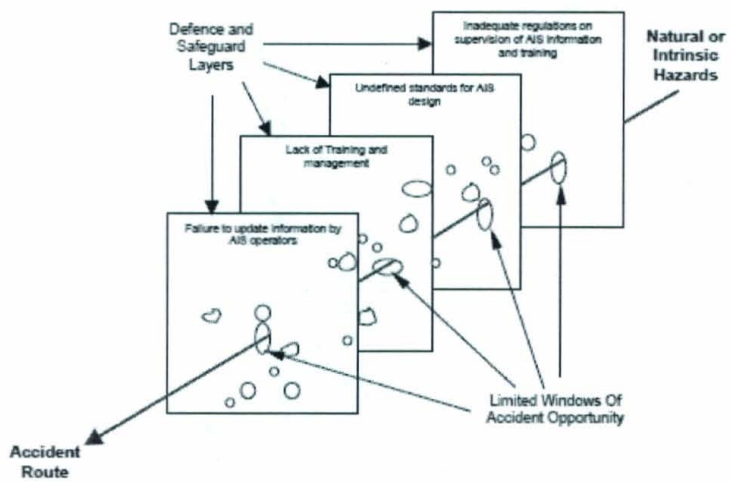

Figure 2.3: The Swiss cheese model of human error (adopted from generic model of Reason, 1990, 1996)

Each layer contains several elements. An arrangement of these elements in the accident model is shown in Figure 2.4.

This model describes an influence of external elements on corporate actions which in turn influence the direct accident process. It has also quantified influence of these factors using quantitative data derived from safety experts' survey. Similarities of physical engineering system and corporate safety programme are utilized in developing the model. Based on this hypothesis, the model is rearranged using the reliability network for quantification. Furthermore, this model uses 'influence coefficients' to quantify the influence at the external-corporate and corporate-direct interfaces.

The model predicts a safety result that enhances individual elements of the direct, corporate or external layers. It also predicts financial rewards and penalties associated with changes in various safety factors. This model is capable of evaluating relative probabilities of occupational accidents under various scenarios or during stages in an asset's deployment cycle.

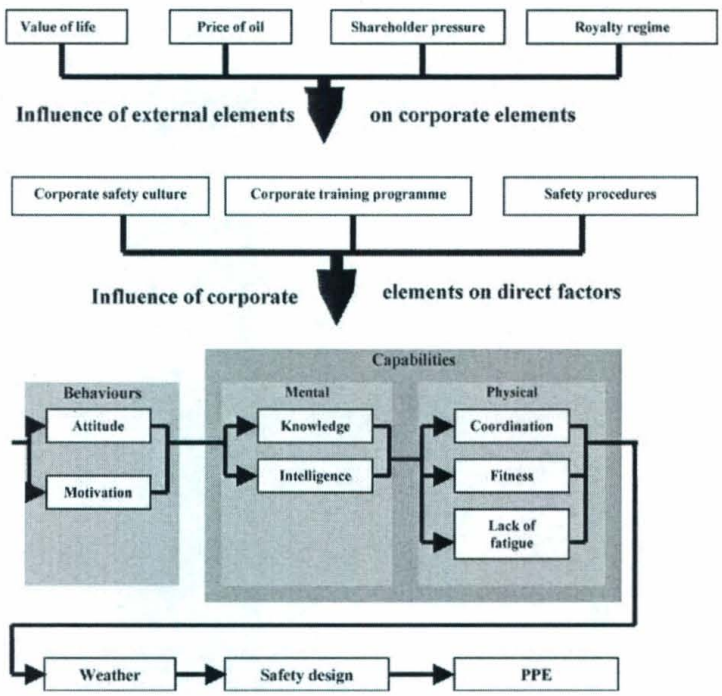

Figure 2.4: Element arrangement of model to predict occupational accidents (Attwood et al., 2006)

Ren's Human and Organizational Factors (HOFs) Model

Ren, et al. (2008) proposed a methodology to model the accidents which are caused by technical and human and organizational malfunctions. Based on the Swiss cheese model, a conceptual model is proposed to represent the latent failures due to human and organizational factors within the causal sequence of accident process. This Ren's HOF

model uses five levels: consequence, accident, incident, trigger event and root cause. Each level provides different cause of contributory to model. The arrangement of each level in the model is shown in Figure 2.5.

The HOFs model adopts Bayesian Network (BN) to enhance the graphical demonstration of causal interrelationship and to compute numerical values of occurrence likelihood of each failure levels. The advantage of this model is its ability for monitoring how safety system changes when information flows forward and backward within the network.

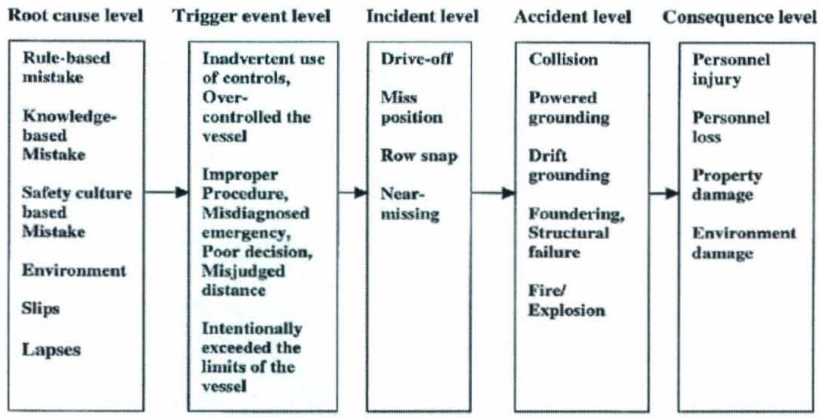

Figure 2.5: Conceptual model for HOFs (Ren et al., 2008)

Kujath's Conceptual Offshore Oil and Gas Process Accident Model

The conceptual accident prevention model highlights the vulnerabilities of an oil and gas (O&G) operation and provides appropriate guidelines to minimize the hazards and associated accidents before occurrence (Kujath et al., 2010).

The safety barriers are identified to prevent, control or mitigate the accident process due to hydrocarbon release. The barriers are placed sequentially similar to Swiss cheese and loss causation models (Figure 2.6). The model construction adopts safety barrier concept rather than causal factor, which is used in most of existing accident modeling approaches.

Kujath's model is flexible as identified safety barriers can be substituted with other appropriate barriers for the specific facility. The safety barriers in the model have been further branched to identify safety barrier sub-elements. This model is rather qualitative than quantitative.

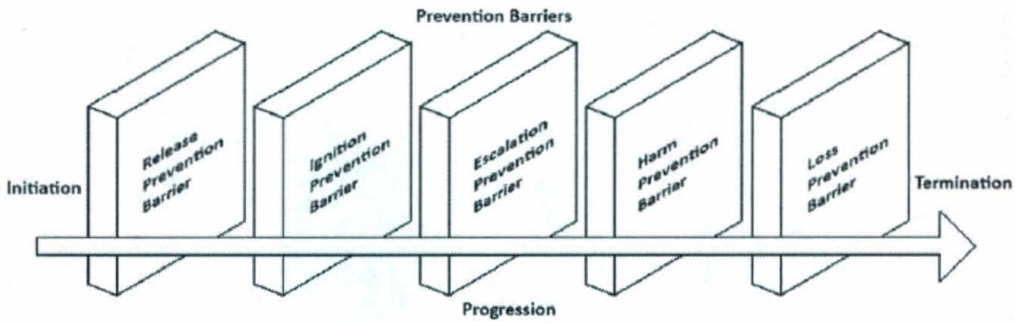

Figure 2.6: The conceptual offshore oil and gas accident model (Kujath et al., 2010)

2.1 Overview of Accident Analysis Techniques

Accident models are theoretical frameworks which explain the accident causation mechanism and it helps to identify and analyze the potential future outcomes. However, accident models alone do not provide sufficient information to evaluate and prevent accidents. Accident analysis techniques are systematic tools that evaluate causal and consequences qualitatively and quantitatively. Therefore, accident model with analysis technique or combination of techniques provide holistic and quantitative information of cause-consequence relationship. Particular accident analysis technique or techniques are not always necessarily linked to specific accident model (Katsakiori et al, 2009). In this study, four key analysis techniques will be discussed.

Fault Tree (FT) and Event Tree (ET) Analyses

Fault tree and event tree analyses have been used extensively in probabilistic risk assessment. Both investigations methods are graphical design techniques (tree-network design) for qualitative and quantitative assessment. Fault tree determines accident causes. The approach is top-down in which analysis begins with possible accident (top-event) and propagates downward to basic events at the bottom of tree (Skelt, 2004; Lehto and Salvendy, 1991). The logical arrangement to describe basic events propagation up to top-event are represented with logical "AND" and "OR" gates. The qualitative structure of how accident occurs can be analyzed using cut set analysis. Minimal cut set is the smallest number of events that must occur to lead top-event. Furthermore, without any quantification, minimal cut set can imply the safety of the system (Woodward and Pitblado, 2010). The fault tree analysis determines top-event frequency and intermediate frequencies based on basic events data.

Event tree is used to analyze event sequence and outcomes from a specific initiating event. It demonstrates paths by which consequences occur and how various safety barriers or safety functions can prevent or mitigate the event sequence. The event sequence propagates to specific consequence with failure or success of specific safety barrier/function. Event tree estimates frequencies of consequences of each accident scenario; thus, risk is estimated. Decisions are made based on the risk estimated. An accident investigation carried out combining FT and ET is known as bow-tie analysis (Dianous and Fievez, 2006). Appropriate safety barriers are identified and applied on bow-tie diagram to prevent or mitigate accidents.

Reliability Block Diagram (RBD)

Reliability Block Diagram (RBD) is a symbolic analytical logic technique that can be applied to analyze system reliability and related characteristics. It provides an alternate to fault tree analysis. Reliability block diagram deals with reliability of component or system. Nodes or blocks represent the system components, whereas lines describe connections between the components. The logical flow of network diagram starts from an input node and flow through intermediate nodes, which has parallel or/and serial arrangements, to an output node. Since reliability block diagram often correspond to physical arrangement of components in the system, it can be successfully applied to a particular system to study the probabilistic events. The model proposed by Attwood et al. (2006) has used reliability block diagram to model the occupational accident process for offshore platforms. In addition to reliability model, Markov method is used for assessing time depending behaviour of many dynamic systems as a reliability modeling technique. It is capable of capturing statistical dependencies between failure events in complex systems (Bucci et al., 2008).

Bayesian Network (BN)

A Bayesian Network (BN) has been recognized as modeling and inference tool for problems involving high degree of uncertainty (Pearl, 1988). BN is used in many different fields such as medical diagnosis (Heckerman, 1990; Spiegelhalter et al, 1989), map learning and vision (Dean, 1990; Levitt et al., 1989), structural system reliability assessment (Mahadevan et al., 2001) and decision making strategies (Jensen, 1996). Recently, it has been used in risk assessment and accident investigation because of its powerful and comprehensive qualitative and quantitative abilities (Castillo et al, 1999;

Kang and Golay, 1999; Kim and Seong, 2006; Ren et al., 2008). BN provides probabilistic graphical model, which describes cause-consequence relationship among various factors and quantifies their relationship in terms of conditional and joint probabilities. It is able to perform adductive (diagnostic) reasoning, deductive (causal) reasoning as well as inter-causal reasoning among a number of variables or factors under high level of uncertainty. This helps to monitor system safety and changes when safety critical information flows forward and backward within the causal network (Ren et al., 2008). BN is able to update as new observations are incorporated into system, and perform prediction of possible future observation, even though data is incomplete or missing (Heckerman and Breese, 1996; Heckerman, 1997). Dynamic Bayesian Network (DBN) is used to model temporal dependencies and applicable to the practical process environment which is more complex and dynamic.

2.2 Accident Models Evaluation

This section discusses the evaluation of key accident models and novelty of the proposed accident model to process hazards accidents in O&G industries. The following seven characteristics are chosen based on literature (Wagenaar and Schrier, 1997; Sklet, 2004; Atwood et al., 2006; Katsakiori et al., 2009) to evaluate accident models.

1. Area of application: whether the model can be applied to the oil and gas industry.
2. Type of hazard (process hazards or occupational hazard).
3. Accident sequence modeling (steps of accident process)
4. Direct focus on Safety barrier (model development based on safety barrier or causal factor)

5. Alignment with accident investigation method
6. Qualitative application (to what extent can the model analyze cause-consequence mechanism)
7. Quantitative application (updating and predictive capabilities)

Each model has different area of application and different qualities and deficiencies. It is observed that many models have focused on general industrial settings (e.g. nuclear, medical and transportation). Less emphasize has been devoted to O&G industry application particularly. Therefore, the first characteristic is to discover whether the application area of the models is for O&G industries specific or not. Models such as Domino, Loss causation, MORT, Swiss cheese were mainly developed focusing on general industrial applications, specifically nuclear industry. However, with the increasing in offshore related accidents, research has been conducted to model O&G related accidents (Daryl et al., 2006; Aven et al., 2006; Ren et al., 2008; Kujath et al., 2010).

Accident models vary depending on the types of 'causal factors' that are considered. Many models concentrated in causal factors such as human errors, organizational and management errors; and some direct factors such as unsafe equipment, poor quality of personal protective equipment, hazardous environment, defective tools and unsafe design etc. These factors are commonly considered as 'occupational hazards' which lead to occupational accidents. Domino theory implies that the accident is the result of unsafe act (human error) or unsafe condition at the workplace. Subsequent application of this method has led to the development of loss causation model in which management factors were introduced. Furthermore, human and organizational errors in accident are modeled

in Swiss cheese model. Kletz model analyzes sequence of decisions and action that lead up to an accident, and the preventive action for each steps is recommended. Therefore, Kltez model is capable of adopting both occupational hazards and process hazards for analysis. Modeling accidents due to process hazards (fires, explosion and toxic releases) has been conducted by Kujath et al. (2010) using conceptual accident prevention model.

The third characteristic is devoted to check whether the models provide graphical representation of each steps of accident process. The Domino, Loss causation and Swiss cheese models provide a graphical illustration of the accident sequence steps by placing or modeling factors on a horizontal axis. These models describe the accident as the result of a sequence of events that occur in specific order. However, none of these models are able to illustrate total accident scenario or to capture all steps of accident process. However, steps of accident process may change according to initiating hazardous conditions (e.g. is it process hazard or occupational hazard). MORT model is a representation of multiple sequences of events in the form of hierarchical tree such as fault tree. Such a representation of accident shows that the top-event (accident) is a result of a sequence of combinations of other events or conditions. MORT can be argued as sequential model that represent steps of accident process. However, authors' subjective opinion is that MORT does not provide the best overview the event sequence of accident process, since it is a tree model rather than sequential model. Hierarchical representation of accident is also adopted by the model of Attwood et al. (2006).

Many models focus on the concept of safety barrier without directly involving the safety barriers to develop the model. In the model of Kujath et al. (2010), steps of the accident process were described as failure of particular barriers. In this model, five safety barriers

were identified, and placed in sequential order to depict the accident process due to hydrocarbon release (Figure 2.6). Each safety barrier was further analyzed to find sub-safety element. In the Swiss cheese model, the different slices of the cheese represent the layers of defenses, like barriers or safeguards, a company has installed as part of its risk prevention program. MORT described potential causal factors for accident in a particular order. An important part of MORT model was the relation between energy flow and barriers that used to avoid contacting energy flow to vulnerable target. In MORT model, different types of barriers in the branches can be found. Domino and Loss Causation models suggested that accidents can be prevented through the reduction of unsafe act and conditions. However, these models still emphasize causal factors in the development of accident process rather than the safety barrier. Kletz model shows recommended actions and decisions to prevent the each step of the accident. This did not completely reflect the concept of safety barrier rather some suggestion and decision that would be taken after incident happen to prevent future events. In the models of Attwood et al. (2006) and Ren et al. (2008), causal factors were mainly highlighted rather than safety factors.

Most accident models are theoretical framework; therefore, alignment with the accident investigation methods is paramount to provide comprehensive quantitative and qualitative analyses. Numerous accident investigation methods that identify and analyze hazards have been developed and combined with the accident models to varying degrees. A subjective selection of a suitable accident investigation method depends on model type, purpose, input, output and developer's expectation. In this work, four accident investigation methods, fault tree analysis, event tree analysis, reliability block diagrams and Bayesian networks were specifically considered. Table 2.1 summarizes the author's

evaluation. Domino, Loss causation, Kletz, Swiss cheese models are more capable of adopting accident investigation methods such as root cause analysis, systematic cause analysis techniques (SCAT), hazard and operability studies (HAZOP) and failure modes and effect analysis than methods discussed in this work. These are qualitative analysis rather than quantitative.

Each accident model (with or without accident investigation method) should provide guidelines to analyze causes and their consequences relevance to the accident. Concerning the qualitative ability of models, all models have been able to provide details description of cause-consequence mechanism with varying degrees. The qualitative analysis of models such as Domino and Loss causation does not take multiple causality of accident into account and not able to emphasize important factors in accident sequences (Kjellen, 2000). Swiss cheese model has been recognized as conceptual model that provides limited information on applying this model to real world application (Ren et al., 2008). MORT analyzes a system and identifies the interrelationships among the plant operation and management organizations. However, the tree is so large and complex. Thus, it does not lend to tailoring the tree to a smaller problem. In the model of Ren et al. (2008), Bayesian network is used to provide graphical description cause-consequence relationship whereas Attwood et al. (2006) used reliability block diagram. Kujath et al. (2010) combined of fault tree and event tree analyses to analyze and to provide complete cause-consequence relationship.

The last characteristic assessed the quantitative ability of each model. To prevent the accident, a realistic prediction (i.e. uncertainty of prediction is minimized) is important. Therefore, in this study, model updating and prediction capabilities of accident models

were assessed. Many sequential models are qualitative. However, these models are able to adopt a statistical approach, often using the historical data, to study existing relationship between factors numerically. This approach does not offer predictive information, which can be used to help management decisions, and it is unable to capture dynamic behaviour of process system. Therefore, this type of quantification causes risk of misunderstanding and false interpretation, especially at the higher management levels, where detailed knowledge about the accident occurrences is lacking. In the model of Attwood et al. (2006) reliability concept is used to predict occupational accident frequency and financial rewards and penalties associated with changes in various safety factors. Bayesian network has the ability to update whenever incorporate new information and to predict the future observation. This method has been utilized by Ren et al. (2008) on his occupational accident model to perform much better quantification.

Table 2.1 lists the summary of comparison.

2.3 Summary of Comparison

A review of literature that describes key existing accident models revealed a gap in the knowledge related to oil and gas process accident modeling. Numerous accident models have been developed during last decades. Each of models has different area of application, capabilities and limitations. Furthermore, the model characteristics depend on the types of "causal factor" that it highlights. Accident models in safety assessment plays an important role. They are theoretical framework that is used to establish shared understanding within the organization of how and why accidents happen. Accident investigation techniques which are used to identify and analyze the cause-consequence

relationship in order to develop suitable risk reducing measures to prevent future accident combine to accident models in varying degrees.

Table 2.1:Summary of comparison

Type of model / Characteristics	Domino model	Loss causation model	Kletz model	MORT model	Swiss cheese model	Daryl's model	Ren's model	Kujath's model	Comments
Area of application	GI	GI	GI	NU	AV	O&G	O&G	O&G	Application areas are distinguished based on their utilization of different industries. This does not imply that models should definitely fit only to these applications.
Type of hazard	O	O	O/P	O	O	O	O	P	Kletz's model is a model oriented to incident investigation. Can investigate both type of hazards
Accident sequence modeling	Yes	Yes	Yes	No	Yes	No	Yes	Yes	MORT is tree model and Daryl's model is used hierarchical approach
Focus on safety barrier	No	No	No	Yes	Yes	No	No	Yes	Kujath's model accident represent as a failure of safety barrier. Others use the concept of safety barrier
Alignment with accident investigation methods	Other	Other	Other	FT	Other	RBD	BN	FT/ET	Use of accident investigation method to a model is not fixed. Need to choose suitable method as necessary
Qualitative ability	*Yes	*Yes	Yes	Yes	*Yes	Yes	Yes	Yes	None of models were able to provide holistic view of accident or complete risk profile
Quantitative ability	No	No	No	*Yes	No	Yes	Yes	No	MORT is not able to perform updating and prediction but can perform certain numerical

GI = General Industrial, NU= Nuclear, AV= Aviation and O&G= Oil and Gas. * Yes means method might fulfill the requirement. "O" means "occupational hazards" and "P" means "Process hazards"

Early accident models were developed mainly focusing on areas such as nuclear, medical and transportation. And later, with the increasing complexity in high technological systems and operations of oil and gas related industries, approaches to model oil and gas related accident were taken. However, it is noticed that less attention has been devoted specifically for chemical and process industry. This fact took considerable attention of related individuals and groups to develop comprehensive safety assessment methodology for process industry.

Some models have been developed focusing on process industry, but the approach has usually applied to occupational accidents rather than catastrophic accidents such as fires,

explosions and toxic releases which are generated from process hazards. Even though, these models describe process hazard accidents, they were unable to adopt holistic view of accident. They were not able to represent steps of accident sequence and describe all the risk factors or causal factors that influence of each stage of accident process. Some models used the concept of safety barriers to analysis the accident, but they were not directly applied safety barriers in model development to represent the accident process. In the model of Kujath et al. (2010), model used barriers directly depict the accident and describe an accident as the result of failure of set of particular safety barriers.

Several methods were capable of providing quantitative analysis in terms of either updating or prediction or both. Other models have adopted a statistical approach based on historical data to study existing relationship of causal factors. This way, it will not provide predictive details and quantification consists of significant uncertainty. All models studied here provide graphical demonstration of causal factors of accident process to certain extend. The quantitative and qualitative ability depends on ability of accident investigation method that model can easily adopted. However, no presently available model has adopted a holistic, quantitative approach to chemical and process accidents.

Based on the findings of this literature review and focusing on author's objectives, a new model is proposed to perform safety assessment of process industry. This model is based on the model of Kujath et al. (2010) and set of hypotheses. The novel model is described in subsequent chapters.

Chapter 3

SHIPP METHODOLOGY: PREDICTIVE ACCIDENT MODELING APPROACH
METHODOLOGY AND MODEL DESCRIPTION

Focusing on process hazards, this project aims to contribute to chemical and process industry's safety assessment by proposing a methodology called System Hazard Identification, Prediction and Prevention (SHIPP). The SHIPP methodology can be used to identify most possible process hazards, evaluate, analyze the accident sequences and their consequences, control, and prevent future accidents with knowledge of future likelihood (with prediction capabilities). The process accident model is proposed as the extension of Kujath et al. (2010). In this work, the model of Kujath et al (2010) was modified so that it could be used in any process industries, and it would better represent the accident process. The proposed accident process model can accommodate multiple risk factors considered in chemical and process industry (CPI).

3.1 System Hazard Identification, Prediction and Prevention (SHIPP) Methodology

The purpose of the SHIPP methodology is to identify hazards, evaluate them, predict and prevent their occurrences, and continue monitoring. The SHIPP methodology is a systematic and comprehensive safety analysis procedure that demonstrates how the process accident model integrates process system safety, and is developed by focusing on accident analysis of process hazards. The advantages of the SHIPP methodology are that it can be applied to assess the risk of the entire process system, as well as subsystems, and that it can also identify the system's hidden interactions and their consequences through

modeling the accident process using safety analysis techniques. Application of this methodology helps to determine the critical safety areas that should be prioritized and implemented in order to prevent future accidents based on predictive accident occurrence and accident precursor data. The SHIPP methodology comprises four phases: (1) system definition, (2) hazard identification and analysis, (3) accident modeling and prediction, and (4) updating, decision making and implementation of accident prevention strategies. This methodology is shown in Figure 3.1.

3.1.1 System Definition

The first step of the SHIPP methodology is to define the system and its boundaries. The system is composed of many interacting subsystems such as process units, people, software, hardware, procedures, support equipment, facilities and the operating environment. The nonlinearity and complexity of the system's interactions can cause failure with severe consequences. Therefore, it is important to identify major subsystems, their functions, interactions and their dependencies. Understanding of the systems, subsystems, system interfaces and their interactions is critical to identify the hazards, accident process and required safety barriers (Bahr, 1997).

3.1.2 Hazard Identification and Analysis

Once the system is defined, the next step is to identify and analyze the hazards. The primary objective of the hazard identification and analysis phase is to identify all potential process hazards and analyze how these hazards would lead to an accident.

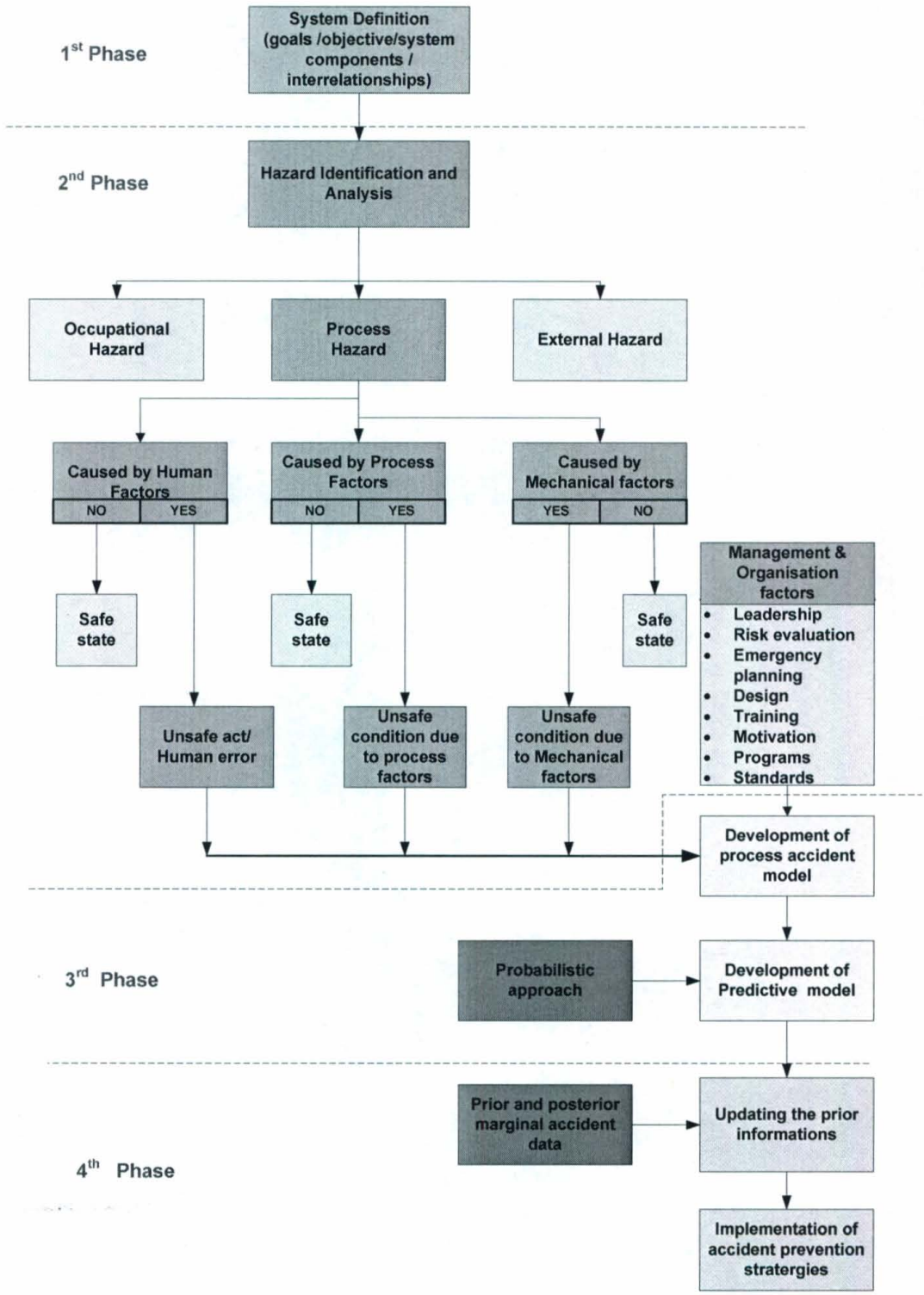

Figure 3.1: System Hazard Identification, Prediction, and Prevention (SHIPP) methodology

It must categorize the hazards in terms of severity of consequences, and then accident process steps (accident sequence process) are evaluated and related to each possible accident scenario. There are several techniques and methodologies available to carry out hazard analysis in the process industry. Khan and Abbasi (1998) reviewed their applicability, limitations and capabilities.

The American Institute of Chemical Engineers has published a manual called "Guidelines for Hazard Evaluation Procedures" (2008) providing guidelines on how to use these techniques. The following methods may be used to identify the hazards: what-if analysis, accident and failure statistics, hazards and operability study (HAZOP), preliminary hazard analysis (PHA) and failure modes and effects analysis (FMEA). However, the choice of the particular hazard identification technique depends on the purpose for which the study is done.

Typically, in the process facility, types of hazards are characterized as: (1) occupational hazard, (2) process hazard, and (3) external hazard. This work focuses on process hazard. The following scenarios characterize process hazards commonly observed in a process facility:

- Unexpected releases of toxic, reactive and flammable liquids and gases
- Unexpected energy release such as mechanical, electrical, thermal or radiation
- Process upsets such as high temperatures, cryogenic temperatures, high pressures, vacuum, pressure cycling, temperature cycling, and vibration/liquid or steam hammering

Process hazards are likely to be generated within an operating plant. Thus, the hazard and operability (HAZOP) study is more suitable for process hazard investigation. Further, for identification of the sources of release, it is necessary to carry out a specific review of such sources. However, it is always advisable to ensure that significant hazards are not overlooked.

Once the process hazards, including the causal factors, have been identified, it is important to evaluate accident sequences and their consequences. Identification of safety barriers planned to prevent an accident sequence is important in accident analysis. Thus, an accident could be described as the result of a relevant safety barrier failure. In studies of accident analysis, application of the concept of the safety barrier has been discussed in the literature extensively. Johnson's (1980) MORT accident model discussed the relationship between energy transportation and barriers. Further, the MORT model discussed the purpose of barriers in three different ways: prevention, control and minimization (Hollnagel, 2004). Svenson (1991) described barrier functions and barrier systems and their distinction in the Accident Evaluation and Barrier (AEB) model. Application of the bow-tie method in risk analysis was used in the ARAMIS project (Dianous and Fievez, 2006) combining safety barriers to analyze hazards. BORA-Release (Aven et al., 2006) analyzed the effect of safety barriers to prevent hydrocarbon releases, and how plant-specific conditions such as technical, human, operational and organizational risk-influencing factors affect barrier performance.

Therefore, integration of hazard and barrier analysis provides comprehensive results for accident analysis rather than just causal-consequences analysis. Further, it may be noted

that human, management and organizational elements contribute significantly not only initiate the accident process, but may also propagate the accident sequences.

3.1.2.1 Human Factors/Human Errors and Organizational Factors

The area of human factors is the scientific study of the interaction between man and machine (Gordon, 1998). Literature reveals different definitions for human error. Rasmussen (1993) defined human error as "human acts which are judged by somebody to deviate from some kind of reference act; they are subjective and vary with time". Senders and Moray (1991) defined human error as the result of observable behavior originating from psychological processes on different levels. These behaviors can be evaluated using performance standards, initiated by an event in a situation where it was possible to act in another way than that assumed to be correct. According to Hollangel (1998), human error cannot be observed directly. The terms "human factor" and "human error" are often used interchangeably in the literature, and can be distinguished as the underlying causes of accidents (human factors) and immediate causes (human errors) (Schondeck et al., 2009). Wagenaar et al. (1994) pointed out that accidents occurring due to human behavior constitute a necessary condition. Such human behavior is called an *unsafe act*. This unsafe act may cause accidents. However, the accidents are not always caused purely by an unsafe act. This is reflected in the proposed methodology (Figure 3.1).

