CUMULATIVE RISK ASSESSMENT TO ANALYZE INCREASED RISK DUE TO IMPAIRED BARRIERS IN OFFSHORE FACILITIES

A Dissertation

by

SYEDA ZOHRA HALIM

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Mahmoud El-Halwagi
Committee Members,	M. Nazmul Karim
	Chad Mashuga
	Jerome Schubert
Head of Department,	M. Nazmul Karim

May 2019

Major Subject: Chemical Engineering

ABSTRACT

Investigation of past incidents always reveal deficiencies that are not directly equipment-related, but may be non-technical in nature, such as procedural deviation, inadequate communication *etc*. Past risk assessment models only provide semi-quantitative approaches to incorporate such learning from past incidents and cannot capture their dynamic nature and dependency within a single model. Current research takes up the challenge of developing a novel approach and step-by-step methodology for quantitatively merging technical, operational, human and organizational factors contributing to the cumulative risk of barrier failure. It also addresses their dynamic changes with time, considers interactions among each other and incorporates uncertainty of parameter estimation to assess the total risk.

First, a methodology is developed and implemented for extracting statistical data of contributing factors behind past incidents from investigation reports. The study produces a generic dataset of contributing factors in 137 fire incidents from the US Outer Continental Shelf (OCS). Analysis shows that failures rates of contributors are non-constant and can be modelled as non-homogenous Poisson process with Power Law distribution. Hierarchical Bayesian Analysis is utilized to predict probability of failure within a time period and next time of occurrence from the generic data. Results show reliability growth for contributors related to 'design flaw' and 'inadequate job safety analysis' in the OCS, although a majority of other contributors show deterioration. In the next stage, near-miss data from a particular facility is incorporated to obtain plant-

specific understanding of how and when their next critical failure may occur. Interaction among contributing factors are measured from the analysis of investigation reports. Finally, a cumulative risk assessment model for an offshore unit with safety instruments is developed, where the contributing factors are mapped onto Bayesian Network to provide probability distributions of barrier failure and subsequent incidents. A case study is adopted to show how extracted information from investigations can be utilized to update generic data and obtain probability distributions of individual barrier failure. This research will aid management to identify key organizational issues that contribute to an increased risk of barrier failure, so that better resource allocation can be ensured.

DEDICATION

For my children Arkam and Ameera, in hope of a safer future

ACKNOWLEDGEMENTS

My journey to this PhD dissertation has been made enjoyable by the contribution of a handful of wonderful and outstanding people. Starting a PhD with two toddlers seemed like an impossible task 5 years back, but it was made possible because of the exceptional encouragement provided by my past supervisor Dr. Sam Mannan. His passion for process safety somehow seemed to rub off into anyone, including me and I will always remember his saying "Zohra, you have to live, breathe and think process safety". Thank you Dr. Mannan! May Allah grant you Eternal Heaven.

I also thank my supervisor Dr. Mahmoud El-Halwagi for taking me up as his student with the kindest words, and supporting me in my most difficult times.

I am grateful to have been mentored by some top-notch experts in the field of process safety. Thanks goes to Dr. Hans Pasman for always answering my questions with patience and always providing me with good literature to review. Members of the MKOPSC Steering Committee (SC) and Technical Advisory Committee (TAC) had always been helpful by providing valuable suggestions and ideas. Mike Neill, President at Petrotechnics USA Inc., provided me with ample time and helped shape up the concept of cumulative risk in the early phases of my research. Special thanks to Kevin Watson from the TAC for reviewing some part of this work as it progressed.

A special thank goes to the Bureau of Safety and Environment Enforcement (BSEE), especially Andre King, for being just an email away whenever I needed help, Michael Pittman, Adam Boone and Melinda Mayes for taking time to review my paper

and to all members at the BSEE Houston office for listening to my talk and giving me insights and feedback.

Thanks goes to everyone at the Mary Kay O'Connor Process Safety Center (MKOPSC), who have tolerated my sudden outbursts, moments of panic attacks, forgetfulness and clumsiness, but have still been there to support me in times of despair. This has been an excellent journey mostly because of them. Jim Pettigrew, Director of Operations and Principle Investigator at the Ocean Energy Safety Institute (OESI), have backed me up on many cases, especially in the absence of Dr. Mannan, journeyed to Houston for me, given me the first idea of where to look for data and have constantly tried to get me more involved with the offshore community. Thanks for all that you did.