Management and organizational factors involved in accident causation have received considerable attention. There are correlations between the organizational factors and safety performance, yet the way they influence safety performance is not clear. Organizational factors such as leadership, motivation, safety management procedure,

training, and safety culture play major roles in system safety and lack of these factors contributes to causing accidents.

3.1.2.2 The Accident Process Sequence

The accident process usually follows three steps (Crowl and Louvar, 2002):

- Initiation (the event where an accident begins)
- Propagation (the events or events that maintain or expand the accident)
- Termination (the events or events where the accidents are stopped or diminished in size)

It is important to study the accident sequence pattern in order to prevent the initiation and progression of the accident process. It also helps to identify the safety functions and barriers related to different accident levels. Figure 3.2 depicts a simplified illustration of the event sequences and safety functions.

In a typical process accident, the event sequence is initiated with a material or energy release, and is followed by dispersion of material and/or energy, ignition of flammable material, escalation of fire or strong explosion, and exposure to property, humans and the environment. Finally, the accident terminates, causing substantial loss and harm to humans, property and production.

The main safety barriers used to prevent, control and mitigate the consequences of the accident process need to prevent release of material/energy, dispersion of material or energy, ignition, explosion or escalation of fire or release of toxic gas and control the damage and prevent fatalities. The determination of the type, performance, and

requirement of safety barriers and their functions depends on specific hazardous events and severity of consequences.

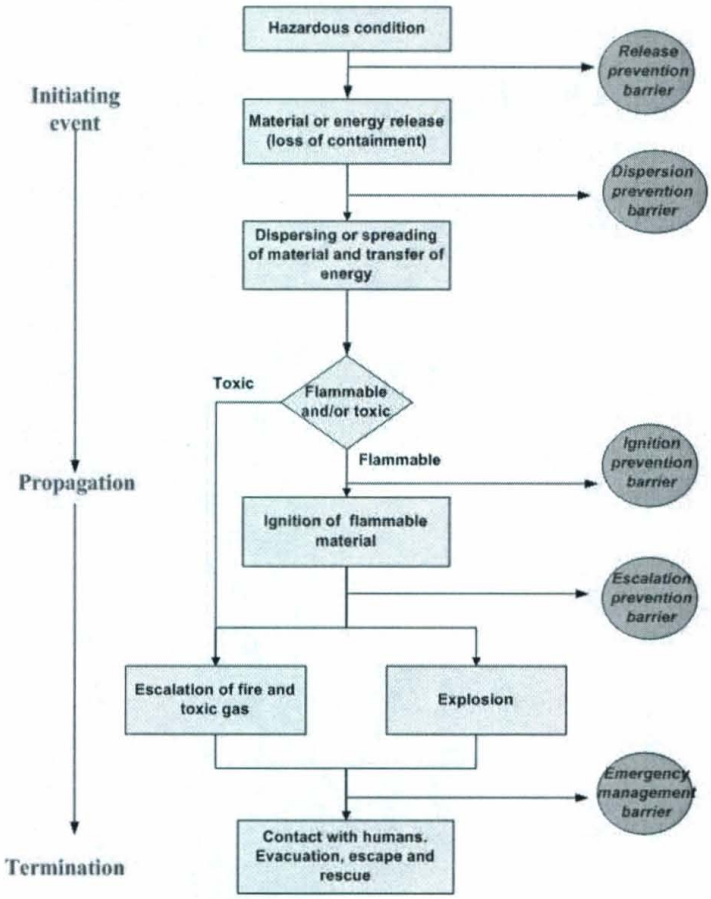

Figure 3.2: Accident process sequence and relevant barriers

3.1.2.3 Definition of Safety Barrier (SB) and Safety Function (SF)

In a general sense, a barrier is an obstacle, a hindrance, or an obstruction that prevents the event occurs and mitigates the impact of the consequences. However, Skelt (2006) has proposed a definition as "the safety barriers are physical and/or non physical means

planned to prevent, mitigate, or control undesired events or accidents", and "a barrier function is a function planned to prevent, control, or mitigate undesired events or accidents".

There are other definitions that are introduced by Hollnagel (2004), Johnson (1980) in the MORT accident model, Duijm (2009). A barrier function represents the action which assigned for particular safety function can be arrest the accident process, so that the next event in the accident sequences will not occur. The performance of the barrier function is important in accident analysis because of it is directly relationship to the occurrences of consequences.

3.1.3 Accident Modeling and Prediction

The process accident model is proposed based on the following considerations:

- Accidents are events resulting from a series of failures or errors; i.e. accidents cannot be described by using a single cause. The causal relationship of the accident process is represented by causal chains or networks.
- The accident sequential path can be blocked by applying a suitable barrier. In so doing, the severity of undesired consequences can be prevented, controlled or mitigated.
- Releases of material or energy and/or process upsets are considered as initiating events.
- The performance (failure or success) of a safety function determines the progression of the accident process; i.e. the accident is described as one or more barriers that have failed.

- Management and organizational and human elements are influenced during all stages of the accident process. Therefore, these two factors are considered as common influencing factors.

As previously described, Kujath et al. (2010) developed a conceptual accident model for the offshore oil and gas process environment. In their model, five safety elements were considered and placed in sequential order to depict a hydrocarbon release accident. The model is a qualitative description of accident propagation initiating with hydrocarbon release in terms of the safety barrier. However, it has not considered the interventions of human, management and organizational factors in the accident process. Therefore, in the current work, the conceptual model limitations have been overcome and a new updated quantitative process accident model is proposed. The proposed process accident model uses a sequential modeling approach by applying five distinct safety barriers to describe the accident process in conjunction with two common safety barriers. The additional two barriers were not considered in the model of Kujath et al. (2010). Further, in the proposed model, the last two barriers of the model of Kujath et al. (2010) (harm and loss prevention barriers) were replaced by one single barrier called damage control and emergency management barrier. Also, a new barrier called dispersion prevention was placed between the release and ignition prevention barriers. The logical relationship of different stages is shown in Figure 3.3.

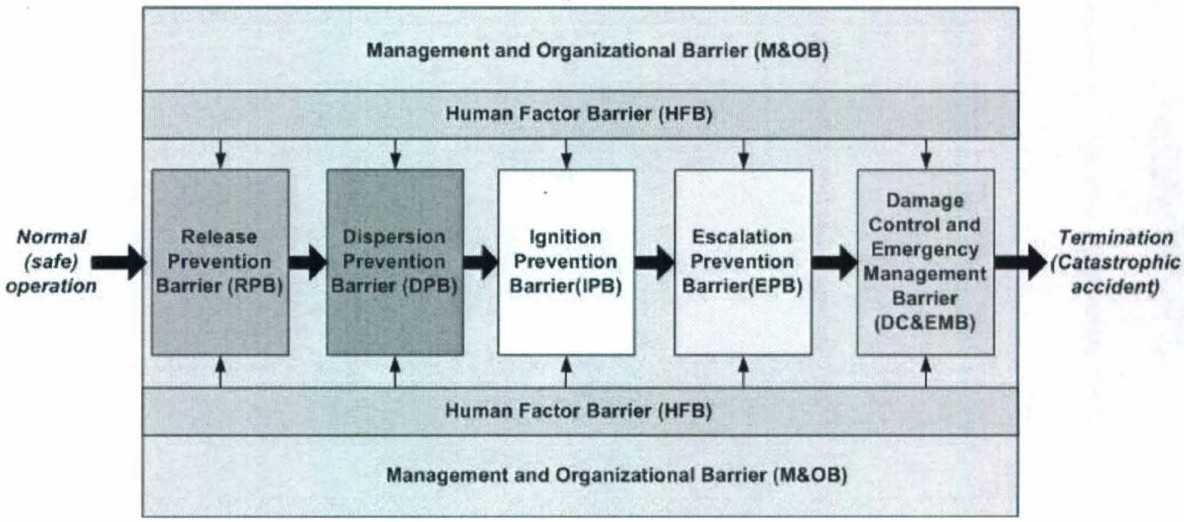

Figure 3.3: The process accident model

The sequential cause-consequence relationship is presented with the help of fault tree and event tree analysis. The safety barriers in the process accident model are analyzed using fault tree analysis (FTA) to establish causal relationship. The top event denotes the failure of the safety barrier. The second layer of the fault tree associated with each safety barrier represents sub safety-barriers; their failure will cause a top event failure. Further analyzing these sub-safety elements, it is recognized subsequent events that cause the failure of sub-safety barriers are causal factors rather than safety elements. A description of the safety barriers and their sub-safety barriers is given in the following paragraphe. The logical relationship between sub-safety elements and main safety barriers is constructed using fault tree analysis.

Release Prevention Barrier (RPB): In most cases, the release of materials is the main initiating event that causes loss of containment. Each release scenario can be described

using different initiating events. The main sub-safety elements that cause RPB failure are: (1) operational error prevention barrier failure (Failures occur when the system is in an operating condition. Manual operational errors are often recognized as the main cause for this sub-safety element failure), (2) physical/technical prevention barrier failure (3) maintenance prevention barrier failure (Poor maintenance, release during maintenance, and erroneous maintenance are some of causes for the failure this sub-safety element) and (4) process upsets prevention barrier failure. The function of this last barrier is to prevent releases occurring by providing early warning or information, or activating the safety system automatically (Figure A.1).

Dispersion Prevention Barrier (DPB): The function of the DPB is to limit the extent and/or duration of hazardous events to prevent the spreading of material or energy. Passive and active barriers are applied to prevent and mitigate the dispersion of hazardous energy. The fault tree for this safety barrier (Figure A.2) identified passive barriers such as bunds, retention walls, dikes and drainage and active barriers such as inerting, ventilation and detection systems as sub-safety elements. Safety elements such as manual and automatic isolation and emergency shut down systems are also applied to limit the dispersion of hazardous material. Such types of barriers are known as activated- manual, -automated, and -procedural barriers (Skelt, 2006).

Ignition Prevention Barrier (IPB): Ignition prevention is very important in facilities that handle flammable material such as oil and gas, paints, adhesives and cleaning agents. When the DPB fails, a flammable chemical mixture may ignite causing a fire and explosion. Therefore, to prevent fires and explosions, safety barriers must be applied by focusing on all possible ignition sources existing in a process facility. There are a number

of ignition sources in a process facility, such as flames, hot works, hot surfaces, hot materials and gases, friction and impact and static electricity sparks. Permanent passive barriers such as insulation and hot surface shielding, and permanent passive controllers such as inadvertent flame detection, function to avoid flammable mixtures contacting ignition sources. Hot-work permits and check lists fall into the category of procedural barriers that are extensively used in the process industry. Figure A.3 shows the fault tree for this safety barrier failure.

Escalation Prevention Barrier (EPB): Once ignition occurs, the hazardous event propagates to nearby equipment, triggering one or more secondary events. This process is known as a "domino accident". Secondary events occur after primary events due to physical effects such as heat radiation, overpressure and fragment projection. The severities of domino or secondary events are significantly higher with respect to primary accident scenarios. Therefore, the relevant and adequate active and passive barriers must be installed to isolate the surroundings to prevent domino accident scenarios. Passive safety barriers such as physical barriers (e.g. fire wall, blast wall, etc.) and protection systems must be installed to be activated on demand without any internal intervention. Active barriers such as fire suppression systems are used to prevent accidents such as jet or pool fires (Figure A.4).

Damage Control and Emergency Management Barrier (DC&EMB): Emergency management and damage control is the last layer of protection that is intended to control hazardous events as much as possible or to reduce their consequences. The main objective of this barrier is to prevent fatalities. The three main elements of the DC&EMB are preparedness, response and recovery. Emergency planning and inherent safety designs are

integral and essential parts of safety and loss prevention. Adequate capabilities of onsite medical facilities would be able to provide a considerable contribution to minimize impact. Emergency safe places and personal protective equipment (PPE) are also helpful to mitigate or control human injuries and fatalities. Figure A.5 shows the fault tree for this barrier.

Human Factor Barrier (HFB): Modern control, automated safety and structured documentation systems are able to achieve a safer operational environment. However, the process operator still has the overall immediate responsibility for the safe operation of the facility. Therefore, human intervention at all levels (not just at the operator level) is a crucial element in the accident process. In the current work, studies were carried out to find possible accident scenarios related to human errors. It is suggested that seventeen major factors may cause HFB failure, and they are allocated to five sub-safety barriers as shown in Figure A.6. These sub-barriers can be categorized in to four types of barriers: procedural, symbolic, activated-warned and activated-automated barriers. For instance, a human-system interface barrier containing displays and alarms, labels and signs, and field control panels are some of the safety elements.

Management & Organizational Barrier (MOB): Often the most important underlying causes for accidents are management and organizational factors. The intervention of these factors may exist at all stages of the accident process; however, their effect is difficult to assess qualitatively as they may change from industry to industry. Similar to previous analysis in the HFB, seventeen causal factors are identified, and they are allocated to two sub-safety barriers which are known as the management barrier and the organizational barrier. The logical relationship of these factors is shown in Figure A.7.

Event tree analysis is used to depict the consequences at each stage of the accident process. The qualitative description of consequences related to each stage of the accident process associated with failure of each safety barrier in the accident chain is shown by an accident sequence event tree as shown in Figure 3.4.

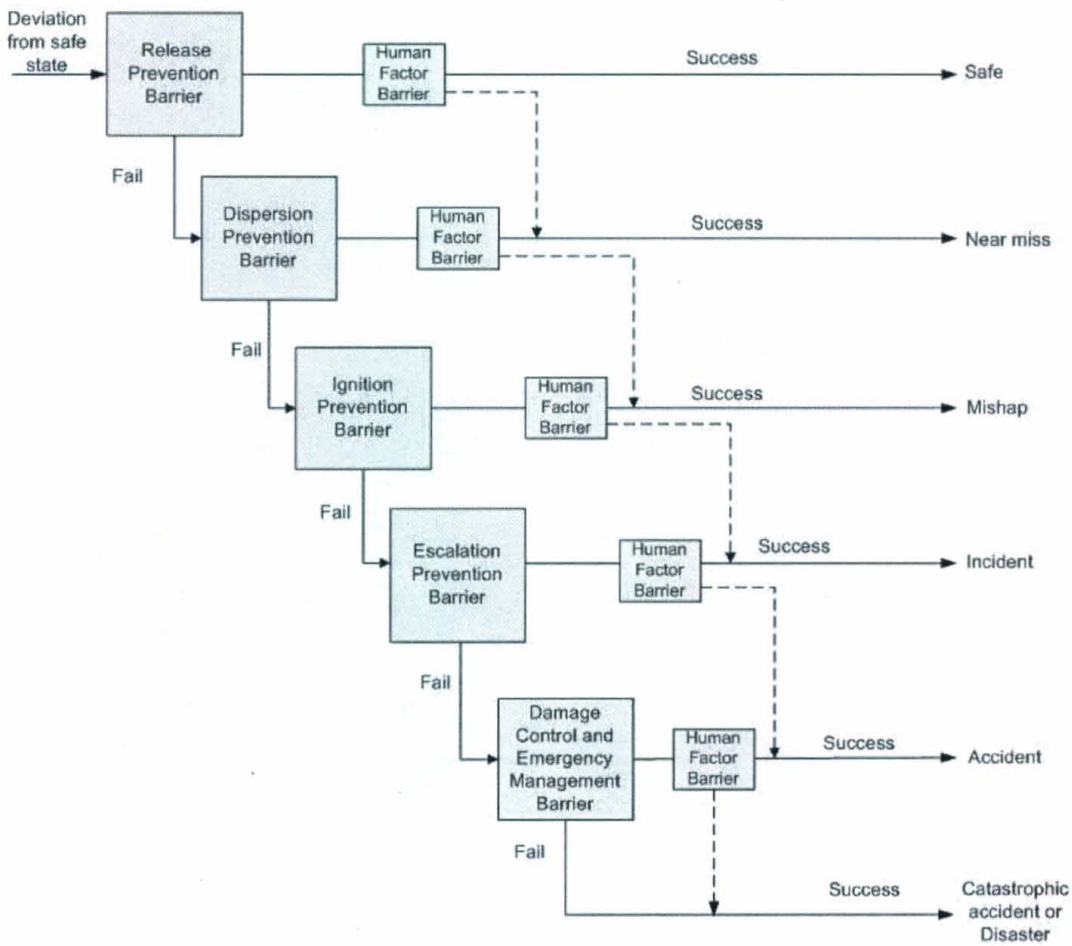

Figure 3.4: Accident sequence event tree based on process accident model

3.1.3.1 Definitions for Abnormal Events

Words and phrases such as 'incident', 'accident' and 'near miss' are often used interchangeably. However, in the context of accident analysis these words need to be tightly defined. The following definitions are introduced for these words using the information derived from a review of relevant literature (Mannan, 2005, Phimister et al., 2003) and also considering the probabilities and consequence levels.

Near Miss: The term 'near miss' describes an event that does not result in an actual loss but that has the potential to do so. For instance, if the process conditions go outside safe operating limits but do not cause a release, then the incident is termed a near miss. The following event scenarios are examples for events that are the result of near miss.

- An emergency shutdown system is unnecessarily activated;
- A safeguard such as a relief valve or fire suppression system is called upon to operate;
- A hazardous chemical is released but does not affect workers in the area.

Mishap: A mishap is an event or sequence of events that could cause minor health effects and/or minor impact to property and the environment. The effect of mishap events could cause production loss or work hours loss.

Incident: An incident is an event that may cause considerable harm or loss. It may also cause a major health effect or injury (temporary disability or permanent minor disability), localized damage to assets and environment, considerable loss of production and considerable impact to company reputation.

Accident: An Event that may cause one or more fatalities or permanent major disabilities, and/or heavy financial loss is considered as accident. An event like this receives national media attention.

Catastrophic accident or disaster: A catastrophic accident or disaster is an event that may cause multiple fatalities and extensive damage to property, system and production. It may cause a shut down of the plant for a significant time period and sometimes forever. It may also cause massive environmental effects. Such an event receives international media attention.

The categorization may vary from industry to industry according to different definitions.

3.1.3.2 Predictive Modeling

Accident prediction based on available information about abnormal events or accident precursor data is the most important aspect of the current model. A predictive model is requested to enhance existing safety strategies to prevent accidents by using the latest information. The prediction model includes two main features: qualitative and quantitative analysis. Quantitative analysis estimates the numerical values about any future likelihood of an abnormal event, while qualitative analysis helps to provide information about specific safety systems that need to be implemented or strengthened so that particular failure modes can be avoided. Event tree and fault tree analysis are combined to develop the predictive model. The event tree (ET) represents all possible accident scenarios associated with the failure of the safety barrier, while fault tree (FT) analysis visualizes all possible causal factors that lead to the failure of a particular safety barrier. The FT-ET model is comprehensive and flexible for accident forecasting, and the

analysis provides a holistic picture of accidents (Zheng and Liu, 2009). Numerical estimation is performed based on deterministic values because this method is quick and easy to apply and also avoids the problem of communicating risk in terms of probability and statistics that non-experts often find difficult to follow. In this section, the predictive model is introduced to estimate the number of abnormal events in the next time interval. The general predictive equation for the discrete random variable z, given observed data can be estimated by using equation 3.1 (Hamada et al., 2008):

$$p(z/\pi) = \sum_{all\theta} p(z/\theta)\, p(\theta/\pi) \tag{3.1}$$

where, θ denotes the unknown parameter, $p(\theta/\pi)$ is the posterior distribution based on data $\pi = (\pi_1, \pi_2, \pi_3, ..., \pi_n)$, and $p(z/\theta)$ is the sampling distribution of z given θ.

Using equation (3.1), the number of abnormal events in the next time interval, y_{t+1} given the observed information, i.e. abnormal event data, is established as equation (3.2). This assumes the number of abnormal events is discrete and an independent random variable.

$$p(y_{t+1}/data) = \sum_{all\lambda} p(y_{t+1}/\lambda)\, p(\lambda/data) \tag{3.2}$$

where, $data = (y_1, y_2, y_3, ..., y_t)$ is the observed number of abnormal events data in the time t, $p(\lambda/data)$ is the posterior distribution of λ, $p(y_{t+1}/\lambda)$ is the sampling distribution, and λ is the average number of abnormal events. The commonly used prior

distribution for λ is the gamma distribution (Hamada et al., 2008). The gamma distribution is a conjugate prior distribution and has a probability density given by:

$$p(\lambda / \alpha, \beta) = \frac{\beta^{\alpha}}{\Gamma\alpha} \lambda^{\alpha-1} e^{-\beta\lambda} \tag{3.3}$$

where, α and β are distribution parameters.

The number of abnormal events y_t is considered as a Poisson distribution with rate λ. Then the likelihood distribution for $data = (y_1, y_2, y_3, ..., y_t)$ given λ can be written as:

$$p(data / \lambda) = \frac{\lambda^{\sum_{i=0}^{n} y_n} e^{-n\lambda}}{\prod (y_n!)} \tag{3.4}$$

Based on the conjugate property, the posterior distribution of λ, $p(\lambda / data)$ is also a gamma distribution with the parameter α_p and β_p, having $\alpha_p = \alpha + \sum_{i=0}^{n} y_n$ and $\beta_p = \alpha + n$.

where, $\sum_{i=0}^{n} y_n$ is the total number of abnormal events in n time intervals.

However, the mean value of posterior distribution of λ provides an updated value that it can be written as:

$$\lambda_p = E[\lambda / data] = \frac{\alpha + \sum_{i=0}^{n} y_n}{\beta + n} \tag{3.5}$$

To simply the predictive model which is shown in equation (3.2), it is approximated to a Poisson process, with the parameter λ_p. Thus, the predictive probability distribution of occurrence of an abnormal event in the next time interval given observed data can be written as:

$$p(y_{t+1} / data) = \frac{\lambda_p^{y_{t+1}} e^{\lambda_p}}{y_{t+1}!} \tag{3.6}$$

The cumulative probability distribution can be simply estimated taking a cumulative value for different numbers of abnormal events.

3.1.4 Updating, Decision Making, Implementation of Accident Prevention Strategies

Apart from qualitative analysis, The FT-ET model provides quantitative analysis. The objective of quantification is to estimate failure probabilities of safety barriers and occurrence probabilities of consequences. However, this procedure includes uncertainties. In the fault tree calculation, basic event probabilities used in point value form which are adopted from reliability data bases, literature and expert judgment can be utilized to estimate the system failure and occurrence probabilities (Yang et al., 2010). However, these data may increase the uncertainty of quantification; thus the accuracy of the results is reduced. Therefore, the Bayesian updating mechanism is used to minimize the uncertainty and to improve accuracy of the quantification.

The prior probabilities estimated using the FT-ET model represent the initial beliefs about the system before observing the new information. Bayes' theorem updates the initial estimate using the newly observed data as likelihood probabilities.

The failure probability of the safety barrier x_i, is assumed to be an identical and independent random variable. The updated failure probability or posterior failure probability is estimated using Bayes' theorem as shown in equation (3.7):

$$p(x_i / data) = \frac{p(data / x_i)\, p(x_i)}{\sum p(data / x_i)\, p(x_i)} \tag{3.7}$$

where, $p(x_i)$ is the prior probability of x_i, $p(data / x_i)$ is the likelihood probability based on the abnormal event data, and *data* is the new information or evidence observed in the system. The denominator denotes the normalizing factor.

The prior probability $p(x_i)$ is estimated using fault tree analysis. The likelihood probability is estimated using real plant abnormal event data as follows:

- Find the number of abnormal events in each month
- Using these numbers, estimate the number of potential success and failure states for each barrier

  $N_{S,i} = N_{C,k}$, for $k = i$

  $N_{F,i} = \sum_{k>i} N_{C,k}$, for $k > i$; $i = 1,2,3,4$ and $k = 1,2,3,4,5$

Where, $N_{c,k}$ is the number of abnormal events of consequence k^{th} level, and $N_{S,i}$ and $N_{F,i}$ are the number of success and failures, respectively, for the i^{th} barrier.

- Once the success and failure are estimated for each barrier, the likelihood probabilities, i.e. the probabilities of particular abnormal events' occurrence given the failure of safety barriers , $P(data / x_i)$ is calculated as:

$$P(data / x_i) = \frac{N_{F,i}}{N_{F,i} + N_{S,i}} \tag{3.8}$$

Substituting prior and likelihood probabilities into equation (3.7), the posterior failure probabilities are estimated.

Event tree analysis is used to estimate updated occurrence probability. This can be obtained by equation (3-9):

$$P(c_k / data) = \prod_{i=SB_k} (x_i / data)^{\theta_{i,k}} (1 - (x_i / data))^{1-\theta_{i,k}} \quad k = 1,2,3,4,5 \tag{3.9}$$

Where, $P(c_k / data)$ is the updated occurrence probability of the k^{th} severity level, SB_k denotes the safety barrier associated with the level, and

$\theta_{i,k} = 1$ if the level k failure passes the down-branch of safety barrier i

$\theta_{i,k} = 0$ if the level k failure passes the up-branch of safety barrier i

The SHIPP methodology provides comprehensive safety analysis and precise information in the process of decision making in risk management, and also supports the critical process safety design implementation.

Chapter 4

MODEL TESTING WITH CASE STUDY DETERMINSTIC AND PROBABILISTIC APPROACH

Validation of SHIPP methodology is demonstrated in case study related to the process industry. The required data were collected from particular oil and gas industry within defined boundary condition. The quantitative analysis is performed using deterministic as well as probabilistic approach. Results of case study show that the methodology is appropriate to apply real time application. Furthermore, the results provide significant insight how safety barriers deteriorate with time and how the likelihood of accident occurrence increases with time. In a deterministic approach, the predictive model estimates the expected number of abnormal events in the next time interval.

Instead of a point value, to represent results in terms of distribution, the probabilities approach is used. However, comparison of the two approaches did not show significant deviation. This proves further confirming the model is suitable for real application. In addition the predictive model to estimate time to observe next abnormal event is developed using probabilistic approach.

The following sections describe steps of SHIPP methodology; hazard identification and analysis, predictive modeling and updating, and quantification is performed in both deterministic and probabilistic approach respectively.

4.1 Hazard Identification and Analysis

Event scenarios associated with process hazards were identified by analyzing incident notification records of the process facility. As a process hazard analysis method, a

HAZOP study (Crowl and Louvar, 2002) is used because it is one of the most systematic hazard identification methods that can be used especially when system is in operating condition. Therefore, HAZOP study is used to identify and develop incident scenarios. Once the event scenarios had been identified, they were subjected to event sequence analysis. First, all possible hazards, for example a significant inventory of flammable and toxic materials were identified. Subsequently, initiating, propagating and terminating events were determined for each event scenario. Then, the consequences of each event scenario were assessed, and severity levels were assigned accordingly. The significant factor of this analysis is the determination of safety functions which should apply to prevent initiation, prevent or mitigate propagation and terminate the accident process.

The results of the analysis illustrate that four severity levels were observed, which are known as: near miss, mishap, incident and accident in this particular case study. The severity level "safe" denotes that the system has started to deviate from normal operation, but the accident initiating event has not yet triggered. Table 4.1 lists the event scenarios and severity levels associated with them for the month of January, 2009.

As an example, the severity level of consequence for the event scenario, "Gland leak from level control valve when open flame job was in progress inside the low pressure knock-out-drum", was classified as "Incident". The definitions for each severity level were discussed in chapter 3. This particular event scenario started with hydrocarbon release while an open flame job was ongoing. The potential hazard is flammable gas (hydrocarbon gas).

Table 4.1: Incident scenario analysis and severity level of consequences

No.	Date	Scenarios	Severity Level
1	04.Jan 09	Steam hammering in the low pressure steam line caused a valve stem cover for a gear operated gate valve to loosen and fall approximately 15 m to the ground	Near miss
2	12.Jan 09	Upper master valve did not close as required During train three depressurization	Safe
3	13.Jan 09	Inadvertent flaring due to wrong opening of pressure control valve on flare line	Near miss
4	14.Jan 09	Gland leak from level control valve when open flame job was in progress inside low pressure knock-out-drum	Incident
5	15.Jan 09	Inadvertent flaring due to wrong opening of pressure control valve on flare line	Near miss
6	17.Jan 09	Welded foundation of davit cracked completely and damaged	Near miss
7	20.Jan 09	Start compressor did not build pressure due to broken link	Safe
8	19.Jan 09	Flame noticed from main combustion chamber of sulphur recovery unit top side	Mishap
9	20.Jan 09	Emergency shutdown valve found stuck in closed condition	Safe
10	21.Jan 09	Gas leak from pressure transmitter tapping due to corroded stainless steel bolts failure	Mishap
11	21.Jan 09	Emergency shutdown valve closed inadvertently	Safe
12	24.Jan 09	Job carried out on east crane without isolation while starting up	Safe

The safety function applied to prevent release failed and led to initiation release. Hydrocarbon then started to disperse inside the knock-out-drum. Further, the safety barriers installed to prevent or minimize the spreading of gas also failed. An open flame was the ignition source that may have caused fire. To avoid contact of flammable material with ignition sources, ignition prevention barriers were introduced. Hot work permit is

normally used in the industry as a safety barrier to prevent ignition and other potential hazards while hot work is progressing. However, a failure or inadequate work permit procedure caused a minor fire. The fire was extinguished as escalation prevention barriers were successful. The accident process of this event scenario can be described in terms of accident barrier failures as follows: the accident process initiated, causing release prevention barrier (RPB) failure, followed by failure of the dispersion prevention barrier (DPB) and ignition prevention barrier. Finally, the escalation prevention barrier (EPB) was successful, and at this stage the accident process was terminated.

4.2 Accident Process Modeling and Prediction

The third phase of the SHIPP methodology is to set up the accident model and predict future outcomes based on available data. The proposed process accident model (Figure 3.3) is used to describe the accident scenarios in the LNG facility. An analysis carried out in phase two illustrates that only the first four barriers were involved with all event scenarios. These barriers are the release prevention barrier (RPB), dispersion prevention barrier (DPB), ignition prevention barrier (IPB), and escalation prevention barrier (EPB). However, other barriers still exist within the model, but their effects are negligible for this case study. Therefore, the accident process model for this LNG case study comprises release prevention, dispersion prevention, ignition prevention, and escalation prevention barriers. The model of safety barriers and consequences associated with their failure is shown in Figure 4.1.Phase three is further discussed in terms of fault tree and event tree construction to depict the cause-consequence relationship and to perform quantification.