I am thankful to the Bangladeshi community in College Station. For them, I have been able to stay close to home food, had my children felt loved, and basically make College Station my home.

My two dear friends Afifa and Kazi, whose demand for daily updates helped me keep a focus on the good things in life, deserve special credit for the enormous mental support they provided throughout my research.

I am grateful to the Almighty for giving me parents who journeyed half way across the world just to babysit my children so that I could survive my qualifying exam with a 3 course-semester. Thanks to them for making those frequent long-distance phone calls where I mostly talked, or rather complained, about my grad life. Gratitude is also for my two brothers, Amar and Enayet who have provided immense love all through my life and have always been my support system.

Last, but the most heart-felt and deepest thanks goes to my husband Noor and my two children Arkam and Ameera. Noor, you have been with me through thick and thin, supporting me and lifting me. Words cannot describe how much your support and help are appreciated. Being with me may have been a ‘hazard’ itself on days when I was trying to ‘assess cumulative risk’, but honestly, you three complete my life. This PhD was made possible because of you.

Thank you Almighty, for these people.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supervised by a dissertation committee consisting of Professor and Head of Artie McFerrin Department of Chemical Engineering Dr. Nazmul Karim, Assistant Professor Dr. Chad Mashuga of Artie McFerrin Department of Chemical Engineering and Professor Dr. Jerome Schubert, of Harold Vance Department of Petroleum Engineering at Texas A&M University.

The data analyzed in Chapter IV was obtained from Bureau of Safety and Environmental Enforcement (BSEE)'s website and the analyses were conducted in part by Sunder Janardhanan and Leidy Tatiana Flechas of the of Artie McFerrin Department of Chemical Engineering and were published in 2018. All other work conducted for the dissertation was completed by the student independently.

Funding Sources

This work was supported by the Mary Kay O'Connor Process Safety Center at Texas A&M University.

Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the Mary Kay O'Connor Process Safety Center.

TABLE OF CONTENTS

Page

LIST OF FIGURES

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1. Background

It is well accepted that a good understanding of risk is essential for day-to-day safer operations of a chemical process facility. Safer operations with minimal risks ensure continued production, profitability, and survival in a competitive market without unforeseen mishaps [1] . Concatenation of multiple factors that have deviated from their safe state may lead to unsafe situations, and in worst case, cause disastrous incidents.

The Texas City Refinery incident that occurred in 2005 [2] or the Deepwater Horizon incident in 2011 [3] brings a gloomy throwback at how small deviations added up to a disastrous event. In both cases, as in others, such deviations have been existing within their system for some time preceding the incident, but had not imposed an immediate threat, or their threat may not have been noted on time. Due to the insufficient measures to recognize these deviations and prevent the propagation of mishaps, these incidents could not be prevented.

Although many measures are taken post-incident and many amendments suggested, it is the sad truth that incidents still keep happening. For example, following the Deepwater Horizon incident in 2011, modifications to regulations and regulatory bodies were put in place [4]. However, according to the public information released by the Bureau of Safety and Environmental Enforcement (BSEE), in the fiscal year 2016 (October 1, 2015- September 30, 2016) alone, 473 incidents of various types, causing 2 fatalities and 150 injuries, were reported to have occurred in the offshore oil and gas

facilities in the US Outer Continental Shelf [5]. In fiscal year 2017, a total of 429 incidents, including fires, explosions, collisions, gas releases *etc*. were reported in the US Outer Continental Shelf alone. The same source shows that from 2011 to 2016 (fiscal year) 13 people have died and 997 were injured through various mishaps. This signifies that incidents continue to happen and that our understanding of risk and requirement of taking appropriate modifications to reduce that risk are still not sufficient.

1.2. Motivation

Although deviation of multiple factors may suffice frequently, only in rare cases will these deviations arise and interact in a manner that will create a possible trajectory for an incident [6]. The risk arising from a single deviation of equipment, person or operation from a defined safe state of a small system is usually understood. But with large numbers of deviations existing throughout a plant, it is essential to understand how their holistic effect is changing the overall risk of the facility. This 'cumulative risk' may have a variety of origins such as maintenance backlog, supply delays, aging assets, deviation from technical standard and questionable competency of operators [7].

Quantification of risk is essential to compare and evaluate alternate options available for risk reduction [8]. Quantitative risk assessments (QRAs) provide a magnitude of the risk showing us whether it is within an acceptable range and allows us to trace back to the causes that led to such high-risk values. This further enables work prioritization through pinpoint determination of where, when and what mitigative measures are required.

In the industry, preventive and mitigative measures are taken against the possibility of incidents by putting barriers in place to prevent the propagation of such incidents to catastrophic consequences. The interrelation between deviations such as that arising between unsafe acts by frontline operators and latent conditions that can lead to an incident was graphically modeled by James Reason in 1990 through the Swiss Cheese Model [6]. The Defense in Depth approach in the nuclear industry pioneered the concept of barriers and Reason modified it. Each slice of cheese was seen as a barrier that broke the incident trajectory. Eventually factors that influenced barrier failures were studied and extended to provide a better visual understanding of what caused a system to fail via use of methods such as fault trees, event trees and bowties. [6, 9-12]. In the industry, the concept of using barriers to prevent incidents, and maintaining barriers in proper condition to ensure safe operation is a well-accepted approach towards process safety. However, as the factors that influence a barrier evolve with time, the system behaves dynamically. Conventional fault trees and event trees *etc.* consider only static relationships between factors and do not explicitly consider the effect of time or changes made to the process variables [1, 13]. Systems dynamics will also require consideration of the interdependence of each factor since changes made to one will, with time, impact another. An attempt to consider the dynamicity and interaction of barriers and their influencing factors for risk assessment makes it a challenging task.

Performance of barriers are influenced by a variety of factors which change with time and some of which show interdependency on each other. It is realized that deviations can arise from all quarters of the facility and can be technical, operational,

human or organizational in nature. Environmental or external factors can add to the challenge as well. Traditionally, risk assessment methods had focused only on the technical aspects of a system mainly because of the ease of a quantitative representation of their failure. However, over the last few decades, with realization sprouting mainly from numerous catastrophic incidents, there has been a growing effort to incorporate 'non-technical' factors, namely human and organizational factors (HOF) into the traditional risk assessment methods. Even so, a large gap exists in merging the more abstract HOF with the more quantifiable technical factors of a system [1]. A study reported by Skogdalen *et al.* showed that of the 15 offshore installations considered in his study, the majority conducted QRAs with "HOF Explained" and considered HOF only to some extent and not separately [14]. None of them fell in the category "HOF explained, models adjusted and included in the overall risk management" where HOF were given as much importance as the technical factors and formed an integral part of the overall risk management system. The biggest challenge in getting a holistic look into risk is consideration of all factors together: technical, operational, human and organizational.

To understand the dynamic nature of risk, it is essential to ensure that the risk assessment conducted uses data that is specific to the plant and is always current. Usual practices in risk assessment include utilization of generic data based mostly on historical failure rates of equipment and includes all causes of failure, thus representing industry averages [15, 16]. However, service condition of each plant may be different, and how an equipment is maintained and operated (operational, human and organizational factors)

may have an influence on failure rates too. Also, data sample size may not be sufficient for a good estimation and the definition of failure may be different from that being used in the risk assessment. To make the data plant specific, efforts have been made to utilize expert opinion to update the generic values. But gathering expert opinions for all technical and managerial issues of a facility it is a tedious process and variation of opinions may lead to over or under estimation if the number of experts is not large. This approach has been subject to much scrutiny in this regard [17]. It has therefore become essential to use information obtained from various databases of a plant to update the generic values for better risk estimation.

Since the effect of most deviations are not known deterministically, and the data used for risk assessment itself has questionable precision, a proper risk assessment should consider the uncertainty in the results. This makes cumulative risk assessment even more complicated.

Operation in offshore oil and gas facilities impose a particular challenge to process safety issues because of multiple reasons. The potential for large blowouts and the handling of highly flammable hydrocarbon which can lead to fires, explosions and fatalities are a constant threat to these systems. The dynamicity of operation, especially during drilling and simops (simultaneous operations) can add to the threat. The offshore environment itself imposes a challenge to organizational and human factors as does the limitation of space and time. Assessment of dynamic risk for such cases are still in the cradle phase.

It is with the motivation of overcoming these challenges that the current research focuses on developing a framework and model for cumulative risk assessment to analyze increased risk due to impaired barriers in offshore facilities.