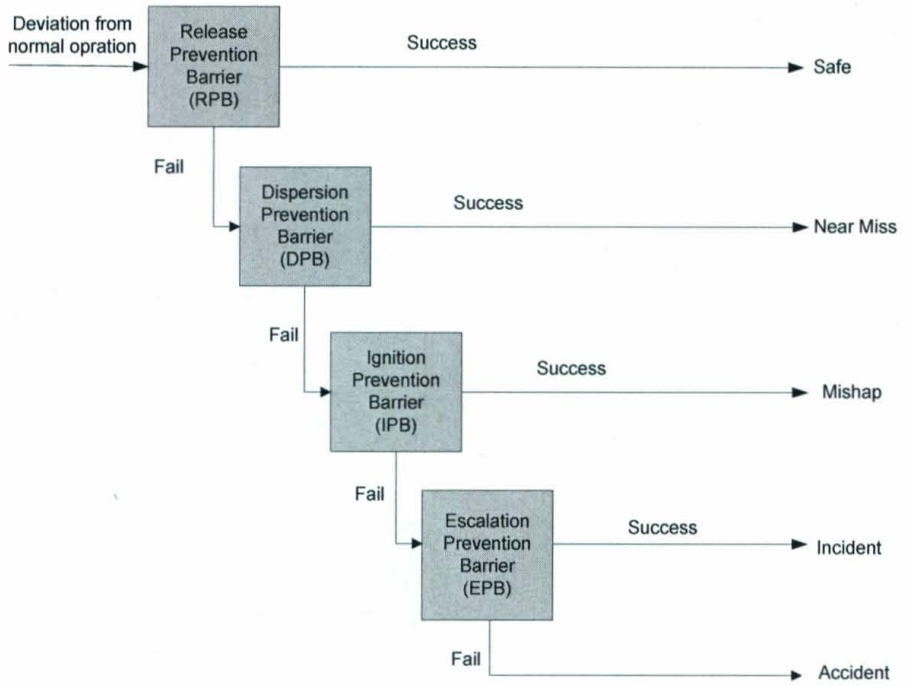

Figure 4.1: Event sequence diagram for case study process facility

4.2.1 Fault Tree (FT) Construction

The fault trees for each safety barrier are shown in Figures B1-B4. They are constructed using the proposed generic fault tree models as discussed in chapter 3. The failure probabilities of basic events were estimated by using OREDA (Offshore Reliability Data Handbook, 2002), Lees' Loss Prevention in the Process Industries Handbook (Mannan, 2005), literature (Skelt et al., 2006 and Khan et al., 2002), and using data directly gathered from the plant. Tables C1-C4 list the failure probabilities of each basic event. The results obtained using the fault tree simulations are shown in Table 4.2.

Table 4.2: Failure probability data for each primary safety barrier

Safety barrier (x_i)	Failure Probability $P(x_i)$
Release Prevention Barrier (RPB)	0.0527
Dispersion Prevention Barrier (DPB)	0.0616
Ignition Prevention Barrier (IPB)	0.1060
Escalation Prevention Barrier (EPB)	0.0271

The failure of barriers is assumed to be independent and mutually exclusive. The probability of failure is denoted by x_i (i.e. failure probability of i^{th} safety barrier which is also known as prior probability or initial belief). The prior failure probability $p(x_i)$, where $i = 1, 2, 3, 4$ denotes the failure probabilities for the safety barriers, RPB, DPB, IPB and EPB, respectively.

4.2.2 Event Tree Construction

The event tree model associated with the event scenarios was developed as shown in Figure 4.2. Initially, the release prevention barrier (RPB) is triggered. The two branches in the tree represent failure and success of a particular safety barrier. If RPB is successful, the favourable consequence is "safe" which is denoted by "C_1". If it is unsuccessful, the next safety barrier, DPB is activated. The end state "C_2" denotes "near miss" if this branch is successful. Then, the safety function of IPB is triggered. The branch's successful consequence is denoted by "C_3", which is called "mishap". EPB is the last safety barrier involved is the escalation prevention barrier. When EPB is successful, following the upper branch, the end state is "C_4", which is the "incident". When EPB is unsuccessful, following the lower branch, the end state results in "C_5"; this is the "accident".

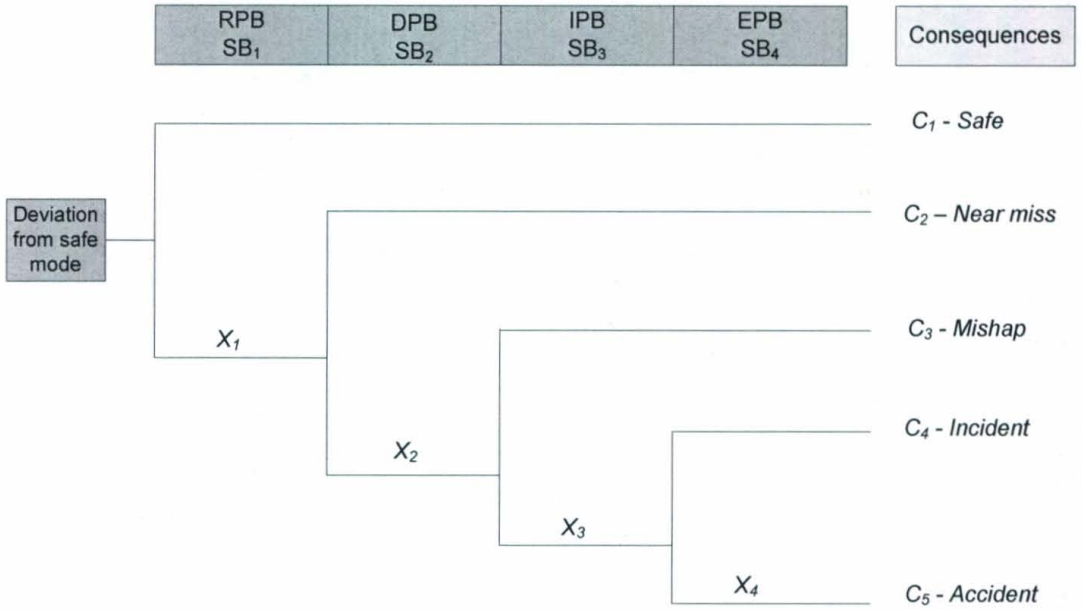

Figure 4.2: Event tree analysis for LNG facility

The failure probabilities of safety barriers are estimated using fault tree analysis as discussed earlier. Then these failure probabilities are used in the event tree branches to estimate the occurrence probabilities of consequences. The prior probability of consequence of severity level k (k =1, 2, 3, 4, 5), denoted by $P(c_k)$, is given as:

$$P(c_k) = \prod_{j \in SB_k} x_i^{\theta_{i,k}} (1 - x_i)^{1-\theta_{i,k}} \tag{4.1}$$

where, SB_k denotes the safety barrier associated with the level k and;

$\theta_{i,k} = 1$ if the level k failure passes the down-branch (failure) of safety barrier i;

$\theta_{i,k} = 0$ if the level k failure passes the up-branch (success) of safety barrier i;

Table 4.3 illustrates prior probabilities of occurrence of consequence for the event tree.

Table 4.3: Prior estimate of occurrences probability of each consequence

Consequences (C_k)	Occurrence Probability $P(c_k)$
C_1 (Safe)	9.4×10^{-1}
C_2 (Near Miss)	4.9×10^{-2}
C_3 (Mishap)	2.9×10^{-3}
C_4 (Incident)	3.3×10^{-4}
C_5 (Accident)	9.3×10^{-6}

4.2.3. Predictive Modeling

The most significant factor of the SHIPP methodology is its predictive ability. This helps to forecast future outcomes based on existing information. The predictive model to estimate the number of abnormal events in the next time interval y_{t+1}, given observed data, is estimated using equation 4.2. The derivation of this model has been discussed in the Chapter 3.

$$p(y_{t+1} / data) = \frac{\lambda_p^{y_{t+1}} e^{\lambda_p}}{y_{t+1}!} \tag{4.2}$$

where, $data = (y_1, y_2, y_3, ..., y_t)$ is the number of abnormal event data in the time t, λ_p is the updated rate of abnormal events as estimated using equation 4.3:

$$\lambda_p = E[\lambda / data] = \frac{\alpha + \sum_{i=0}^{n} y_n}{\beta + n} \tag{4.3}$$

where, α and β are gamma distribution parameters of λ (i.e. average number of abnormal events in the time interval), and $\sum_{i=0}^{n} y_n$ is the total number of abnormal events in the time interval *n*.

Table 4.4 lists the cumulative number of abnormal events of each severity level over the first ten months of year 2009, and obtained using the hazard identification and analysis process.

Table 4.4: Cumulative number of abnormal events over first ten months of year 2009 (real data gathered through analysis of event scenarios of LNG facility)

Month	N_{C1}	N_{C2}	N_{C3}	N_{C4}	N_{C5}
	Safe	Near miss	Mishap	Incident	Accident
1	5	4	2	1	0
2	9	10	4	1	0
3	14	17	6	2	0
4	32	61	18	10	1
5	37	79	23	12	1
6	40	88	24	13	1
7	44	94	24	14	2
8	48	101	27	15	2
9	51	111	30	16	2
10	53	114	32	18	2

Prior distribution for λ is considered as the gamma distribution with the distribution parameters α and β (Hamada et al., 2008). The gamma distribution is a conjugate prior distribution. As enough information are not available to determine prior distribution parameters, i.e. the prior distribution of λ is non-informative prior, α and β are taken as 0.01 providing a uniform distribution. Thus the posterior value of average abnormal events λ_p is estimated using Equation 4.3. Then, this value is substituted in the Poisson

predictive model, and the results are presented in the form of probability mass and density functions as shown in Figure 4.3.

According to probability plots in Figure 4.3, the mean value of the number of events is estimated as 22. This implies that the average number of events predicted in the eleventh month is 22.

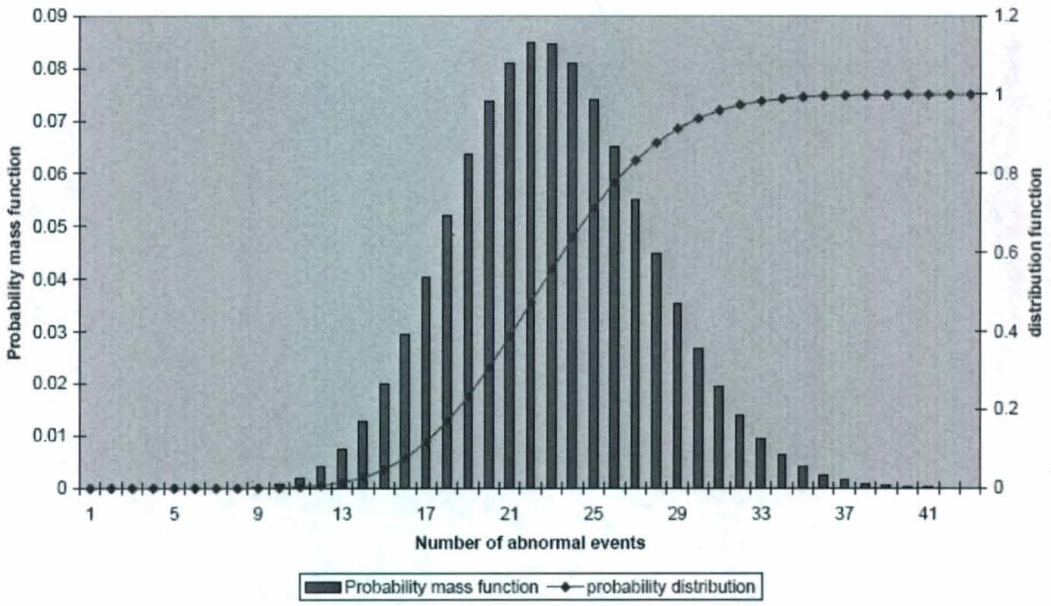

Figure 4.3: Probability mass and density function of number of abnormal events in the next time interval

4.3 Updating Mechanism

The last phase of the SHIPP methodology is to conduct follow-up activities which include updating, implementation of accident prevention strategies and safety critical decision making. Further, it is important to monitor the system to assure the effectiveness of the implemented and existing safety functions (hazard controls).

Basic event failure rates of the fault tree are derived using reliability data bases, literature, and available data in process plants. These failure rates often have significant uncertainty

associated with them. Therefore, to minimize uncertainty of the quantification, a Bayesian updating mechanism is used to update the prior failure probability of safety barrier. By using updated failure probabilities, the consequence occurrence probabilities are also updated using event tree analysis. As described in Chapter 3, Bayes' theorem is used to update the failure probability of safety barriers using data adopted from the plant. This process converges theoretically to more realistic quantification.

The failure probability of a safety barrier x_i is considered as an independent random variable, which represent initial belief or prior information about safety barrier failure. Then, the posterior failure probability is obtained using Bayes' theorem (Bedford & Cooke, 2001) as shown in Equation 4.4:

$$p(x_i / data) = \frac{p(data / x_i)\, p(x_i)}{\sum p(data / x_i)\, p(x_i)} \tag{4.4}$$

where, $p(x_i)$ is the prior probability of x_i, $p(data / x_i)$ is the likelihood or sampling probability derived from abnormal event data from the plant, and *data* is the new information or evidence from the plant. The denominator denotes the normalizing factor.

4.3.1 Estimation of Likelihood Failure Probability

To estimate the likelihood failure probability, plant real time abnormal event data are used. These data are regularly collected in process facilities for further investigation and to diagnose system faults. Table 4.4 lists the cumulative abnormal event data adopted from the LNG facility studied here. The likelihood probabilities are estimated using subsequent steps:

- Find the number of abnormal events in each month (Table 4.4),
- Using these numbers, estimate the number of potential success and failure states for each barrier, and

$$N_{S,i} = N_{C,k}, \text{ for } k = i \tag{4.5}$$

$$N_{F,i} = \sum_{k>i} N_{C,k}, \quad \text{for } k > i \; ; \quad i = 1, 2, 3, 4 \text{ and } k = 1, 2, 3, 4, 5 \tag{4.6}$$

Where, $N_{c,k}$ is the number of abnormal events of consequence k^{th} level, $N_{S,i}$ and $N_{F,i}$ are the number of successes and failures for the i^{th} barrier. For instance, for month one and the first barrier (i.e. $i = 1$),

$$N_{S,1} = N_{C,1} = 5$$

$$N_{F,1} = \sum_{k>1} N_{C,k} = N_{C,2} + N_{C,3} + N_{C,4} + N_{C,5} = 4 + 2 + 1 + 0 = 7$$

- Once the number of successes and failures are estimated for each barrier, calculate the likelihood probability (i.e. the probability of particular abnormal event occurrence given that failure of safety barriers), $p(data / x_i)$,

$$p(data / x_i) = \frac{N_{F,i}}{N_{F,i} + N_{S,i}} \tag{4.7}$$

For the above example:

$$P(data / x_1) = \frac{7}{7+5} = 0.583$$

Similarly, the likelihood failure probabilities for all safety barriers are estimated using equation 4.7. These are listed as in Table 4.5.

Table 4.5: Likelihood probability data for each barrier

Month	Likelihood probabilities $p(data / x_i)$			
	RPB	DPB	IPB	EPB
1	0.583	0.429	0.333	0.000
2	0.625	0.333	0.200	0.000
3	0.641	0.320	0.250	0.000
4	0.738	0.322	0.379	0.091
5	0.757	0.313	0.361	0.077
6	0.759	0.302	0.368	0.071
7	0.753	0.299	0.400	0.125
8	0.751	0.303	0.386	0.118
9	0.757	0.302	0.375	0.111
10	0.758	0.313	0.385	0.100

4.3.2 Posterior Estimation of Failure Probability

Using prior and likelihood probabilities, the posterior probabilities (updated probabilities) for the safety barriers are derived using Bayes' equation (equation 4.4). Table 4.6 lists the updated failure probability for ten months and Figure 4.4 illustrates their distribution with the time.

Table 4.6: Posterior failure probability data for safety barriers over ten months

Month	Posterior failure probabilities $p(x_i / data)$			
	RPB	DPB	IPB	EPB
1	0.0729	0.0469	0.0560	0.0000
2	0.0856	0.0318	0.0288	0.0000
3	0.0911	0.0300	0.0380	0.0000
4	0.1364	0.0303	0.0676	0.0028
5	0.1486	0.0290	0.0628	0.0023
6	0.1503	0.0276	0.0647	0.0021
7	0.1461	0.0272	0.0733	0.0040
8	0.1450	0.0278	0.0695	0.0037
9	0.1490	0.0276	0.0664	0.0035
10	0.1496	0.0291	0.0690	0.0031

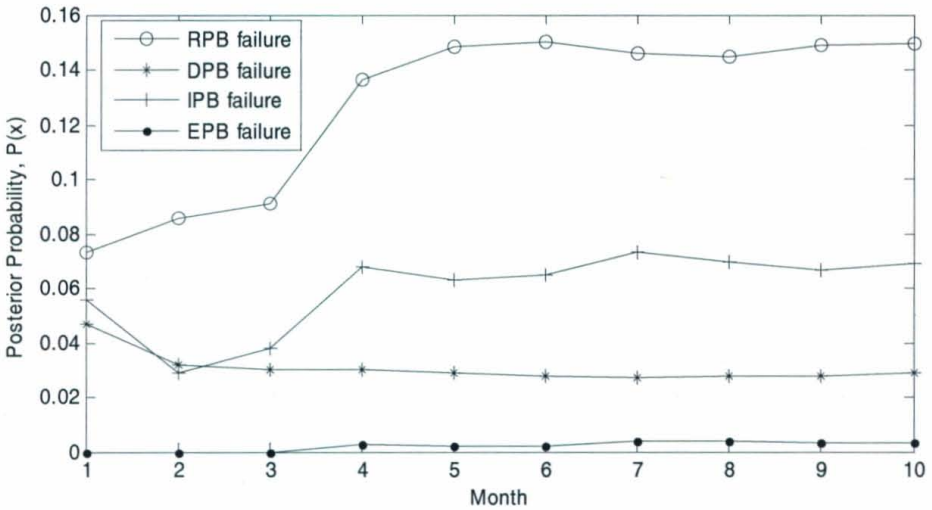

Figure 4.4: Posterior failure probability distribution of safety barriers for ten months

4.3.3 Estimation of Updated Consequence Occurrence Probability

With the updating of the failure probabilities of safety barriers, probabilities of occurring consequences of each severity level are updated. It implies that, as new observations arrive, the consequence occurrence probability will update accordingly. This is estimated using event tree analysis.

The updated failure probabilities are used in relevant branches of the event tree. The failure probabilities are propagated through the event tree branches. Using equation 4.1, the posterior occurrence probabilities of each severity level are estimated for ten months, and the results are listed in Table 4.7.

Figures 4.5 to 4.9 illustrate the variation of updated consequence occurrence probability distributions over a period of ten months.

Table 4.7: Posterior occurrences of each abnormal event over ten months

Month	Posterior probabilities over ten months				
	C_1 (Safe)	C_2 (Near miss)	C_3 (Mishap)	C_4 (Incident)	C_5 (Accident)
1	9.27×10^{-1}	6.90×10^{-2}	3.20×10^{-3}	1.90×10^{-4}	0
2	9.14×10^{-1}	8.30×10^{-2}	2.60×10^{-3}	8.00×10^{-5}	0
3	9.09×10^{-1}	8.80×10^{-2}	2.60×10^{-3}	1.00×10^{-4}	0
4	8.64×10^{-1}	1.32×10^{-1}	3.80×10^{-3}	2.80×10^{-4}	7.68×10^{-7}
5	8.51×10^{-1}	1.44×10^{-1}	4.00×10^{-3}	2.70×10^{-4}	6.24×10^{-7}
6	8.50×10^{-1}	1.46×10^{-1}	3.90×10^{-3}	2.70×10^{-4}	5.69×10^{-7}
7	8.54×10^{-1}	1.42×10^{-1}	3.70×10^{-3}	2.90×10^{-4}	1.14×10^{-6}
8	8.55×10^{-1}	1.41×10^{-1}	3.80×10^{-3}	2.80×10^{-4}	1.03×10^{-6}
9	8.51×10^{-1}	1.45×10^{-1}	3.80×10^{-3}	2.70×10^{-4}	9.42×10^{-7}
10	8.50×10^{-1}	1.45×10^{-1}	4.00×10^{-3}	3.00×10^{-4}	9.21×10^{-7}

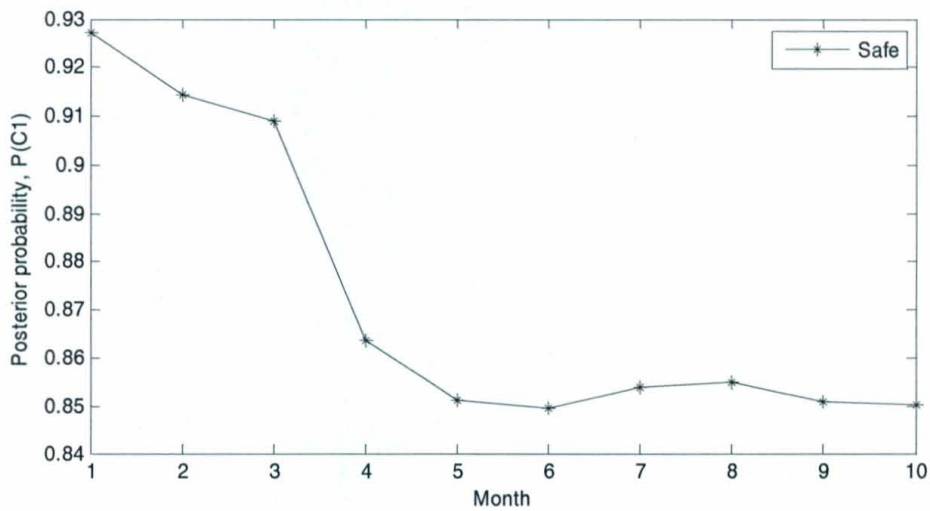

Figure 4.5: Updated consequence occurrence probability distribution of safe events over ten months

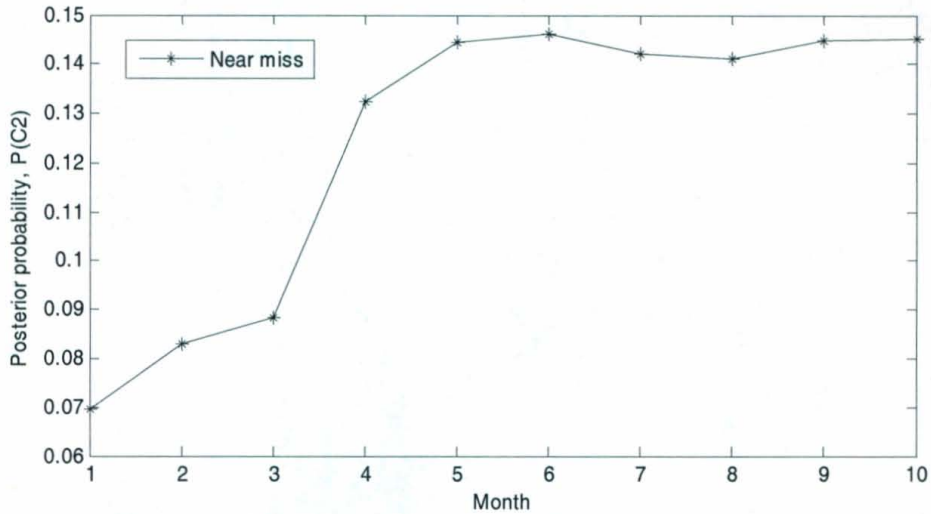

Figure 4.6: Updated consequence occurrence probability distribution of near miss events over ten months

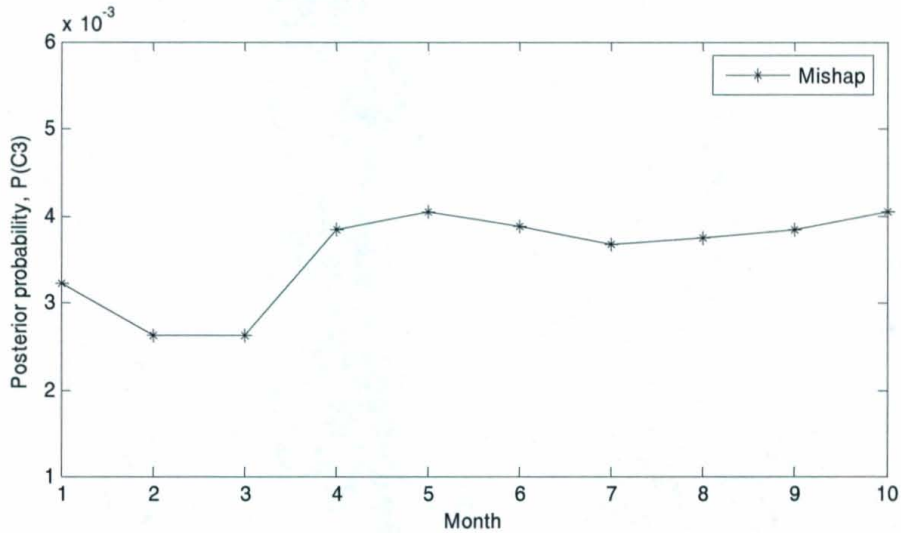

Figure 4.7: Updated consequence occurrence probability distribution of mishap events over ten months

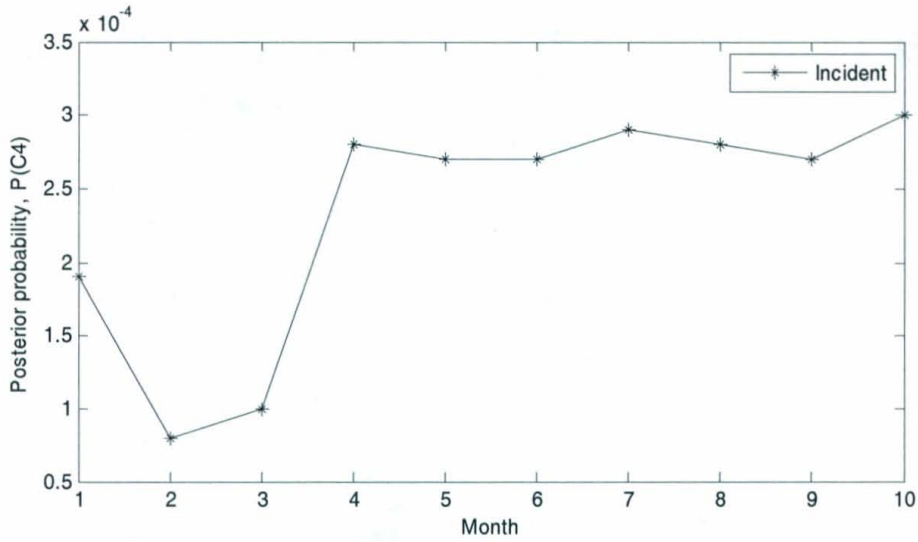

Figure 4.8: Updated consequence occurrence probability distribution of incident events over ten months

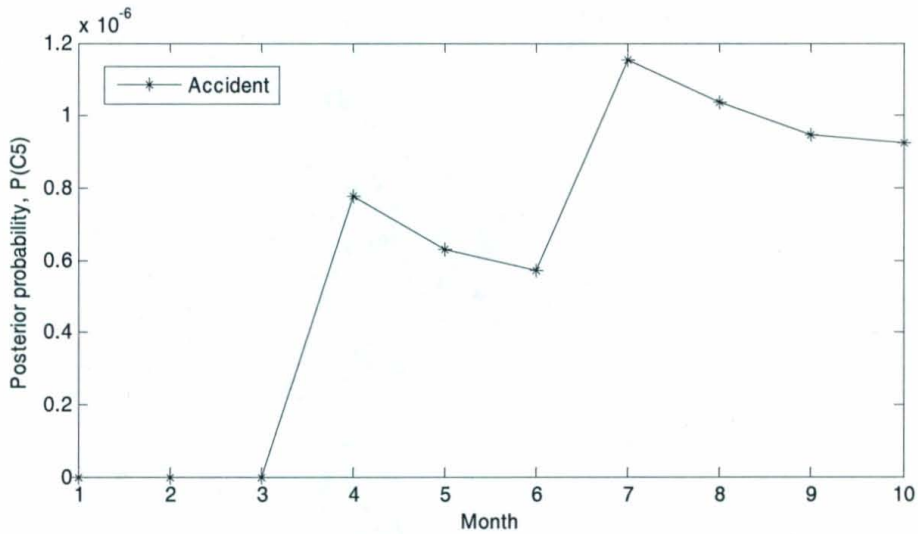

Figure 4.9: Updated consequence occurrence probability distribution of accident events over ten months

4.4 Quantification using Probabilistic Approach

The quantification can be performed in two different ways. One method is the single point estimates, or is deterministic in nature. The quantification of previous sections is discussed by using first approach. Using deterministic approach, an analyst may assign values for discrete scenarios to see what the outcome might be in each. The advantage of this approach is that it is quick and easy to apply. It also avoids the problems of communicating risk in terms of probability and statistics that are often difficult to follow for non-experts. However, in this deterministic approach, uncertainty is not explicitly addressed. Therefore, the deterministic approach may give false sense of accuracy and ignores variability in the population. As well as, it is evident that, the failure probabilities of the safety systems are not deterministic in the nature and tends to follow distribution (Kalantarnia et al., 2009).

The probabilistic approach takes variability and uncertainty in to account of by using probability distributions rather than point estimates (Vose, 2000). They can be used to estimate distributions for occurrence probabilities, which provide a more complete and balanced description of risk for the decision-maker.

4.4.1 Estimation of Prior Probability Density Function for Top Event of Fault Tree (Main Safety Barriers)

The input failure probability (failure probability of basic event) data are assigned as a distribution. The reliability data of OREDA (2002) were estimated by collecting data from multiple companies. The variation from multiple samples is described by a gamma distribution. Lognormal distribution is chosen for input failure rates which are derived from the CCPS hand book and literature due to the general shape and ease of calculation

(Yang et al., 2010). The failure probabilities derived by expert judgment and the Lees' Loss Prevention Handbook (Mannan, 2005) are assumed as a normal distribution because of ease of data analysis.

Monte Carlo simulation was performed to obtain the top event probability distribution. Random numbers were generated for input failure rates using their distributions. The failure probabilities of input variables or basic events are assumed as exponentially distributed the time. Hence, the failure probabilities can be estimated using equation 4.8.

$$p_j = 1 - e^{-\lambda_j t} \tag{4.8}$$

where:

P_j = failure probability of j^{th} basic event

λ_j= Failure rate of j^{th} basic event

t = operational time (considered as 8760hrs)

The fault tree calculation is coded by using the MATLAB simulation tool. Finally, sufficient numbers of simulations are performed to obtain a steady state condition and then, data are fitted to the most suitable distribution. Based on the simulation results, the prior distribution for the i^{th} safety barrier can be modeled by Beta distribution with parameters α_i and β_i:

$$f(x_i) = \frac{1}{B(\alpha_i, \beta_i)} x_i^{\alpha_i - 1}(1 - x_i)^{\beta_i - 1}, \quad i = 1,2,3,4 \tag{4.9}$$

The mean and variance for the prior failure probabilities of safety barriers can be calculated using equations (4.10) and (4.11) respectively.

$$mean = E(x_i) = \frac{\alpha_i}{\alpha_i + \beta_i} \tag{4.10}$$

$$Variance = Var(x_i) = \frac{\alpha_i \beta_i}{(\alpha_i + \beta_i + 1)(\alpha_i + \beta)^2} \tag{4.11}$$

The results of Monte Carlo simulation are shown in Table 4.8.

Table 4.8: Prior distribution of failure of safety barriers and its parameters

Safety Barrier	Distribution	Parameters	Mean	Variance
Release prevention	Beta	α= 16.4 β= 294.5	5.27×10^{-2}	1.60×10^{-4}
Dispersion prevention	Beta	α= 21.2 β= 339.7	5.87×10^{-2}	1.53×10^{-4}
Ignition prevention	Beta	α= 199.1 β= 1679.7	1.06×10^{-1}	5.04×10^{-5}
Escalation prevention	Beta	α= 49.9 β= 1385.8	3.46×10^{-2}	2.31×10^{-5}

4.4.2 Prior Occurrence Probability Density of the Consequences

The probability propagation of the event tree is coded using the MATLAB simulation tool to perform the Monte Carlo simulation. Probabilities of breaching the barriers are estimated using fault tree analysis. The event tree for this case study is shown in Figure 4.2. The results are shown in Table 4.9.