1.3. Defining Cumulative Risk

Cumulative risk assessment involves achieving an updated information about the dynamic risk through merging of technical, operations, human and organizational deviations existing within a facility. Data used for risk assessment should be specific to the facility and current in time. This gives several points to consider:

a. The influence of time and process dynamics cannot be ignored if we are to consider deviations [18]. The dynamicity of the plant refers to the various factors that evolve or change with time and includes operational and organizational changes that may occur due to say changes made in the maintenance program, or changes made due to management decisions. These temporal aspects capture the ever-evolving nature of the plant and its management system with time.

b. Merging of factors that are quantitative in nature (such as technical factors including reliability of equipment) with factors that are abstract in nature and cannot be readily quantified (such as organizational factors including effectiveness of training programs) [1]. These abstract factors can influence the failure function of the quantifiable ones and hence must be considered.

c. Dependencies of the different technical, operational, human and organizational factors also need to be considered to assess cumulative risk [1]. For example, a

standby pump may only need to operate if the primary pump fails. Whether the standby pump fails to operate will be known when the primary pump fails and thus, its operation depends on the initial failure of the primary pump.

d. Failure data may come from the equipment manufacturer who tested it, or from databases that provide industry average values (generic data) or, experts' opinion in many cases (especially for non-technical factors). As management system varies from company to company, so does equipment installation, design, engineering practices, inspection and maintenance programs *etc*. over the lifetime of the plant. So, the conditions in which equipment is exposed to may vary significantly from the data. This makes use of generic data, or even the manufacturer provided data, misleading when it comes to risk analysis. Data used for risk assessment should be plant specific and up-to-date.

e. Usually point value estimates are used when quantifying risk, whereas the influences of environment and other issues may give rise to variations. A failure parameter may be distributed over a range of values and a proper understanding of risk would require consideration of its distribution rather than a single value. Thus, uncertainties involved in parameter estimations should be considered.

An assessment of risk that considers the above factors will lead to an understanding of the cumulative risk spawning from a plant's operation. It is the purpose of this thesis to provide a method for assessing the cumulative risk.

1.4. Problem statement

To gain a better insight of cumulative risk, it is required to develop a model that meets the following challenges [1]:

1. Considers how systems change with time, *i.e.* the dynamic aspect of the various factors
2. Merges technical, operational, human and organizational factors affecting risk in one framework
3. Considers dependency of the factors
4. Keeps data up-to-date and plant-specific
5. Considers uncertainties in parameter estimation

Current research focuses on developing a model for cumulative risk assessment that meets the mentioned challenges, with focus given on operation in offshore oil and gas facilities.

2. PREVIOUS WORK

2.1. History of Risk Assessment

Assessing risk to compare which option is more (or less) beneficial, or safer, or more profitable or just better has been practiced within the human mind from the very beginning of time. Assessing risk in a formal way requires study of chances or probabilities. The modern concept of risk has been traced as far back as 3200 B.C. when the members of the Asipu group in the Tigris-Euphrates valley used best available 'data' (seen as signs from gods) to analyze alternatives and provide a decision based on their understanding of the 'data' [19]. However, it was not till the Renaissance period (1300-1600 A.D) that an extensive study of risk began. [20].

As Bernstein narrates in his book '*Against the gods- The remarkable story of risk'*, in around 1654, a French nobleman Chevalier de Méré, with a keen interest in gambling, challenged the famed French mathematician Blaise Pascal to an aged old problem of dividing the stakes of an unfinished game between two players based on who was ahead in the game. The search for a solution laid foundation of the modern day theory of probability [20].

The probability theory soon found application beyond settling gambling stakes. By the seventeenth century, it was being used for determining life expectancies for the sale of life annuities and soon the business of marine insurance became a 'hot cake' in London. Around the same time, Jacob Bernoulli's work on the Law of Large Numbers provided methods of statistical sampling [21, 22]. Other contemporaries further

developed the statistical methods associated with probabilities and showed how decision can be made based on information about choices [20, 22], paving way for development in understanding risk and the principles of investment management.

Later in the century, Thomas Bayes developed the Bayes's Theorem that allowed the understanding of the probabilities of an event to be modified based on information as it became available. Most modern-day risk assessment and management decisions had their foundations laid during this period, starting from the challenge thrown by Chevalier de Méré.

In current day, the theory of probability and methods for informed decision-making finds application not only in Wall Street, but also in the core of measures taken for productive and safe operation of chemical and manufacturing industries around the globe.

2.1.1. The Chauncey Starr papers and the start of a new discipline

As the understanding of the theory of probability grew, it found application in multiple fields such as the medical industry, insurance companies, election polling *etc*. It became more demanding to understand the risks of taking decisions in terms of the impact the decisions will have. It was Chauncey Starr who, in 1969, suggested that the society's perception of risk was skewed and was probably the first to bring out the need to quantitatively evaluate risk to understand the impact of new technology on society [23, 24]. He noted that as technological developments are made at increasingly faster pace, it is not possible to understand their impact on society ahead of time until they are

totally absorbed into systems of the society itself. This makes understanding the benefit of the new technology and the cost it may have on the society due to its side effects even more difficult. He provided quantitative correlations to compare the physical risk of an activity to the social benefit derived from that activity and also showed how advertisement could impact risk awareness. Amongst other things, he suggested that people would take voluntary risks a thousand times more willingly than involuntary ones. In later work, Starr brought out the need for risk management, assessment and acceptability, suggesting the famous example of how people were willing to take the risk and come to the zoo to see a tiger if the management did a good job of keeping the animal locked properly inside the cage. It revolutionized the idea that there will always be hazards and placement of proper constraints can mitigate the risk arising from those hazards.

The concept of organizational influences on failure rates have been discussed much in literature. Amburgey *et al.* in *Resetting the clock: The dynamics of organizational change and failure* talked about the dynamic aspect of organizational failure and change, stating that the immediate effect of organizational change is an increase in the hazard of the system's failure and an increase in the likelihood of similar additional changes [25]. The data for the study was collected from more than a thousand Finnis newspaper organizations over a period of 193 years. If extrapolated in the context of a chemical facility, this work showed that external and internal influences leading to changes within an organization can lead to an increased hazard within the system, thus

increasing the chances of failure. This failure can be failure in the market (as with the newspapers studied), or failure in production or safe operation.

2.1.2. Risk assessments and the high hazard industries

As technology progressed and the process industries grew larger and more complex, so did the consequences that arose from incidents in these industries. Highly hazardous industries were being developed, such as the nuclear industries and certain chemical plants with potential for large impact on surroundings in case of an incident. Assessing risk at this point was challenging, not only because of the size of the systems (the facilities) but also because of the complex interaction that each element of the system had with each other.

Towards the middle of the last century, experts were probing into the field of accident causation, trying to identify contributors to risk and suggesting multiple accident causation models to character how and why accidents occurred. Heinrich, Reason, Rasmussen are famous names in this field [6, 26, 27].

A systematic approach to quantitative probabilistic risk assessment is rather new [28]. It began in the aerospace sector following the 1967 Apollo test flight disaster that led to fatality of three astronauts [29]. Methods to assess risk of a major event from the failure probability of various equipment was developed. The ideas and principles developed during this time forms a basis for current day risk assessment and risk management [28]. Much modification has been brought about. The 1979 Three Mile Island incident provided an inspiration behind Perrow's 1984 book '*Normal Accidents-*

Living with High-Risk Technologies' which now suggested that instead of looking only at the technical factors, it was time to focus on organizational issues that were influencing risk [30].

Most of the models developed during this time used the notion of linear causality to assess how incidents occurred. But Perrow argued that current day systems were complex and tightly coupled and multiple failures can interact with each other, causing a major incident [30]. Technology was not the problem in such cases, but organization and management factors were. This idea revolutionized how risk was assessed and further propagated the development of methods of risk assessment whereby human and organizational factors were being considered.

2.2. Approaches to Assess Overall Risk

Over time, many frameworks and models have been proposed to assess risk arising from various conditions existing in a facility[31]. As part of the study, an extensive and in-depth literature review was conducted to gain an understanding of the pros and cons of each approach [32].

It was found that there are two approaches applied in the industry for risk assessment purposes. One is based on causal chain and event modeling methods in which a system is decomposed for analysis and the components (machine, human, and organization) undergo linear interaction and follow a sequence of failure that leads to an incident. Numerous risk assessment methods have been developed based on this approach [31, 33]. The other approach that has been gaining momentum recently is the

systems approach which analyzes the outcome of a system as emergent where the whole is larger than the sum of the individual parts. Non-linear interaction and self-organization with evolving dynamics are well handled by this approach [34, 35].