Table 4.9: Prior occurrence probability distribution of the consequences and its parameters

Consequences	Distribution	Parameters	Mean	Variance
C_1	Beta	α= 293.7 β= 16.4	9.47×10^{-1}	1.61×10^{-4}
C_2	Beta	α= 16.4 β= 313.2	4.97×10^{-2}	1.43×10^{-4}
C_3	Beta	α= 9.8 β= 3525.4	2.77×10^{-3}	7.82×10^{-7}
C_4	Beta	α= 9.4 β= 29724.3	3.16×10^{-4}	1.06×10^{-8}
C_5	Beta	α= 8.0 β= 701547	1.14×10^{-5}	1.63×10^{-11}

4.4.3 Estimation of Likelihood Failure Probability Function of Safety Barrier

The determination of an appropriate likelihood function is often more problematic. However, assuming the failure probabilities are random numbers and independent of their consequences, the likelihood function is approximated by a binomial distribution. Hence, the likelihood function for the i^{th} safety barrier is given as a binomial distribution with the parameters $n_{f,i}$ and $n_{s,i}$:

$$f(data/x_i) = \binom{n_i}{n_{f,i}} x_i^{n_{f,i}} (1-x_i)^{n_{s,i}}, \quad i = 1,2,3,4 \tag{4.12}$$

where:

$n_{f,i}$ = cumulative number of failures associated with the i^{th} safety barrier

$n_{s,i}$ = cumulative number of successes associated with the i^{th} safety barrier.

n_i = total number of events associated with the i^{th} safety barrier, i.e. $n_{f,i} + n_{s,i}$.

x_i = failure probability of i^{th} safety barrier.

The parameters $n_{s,i}$ and $n_{f,i}$ can be estimated using the data in Table 4.4.

4.4.4 Estimation of Posterior Probability of Safety Barriers

The posterior probability density function for continues random variable θ is given by:

$$f(\theta/y) = \frac{g(y/\theta)h(\theta)}{l(y)} \tag{4.13}$$

where, $l(y) = \int g(y/\theta)h(\theta)d\theta$.

The function $f(\theta / y)$ is the posterior density, $h(\theta)$ is the prior density, $g(y/\theta)$ is the likelihood density or sampling density of the data, and $l(y)$ is the marginal density or normalization density.

Equations 4.9 and 4.10 are substituted for Bayes' theorem to generate the posterior distribution. In this case, the likelihood function has been chosen as the binomial function, then their conjugate prior exists, often also in the Beta family. Hence, we have the posterior function in the form of Beta with the parameters α_i^* and β_i^*. The derivation is shown in the Appendix D.

$$f(x_i / data) = \frac{1}{B(\alpha_i^*, \beta_i^*)} x_i^{\alpha_i^* - 1} (1 - x_i)^{\beta_i^* - 1}, \qquad i = 1,2,3,4 \tag{4.14}$$

Then, the posterior distribution parameters are given by:

$$\alpha_i^* = \alpha_i + n_{f,i} \tag{4.15}$$

$$\beta_i^* = \beta_i + n_{s,i} \tag{4.16}$$

Table 4.10 lists the updated distribution parameters of safety barrier failure.

4.4.5 Estimation of Updated (Posterior) Occurrence Probability of Consequences

Using the posterior failure distribution, the event tree estimates the posterior occurrence probability distributions. The posterior distributions are also fitted to a beta distribution and the distribution parameters are shown in Table 4.11.

Table 4.10: Posterior distribution parameters

Months	RPB (x1)		DPB (x2)		IPB (x3)		EPB (x4)	
	α_1^*	β_1^*	α_2^*	β_2^*	α_3^*	β_3^*	α_4^*	β_4^*
1	23.4	299.5	24.2	343.7	200.1	1681.7	49.9	1386.8
2	31.4	303.5	26.2	349.7	200.1	1683.7	49.9	1386.8
3	41.4	308.5	29.2	356.7	201.1	1685.7	49.9	1387.8
4	78.4	318.5	39.2	383.7	205.1	1691.7	50.9	1390.8
5	101.4	321.5	47.2	398.7	207.1	1697.7	50.9	1392.8
6	110.4	324.5	49.2	405.7	208.1	1698.7	50.9	1393.8
7	118.4	328.5	51.2	411.7	210.1	1698.7	51.9	1394.8
8	129.4	332.5	55.2	418.7	211.1	1701.7	51.9	1395.8
9	143.4	335.5	59.2	428.7	212.1	1704.7	51.9	1396.8
10	150.4	337.5	63.2	431.7	214.1	1706.7	51.9	1398.8

Table 4.11: Posterior occurrence probability distributions parameters

Month	C_1		C_2		C_3		C_4		C_5	
	$\alpha_{1,p}$	$\beta_{1,p}$	$\alpha_{2,p}$	$\beta_{2,p}$	$\alpha_{3,p}$	$\beta_{3,p}$	$\alpha_{4,p}$	$\beta_{4,p}$	$\alpha_{5,p}$	$\beta_{5,p}$
1	297.6	23.2	23.2	321.1	13.1	2937.1	12.4	24361.7	10.1	551319.0
2	301.4	31.2	31.2	326.7	15.3	2609.2	14.5	21562.0	11.4	470923.0
3	307.5	41.3	41.2	335.6	18.9	2344.2	17.6	19059.9	13.1	394895.0
4	317.1	78.1	78.2	358.1	29.2	1759.7	26.2	13693.8	17.6	251968.0
5	320.6	101.1	101.0	370.0	37.0	1596.3	32.4	12148.4	20.3	208364.0
6	325.3	110.7	110.1	376.3	38.9	1554.9	34.2	11822.1	20.9	198450.0
7	329.7	118.9	118.2	383.3	41.3	1539.2	35.9	11493.8	21.9	189484.0
8	329.6	128.3	127.8	388.2	44.7	1496.4	38.4	11039.5	22.5	174241.0
9	337.5	144.2	143.1	400.9	49.4	1479.5	42.0	10789.8	23.9	165558.0
10	336.3	149.8	148.8	404.7	52.3	1444.1	44.2	10390.3	24.4	155725.0

Based on these parameters, the mean probability of the consequences over ten months of 2009 are shown in Table 4.12.

Table 4.12: Posterior occurrence probability (mean) over ten months

Month	Posterior occurrence probability (Mean)				
	Safe (C_1)	Near miss (C_2)	Mishap (C_3)	Incident (C_4)	Accident (C_5)
1	9.28×10^{-1}	6.74×10^{-2}	4.44×10^{-3}	5.09×10^{-4}	1.83×10^{-5}
2	9.06×10^{-1}	8.72×10^{-2}	5.83×10^{-3}	6.72×10^{-4}	2.42×10^{-5}
3	8.82×10^{-1}	1.09×10^{-1}	7.99×10^{-3}	9.23×10^{-4}	3.32×10^{-5}
4	8.02×10^{-1}	1.79×10^{-1}	1.63×10^{-2}	1.91×10^{-3}	6.98×10^{-5}
5	7.60×10^{-1}	2.14×10^{-1}	2.27×10^{-2}	2.66×10^{-3}	9.74×10^{-5}
6	7.46×10^{-1}	2.26×10^{-1}	2.44×10^{-2}	2.88×10^{-3}	1.05×10^{-4}
7	7.35×10^{-1}	2.36×10^{-1}	2.61×10^{-2}	3.11×10^{-3}	1.15×10^{-4}
8	7.20×10^{-1}	2.48×10^{-1}	2.90×10^{-2}	3.47×10^{-3}	1.29×10^{-4}
9	7.01×10^{-1}	2.63×10^{-1}	3.23×10^{-2}	3.88×10^{-3}	1.44×10^{-4}
10	6.92×10^{-1}	2.69×10^{-1}	3.50×10^{-2}	4.24×10^{-3}	1.57×10^{-4}

4.4.6 Predictive Mechanism

The model to predict the number of abnormal event in the next time interval is develop and discussed in Chapter 3. The prediction of the time for the next abnormal event to occur is discussed in this section.

The general predictive equation for continues random variable can be estimated by using the equation 4.17 (Hamada et al., 2008).

$$f(z/y) = \int_{\theta} g(z/\theta)h(\theta/y)d\theta \qquad (4.17)$$

where, θ is a variable, $h(\theta/y)$ its posterior distribution based on,

data $y = (y_1, y_2, y_3 ..., y_n)$, and $g(z/\theta)$ is the sampling distribution of z given θ.

The predictive distribution to estimate the time to an event of severity level $k, t_{k,i+1}$, is written as equation 4.18.

$$f(t_{k,i+1} / data) = \int_0^\infty g(t_{k,i+1} / \lambda_k) h(\lambda_k / data) d\lambda \tag{4.18}$$

where, λ_k is the rate of k^{th} severity level, i.e. the mean number of failures per unit time is the rate parameter. The commonly used prior distribution for λ_k is the gamma distribution (Hamada et al., 2008). The gamma distribution is a conjugate prior distribution and has a probability density given by:

$$p(\lambda_k / \alpha_k, \beta_k) = \frac{\beta_k^{\alpha_k}}{\Gamma \alpha_k} \lambda_k^{\alpha_k - 1} e^{-\beta_k \lambda_k} \tag{4.19}$$

where, α (>0) is the shape parameter and β (>0) is the scale parameter.

Considering t, the time of event occurrence, is following exponential distribution with the rate λ_k. Then the distribution for t given λ_k can be written as:

$$p(t \ / \lambda_k) = \lambda_k e^{-\lambda_k t} \tag{4.20}$$

Suppose that we observe n conditionally independent events in the time interval t_1 to t_n, and each follow exponential distribution, then the sampling distribution can be written as (Bedford and Cooke, 2001):

$$p(t_1, t_2, t_3, ..., t_n / \lambda_k) = \lambda_k e^{-\lambda_k t_1} \times \lambda_k e^{-\lambda_k t_2} \times \lambda_k e^{-\lambda_k t_{31}} \times ... \times \lambda_k e^{-\lambda_k t_n}$$

$$p(data/\lambda_k) = \prod_{i=0}^{n} \lambda_k e^{-\lambda_k t_n}$$

$$= \lambda_k^n e^{-\lambda_k \sum_{i=0}^{n} t_n}$$

$$= \lambda_k^n e^{-\lambda_k T_n} \tag{4.21}$$

where:

$data = t_1, t_2, t_3, ..., t_n$

$T_n = \sum_{i=1}^{n} t_i$ (The total time period).

Applying Bayes' theorem, with an exponential likelihood function, the posterior distribution of λ_k can be estimated using Equation 4.22.

$$h(\lambda_k / data) = \frac{p(data/\lambda_k)\, p(\lambda_k)}{\int_0^{\infty} p(data/\lambda_k)\, p(\lambda_k) d\lambda_k}$$

$$= \frac{\lambda_k^n e^{-\lambda_k T_n} \frac{\beta_k^{\alpha_k}}{\Gamma\alpha_k} \lambda_k^{\alpha_k - 1} e^{-\beta_k \lambda_k}}{\int_0^{\infty} \lambda_k^n e^{-\lambda_k T_n} \frac{\beta_k^{\alpha_k}}{\Gamma\alpha_k} \lambda_k^{\alpha_k - 1} e^{-\beta_k \lambda_k} d\lambda_k} = \frac{\frac{\beta_k^{\alpha_k}}{\Gamma\alpha_k} \lambda_k^{\alpha_k + n - 1} e^{-(\beta_k + T_n)\lambda_k}}{\frac{\beta_k^{\alpha_k}}{\Gamma\alpha_k} \int_0^{\infty} \lambda_k^{\alpha_k + n - 1} e^{-(\beta_k + T_n)\lambda_k} d\lambda_k}$$

$$= \frac{\lambda_k^{\alpha_k + n - 1} e^{-(\beta_k + T_n)\lambda_k}}{\int_0^{\infty} \lambda_k^{\alpha_k + n - 1} e^{-(\beta_k + T_n)\lambda_k} d\lambda_k} = \frac{\beta_p^{\alpha_p}}{\Gamma\alpha_p} \lambda_k^{\alpha_p - 1} e^{-\beta_p \lambda_k} \tag{4.22}$$

Where: $\frac{\beta_p^{\alpha_p}}{\Gamma\alpha_p} = \int_0^{\infty} \lambda_k^{\alpha_k + n - 1} e^{-(\beta_k + T_n)\lambda_k} d\lambda_k$

$\alpha_p = \alpha_k + n$; the posterior shape parameter.

$\beta_p = \beta_k + T_n$; the posterior scale parameter.

The posterior distribution of λ_k is also a gamma distribution with the parameters α_p and β_p. The posterior distribution of λ_k and the sampling distribution are substituted for equation 4.18 to estimate the predictive density function of time to the next event occurrence.

$$f(t_{k,i+1} / data) = \int_0^\infty \lambda_k e^{-\lambda_k t_{k,i+1}} \frac{\beta_p^{\alpha_p}}{\Gamma \alpha_p} \lambda_k^{\alpha_p - 1} e^{-\beta_p \lambda_k} d\lambda$$

$$= \frac{\beta_p^{\alpha_p}}{\Gamma \alpha_p} \int_0^\infty \lambda_k^{\alpha_p} e^{-(\beta_p + t_{k,i+1})\lambda_k} d\lambda_k \qquad (4.23)$$

By integrating equation 4.23:

$$f(t_{k,i+1} / data) = \frac{\alpha_p \beta_p^{\alpha_p}}{(t_{k,i+1} + \beta_p)^{\alpha_p + 1}} \qquad (4.24)$$

As we know α_k and β_k, we substitute α_p, β_p by α_k and β_k. Then the prediction density becomes:

$$f(t_{k,i+1} / data) = \frac{(\alpha_k + n)(\beta_k + T_n)^{\alpha_k + n}}{(t_{k,i+1} + \beta_k + T_n)^{\alpha_k + n + 1}} \qquad (4.25)$$

Finally, equation 4.25 turns into the Pareto distribution as shown in equation 4.26. Considering $\alpha = (a_k + n)$, $r = (b_k + T_n)$ and variable $x = (b_k + T_n + t_k)$, the Pareto distribution can be rearranged as:

$$f(x = t_{k,i+1} / data) = \frac{\alpha r^\alpha}{x^{\alpha+1}} \qquad (4.26)$$

where, α and r are parameters of Pareto distribution, and mean and variance can be estimated using the Equation (4.27) and (4.28) respectively.

$$mean = \frac{\alpha r}{\alpha - 1}, \ \alpha > 1 \tag{4.27}$$

$$Variance = \frac{\alpha r^2}{(\alpha - 1)^2 (\alpha - 2)}, \ \alpha > 2 \tag{4.28}$$

The values for a_k and b_k are assumed as 0.01. The mean time to the occurrence of the next event is estimated using relevant predictive probability distribution. Table 4.13 lists the results of predictive model.

Table 4.13: Predictive time to the occurrence of the next event

Severity level	Near miss	Mishap	Incident	Accident
Mean time to next event (days)	3.5	12	30	717

4.5 Analysis of Results

During the second phase of the SHIPP methodology, the potential process related accident scenarios in the LNG facility were identified. Analyzing those accident scenarios, the accident sequence process, their causes, consequences and severity levels associated with each consequence were determined. This information was included in the accident model to illustrate the accident process. The model uses four sequential barriers, release prevention, dispersion prevention, ignition prevention and escalation prevention, to depict the accident process. To test the models' validity, a quantitative assessment was performed. The failure probabilities of each safety barriers and consequence occurrence probabilities were estimated using combination of fault tree and event tree analyses.

These probabilities are known as prior estimates or initial beliefs. According to the prior results, the consequences of having higher severity have low probabilities of occurrence, while the consequences of having less severity have higher probabilities of occurrence. The probability of the system remaining safe is obtained as 0.947, whereas the probabilities of severity levels, near misses, mishaps and incidents are dramatically low. The probability of an accident is estimated as 9.32×10^{-6}, which is considerably low. The past accident statistical data in different process industries displayed the same phenomena. In reality, events, such as near misses and mishaps, are more frequent than incidents or accidents. The relationship of industrial accident statistical data and quantified results obtained illustrates that the proposed model is applicable to real applications. A similar conclusion can be made using the results obtained by probabilistic approach. Therefore, this model is able to provide both qualitative and quantitative risk information of the process facility.

The prior failure probabilities of safety barriers were updated using the Bayesian theorem as new information was observed. Plant real-time abnormal events data is used to formulate the likelihood probabilities. Bayesian posterior probability values of safety barriers depict the degradation of safety barriers with the time (Figure 4.4). In deterministic approach, the failure probability of RPB has drastically increased within first five month. Then, it shows slow increasing, whereas, in probabilistic approach it is significantly increasing throughout the period. In deterministic approach, the failure probability of DPB has remained steady for ten months. However, the results in probabilistic approach illustrate that it also increasing throughout the period of ten

months. In the both approach the failure probabilities of IPB and EPB are also slowly degrading with the time.

The event tree analysis is employed to estimate the updated occurrence probabilities based on posterior failure probabilities of safety barriers. These results show that end-state probability or consequences occurrences probability change dramatically over the period of ten months as new information integrated into analysis. Probability distributions of five severity levels are illustrated this phenomenon (Figures 4.5 to 4.9).

According to results of deterministic approach, although the prior probability of safe (C_1) condition has a very high probability of occurrence, as times goes by its posterior probability is gradually reduced from 0.927 to 0.850 (Figure 4.5). However, in probabilistic approach, the posterior probability is reduced from 9.28×10^{-1} to 6.92×10^{-1}. This implies that the system degrades with time. Consequently, its performance is reduced. As a result of system degradation, the posterior probabilities of occurrence of near misses, mishaps, incidents and accident are increased. The posterior probability of near miss (C_2) shows significant improvement with the time (Figure 4.6), whereas mishap (C_3) shows slow fluctuation (Figure 4.7), with an increasing tendency. Most significantly, posterior occurrence probabilities of incident (C_4) and accident (C_5) are dramatically increased (Figures 4.8 and 4.9).When an event occurs (i.e. accident), the preventive measures are applied based on its causal factors. However, as time goes by, the system shows impairment in its performance. The zigzag behaviour of posterior probability distribution of accident indicates this process (Figure 4.9).

In deterministic approach, the predictive model estimates the probability distribution of the number of abnormal events occurring in the next time interval. The average rate of occurring of abnormal events λ is updated whenever a new observation arrives. This is known as updated or posterior rate λ_p. The predictive model is derived based on Poisson distribution with updated rate λ_p. Therefore, the prediction based on updated failure rate information has lower uncertainty than a prediction based on prior information. The mean of the predictive accident in the next time interval is 22 and the standard deviation is 5 events. This means that in eleventh month, 22 events are expected to occur.

In probabilistic approach, the predictive distribution to estimate the time to occurrence of an event with different severity level is developed. Based on predictive results, in this particular process facility, the expected time for an accident to occur is 717 days. However, the plant will observe a near miss, mishap and incident within the first month. According to these results, the expected number of days for a near miss, mishap and incident to occur are 3.5, 12 and 30, respectively. The model updates the predictive results dynamically whenever a new event occurs in the system and continually learns system behaviour as same as deterministic approach.

An uncertainty analysis through the both approach reveals that (1) uncertainty of top event probability or failure probability of safety barrier is reduced significantly by using Bayesian updating method and real life abnormal event data, (2) uncertainty of is reduced significantly using posterior parameters and (3) uncertainty of consequences occurrence probability is also reduced. Furthermore, in probabilistic approach, Using Monte Carlo simulation, the distribution of top event probability and distribution of the

consequences probability were obtained the characterize the uncertainty of the results. This way, the SHIPP provides precise information of how system degrading with time. It also helps to increase the overall safety and performance of the system by applying preventive measures with the knowledge of realistic prediction.

Chapter 5

APPLICATION OF SHIPP METHODOLOGY TO AN LNG PROCESSING FACILITY

Natural gas is considered to be a green fuel as it burns with very few pollutants. In addition, it is relatively safe and economically feasible for storage and distribution to a diverse group of consumers. Global consumption reached 2600 billion m^3 per year in 2003 and there has been continuous growth at an annual rate of 1.8% (Huang et al., 2007). To meet this rapid growth in global demand for natural gas, especially for use as a fuel for power generation in modern combined-cycle gas turbine plants, new LNG processing plants (liquefaction facilities or process trains) need to be designed and existing facilities need to be modified. Complex technologies, production and operation optimization methods and cost reduction strategies are needed to obtain high efficiency and economical feasibility. On the other hand, development in such areas leads to potential disastrous failure modes and new safety issues. In addition, the volatile and cryogenic properties of LNG along, with the flammable and explosive behaviour of its vapours, create risks for those who handle it, for industrial assets and for the general public (Horn and Wilson, 1977). Thus, comprehensive and systematic risk and safety management are of paramount importance during the planning, designing and operating phases of LNG process trains. The objective of this chapter is to test and validate the predictive accident modeling approach.

5.1 Liquefied Natural Gas (LNG) Facility

The LNG value chain is comprised of four components: (1) exploration and production, (2) liquefaction, (3) shipping and (4) storage and regasification. In this work, the liquefaction plant is subjected to a safety assessment using the SHIPP methodology.

5.1.1 The LNG Plant and Process Description

The liquefaction plant is the main capital-intensive unit in the LNG supply chain. A liquefaction facility receives natural gas from the field reservoir through pipelines, and lowers its temperature to liquid form for storage and later shipment to customers. The plant is constructed as one or more processing "trains" which receive the gas, filter and cool it, and store the liquid in a tank until a tanker ship picks it up. The overall process plant contains primary processes such as gas treating, dehydration, acid gas removal, nitrogen (N_2) removal, liquefaction and fractionation, as well as utility supply units. The utilities required to support the main processing unit consist of heating and cooling media (steam, cooling water, chill water, etc.) and a compression unit.

The processes at the liquefaction plant are divided into three main areas: feed gas preparation, fractionation and liquefaction. There are several licensed processes available for liquefaction. Three main processes are commercially used for LNG liquefaction, namely: (1) propane pre-cooled mixed refrigerant (*C3MR*) liquefaction process, (2) ConocoPhillips Optimized Cascade process (COPOC) and (3) multi-fluid cascade process (MFC) (Huang et al., 2007).

Figure 5.1 represents the simplified process flow diagram for the basic C3MR liquefaction process which is used in the majority of LNG plants built to date. The LNG processing facility which is used as the case study in this research employs C3MR liquefaction technology. All LNG plants have field operations and a network of pipelines that feed the raw natural gas and liquid into the plants. The liquefaction cycle requires cooling of natural gas to about -160 °C. Therefore, the incoming gas needs to be cleaned from substances that could freeze at low temperatures and may plug up the equipment. These substances are typically water vapour (H_2O), carbon dioxide (CO_2) and higher molecular weight hydrocarbons which may be commercially useful. Process units involved with this operation include acid gas removal, dehydration, propane refrigeration and heavy hydrocarbon removal. The main processes are refrigeration, absorption and adsorption. The bottom part of the heavy hydrocarbon removal unit entering the plant fractionation unit consists of a de-ethanizer, de-propanizer and de-butanizer.

In the de-ethanizer, most of the ethane and light components are removed. High molecular weight hydrocarbons are removed in the Liquefied Petroleum Gas (LPG) fractionation process. This is a marketable by-product of the LNG plant. Therefore, fractionation is an important unit operation in the overall plant economy. Purified LNG is then sent to the Main Cryogenic Heat Exchanger (MCHE) to liquefy, and the product is sub-cooled through the heat exchange with a circulating Mixed Refrigerant (MR) system. The next step is to decrease the pressure to near storage tank pressure. This is achieved by sending sub-cooled liquefied natural gas through a liquid expander. In the flash unit, vapour and the liquid fraction are further separated. During this process, nitrogen is preferentially ejected to the vapour phase. After heat exchange for refrigeration recovery,

the nitrogen enriched flash vapours are compressed in a motor-driven centrifugal compressor and sent on to the plant fuel system. Finally, the low pressure LNG fraction is recovered and pumped through the LNG rundown line to LNG storage.

5.1.2 LNG Properties and Associated Hazards

Natural gas is composed almost entirely of methane with trace amounts of ethane, propane, butane, nitrogen and carbon dioxide. The percentages of each component depend on the location of origin of the natural gas. As previously discussed, the hazards associated with LNG are mainly due to properties such as cryogenic temperature, flammability and vapour dispersion characteristics.

The boiling point of LNG is typically -162 ^{0}C at 1.7 kPa, i.e. LNG is a cryogenic liquid. Its direct contact with skin causes freeze burns and in contact with the eyes may cause damage. It also causes brittle fracture of metals. The main component of LNG (methane) is considered to be an asphyxiant gas. LNG is a flammable substance of which the flammability range in air is between 5% and 15% by volume. In the presence of an ignition source, a flammable cloud is ignited causing a flash fire or vapor cloud explosion. Upon exposure to an ambient heat source, LNG vapourizes rapidly. The ignition of vapour over an evaporating pool causes a pool fire. LNG has a slightly higher (10-11%) energy density than gasoline. Therefore, it develops a relatively high flame temperature for small fires that are not oxygen starved. Natural gas is lighter than air at standard temperature. However, when LNG is spilled at -162 ^{0}C, the vapour is heavier than air until it warms up to approximately -110 ^{0}C.

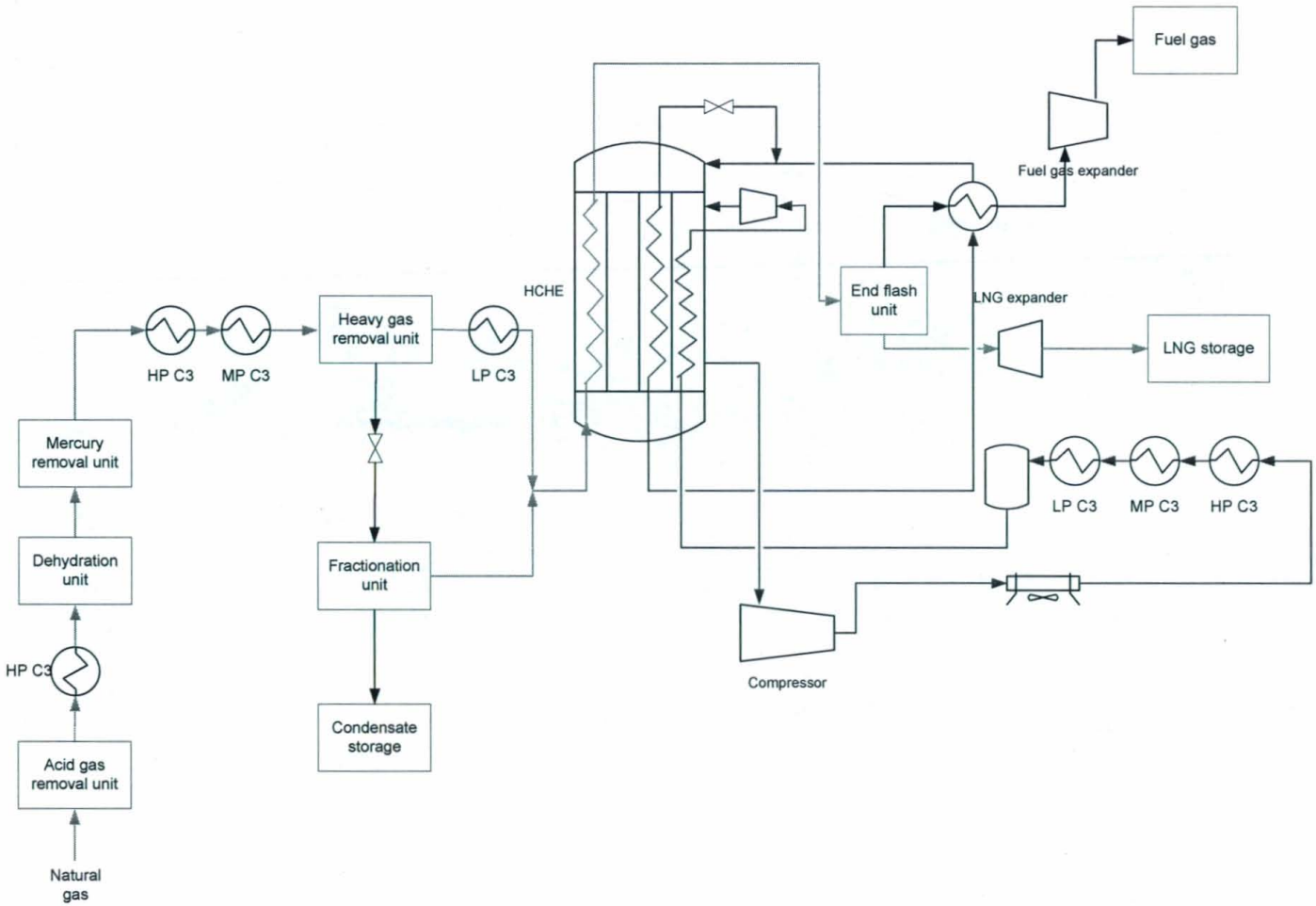

Figure 5.1: The simplified process flow diagram of the basic C3MR liquefaction process (Huang et al., 2007)

In this condition, the vapour cloud travels a relatively long distance before dispersing to its lower flammability level (LFL) (Woodward and Pitblado, 2010). Natural gas in liquid form does not explode. However, when LNG is spilled into water, the explosion scenario known as "Rapid Phase Transition" (RPT) is observed. This happens due to violent vapourization of very cold liquid contacting the water. RPT develops an overpressure which creates low damage. (Woodward and Pitblado, 2010).

5.2 Accident Modeling for an LNG Processing Facility

Prior to developing the process accident model, hazard evaluation studies are performed using available process information of the plant such as incident notification records, flow sheet sketches, piping and instrumentation diagrams, data sheets and procedures. Through HAZOP study, it is possible to identify and understand the potential accident sequences, causal factors and their consequences. Assigning severity for consequences is based on the definitions described in the Chapter 3. The process accident scenario is then developed using the Hazards and Operability Study (HAZOP) to identify the safety barriers that are in place, which have been discussed in the process accident model, prevent the scenario proceeding to end results (consequences) facility during the time period of 2007 to 2009. It is noticed that there were no catastrophic accidents recorded in this time period. Then, it is determined that the barriers: release prevention, dispersion prevention, ignition prevention, escalation prevention, human factor and management and organizational factor were only involved with the process accident scenarios in this particular case study. Although damage control and emergency management barrier exists in the model, its effect has been assumed negligible as it has no involvement with the

accident scenarios. Therefore an accident model is modified according to particular case study.

5.2.1 Failure Assessment of Safety Barriers

Fault trees of release, dispersion, ignition and escalation prevention, human factor and management and organizational barriers are constructed to analyze LNG process accidents using the generic FT models. Figures B.5 and B.6 are the resulting fault tree of the human factor and management and organizational barriers. In the human factor tree, sub-safety elements logically connect through an "OR" gate with the top event, whereas in the management barrier, this is done by means of an "AND" gate. This indicates that one sub-element failure can lead to failure of the human factor barrier. However, both sub-elements of the management and organizational factor barrier need to fail for the top event occur. Construction of fault trees for remaining barriers were developed and discussed in the previous chapter and combined with this work. The failure probabilities of basic events for these two barriers are assigned using plant specific component failure data and industrial expert opinion. Tables C.5 and C.6 list the failure probabilities of each basic events.

The results are obtained by simulating the relevant fault trees and presented in Table 5.1. Assumptions are made that the failures do not occur simultaneously, and they are independent. The probability of failure is denoted by x_i (i.e. the failure probability of the i^{th} safety barrier which is also known as the prior probability or initial belief). The prior failure probability $p(x_i)$, where $i = 1, 2, 3, 4, 5, 6$, denotes the failure probabilities for the safety barriers, RPB, DPB, IPB, EPB, HFB and M&OB, respectively.