Based on each broad category, a large number of models have been developed over time [31, 33], of which only a few well-known ones are discussed below to provide a general idea about how models in each approach work. [31]

2.2.1. Causal Chain and Event Modeling Approaches

2.2.1.1. Cause and Event Chain Trees

Fault trees, event trees, and bow-ties have long been used in the industry for risk assessment purposes. These cause and effect models describe linear propagation of failure through the system. Although the conventional ones can provide simple, quantitative and graphical representation of the failure states of a system whereby the effect of multiple deviations can be observed, they find limited application for dynamic systems with dependent or common cause failures. Many approaches to modification of these methods have been published in literature in an attempt to provide a more realistic model [13, 36] . These include development of sequential gates that allows dependent events to be modeled [37]. Recent literature shows an increased trend in the application of tools such as Bayesian Network and Petri Nets (discussed later) that model fault trees, event trees and bowties to increase their capacity to handle dependencies [1, 5, 38-44].

2.2.1.2. Hybrid Causal Logic

An extended approach of event cause trees mentioned before has led to the development of the hybrid causal logic (HCL), which provides a framework for attaching Bayesian belief network (BBN) to feed information to connected fault trees and event trees and vice versa [45, 46]. Fault trees allow tackling of technical factors while the connection of BBN allows for incorporation of risk influencing factors (RIF), which bring in the human and organizational aspects of the system. The method is simplified by utilization of expert judgment to express causal relationship between the RIFs. This allows development of a model that allows basic event probabilities of a fault tree to be updated through the RIFs and gives a graphical representation of dependencies. Methods such as the HCL are resource intensive and the dependence on opinions of experts can bring variation and uncertainty in the risk evaluation. A similar approach was used in developing the Risk_OMT project which brought in human activities and their contribution to the risk [12, 47]. Both approaches are modifications of the Barrier and Operational Risk Analysis (BORA) model [48].

2.2.1.3. I-Risk

The integrated risk (I-Risk) analysis methodology contains three main components: the technical model, the management model, and their interface [49]. The technical model is developed based on Master Logic Diagrams to identify immediate causes of failure followed by the development of event tree and/or a fault tree in order to quantitatively analyze the identified causes of failure. The management model which

covers functions such as operations and maintenance is quantified based on audits/expert opinion. At the interface, guidance is provided to assign weightage on how the management model will fit with the technical model to make the technical factors plant specific. I-Risk qualitatively as well as quantitatively enables the managerial aspects to be incorporated with the technical ones, but the need for having an audit team to be able to identify management tasks and quantify them is a large challenge. Consequently, frequent updating of the risk assessment may not be possible.

There are numerous other methods that have been developed based on cause-effect approaches with slight changes made depending on application [35, 50]. But all in all, they more or less follow an approach similar to any of the ones mentioned above. An overall look into the limitations of cause and effect models shows their inability to capture differences in risk when there is a variation in the success and failure events or variations in event timing whereby scenarios can change [13]. Variations in parameters that are not explicitly modeled are not considered in the risk, which can have a profound effect whenever the system is changed/ modified. The dynamicity of the plant is not completely considered. However, these approaches do help provide a simplified look at a complex problem and thus finds larger application in the real world [46].

2.2.2. Systems Approaches

2.2.2.1. Accimap

Rasmussen and Svedung were the first to draw a safety control structure within a socio-technical system which provided a graphical representation of the causal flow of

events showing failures to result from contributions across six nested levels of decision-making (Government, Regulators, Company, Management, Staff and Work) [27, 51, 52]. They pointed out that risk management is a control task and proper co-ordination and bidirectional flow of information is needed between all levels of the socio-technical system. Instead of analyzing risk only horizontally at the bottom levels, this procedure enabled a look at the higher levels in the system to identify their contribution and draw logical causal diagram to show their influence on the risk. This revealed the remote causes coming from higher levels in the hierarchy and disseminated complete attention given to frontline operation. In that context, the whole look into risk was obtained. Accimap has been used to analyze different kinds of incidents in several domains and provides a systematic approach to identify gaps in a system, be it technical or HOF related. However, it requires sufficient data and analyst skill, the map itself can become complicated for a simple system and it does not provide any direct information about what measures need to be taken or what barriers need to be placed to prevent and/or mitigate the risk [53].

2.2.2.2. System Theoretic Accident Modeling and Processes (STAMP)

With modification of Rasmussen's approaches, System Theoretic Accident Modeling and Processes (STAMP) is based on three basic components: safety constraints, hierarchical control levels and process models with control loops [54-56]. Leveson emphasizes that complex systems are dynamic and incidents result not from failure of individual components but because of violation or inadequate control of safety

constraints. STAMP views the system as having hierarchical levels of control and constraints indicating that each level in the system contributes to the system's safety or to incidents. Loops are generated when each level enforces safety constraints to a lower level while feedback regarding proper/improper implementation of these constraints are fed bottom up to ensure proper placement of the enforced constraints. Thus, feedback and control operations replace the traditional chain of events model. Inadequate safety controls can arise from deficiency or absence of constraints, improper or inadequate execution of control actions at lower levels, and inadequate or missing feedback communication within the various levels of the system. Based on STAMP, the System Theoretic Process Analysis (STPA) enables identification of a system's weaknesses via a list of guided questions which then enables determination of component flaws in the control loop could cause such a flaw from which appropriate preventive measures can be identified [57]. The method can be used at any stage of the process life cycle to identify and repair system degradation.

STAMP can model dynamic systems which may migrate to a state of increased risk over time due to external disturbances, component failure or dysfunctional interaction of components. It especially focuses on human and organizational subsystems. Although it has been applied in a variety of domains, quantification has not yet been possible. Identification of all loops in the system is an enormous task and requires expertise in the method [35].

2.2.2.3. Functional Resonance Analysis Method (FRAM)

While STAMP is based on a specific causal model (a feedback control system), Functional Resonance Analysis Method (FRAM) is based on the specific theory of functional resonance [58]. FRAM provides a socio-technical approach with principles of resilience engineering to look at the safe state of a system when it is subjected to dynamic operational conditions. Hollnagel explains four principles on which FRAM stands: 1. Outcomes of a process can be different (failure or success) but the underlying processes are not: the reason why some operations fail are the same reason why they succeed; 2. Human and organizations make approximate adjustments to meet existing conditions and their performances can vary which may lead to failure or success; 3. Combinations of variations can have nonlinear effects and the system's outcomes are emergent and not resultant; and 4. Consequences of such variations can be exemplified via tight couplings or functional resonance which cannot be understood simply through cause and effect analysis [59, 60]. FRAM decomposes a system's functions into modules characterized by six parameters: inputs, resource, controls, time, precondition, and output.

FRAM provides a step-by-step guide by identifying system functions, assessing and evaluating the potential variability of the functions, identifying the possible way the variability of one function can affect other functions and spread through the system (functional resonance) and finally identify countermeasures that will enable the system to maintain a safe state. FRAM focuses on the likelihood of functional variability instead of probability of component failure and has not yet been quantified.

2.2.3. Summary of learnings from literature

Table 1 shows a comparison of the various models according to the two approaches discussed above [32].

Table 1. Various approaches are compared based on their prospect for use in cumulative risk assessment (presented at the *AIChE Spring Meeting and Global Congress on Process Safety*. 2017. San Antonio, TX: Center for Chemical Process Safety)

Method	Approach	Provides quantified risk estimate	Shows dynamic evolution of system	Considers dependency of various factors	Data uncertainty understood/ Precision
ET/ FT/ BT	Cause and Effect	Yes	No	No	Yes
HCL	Cause and Effect	Yes	No	Partially	Yes
I-Risk	Cause and Effect	Yes	No	Partially	Yes
Accimap	Systems	No	Yes	Yes	N/A
STAMP/ STPA	Systems	No	Yes	Yes	N/A
FRAM	Systems	No	Yes	Yes	N/A

The very nature of cause and event chain models limits projection of non-linear relationships that arise from feedback loops generated from complex interaction of

components within the system and this prevents prediction of unexpected emergent phenomena. At the same time complex systems are subject to change and transforms itself to adapt to the changes with time, which makes such systems dynamic [13]. Organization and human factors give rise to numerous non-linear cause-effect relationships and their quantification is difficult, with heavy reliance on scoring methods. This brings large uncertainty and ambiguity into the model [11, 12]. Identification of all relations are also difficult. All these issues challenge the cause and event chain approach. Yet their simplicity and ability to easily represent a system has made them widely applied in chemical industries today [61]. Utilization of Bayesian network allows dependencies to be considered to a certain extent. Several modifications to incorporate dynamic aspects of risk with consideration of non-technical factors is discussed later.