Table 5.1: The failure probability data of each primary safety barrier

Safety barrier (x_i)	Failure Probability $P(x_i)$
Release Prevention Barrier (RPB)	0.0527
Dispersion Prevention Barrier (DPB)	0.0616
Ignition Prevention Barrier (IPB)	0.1060
Escalation Prevention Barrier (EPB)	0.0271
Human Factor Barrier (HFB)	0.0029
Management and Organizational Barrier (M&OB)	0.0421

Based on the data available for the LNG facility, the computed results (Table 5.1) are in good agreement with real plant data. This helps to conclude that the developed model is applicable to real situations. However, the results contain a certain degree of uncertainty in quantification. Uncertainty may be reduced using a probabilistic approach as discussed by Kalantarnia et al. (2009), Yang et al. (2010) and and also in this work (Chapters 3 and 4).

5.2.2 Estimation of Occurrence Probabilities of Consequences

An event tree (ET) analysis is used to assess the consequences. Event tree representation of accident scenarios for this particular case study is shown in Figure 5.2. The initiating event is caused by the system deviating from its normal operating conditions. Each of the initiating events of this problem is studied. The frequency of initiating events is estimated using plant specific historical data. For this case study, the probability of initiating events is considered to be unity to simplify the quantification Probabilities of breaching the barriers are estimated using fault tree analysis as discussed above. A particular initiating

event has six barriers to prevent a hazardous outcome. The effects of human factor and management and organizational factor are the most significant.

As described in the model development, the intervention of these in the accident process is applied throughout the process. Considering their independent hierarchical effect and the simplicity of event tree development, they are placed and branched in the event tree as shown in Figure 5. The end states C_1, C_2, C_3, C_4 and C_5 denote severity levels assigned to each consequence, i.e. safe, near miss, mishap, incident and accident. Fault trees are used as inputs to this event tree, and the top-event probability in the fault tree is the failure probability of safety barriers in the event tree. Thus, the probability of final damage states (severity levels) is estimated and presented in Table 5.2.

Table 5.2: Prior estimate of occurrences probability of each consequence

Severity level	C_1	C_2	C_3	C_4	C_5
Probability of occurrence	9.07×10^{-1}	8.71×10^{-2}	4.85×10^{-3}	4.52×10^{-4}	1.45×10^{-5}

The degree of severity of final outcomes, C_1 to C_5, is increasing, whereas their probabilities are gradually decreasing. This inverse relationship between degree of severity and probability reflects the fact that events such as near misses and mishaps occur more frequently than an event such as an accident in this facility. The event tree results are compared with real plant data to test the validity of results. The number of events occurred in different severity levels are estimated using the HAZOP study and its cumulative values have been listed in Table 5.3.

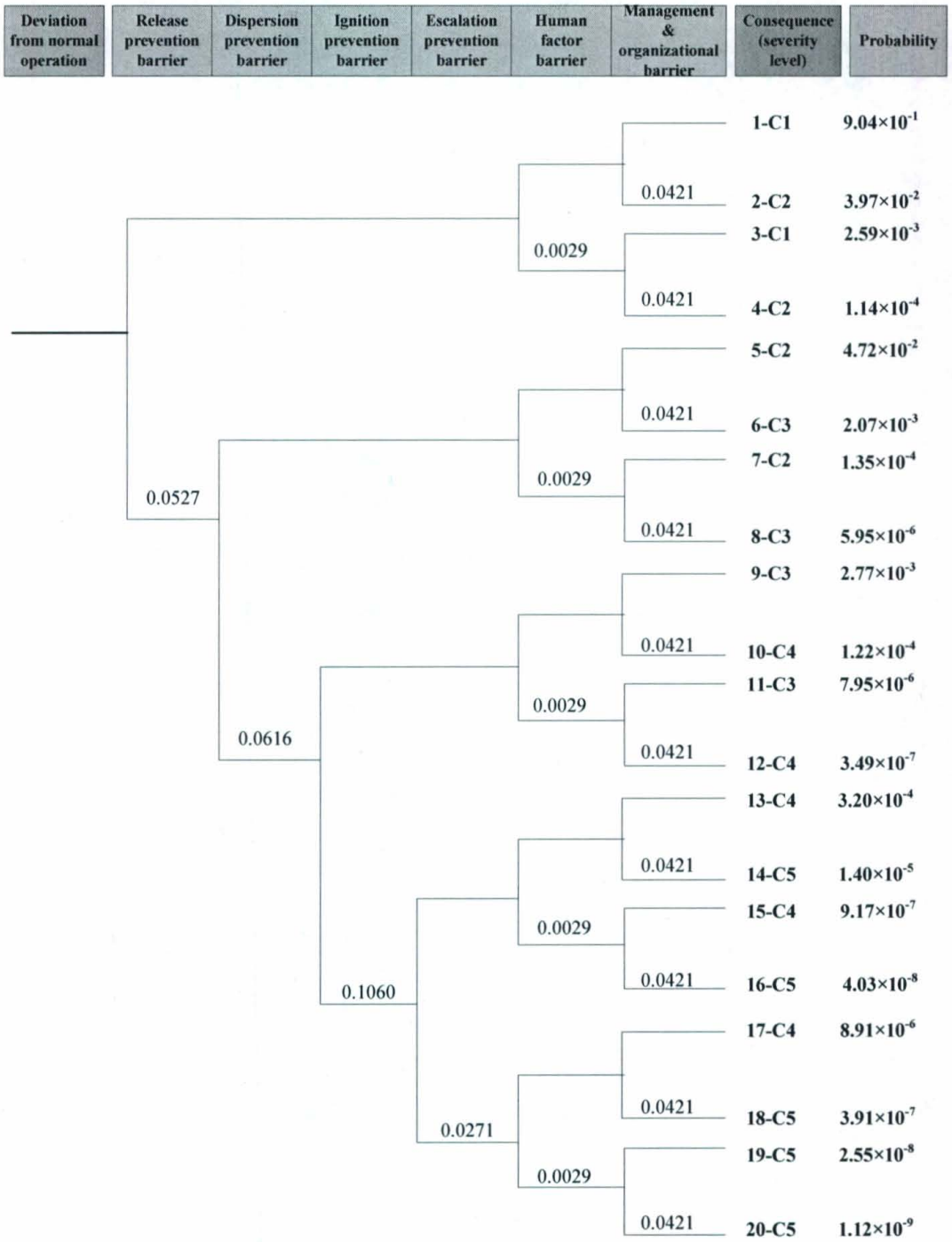

Figure 5.2: Event tree analysis for LNG facility

According these results, it is clear that the numbers of events such as near misses and mishaps which occurred in this LNG facility are higher than events such as incidents and accidents. Therefore, the results follow the real plant accident statistics. It is thus concluded that the developed process accident model is able to represent real life accident scenarios.

Table 5.3: Cumulative number of abnormal events for each month of years 2008 and 2009

Time interval	Severity Level				
	C_1	C_2	C_3	C_4	C_5
1	3	4	0	0	0
2	5	6	2	1	0
3	10	8	2	1	0
4	21	34	10	2	0
5	24	39	11	2	0
6	26	42	11	2	0
7	30	44	12	3	0
8	31	46	12	6	0
9	33	47	12	6	0
10	35	50	13	6	1
11	36	54	15	6	1
12	40	56	15	6	1
13	45	60	17	7	1
14	49	66	19	7	1
15	54	73	21	8	1
16	64	100	27	11	2
17	67	115	33	13	2
18	70	122	34	14	2
19	74	128	34	15	3
20	78	135	37	16	3
21	81	145	40	17	3
22	83	148	42	19	3
23	90	158	44	19	3
24	94	162	46	19	3

Furthermore, the event tree shows the route through which consequences may occur and how various safety functions might prevent and/or mitigate the event. An important point

to highlight is that this quantification inherits uncertainty. The uncertainty is due to determination of basic event probability, development of fault tree analysis (are we capturing all the failures that lead to the top event?), and modeling and determination of hazards (are all the hazards modeled correctly?). As mentioned in Chapters 3 and 4, Bayesian updating is used to update the prior knowledge and thus to reduce the uncertainty in the quantification.

5.3 Predictive Modeling

The expected number of abnormal events in the next time interval predicts using the predictive model discussed in the SHIPP methodology (Chapter 3). In this model, the model parameter (rate of occurrence of abnormal event, λ) is updated using the Bayesian updating mechanism which can be employed to combine sample information (likelihood information) with prior information to arrive at more accurate posterior (updated) information. The prior information is the original distribution of the parameter to be updated and likelihood information related to the data on the parameter collected directly from the LNG processing facility. These two distributions are then combined to arrive at the Bayesian (updated) distribution of the parameter. It is important that the models with the updated parameters had better predictive capability than the models developed using the prior information, and the Bayesian model performed better than all the other updated models.

The prior probability distribution of the rate of abnormal event occurrence, λ, is considered to follow a gamma distribution with distribution parameters α and β (Vose, 2008). Assuming Poisson likelihood function for observing y_n events in period n,

posterior distribution of rate of occurrence of an abnormal event $p(\lambda / data)$ follows gamma distribution with the parameter $\alpha + \sum_{i=0}^{n} y_n$ and $\beta + n$ (Hamada et al., 2008). Then the expected posterior (update) rate of abnormal events is estimated using these two parameters.

The model discussed in Chapter 3 is modified to obtain the predictive model to estimate the number of abnormal events in the m^{th} time interval y_{t+m}, given observed data, as equation 5.1.

$$p(y_{t+m} / data) = \frac{(m\lambda_p)^{y_{t+m}} e^{m\lambda_p}}{y_{t+m}!} \tag{5.1}$$

where, $data = (y_1, y_2, y_3, ..., y_t)$ is the number of abnormal event data in the time t, λ_p is the updated rate of abnormal events and $\sum_{i=0}^{n} y_n$ is the total number of abnormal events in the time interval n. 'm' denotes the number of future time intervals and it can be varied from one to infinity. The equation can be simplified for next time interval, by substituting m equals to one.

5.3.1 Validating of Predictive Model

The mathematical and probability models are generally evaluated in terms of several aspects such as their clarity, generality and testability (also known as validity). Herein, the predictive model is evaluated in terms of testability or validity. Validation is the task of demonstrating that the model is a reasonable representation of an actual system. There

are several approaches such as sensitivity analysis, response analysis, response surface modeling and external validation and they are applied as appropriate to the different aspects of the particular model. In the current work, an external validation approach is used. In this approach the predictive model results are compared with real data. "Real data" refers to the abnormal event data gathered from the particular LNG facility.

The predictive model is used to predict the number of events in the different months of years 2008 and 2009. Table 5.3 lists the cumulative number of events with their severity levels for each month of years 2008 to 2009 (real plant data).

The updated model parameter λ_p, which is the updated abnormal event occurrence rate, is estimated based on event information from the month January to December 2007 using Equation 5.1. To begin, the prior distribution of model parameter λ is considered as a non-informative prior, and parameters α and β are taken as 0.001 (Meel and Seider, 2006). With this prior, 98 events were recorded within this year (2007). The posterior (updated) parameter value of occurrence rate is then estimated as 8.16 based on this information. Using the updated model, the predictive probability mass function for the next time interval (m=1) and for the next two time intervals (m=2) of the year 2008 are estimated and shown in the Figure 5.3.

The predictive mean numbers of event for each month of the years 2008 and 2009 were also estimated. The predicted values were then regressed with the observed values in the LNG facility to check the amount of variation explained by the predictive model. The results of this exercise are given in Table 5.4.

When the predicted number of events is regressed with the observed number of events in the first three time intervals, 14% of the variation (absolute error) is identified, and the predicted values are overestimated. However, when the number of time interval is increased, it can be seen that the model predictions are always less than the observed values (underestimated), and the model predicts events 20 to 50% less than those observed. These results demonstrate that the proposed predictive model is more accurate for short term prediction than for long term prediction.

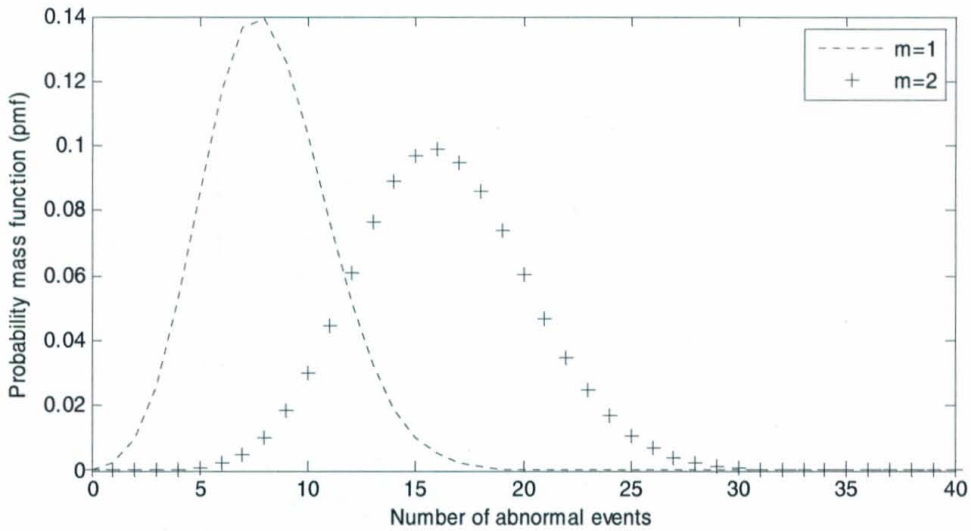

Figure 5.3: Predictive probability mass function of number of abnormal

The model parameter λ is updated continually whenever a new observation arrives in the system. In this case study, the predicted values of the next time interval is estimated and compared with the actual value that has already occurred within this time interval. Figure 5.4 illustrates the variation of predictive mean and actual value. According to the graph, the predictive results fluctuate close to observed value with two exceptions.

Furthermore, the particular LNG facility is observed to have a unique pattern of increased abnormal events in the fourth month (time interval) of each year for which data were analyzed. The reasons for this observation are plant specific and explanations of this are yet to be estabilised.

Table 5.4: The predictive mean, actual number of abnormal events, and error of prediction for the years 2008 and 2009.

Month	Actual number of abnormal events	Predictive number of abnormal events	Standard deviation	Absolute error percentage
1	7	8	3	14
2	14	16	4	14
3	21	24	5	14
4	67	33	6	51
5	76	41	7	46
6	81	49	7	40
7	89	57	8	36
8	95	66	8	31
9	98	74	9	24
10	105	82	9	22
11	112	90	10	20
12	118	98	10	17
13	130	106	11	18
14	142	114	11	20
15	157	122	11	22
16	204	131	11	36
17	230	139	12	40
18	242	147	12	39
19	254	155	12	39
20	269	163	13	39
21	286	171	13	40
22	295	180	13	39
23	314	188	14	40
24	324	196	14	39

In this plot, the significant behavior of predicted value can be observed. The predicted values have been increased or decreased according to the deviation of observed number of events. For an instance, the predicted value has increased in the 5^{th} time interval because of number of observed event has increased significantly in the 4^{th} time interval. Similar behavior of predicted value can be seen in the 10, 17 and 23 time intervals. This can be explained by fact that the predicted model parameter is continuously learning from actual system output and update the predicted results according to system behavior.

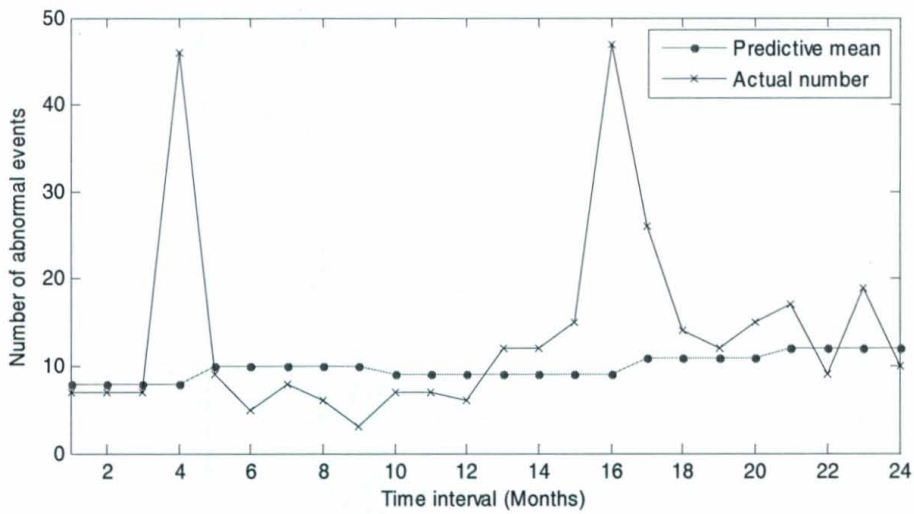

Table 5.5: The variation of prediction mean and actual number of abnormal events from January 2008 to December 2009

Chapter 6

SUMMARY, CONCLUSION AND FURTHER RESERCH

6.1 Summary

A review of existing accident modeling approaches provided insight into limitations for applications to modern complex process systems. It is evident, the majority of existing models have focused on occupational accidents, whereas models focusing on process hazards have been scant. Further, existing models are unable to present a holistic picture of system safety, and are not capable of accounting for multiple causal factors. Since, they are descriptive models, rather than predictive models.

The System Hazard Identification, Prediction and Prevention (SHIPP) methodology is proposed to identify process hazards, evaluate them, model probable accidents, predict, prevent, control and mitigate their occurrences in a process facility. The model has been set up placing five successive safety barriers in sequential order together with two additional safety barriers placed common to all. The five safety barriers: release prevention, dispersion prevention, ignition prevention, escalation prevention and damage control and emergency management, are introduced as necessary safety functions for process accidents. Furthermore, to depict human, management and organizational factors throughout the accident process, two additional safety barriers (human factor, and management and organizational factor) have been kept common to all main safety barriers. To obtain holistic view of cause consequences mechanism, it has been enhanced using accident analysis techniques such as fault tree and event tree. To minimize uncertainty in the quantitative analysis, Bayesian updating is used. Another important

feature of the SHIPP methodology is its predictive capability. The predictive model provides quantitative information that helps to identify the particular failure modes. The SHIPP methodology provides comprehensive safety analysis and precise information in the process of decision making for risk management, and also supports the critical process safety design implementation.

The case study examined here confirms that the proposed accident model can explain the logic of an accident process in the LNG processing facility. Hazards related to LNG properties and process were identified and analyzed to investigate the possible accident scenarios, causes and their consequences. The logical relationship of an accident sequence was modeled using safety barriers. Qualitative validity of accident model is established by corresponding to the real process. A second level of model validation was achieved through comparison of numerical analysis with data. The results (prior estimation) obtained through the fault and event tree analyses are directly supported by plant specific data. A conceptual validation of the model provides confidence that the model could be used for depicting real life process accident. The number of events predicted by the updated predictive model was regressed with the observed number of events to validate the model. The model parameter λ, the rate of abnormal events occurring, was dynamically updated. The adequacy and accuracy of model prediction were better in short term prediction than long term prediction.

Based on the present study, it was observed that the proposed accident model with predictive capabilities can be applied to study real life accident situations.

6.2 Conclusions

This case study illustrates that the SHIPP methodology provides realistic and reliable information for accident modeling and prediction. This in turn provides comprehensive and systematic method to assess and manage the risk by implementing accident prevention strategies (inherent safer design approach). Furthermore, this study shows that the proposed accident model and fault and event tree analyses can be jointly used to depict the process accident sequence. In the present study, uncertainty analysis through the Bayesian updating reveals that (1) uncertainty of the top event probability or failure probability of safety barrier was reduced significantly by using Bayesian updating method with real life abnormal event data, (2) uncertainty in the number of abnormal event prediction in the next time interval was reduced significantly using posterior rate of event occurrence and (3) uncertainty of consequence occurrence probability was also reduced. This way, the SHIPP provides precise information of how system is degrading with time. The other principal finding was that the predictive model performs precise prediction for short term intervals. It also helps to increase the overall safety and performance of the system by applying preventive measures with the knowledge of realistic prediction. Therefore, it is concluded that the proposed methodology including accident process model with predictive capabilities is applicable to real world application to assess system safety.

6.3 Future Research

The present study includes following assumptions:

- Occurrence of events are independent (event dependencies are not incorporated)
- Failure of the safety barrier follows a sequential order. The safety barrier failure generally starts from the failure of release prevention barriers and propagates towards to termination by failing sequential manner.
- Prior information of model parameters is selected using conjugate properties.

Additional research with respect to further development of SHIPP methodology should focus on the following main areas:

- Application of Bayesian Network (BN) instead of fault and event analyses to develop the cause-consequences relationship and accident process sequence. Bayesian network is able to capture the event dependencies and to infer causal relationship both backward and forward. Further, dynamic Bayesian network is able to update the model dynamically.
- Utilization of non-conjugate prior-posterior distribution. The available data was fitted to most suitable distribution rather than using conjugate pairs.

Bibliography

Attwood, D., Khan, F. & Veitch, B. (2006). Occupational accident models - Where have we been and where are we going?. *Journal of Loss Prevention in the Process Industries 16*, 664-682

Aven, T., Sklet, S. & Vinnem, J.E. (2006). Barrier and operational risk analysis of hydrocarbon releases. (BORA-Release). Part I. Method description. *Journal of Hazardous Materials A137*, 681–691

Bahr, N.J. (1997). *System safety engineering and risk assessment: A practical approach.* Taylor & Francis, NY.

Bedford, T. & Cooke, R. (2001). *Probabilistic risk analysis: Fundamentals and Methods.* Cambridge university press, UK.

Benner, L. (1978). *Accident theories and their implication for research.* AAM/IAATH conference, July 10-14, Ann Arbor, MI, USA.

Bird, F.E. (Ed.)(1974). *Management guide to loss control.* International Loss Control Institute, Atlanta, USA.

Bird, F.E. & Germain, G.L. (1996). *Practical loss control leadership*. Det Norske Veritas. Georgia, USA.

BP. (2010). Deep water horizon accident investigation report. BP internal investigation team. http://www.bp.com/.

Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C. & Wood, T. (2008). Construction of event-tree/fault-tree models from a Markov approach to dynamic system Reliability. *Reliability Engineering and System Safety 93*, 1616–1627

Castillo, E., Sarabia, J.M., Solares, C. & Gomez, P. (1999). Uncertainty analysis in fault trees and Bayesian networks using FORM/SORM methods. *Reliability Engineering and System Safety 65(1,*29–40

CCPS, (2008). *Guidelines for Hazard Evaluation Procedures, 3rd Edition.* John Wiley & Sons, Inc., Hoboken, NJ.

Crowl, D. & Louvar, J.F. (2002). *Chemical process safety. Fundamentals with application*. Second edition. Prentice hall inc. NJ.

CSB. (2007). BP America refinery explosion Texas City, TX, March 23, 2005. Final report finding. http://ww.csb.gov/

CSB. (2009). Imperial Sugar dust explosion and fire, Georgia, February 7, 2008. Final investigation report. http://ww.csb.gov/

Dean, T. (1990). Coping with Uncertainty in a Control System for Navigation and exploration. *In Proceedings of the Ninth National Conference on Artificial Intelligence*, 1010–1015. Menlo Park, Calif.: American Association for Artificial Intelligence.

Dianous, D.V. & Fievez, C (2006). ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials 130,* 220–233

Duijm, N.J. (2009). Safety barrier diagram as a safety management tool. *Relibility engineering and system safety 94*, 332-341

Eckerman, I. (2005). *The Bhopal saga: Causes and consequences of the world's largest industrial disaster*. Universities press. India.

Gordon, R.P.E. (1998). The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering and System Safety 61*, 95-108.

Hamada, M.S., Wilson, A.G., Reese, C.S. & Martz, H.F. (2008). *Bayesian Reliability.* Springer Series in Statistics. NY.

Heckerman, D. (1990). *Probabilistic Similarity Networks*, Technical Report, STAN-CS-1316, Department of Computer Science and Medicine, Stanford University.

Heckerman, D. & Breese, J. (1996). Causal independence for probability assessment and inference using Bayesian networks. *IEEE Transactions on Systems, Man, and Cybernetics, 26(6),*826–831.

Heckerman, D. (1997*). Bayesian networks for data mining*. Data Mining and Knowledge Discovery, *1,* 79–119.

Heinrich, W.H. (1941). *Industrial accident prevention.* McGraw-Hill, NY.

Hollnagel, E. (Ed.) (1998). *Cognitive reliability and error analysis method (CREAM).* Elsevier Science. NY

Hollnagel, E. (2004). *Barrier and accident prevention.* Hampshire, UK.

Horn, A.J.V. & Wilson, R. (1977). The potential risk of liquefied natural gas. *Energy, 2,* 375-389

Huang, S., Chiu, C. & Elliot, D. (2007). *LNG: Basics of liquefied natural gas*. University of Texas, USA.

Jensen, F.V. (1996). *An introduction to Bayesian network.* Springer, NY

Johnson, W. G. (1980). *MORT safety assurance systems*. NY.

Kalantarnia, M., Khan, F. & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. *Journal of Loss Prevention in the Process Industries 22,* 600-606.

Kang, C.W. & Golay, M.W. (1999). A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. *Expert Systems with Applications 17*, 21–32

Katsakiori, P., Sakellaropoulos, G. & Manatakis, E. (2009). Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. *Safety Science 47*, 1007–1015.

Khan, F.I. & Abbasi, S.A. (1998). Techniques and methodologies for risk analysis in chemical process industries. *Journal of Loss Prevention in the Process industries 11*, 261-277.

Khan, F.I. & Abbasi, S.A. (1999). Major accidents in process industries and an analysis of causes and consequences. *Journal of Loss Prevention in the Process Industries* 12, 361–378

Khan, F.I., Sadiq, R. & Husain, T. (2002). Risk-based process safety assessment and control measures design for offshore process facilities. *Journal of Hazardous Materials A94*, 1–36

Kim, M. C. & Seong, P. H. (2006). A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety, 91(5),* 580–593.

Kjellen, U. (Ed.). (2000). *Prevention of accidents through experience feedback.* Taylor and Francis, London.

Kletz, T.A. (1988). Piper Alpha: latest chapter in a long history. *The Chemical Engineer. 4*, 277.

Kletz, T. (2001). *Learning from accident*. Third edition. Gulf Professional Publishing. Oxford.

Kujath, M.F., Amyotte, P.R. & Khan, F.I. (2010). A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries 23*, 323-330.

Lehto, M. & Salvendy, G. (1991). Models of accident causation and their application: Review and reappraisal. *Journal of Engineering and Technology Management, 8,* 173-205.

Levitt, T., Mullin, J. & Binford, T. (1989). Model- Based Influence Diagrams for Machine Vision. *In Proceedings of the Fifth Workshop on Uncertainty in Artificial Intelligence,* 233–244. Mountain View, Calif.: Association for Uncertainty in Artificial Intelligence.

Mahadevan, S., Zhang, R. & Smith, N. (2001) Bayesian networks for system reliability reassessment. *Structural Safety 23*, 231–251

Mannan, S. (2005). *Lee's Loss Prevention in the Process Industries*. Volume 3. Elsevier Inc.

Meel, A. & Seider, W.D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. *Chemical Engineering Science 61,* 7036 – 7056

OREDA, (2002). *Offshore reliability data handbook*. SINTEF Industrial management, Det Norske Veritas.

Pearl, J. (1988). Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Morgan Kaufmann, San Mateo, CA

Petrie, J.R. (1989). Piper Alpha Technical Investigation Interim Report. London: Department of Energy.

Phimister, J.R., Oktem, U., Kleindorfer, P.R. & Kunreuther, H. (2003). Near miss Incident management in chemical process industry. *Risk Analysis, 23,* 445-449

Rasmussen, J. (1993). *Perspectives on the concept of human error.* Society for Technology in Anesthesia Conference, New Orleans.

Rasmussen, J. (1997). Risk Management in a dynamic society: A modeling problem. *Safety Science 27*, 183-213

Reason, J. (1990) *Human error.* University press, Cambridge.

Schonbeck, M., Rausand, M. & Rouvroye, J. (2009). Human and organizational factors in the operational phase of safety instrumented systems: A new approach. *Safety Science 48,* 310-318.

Senders, J.W. & Moray, N.P. (Ed.). (1991). *Human errors: Their causes, prediction, and reduction.* Lawrence Erlbaum Associates Inc. Hillsdale, NJ

Skelt, S. (2004). Comparison of some selected methods for accident investigation. *Journal of Hazardous Material 111*, 29-37.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries 19*, 494–506

Spiegelhalter, D., Franklin, R. & Bull, K. (1989). Assessment Criticism and Improvement of Imprecise Subjective Probabilities for a Medical Expert System. *In Proceedings of*

the Fifth Workshop on Uncertainty in Artificial Intelligence, 335–342. Mountain View, Calif.

Svenson, O. (1991). The Accident Evolution and Barrier Function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis 11,* 499-507.

Turney, R. & Pitblado, R.M. (1996) Risk assessment in process industries. 2nd edition. Institute of chemical engineers, Rugby.

Wagenaar, W.A., Hudson, P.T.W., Groeneweg. J. & Reason, J.T. (1994). Promoting safety in the oil industry. *Ergonomics 37 (12),* 1999-2013.

Wagenaar, W.A. & Schrier, J.V.D. (1997). Accident analysis: The goal, and how to get there. *Safety Science, 26,* 25-33

Woodward, J.L & Pitalado, R.M. (2010). *LNG Risk based safety: Modeling and consequences analysis.* John Wiley. NY

Vose, D. (2008). Risk analysis: A quantitative guide. John Wiley & Sons Ltd, England.

Zheng, X. & Liu, M. (2009). An overview of accident forecasting methodologies. *Journal of Loss Prevention in the Process Industries, 22*: 484-491.

Yang, X., Rogers, W.J. & Mannan, M.S. (2010) Uncertainty reduction for improved mishap probability prediction: Application to level control of distillation unit. *Journal of Loss Prevention in the Process Industries 23*: 149–156

Appendix A: Generic Fault Tree Models for Safety Barriers

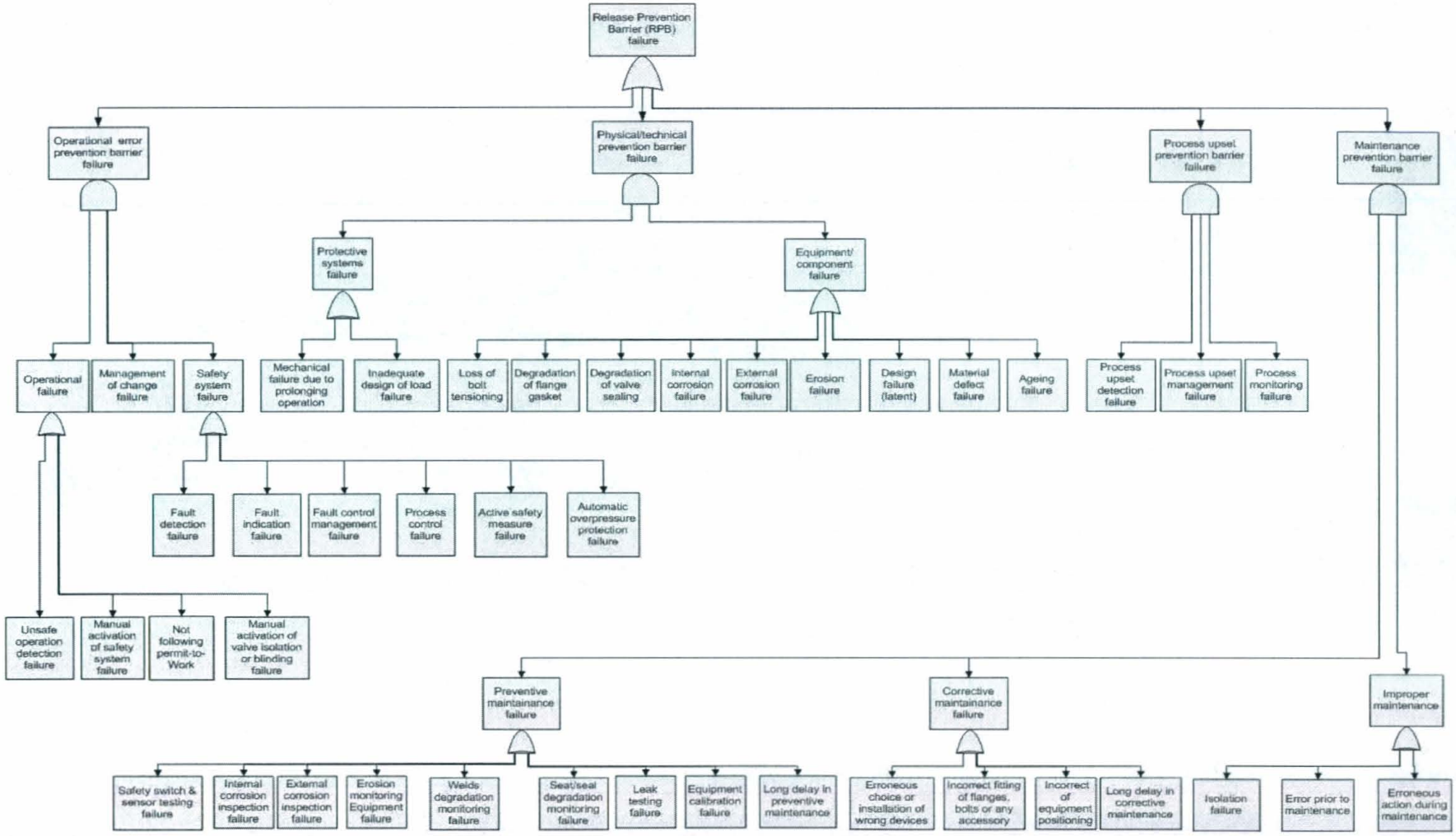

Figure A.1: Proposed generic fault tree model for release prevention barrier (RPB)

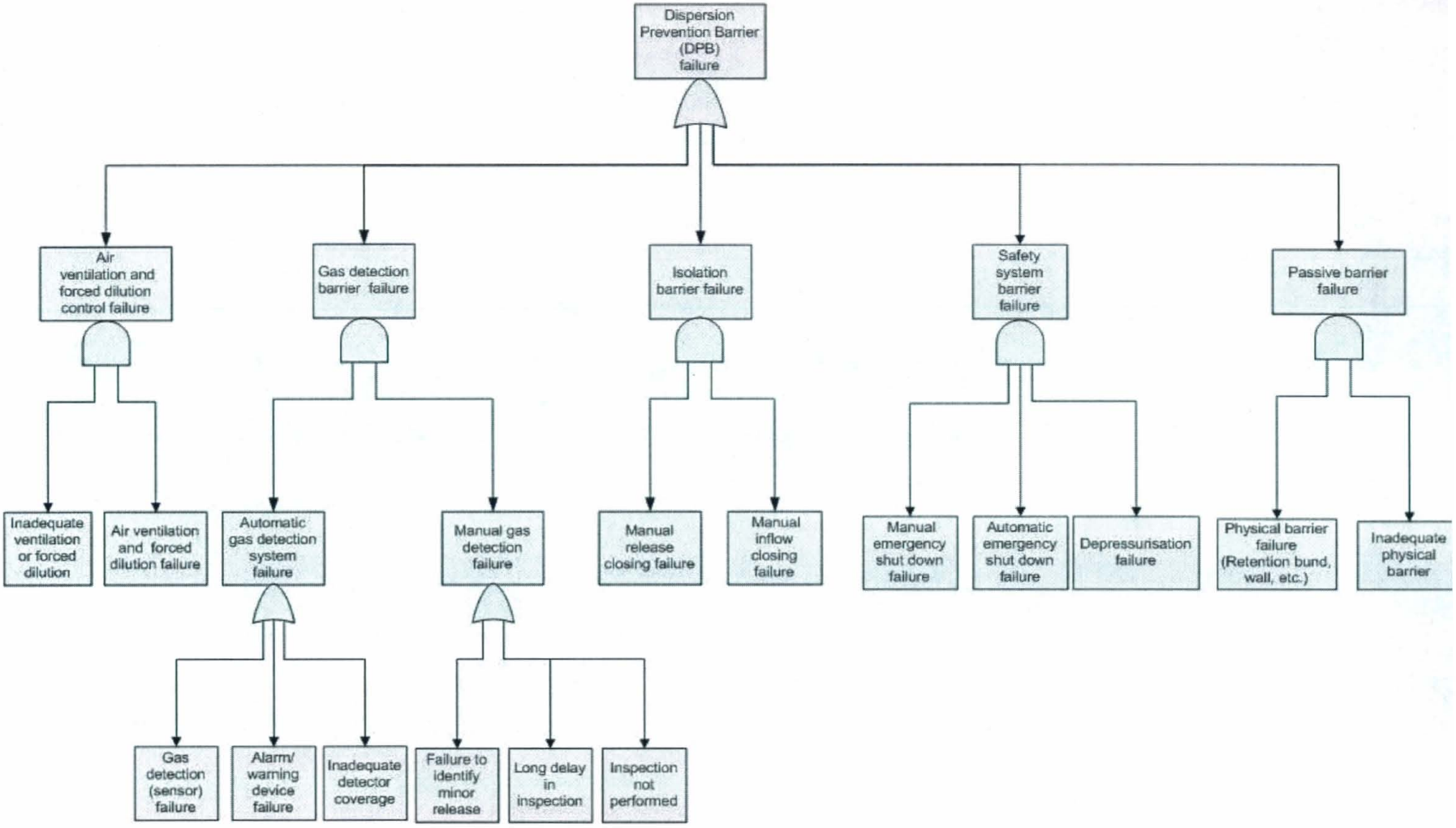

Figure A.2: Proposed generic fault tree model for dispersion prevention barrier (DPB)

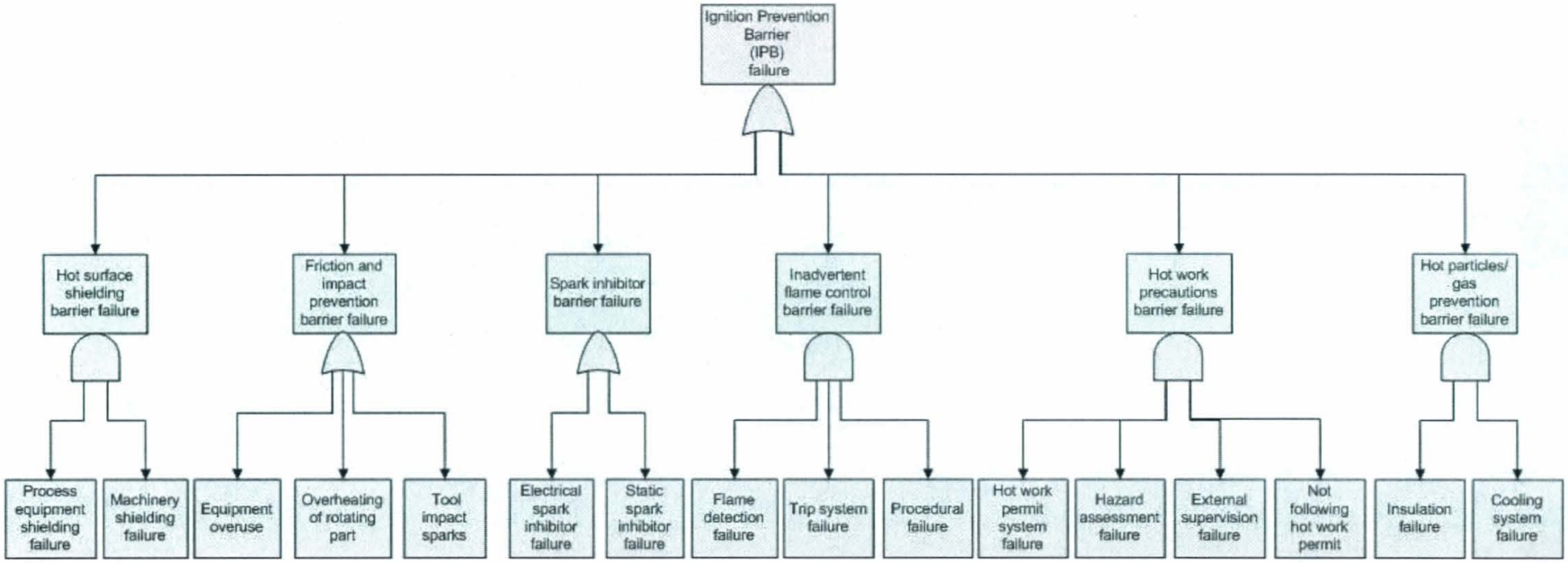

Figure A.3: Proposed generic fault tree model for ignition prevention barrier (IPB)

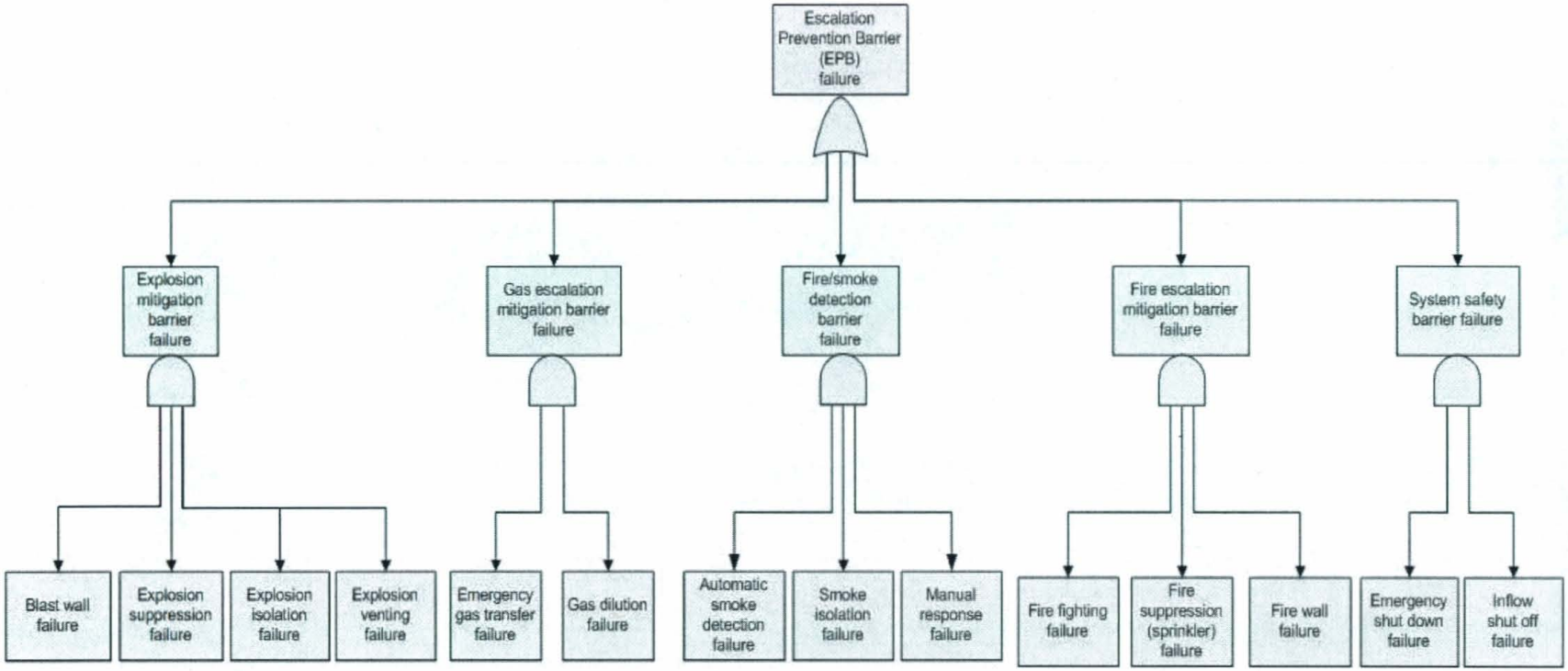

Figure A.4: Proposed generic fault tree model for escalation prevention barrier (EPB)

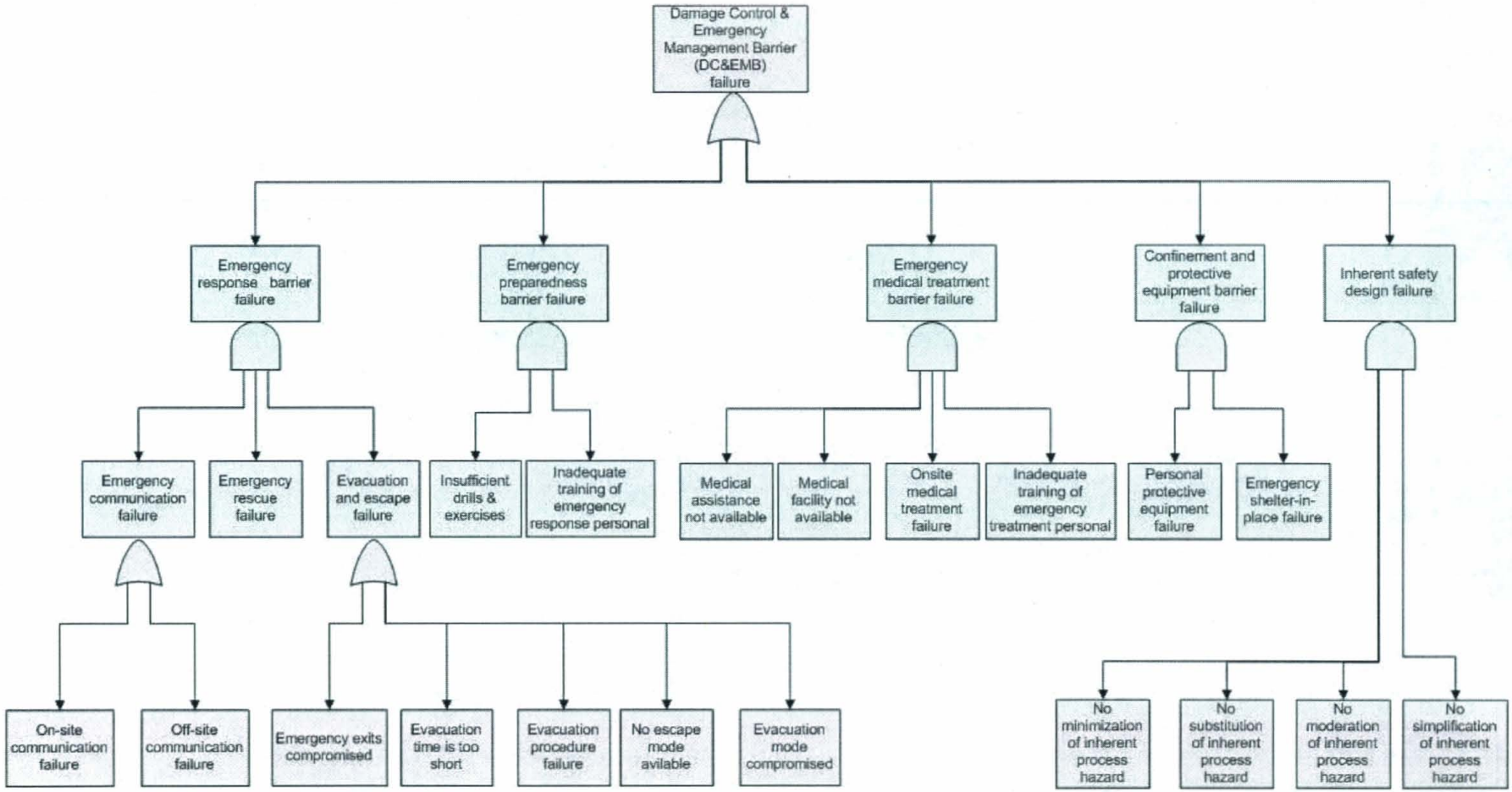

Figure A.5: Proposed generic fault tree model for damage control and emergency management barrier (DC&EMB)

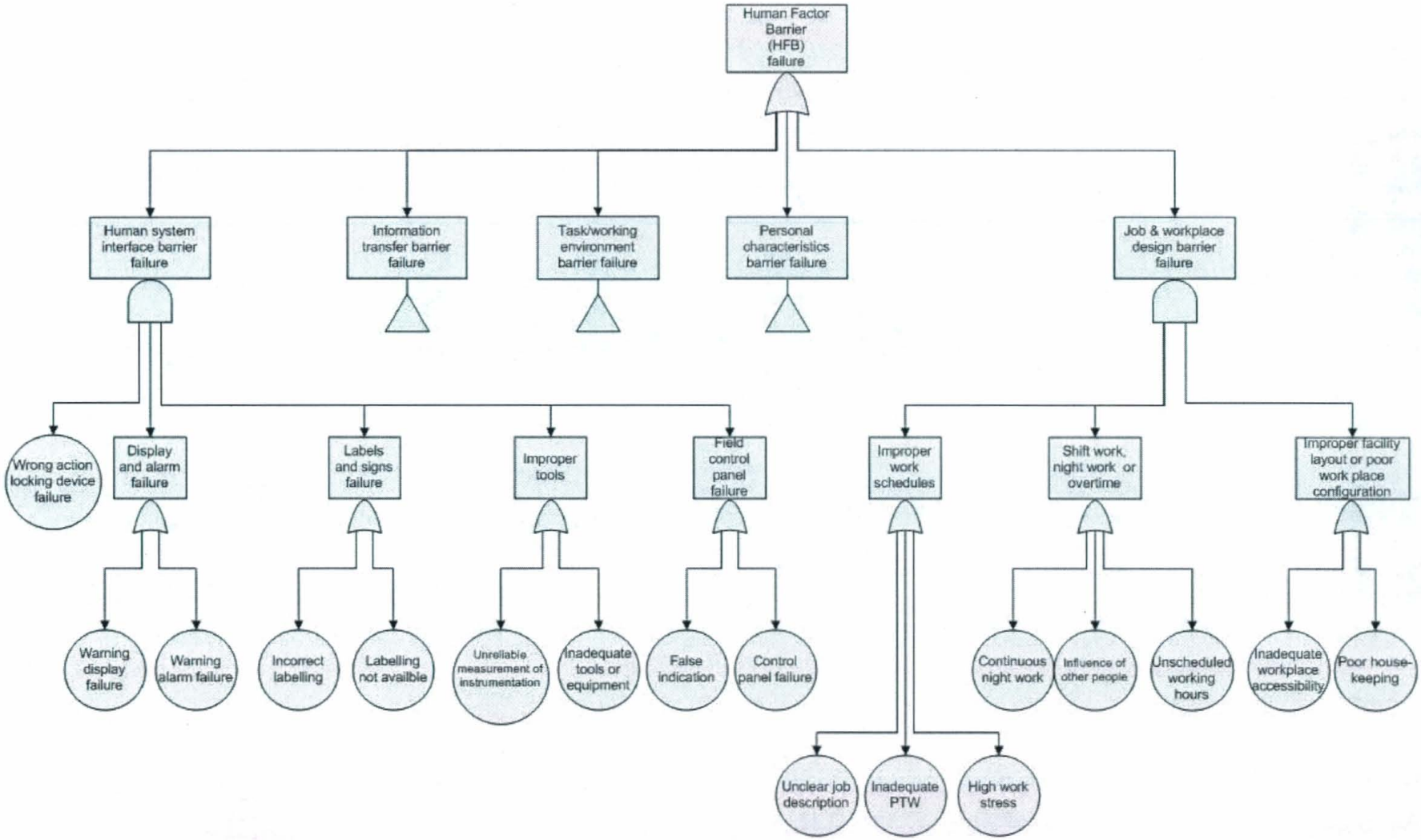

Figure A.6: Proposed generic fault tree model for human factor barrier (HFB)

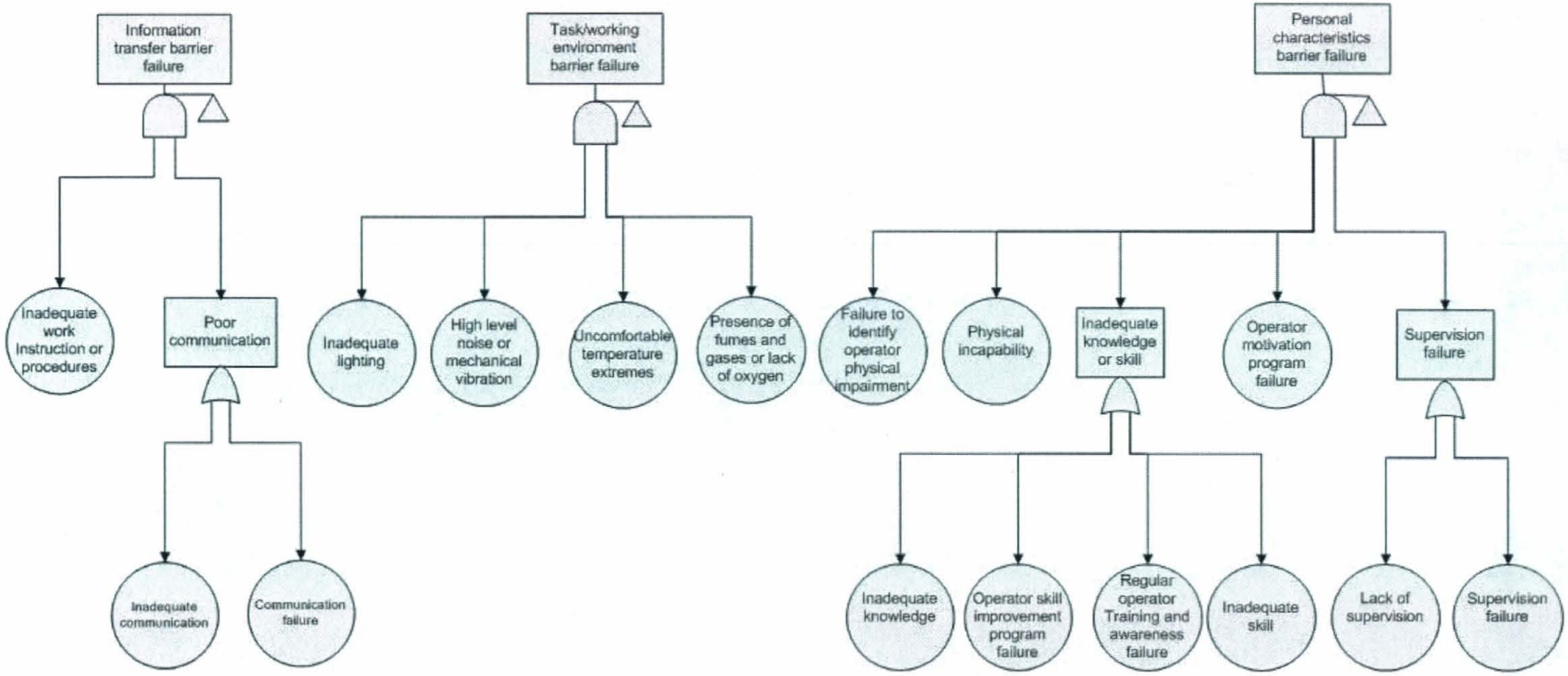

Figure A.6: Proposed generic fault tree model for human factor barrier (HFB) (cont..)

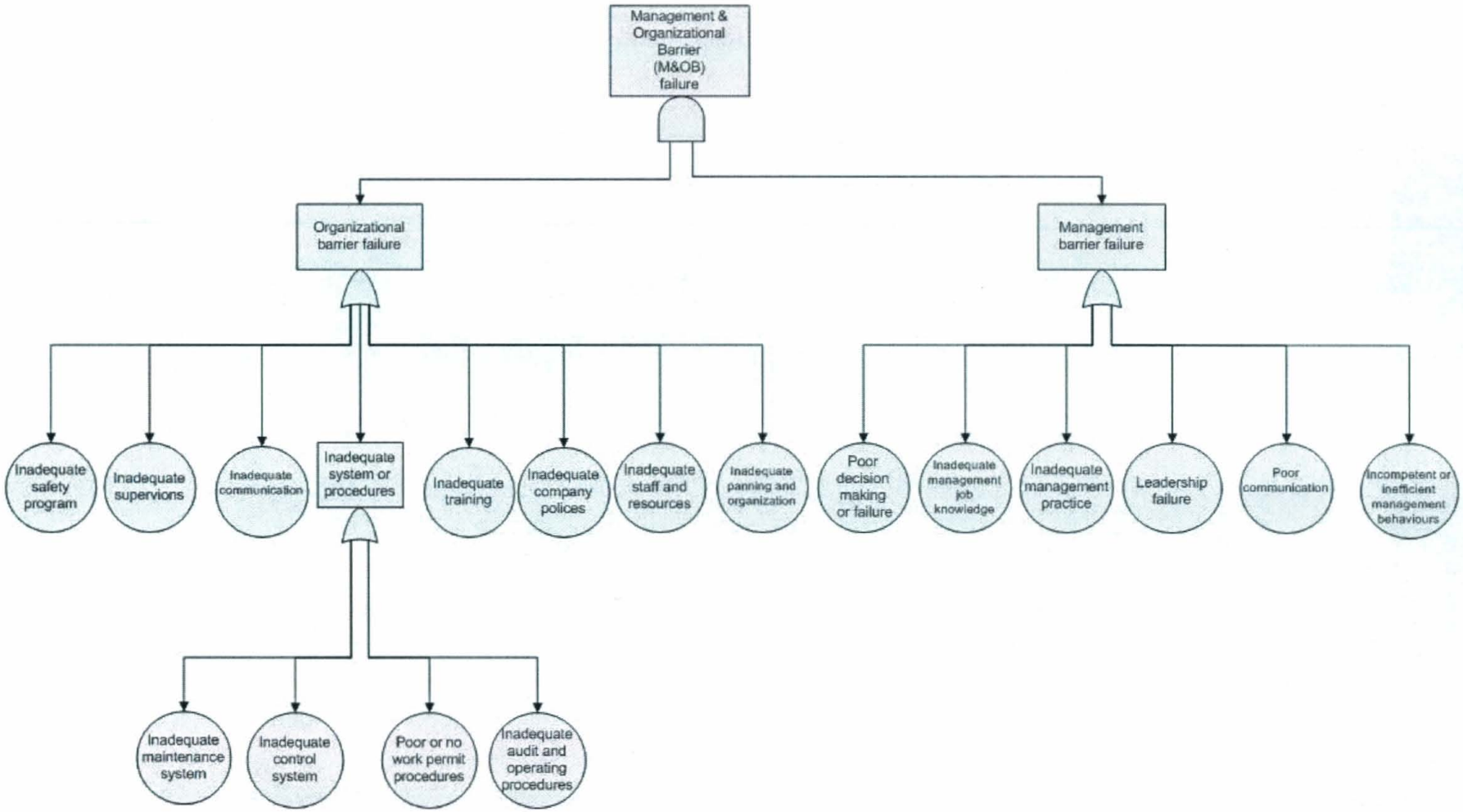

Figure A.7: Proposed generic fault tree model for management and organizational barrier (M&OB)

APPENDIX B : Case Study Fault tree analysis of safety barrier

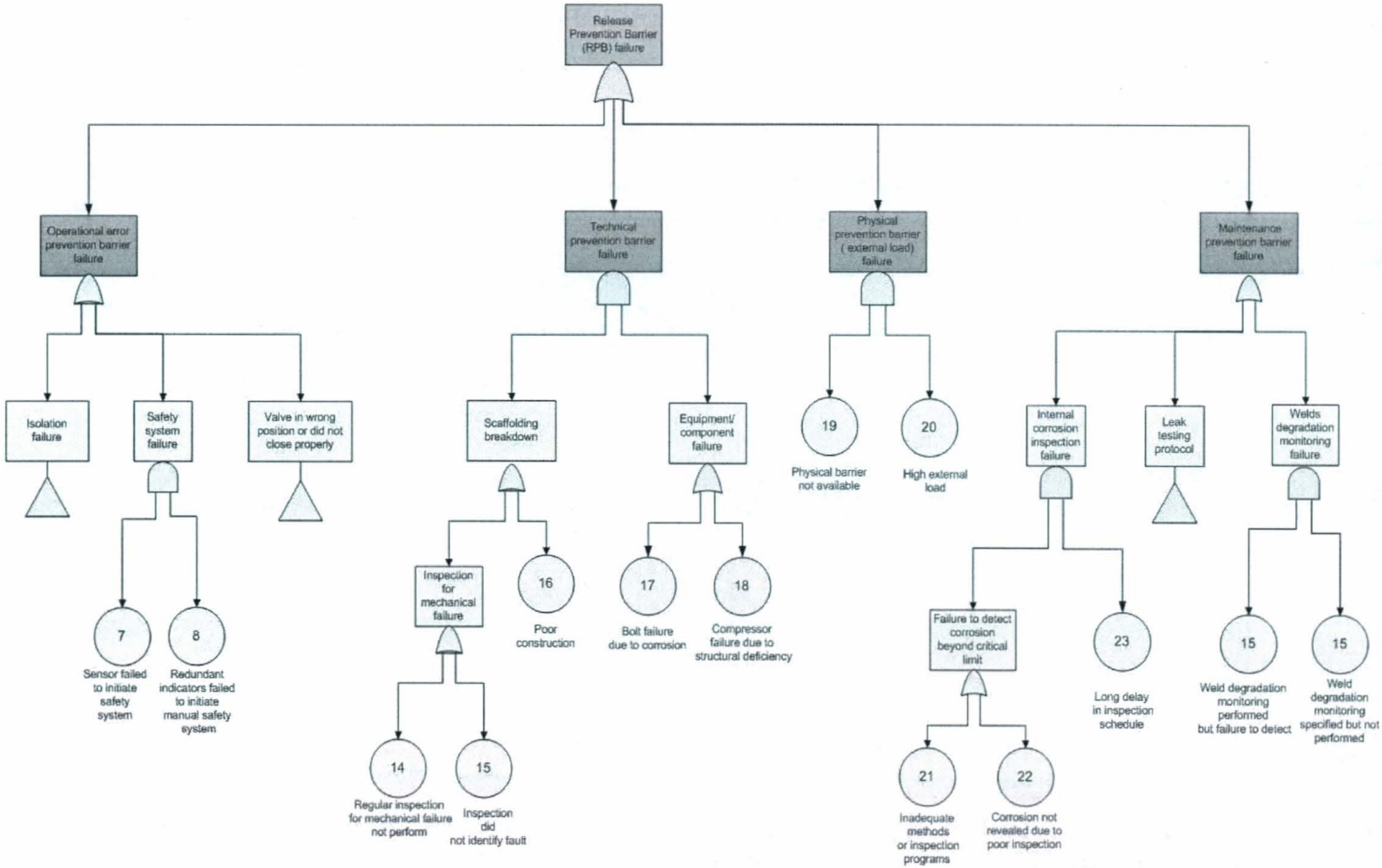

Figure B.1: Fault tree analysis of Release Prevention Barrier (RPB) failure

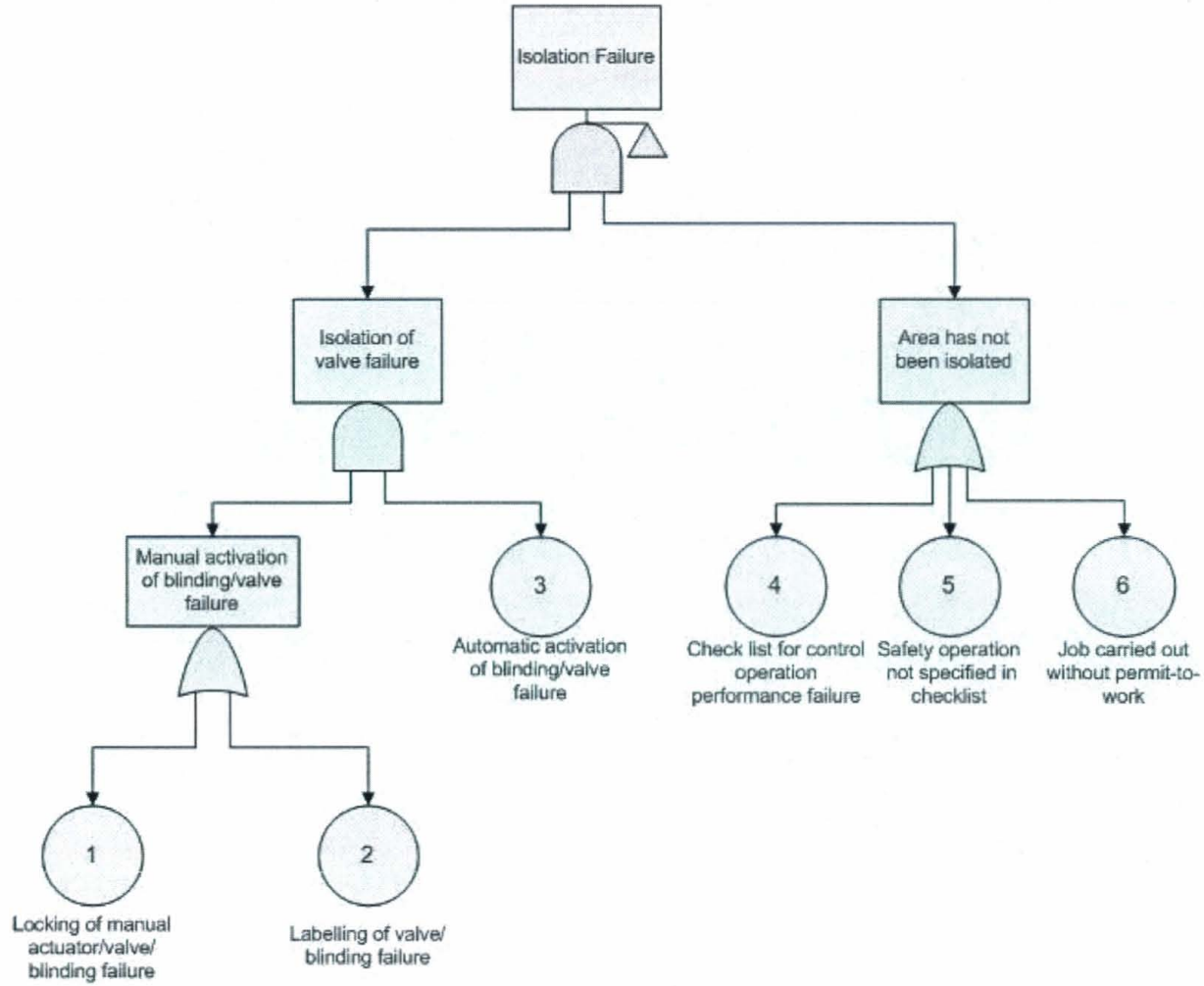

Figure B.1: Fault tree analysis of Release Prevention Barrier (RPB) failure (Continuing)

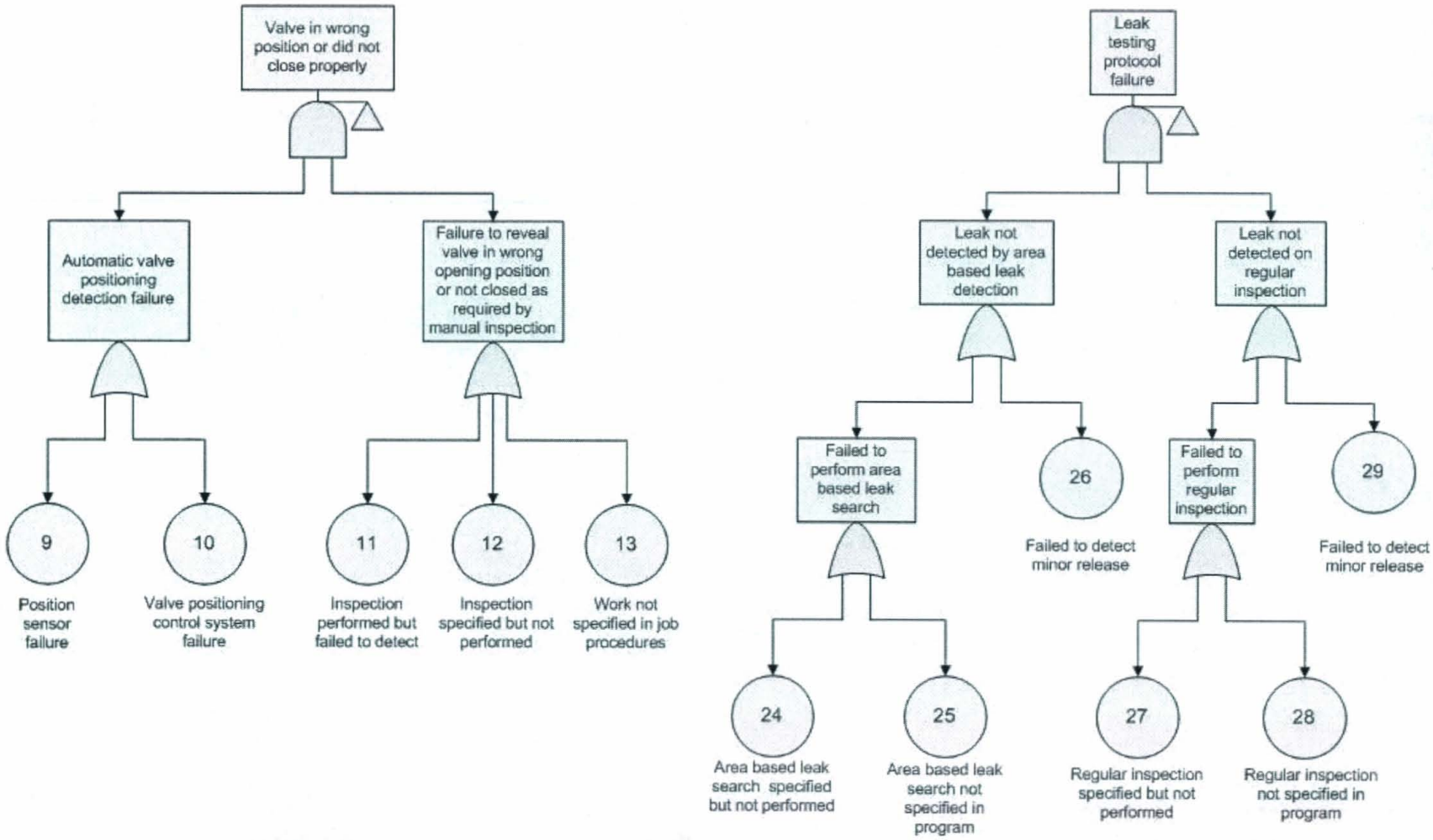

Figure B.1: Fault tree analysis of Release Prevention Barrier (RPB) failure (Continuing)

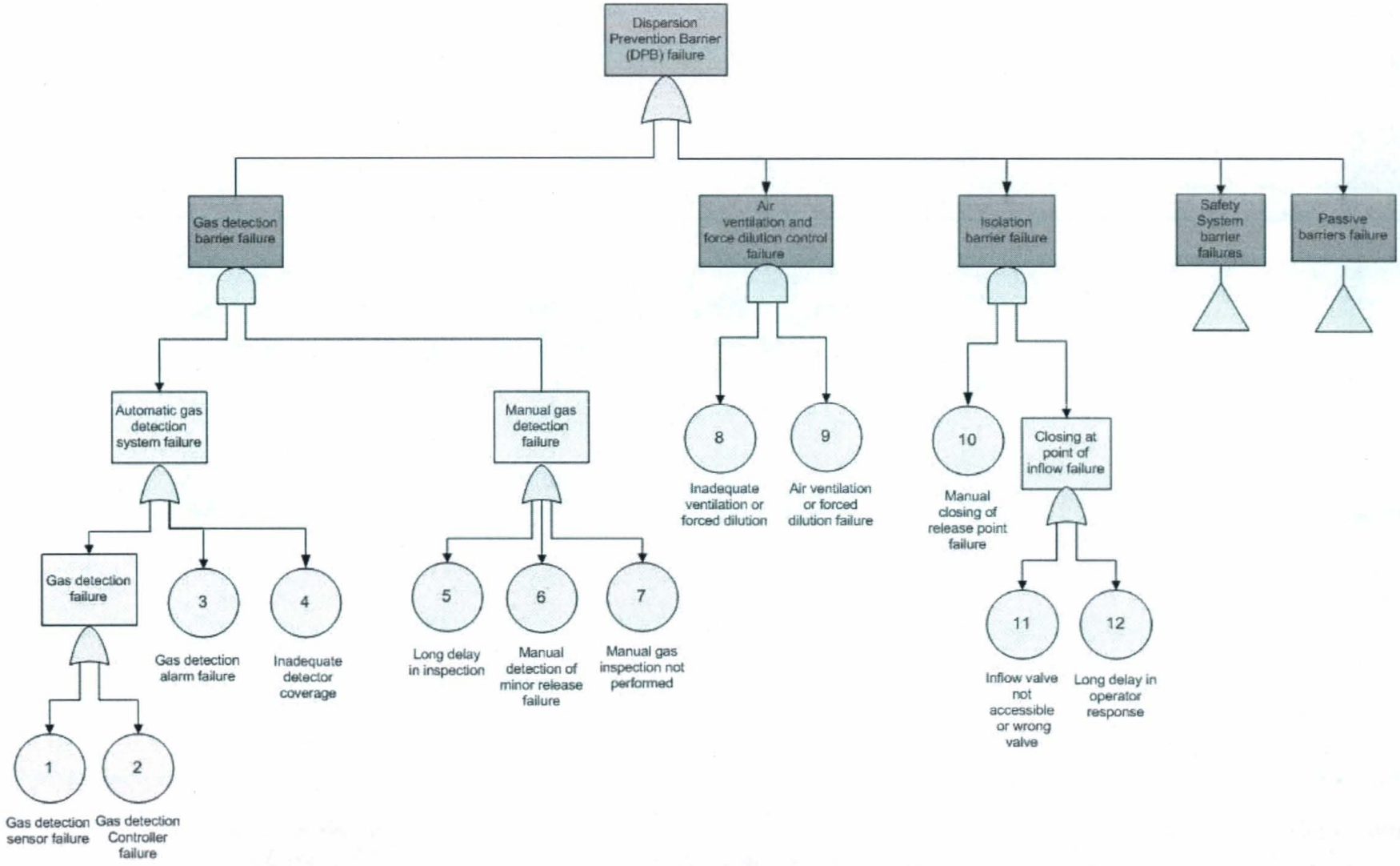

Figure B.2: Fault tree analysis of Dispersion Prevention Barrier (DPB) failure

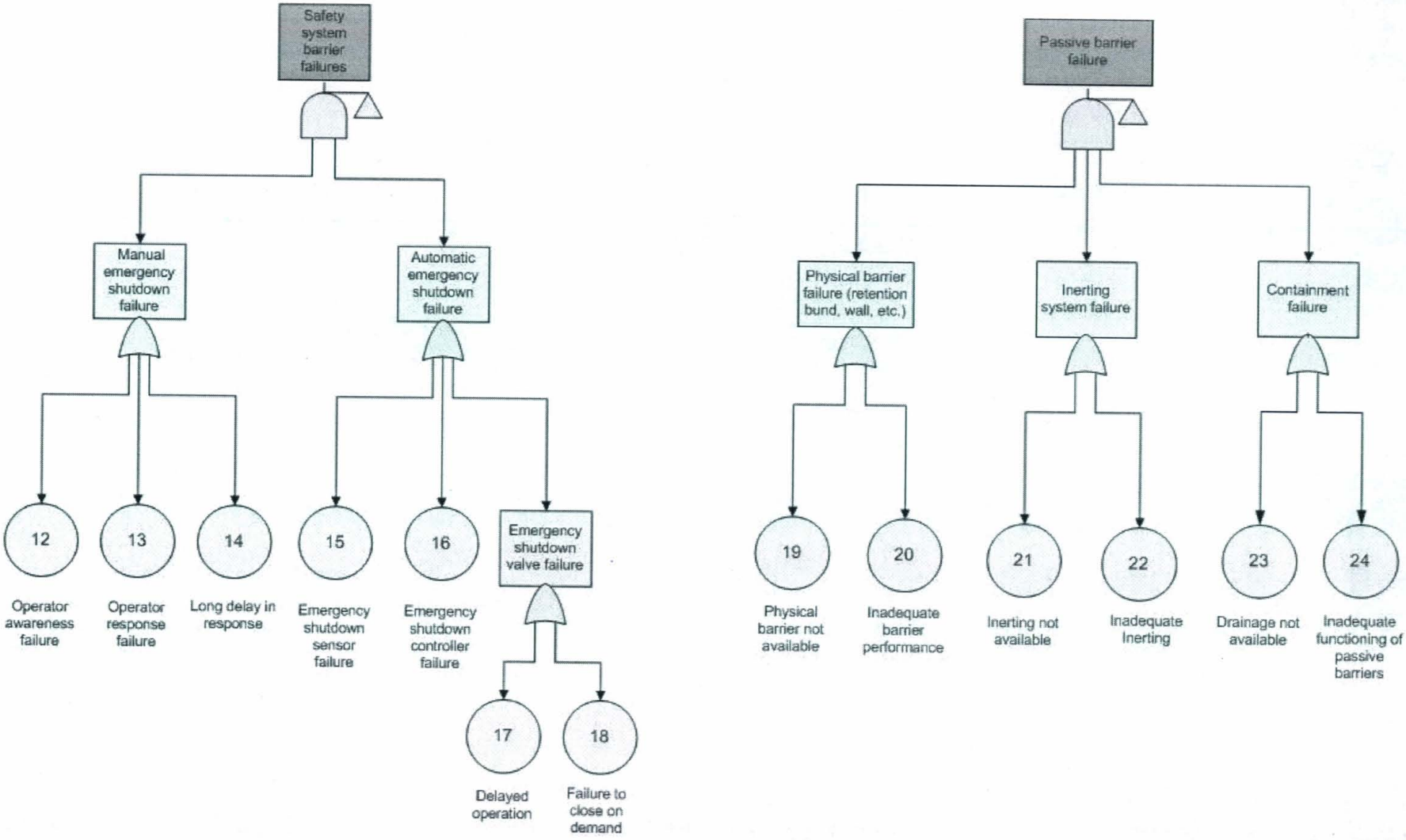

Figure B.2: Fault tree analysis of Dispersion Prevention Barrier (DPB) failure (Continuing)

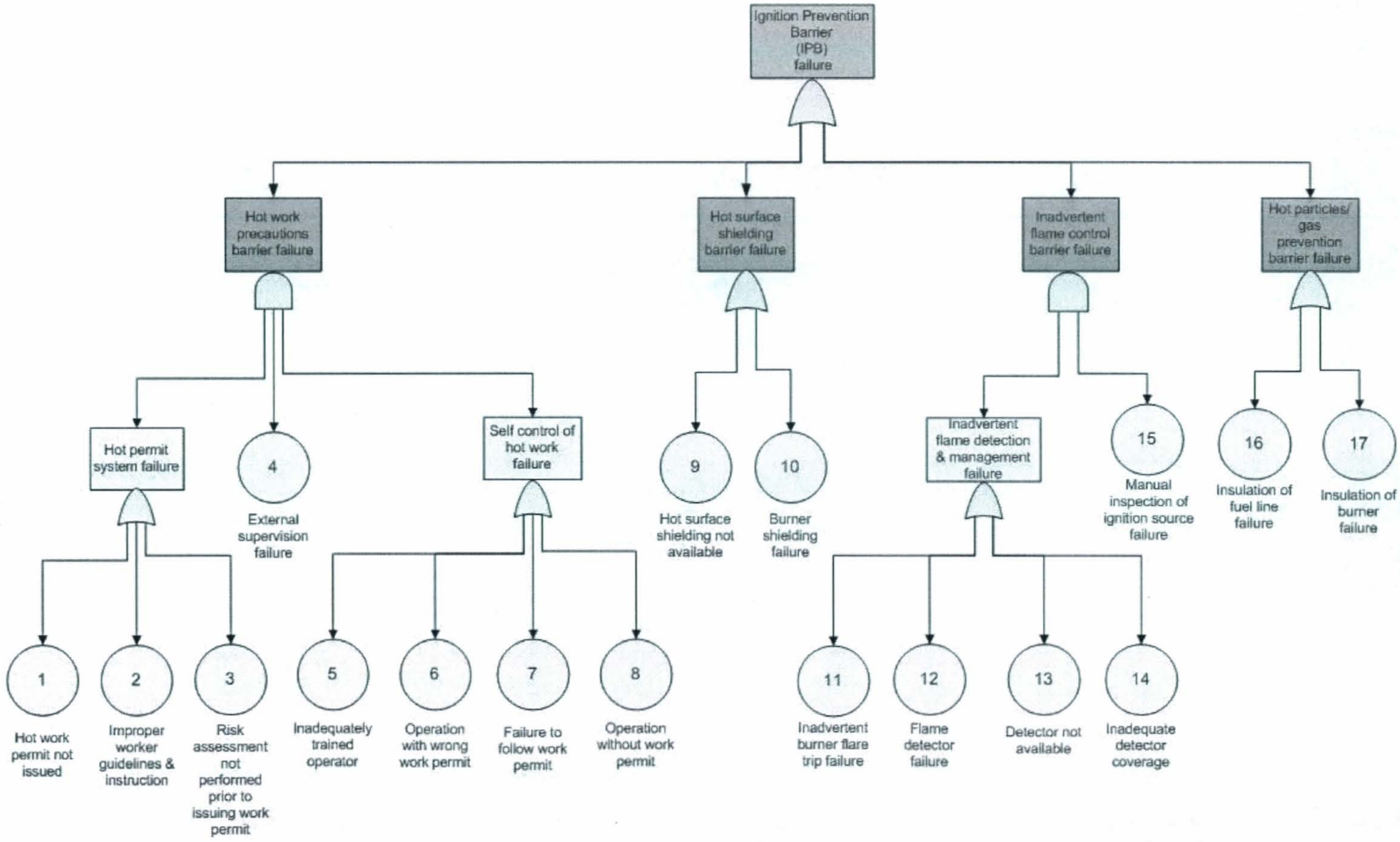

Figure B.3: Fault tree analysis of Ignition Prevention Barrier (IPB) failure

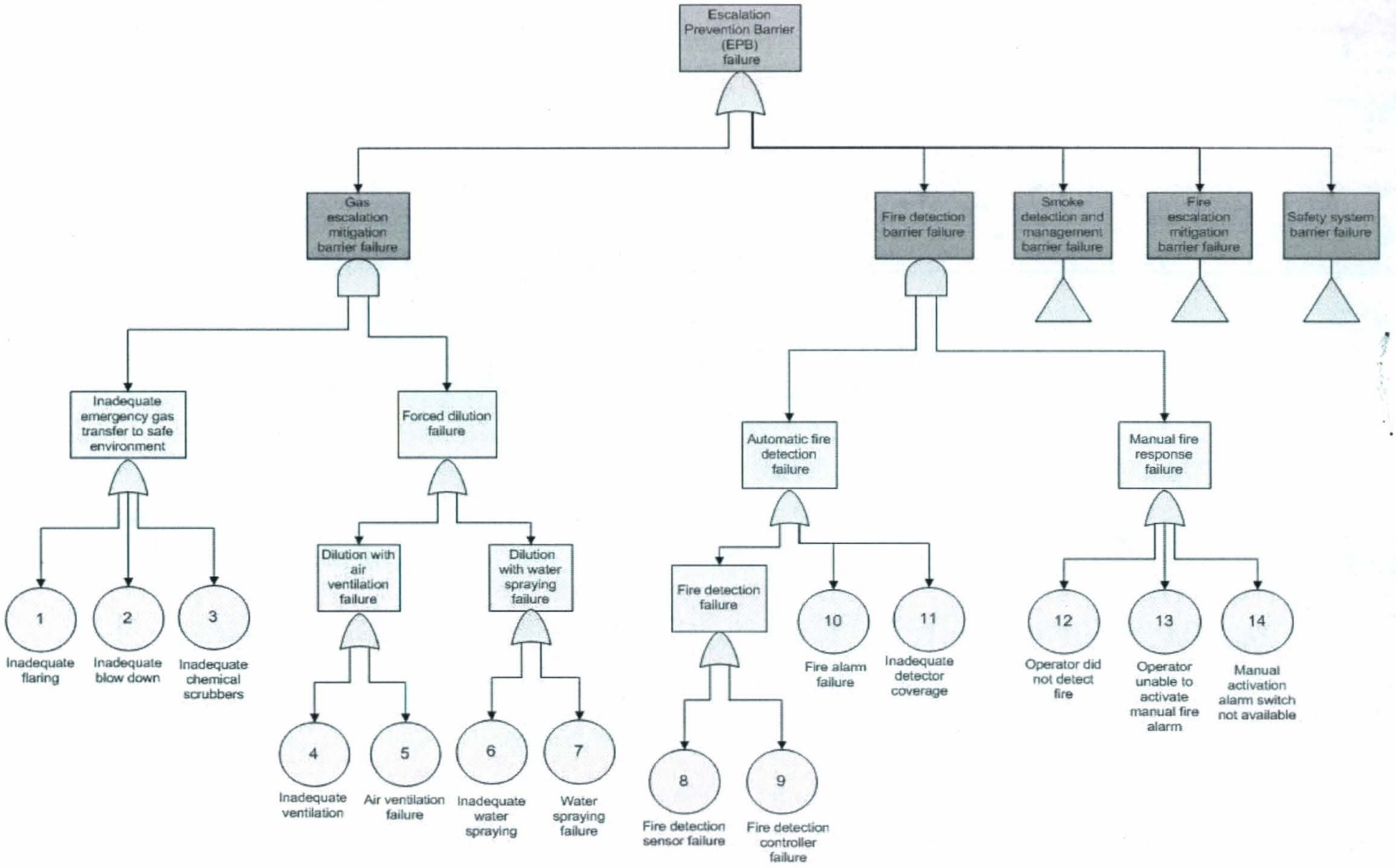

Figure B.4: Fault tree analysis of Escalation Prevention Barrier (EPB) failure

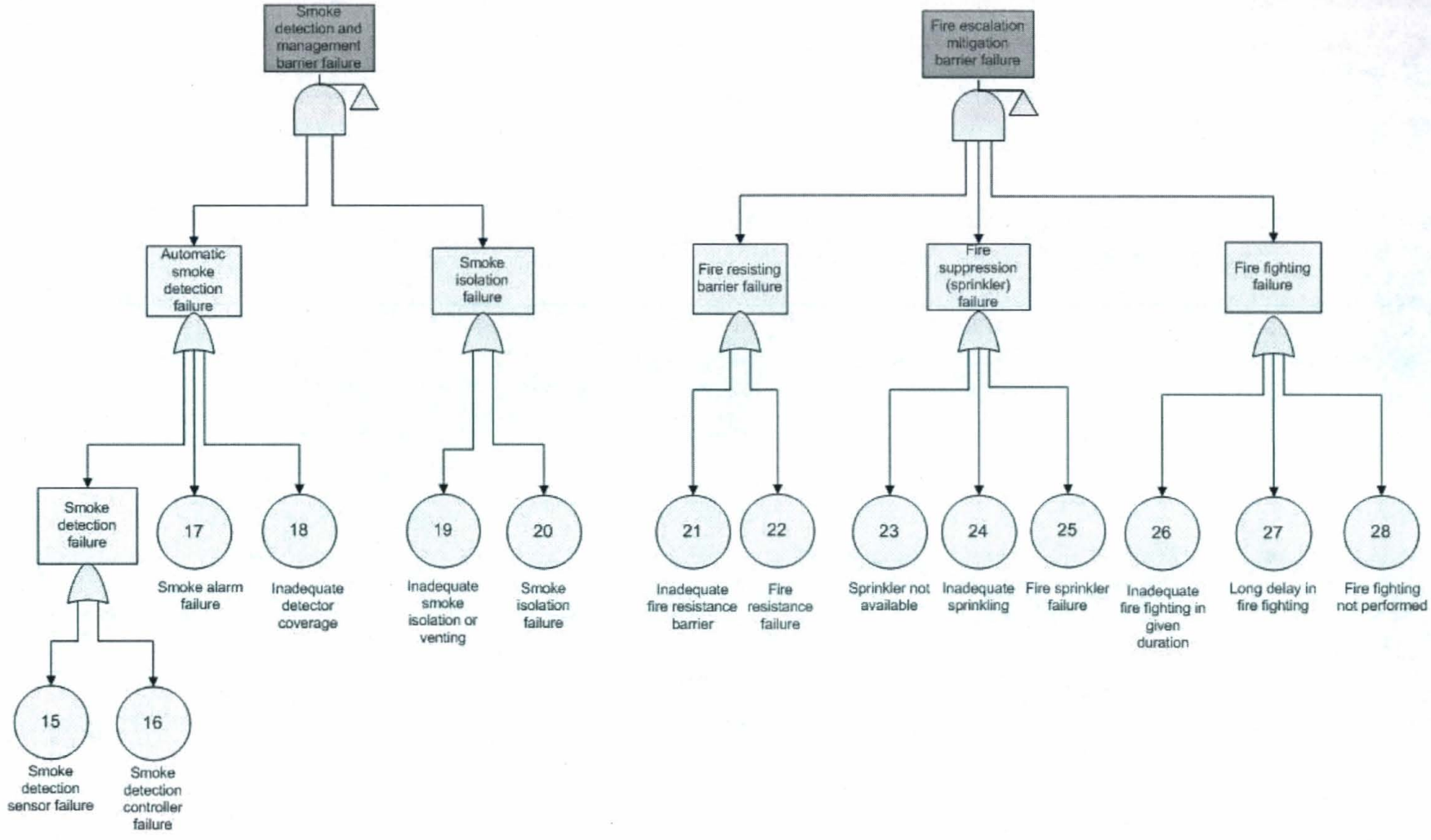

Figure B.4: Fault tree analysis of Escalation Prevention Barrier (EPB) failure (Continuing)

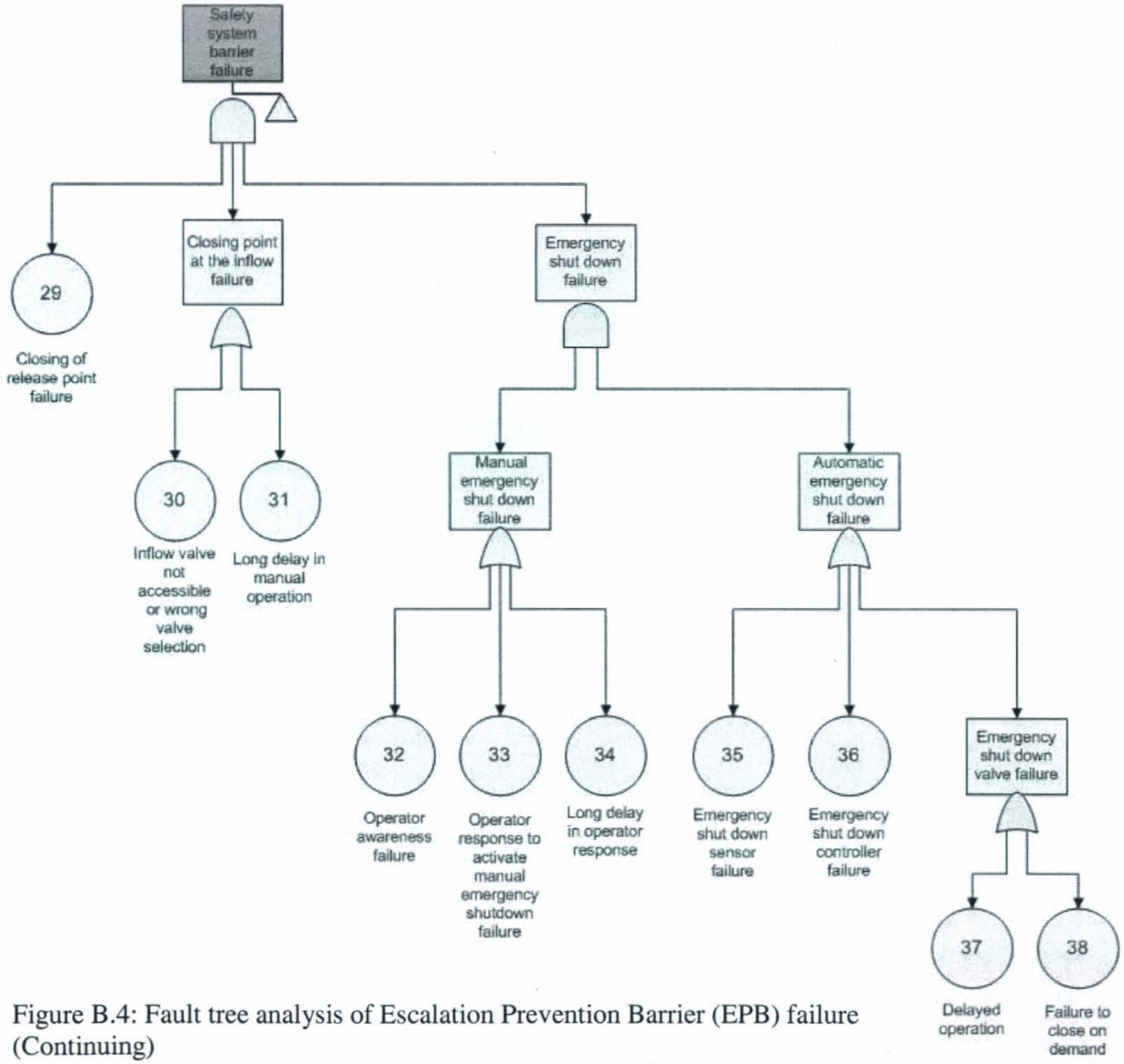

Figure B.4: Fault tree analysis of Escalation Prevention Barrier (EPB) failure (Continuing)

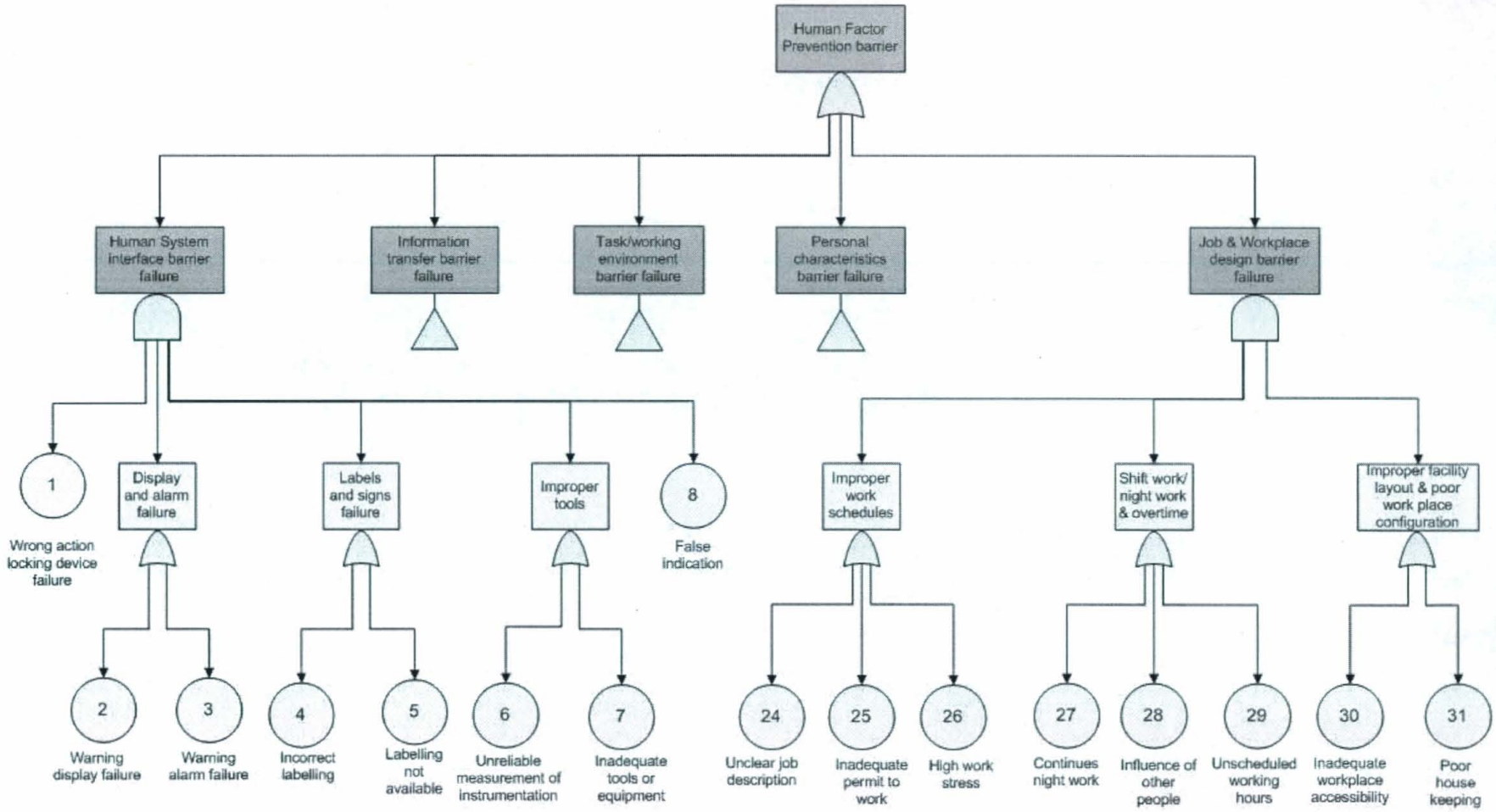

Figure B.5: Fault tree analysis of Human Factor Barrier (HFB) failure

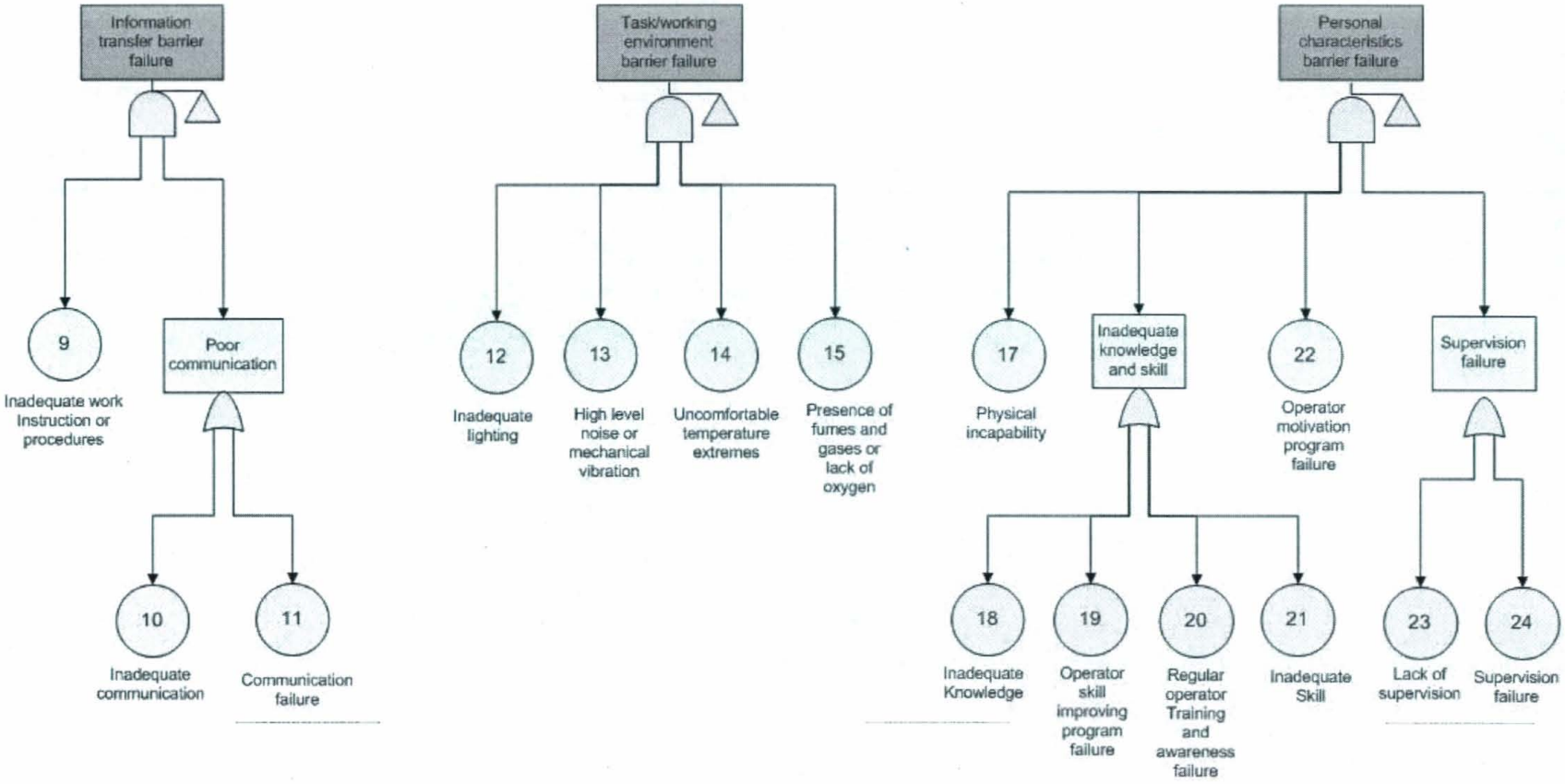

Figure B.5: Fault tree analysis of Human Factor Barrier (HFB) failure (continuing)

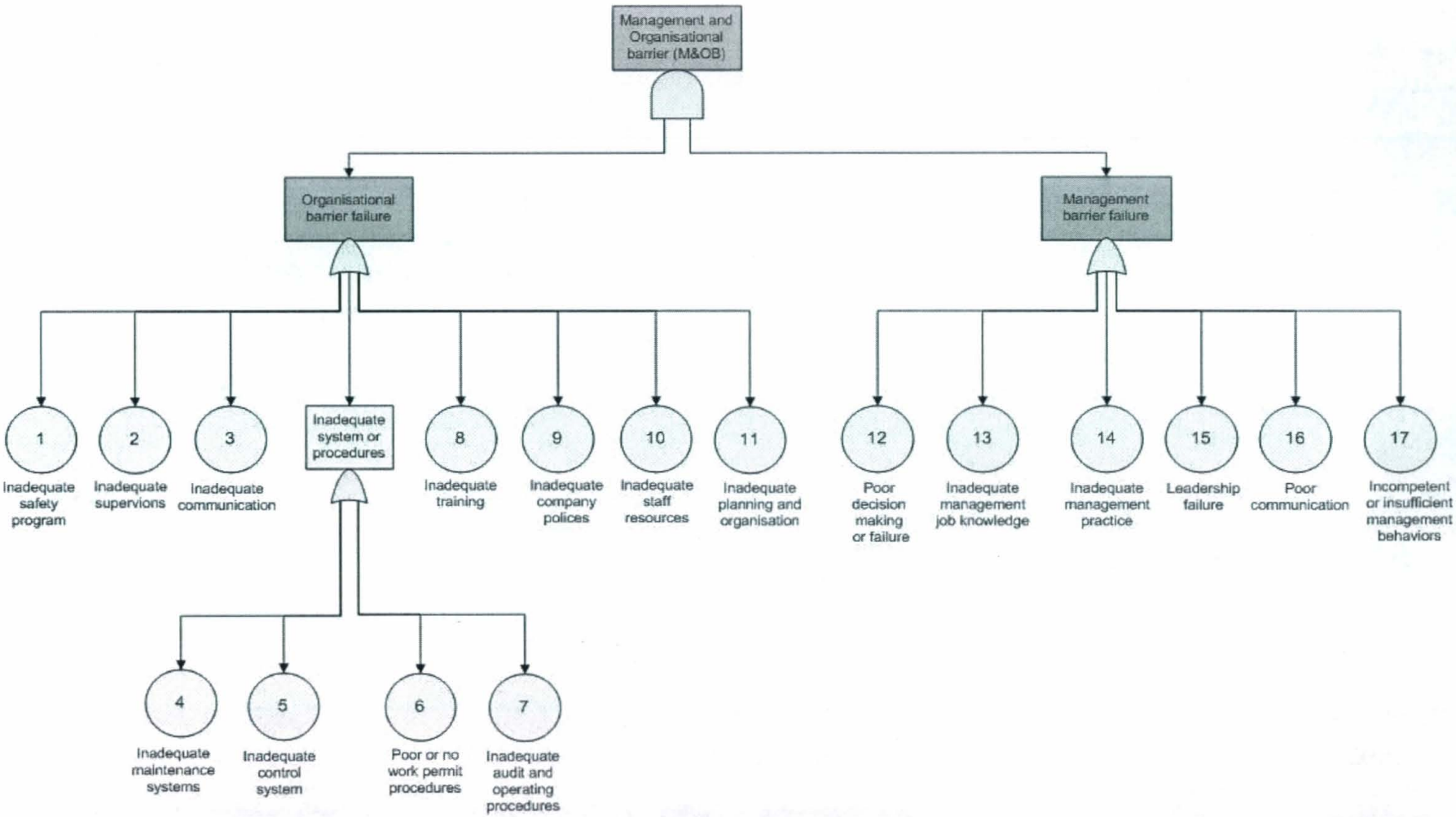

Figure B.6: Fault tree analysis of Management and Organizational Barrier (IPB) failure

APPENDIX C: Basic event failure probability Tables

Table C.1 : Basic event failure probability for Release Prevention Barrier (RPB)

Event	Event Description	Assigned probability
1	Locking of manual actuator / valve / blinding failure	0.050
2	Labeling of valve / blinding failure	0.008
3	Automatic activation of blinding failure	0.071
4	Check list for control operation failed to perform	0.010
5	Adequate safety operations are not specified	0.040
6	Operating with out Permit to Work (PTW)	0.010
7	Sensors failed to initiate the safety system	0.024
8	Redundant indicators failed to initiate manual safety system	0.020
9	Valve positioning sensor failure (function on demand)	0.090
10	Valve positioning control system failure	0.0147
11	Inspection of valve positioning performed but failed to detect	0.150
12	Inspection specified but not performed	0.015
13	Inspection is not specified in program	0.050
14	Regular inspection for mechanical failure did not perform	0.010
15	Regular inspection perform but did not identified the fault	0.050
16	Construction deficiency	0.010
17	Instruments (bolt) failure due to corrosion	0.0138
18	Compressor failure due to material deficiency	0.0198
19	Physical barriers are not available	0.010
20	High external load	0.010
21	Inadequate corrosion inspection program or method	0.090
22	Poor inspection	0.100
23	Long delay in inspection schedule	0.050
24	Area based leak search specified but did not perform	0.050
25	Area based leak search is not specified in program	0.070
26	Failed to detect minor release by area based leak search	0.050
27	Regular leak inspection specified but did not perform	0.050
28	Regular leak inspection is not specified in program	0.010
29	Failed to detect minor release by Regular inspection	0.050
30	Welding degrading monitoring performed but failed to detect	0.066
31	Welding degrading monitoring specified but did not perform	0.050

Table C.2: Basic event failure probability for Dispersion Prevention Barrier (DPB)

Event	Event Description	Assigned probability
1	Automatic gas detection sensor failure	0.128
2	Automatic gas detection controller failure	0.001
3	Automatic gas detection Alarm failure	0.020
4	Inadequate detector coverage	0.050
5	Long delay in Inspection	0.010
6	Manual detection of minor release failure	0.050
7	Manual inspection did not perform	0.050
8	Inadequate Ventilation or forced dilution	0.067
9	Ventilation or forced dilution failure	0.040
10	Manual closing of release failure (Clamping, Remediation, etc...)	0.025
11	Wrong Inflow valve selection or valve not accessible	0.050
12	Long delay in response	0.010
13	Operator awareness failure	0.040
14	Operator response failure	0.050
15	Long delay in manual response	0.010
16	ESD sensor failure	0.024
17	ESD controller Failure	0.250
18	ESD valve delayed operation	0.050
19	ESD valve failure to close on demand	0.130
20	Physical barrier not available	0.001
21	Inadequate barrier performance	0.010
22	Inerting not available	0.050
23	Inerting failure	0.080
24	Drainage not available	0.001
25	Inadequate functioning	0.001

Table C.3: Basic event failure probability for Ignition Prevention Barrier (IPB)

Event	Event Description	Assigned probability
1	Hot work permit has not been issued	0.033
2	Inadequate procedures or instruction in work permit	0.067
3	Risk assessment not performed prior to issue work permit	0.100
4	External supervision failure	0.083
5	Inadequate trained operator	0.100
6	Operation with wrong work permit	0.040
7	Failure to follow work permit	0.045
8	Operation without work permit	0.010
9	Hot surface shielding not available	0.067
10	Burner shielding failure	0.010
11	Inadvertent burner flare trip failure	0.044
12	Flame detector failure	0.056
13	Flame detector not available	0.050
14	Inadequate detector coverage	0.070
15	Manual inspection of ignition source failure	0.050
16	Insulation of fuel line failure	0.010
17	Insulation of burner failure	0.010

Table C.4: Basic event failure probability for Escalation Prevention Barrier (EPB)

Event	Event Description	Assigned probability
1	Inadequate flaring	0.001
2	Inadequate blow down	0.001
3	Inadequate chemical scrubbers	0.008
4	Inadequate air ventilation	0.067
5	Air ventilation failure	0.030
6	Inadequate water spraying	0.067
7	Water spraying failure	0.045
8	Fire detection Sensor failure	0.080
9	Fire detection Controller failure	0.001
10	Fire Alarm failure	0.021
11	Inadequate detector coverage	0.200
12	Operator did not detect the fire	0.050
13	Operator unable to activate the manual fire alarm	0.001
14	Manual fire alarm activator failure	0.001
15	Smoke detection sensor failure	0.080
16	Smoke detection Controller failure	0.001
17	Smoke Alarm failure	0.021
18	Inadequate detector coverage	0.070
19	Inadequate smoke isolation or venting	0.060
20	Smoke isolation failure	0.005
21	Inadequate fire resistant barrier	0.003
22	Fire resistant failure	0.030
23	Sprinkler not available	0.010
24	Inadequate sprinkling	0.040
25	Sprinkler failure	0.045
26	Inadequate Fire fighting in given duration	0.020
27	long delay Fire fighting	0.080
28	Fire fighting did not perform	0.0001
29	Closing release failure	0.013
30	Inflow valve not accessible or wrong valve	0.050
31	Long delay in manual operation	0.010
32	Operator awareness failure	0.040
33	Operator response to activate manual ESD failure	0.050
34	Long delay in response	0.010
35	ESD sensor failure	0.024
36	ESD Controller Failure	0.100
37	ESD valve delayed operation	0.050
38	ESD valve failure to close on demand	0.070

Table C.5: Plant specific and expert opinion data of basic event for Human Factor Barrier (HFB)

Event	Event Description	Assigned probability
1	Wrong action locking device failure	0.050
2	Warning display failure	0.050
3	Warning alarm failure	0.020
4	Incorrect labeling	0.100
5	Labeling not available	0.100
6	Unreliable measurement of instrumentation	0.001
7	Inadequate tools or equipments	0.020
8	False indication	0.020
9	Inadequate work instruction or procedures	0.025
10	Inadequate communication	0.050
11	Communication failure	0.025
12	Inadequate lighting	0.034
13	High level noise or mechanical vibration	0.050
14	Uncomfortable temperature extremes	0.100
15	Presence of fumes or gases or lack of oxygen	0.034
16	Physical incapability	0.050
17	Inadequate knowledge	0.100
18	Operator skill improvement program failure	0.020
19	Regular operator training and awareness failure	0.034
20	Inadequate skill	0.050
21	Operator motivation program failure	0.020
22	Lack of supervision	0.050
23	Supervision failure	0.020
24	Unclear job description	0.034
25	Inadequate permit-to-work	0.050
26	High work stress	0.067
27	Continuous night work	0.050
28	Influence of other people (Colleague, management, senior workers, etc.)	0.020
29	Unscheduled working hours	0.034
30	Inadequate workplace accessibility	0.020
31	Poor house-keeping	0.050

Table C.6: Plant specific and expert opinion data of basic event for Management and Organizational Barrier (M&OB)

Event	Event Description	Assigned probability
1	Inadequate safety program	0.010
2	Inadequate supervision	0.034
3	Inadequate communication	0.050
4	Inadequate maintenance system	0.020
5	Inadequate control system	0.025
6	Poor or no work permit procedures	0.050
7	Inadequate audit and operating procedures	0.034
8	Inadequate training	0.025
9	Inadequate company polices	0.020
10	Inadequate staff resources	0.020
11	Inadequate planning and organization	0.025
12	Poor decision making or failure	0.040
13	Inadequate management job knowledge	0.020
14	Inadequate management polices	0.025
15	Leadership failure	0.010
16	Poor communication	0.050
17	Incompetent or insufficient management behaviors	0.020

Table C.7: Basic event Failure rates distribution parameters for Release Prevention Barrier (RPB)

Event	Probability distribution	Parameters	
1	Normal	$\mu = 5.85$	$\sigma = 5.85\times10^{-1}$
2	Normal	$\mu = 9.17\times10^{-1}$	$\sigma = 9.20\times10^{-2}$
3	Gamma	$a = 3.97\times10^{-1}$	$b = 1.712\times10^{-5}$
4	Normal	$\mu = 1.14$	$\sigma = 1.14\times10^{-1}$
5	Normal	$\mu = 4.66$	$\sigma = 4.66\times10^{-1}$
6	Normal	$\mu = 1.14$	$\sigma = 1.14\times10^{-1}$
7	Gamma	$a = 1.99$	$b = 1.41\times10^{-6}$
8	Lognormal	$\mu = -1.30\times10^{1}$	$\sigma = 9.97\times10^{-2}$
9	Gamma	$a = 1.49$	$b = 7.2\times10^{-6}$
10	Normal	$\mu = 1.69$	$\sigma = 1.69\times10^{-1}$
11	Lognormal	$\mu = -1.09\times10^{1}$	$\sigma = 9.97\times10^{-2}$
12	Lognormal	$\mu = -1.33\times10^{1}$	$\sigma = 9.97\times10^{-2}$
13	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
14	Normal	$\mu = 1.14$	$\sigma = 1.14\times10^{-1}$
15	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
16	Normal	$\mu = 1.15$	$\sigma = 1.15\times10^{-2}$
17	Lognormal	$\mu = -1.27\times10^{1}$	$\sigma = 9.97\times10^{-2}$
18	Gamma	$a = 1.65\times10^{-1}$	$b = 1.39\times10^{-5}$
19	Normal	$\mu = 1.15$	$\sigma = 1.15\times10^{-2}$
20	Lognormal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$
21	Lognormal	$\mu = -1.14\times10^{1}$	$\sigma = 9.97\times10^{-2}$
22	Lognormal	$\mu = -1.14\times10^{1}$	$\sigma = 9.97\times10^{-2}$
23	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
24	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
25	Normal	$\mu = 8.28$	$\sigma = 8.28\times10^{-1}$
26	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
27	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
28	Normal	$\mu = 1.14$	$\sigma = 1.14\times10^{-1}$
29	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
30	Normal	$\mu = 7.79$	$\sigma = 7.80\times10^{-1}$
31	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$

Table C.8: Basic event Failure rates distribution parameters for Dispersion Prevention Barrier (DPB)

Event	Probability distribution	Parameters	
1	Gamma	a=1.01	$b=1.31\times10^{-5}$
2	Gamma	a=1.02	$b=1.63\times10^{-7}$
3	Lognormal	$\mu=-1.30\times10^{1}$	$\sigma=9.97\times10^{-2}$
4	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
5	log normal	$\mu=-1.37\times10^{1}$	$\sigma=9.97\times10^{-2}$
6	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
7	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
8	Normal	$\mu=7.92$	$\sigma=7.92\times10^{-1}$
9	Normal	$\mu=4.66$	$\sigma=4.66\times10^{-1}$
10	Normal	$\mu=2.89$	$\sigma=2.89\times10^{-1}$
11	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
12	Lognormal	$\mu=-1.37\times10^{1}$	$\sigma=9.97\times10^{-2}$
13	Normal	$\mu=4.66$	$\sigma=4.66\times10^{-1}$
14	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
15	Lognormal	$\mu=-1.37\times10^{1}$	$\sigma=9.97\times10^{-2}$
16	Gamma	a=1.64	$b=2.04\times10^{-6}$
17	Lognormal	$\mu=-1.03\times10^{1}$	$\sigma=9.97\times10^{-2}$
18	Gamma	a=2.23	$b=2.44\times10^{-6}$
19	Gamma	$a=6.56\times10^{-1}$	$b=2.43\times10^{-5}$
20	Normal	$\mu=1.14\times10^{-1}$	$\sigma=1.14\times10^{-2}$
21	Normal	$\mu=1.15$	$\sigma=1.15\times10^{-1}$
22	Normal	$\mu=5.86$	$\sigma=5.85\times10^{-1}$
23	Normal	$\mu=9.52$	$\sigma=9.52\times10^{-1}$
24	Normal	$\mu=1.14\times10^{-1}$	$\sigma=1.14\times10^{-2}$
25	Normal	$\mu=1.14\times10^{-1}$	$\sigma=1.14\times10^{-2}$

Table C.9: Basic event Failure rates distribution parameters for Ignition Prevention Barrier (IPB)

Event	Probability distribution	Parameters	
1	Normal	$\mu = 3.83$	$\sigma = 3.83\times10^{-1}$
2	Normal	$\mu = 7.92$	$\sigma = 7.92\times10^{-1}$
3	Normal	$\mu = 1.20\times10^{1}$	$\sigma = 1.2$
4	Normal	$\mu = 9.89$	$\sigma = 9.89\times10^{-1}$
5	Normal	$\mu = 1.20\times10^{1}$	$\sigma = 1.2$
6	Normal	$\mu = 4.66$	$\sigma = 4.66\times10^{-1}$
7	Normal	$\mu = 5.256$	$\sigma = 5.26\times10^{-1}$
8	Normal	$\mu = 1.15$	$\sigma = 1.15\times10^{-1}$
9	Normal	$\mu = 7.92$	$\sigma = 7.92\times10^{-1}$
10	Log normal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$
11	Gamma	$a = 4.13\times10^{-1}$	$b = 1.10\times10^{-5}$
12	Gamma	$a = 1.0$	$b = 6.61\times10^{-6}$
13	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
14	Normal	$\mu = 8.28$	$\sigma = 8.30\times10^{-1}$
15	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
16	Log normal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$
17	Log normal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$

Table C.8: Basic event Failure rates distribution parameters for Escalation Prevention Barrier (EPB)

Event	Probability distribution	Parameters	
1	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
2	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
3	Normal	$\mu = 9.17\times10^{-1}$	$\sigma = 9.20\times10^{-2}$
4	Normal	$\mu = 7.92$	$\sigma = 7.92\times10^{-1}$
5	Log normal	$\mu = -1.26\times10^{1}$	$\sigma = 9.97\times10^{-2}$
6	Normal	$\mu = 7.92$	$\sigma = 7.92\times10^{-1}$
7	Log normal	$\mu = -1.21\times10^{1}$	$\sigma = 9.97\times10^{-2}$
8	Gamma	$a = 1.22$	$b = 7.635\times10^{-6}$
9	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
10	Log normal	$\mu = -1.29\times10^{1}$	$\sigma = 9.97\times10^{-2}$
11	Normal	$\mu = 2.55\times10^{1}$	$\sigma = 2.55$
12	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
13	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
14	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
15	Gamma	$a = 1.22$	$b = 7.635\times10^{-6}$
16	Normal	$\mu = 1.14\times10^{-1}$	$\sigma = 1.14\times10^{-2}$
17	Log normal	$\mu = -1.29\times10^{1}$	$\sigma = 9.97\times10^{-2}$
18	Normal	$\mu = 8.28$	$\sigma = 8.30\times10^{-1}$
19	Normal	$\mu = 7.06$	$\sigma = 7.10\times10^{-1}$
20	Normal	$\mu = 5.72\times10^{-1}$	$\sigma = 5.70\times10^{-2}$
21	Normal	$\mu = 3.43\times10^{-1}$	$\sigma = 3.43\times10^{-2}$
22	Log normal	$\mu = -1.26\times10^{1}$	$\sigma = 9.97\times10^{-2}$
23	Normal	$\mu = 1.15$	$\sigma = 1.15\times10^{-1}$
24	Normal	$\mu = 4.66$	$\sigma = 4.66\times10^{-1}$
25	Log normal	$\mu = -1.22\times10^{1}$	$\sigma = 9.97\times10^{-2}$
26	Normal	$\mu = 2.31$	$\sigma = 2.31\times10^{-1}$
27	Normal	$\mu = 9.52$	$\sigma = 9.52\times10^{-1}$
28	Normal	$\mu = 1.14\times10^{-2}$	$\sigma = 1.14\times10^{-3}$
29	Normal	$\mu = 1.49$	$\sigma = 1.49\times10^{-1}$
30	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
31	Log normal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$
32	Normal	$\mu = 4.66$	$\sigma = 4.66\times10^{-1}$
33	Normal	$\mu = 5.86$	$\sigma = 5.85\times10^{-1}$
34	Log normal	$\mu = -1.37\times10^{1}$	$\sigma = 9.97\times10^{-2}$
35	Gamma	$a = 1.64$	$b = 2.04\times10^{-6}$
36	Log normal	$\mu = -1.13\times10^{1}$	$\sigma = 9.97\times10^{-2}$
37	Gamma	$a = 2.22$	$b = 2.44\times10^{-6}$
38	Gamma	$a = 6.56\times10^{-1}$	$b = 2.42\times10^{-5}$

APPENDIX D: Derivation of Beta-Binomial model

The estimation of posterior probability density function using beta-binomial model is followed below steps.

The prior probability density function for continues random variable x_i, failure probability of safety barrier, is considered as Beta distribution,

$$f(x_i) = \frac{1}{B(\alpha_i, \beta_i)} x_i^{\alpha_i - 1}(1 - x_i)^{\beta_i - 1},\ 0 \le x_i \le 1 \qquad \text{(D.1)}$$

Where, α_i and β_i are shape parameters.

The beta function, $B(\alpha_i, \beta_i)$ in the equation (1) can be shown to be,

$$B(\alpha_i, \beta_i) = \int_0^1 x_i^{\alpha_i - 1}(1 - x_i)^{\beta_i - 1} dx_i \qquad \text{(D.2)}$$

The integration can be simplifies as,

$$B(\alpha_i, \beta_i) = \frac{\Gamma\alpha_i \Gamma\beta_i}{\Gamma(\alpha_i + \beta_i)} \qquad \text{(D.3)}$$

The likelihood probability density function is considered as Binomial distribution as equation (4).

$$f(data / x_i) = \binom{n_i}{n_{f,i}} x_i^{n_{f,i}}(1 - x_i)^{n_{s,i}} \qquad i = 1,2,3,4 \qquad \text{(D.4)}$$

Where, Where, $n_{f,i}$ is the cumulative number of failures associated with i^{th} safety barrier and n_i is the total number of events associated with i^{th} safety barrier, i.e. $n_{f,i} + n_{s,i}$. The $n_{s,i}$ is the cumulative number of successes associated with i^{th} safety barrier.

The Bayes' theorem can be expressed as equation D.5 to estimate posterior density funvtion for failure probability of safety barrier.

$$f(x_i / data) = \frac{f(data / x_i) f(x_i)}{\int_0^1 f(data / x_i) f(x_i) dx_i} \tag{D.5}$$

Equation D.1 and D.2 are substitute for Bayes' formula:

$$f(x_i / data) = \frac{\binom{n_i}{n_{f,i}} x_i^{n_{f,i}} (1-x_i)^{n_{s,i}} \frac{1}{B(\alpha_i, \beta_i)} x_i^{\alpha_i - 1} (1-x_i)^{\beta_i - 1}}{\int_0^1 \binom{n_i}{n_{f,i}} x_i^{n_{f,i}} (1-x_i)^{n_{s,i}} \frac{1}{B(\alpha_i, \beta_i)} x_i^{\alpha_i - 1} (1-x_i)^{\beta_i - 1} dx_i}$$

$$= \frac{\binom{n_i}{n_{f,i}} \frac{1}{B(\alpha_i, \beta_i)} x_i^{\alpha_i + n_{f,i} - 1} (1-x_i)^{\beta_i + n_{s,i} - 1}}{\binom{n_i}{n_{f,i}} \frac{1}{B(\alpha_i, \beta_i)} \int_0^1 x_i^{\alpha_i + n_{f,i} - 1} (1-x_i)^{\beta_i + n_{s,i} - 1} dx_i}$$

$$= \frac{x_i^{\alpha_i + n_{f,i} - 1} (1-x_i)^{\beta_i + n_{s,i} - 1}}{\int_0^1 x_i^{\alpha_i + n_{f,i} - 1} (1-x_i)^{\beta_i + n_{s,i} - 1} dx_i} \tag{D.6}$$

Let $\alpha_i^* = \alpha_i + n_{f,i}$ and $\beta_i^* = \beta_i + n_{s,i}$, then, equation D.6 is further simplified:

$$f(x_i / data) = \frac{x_i^{\alpha_i^* - 1} (1-x_i)^{\beta_i^* - 1}}{\int_0^1 x_i^{\alpha_i^* - 1} (1-x_i)^{\beta_i^* - 1} dx_i} \tag{D.7}$$

According to equation D.2, the denominator of equation D.7 can be written as Beta function,

$$B(\alpha_i^*, \beta_i^*) = \int_0^1 x_i^{\alpha_i^* - 1} (1-x_i)^{\beta_i^* - 1} dx_i = \frac{\Gamma\alpha_i^* \Gamma\beta_i^*}{\Gamma(\alpha_i^* + \beta_i^*)} \tag{D.8}$$

Therefore, the equation D.8 is turned in to beta distribution with the parameters α_i^* and β_i^*,

$$f(x_i / data) = \frac{1}{B(\alpha_i^*, \beta_i^*)} x_i^{\alpha_i^* - 1} (1 - x_i)^{\beta_i^* - 1}$$

This model called *beta-binomial model*. Prior distributions that take the same functional form as the posterior distribution are called *conjugate prior distribution*.