On the other hand, attempting a systems approach brings about a different kind of limitation. These models require extensive resources and demand deep understanding of the system. This approach tends to identify all links within a large hierarchical system, both horizontally as well as vertically, to understand how factors may evolve with time and affect other. Though this allows understanding the dynamicity of the system, it is indeed a daunting task to complete, and is more doable once an incident occurs (when the inter relation of factors become known) rather than for developing a predictive model. As the system evolves with time, updating it may become difficult and require a lot of effort and expertise. Although systems approach such as FRAM claims to

capture the emergent property, it is still in the theoretical phase and quantification is not available. This approach is yet to find acceptance for large-scale usage in the industry.

From the above analysis, it seems apparent that using the cause and event chain modeling approach and modifying it to adjust to the requirements for a quantified cumulative risk assessment would be a more attainable goal with greater applicability than a systems approach. Emergence property as described by systems approach is yet to be properly defined, and provisions developed to understand if the complete emergence effect of all factors has been incorporated in the model. The cause and event chain approaches require modification to include a feedback method of system changes and incorporate the effect of passage of time to capture the dynamicity of a system. Henceforth, the work is developed using a barrier analysis brought about by the cause and event chain modeling approach.

2.3. Tools for Cumulative Risk Assessment

2.3.1. Fault Tree Analysis

Fault Tree (FT) analysis is a deductive (top-down) method that uses Boolean logic to break a system into multiple base events that are connected via AND and OR gates to lead to the top undesirable event. FT can also be analyzed using minimal cut sets. In context of this paper, FT appear helpful in that they allow combination of different deviations for obtaining their overall effect in the top event. It is easy to use and provides a quick understanding of how various factors are affecting the top event. However, when deviations can lead to multiple failures, conventional FT fails due to its

inability to show multiple top events together. It is also limited in its ability to handle complex systems where dependency or common cause failures need to be addressed. In dynamic systems, where sequential failure needs to be considered, the static fault tree (SFT) is incapable of providing a complete system representation. As an extension to the SFT, dynamic fault tree (DFT) allows usage of functional gates such as sequence enforcing gates (SEQ) that overcome such limitations [36]. DFT needs to be converted to Markov Chain model for analysis and this becomes difficult for large system particularly because of the tendency of state space explosion due to the countless states that can be reached in a large Markovian system at a given time. The method is also prone to errors [41].

2.3.2. Event Tree Analysis

Event Tree (ET) analysis is an inductive (bottom-up) method that begins with an initiating event (IE) and propagates through branches or pivotal events (PE) and terminates with multiple end states or consequences depending on the path followed in the event. Pivotal events may represent success or failure of barriers. The success and failure probabilities at branch points can in turn be analyzed by FT and hence an event tree can represent a full incident starting from base causes upto consequence determination. Determination of probability of consequences is then easily done for a known path. ET however cannot address interdependence of basic events in the different FT that are attached to it [5]. Static or time independent ET are simple and easy to compute due to their assumption but are not realistic. On the contrary, the dynamic event

tree (time dependent) allows realistic modeling. They assume that among common base event nested in different FT connected to the ET, if one base event did not occur in a FT connected to a prior pivotal event then that event does not occur in the FT connected to a later pivotal event also. [42].

2.3.3. Markov Chain Analysis

A probability model is a stochastic process that describes the evolution of a system changing randomly in time. A Markov Chain (MC) represents such a process through description of states of the system and their transition rates. This enables modeling of time dependent behavior of dynamic stochastic systems. A system is said to be Markovian if it exhibits the property that the probability of being in a particular state depends only on the state attained in the previous transition and not on ones before that [62]. This assumption to an extent, limits the applicability of MC to general dynamic systems [13]. The biggest limitation is seen during modeling of large complex systems where it is possible to attain numerous states from one previous state. In such cases there occurs state space explosion that can exponentially increase computational requirements and time (for example, in a system with n basic components, the number of states can be 2^n).

2.3.4. Bayesian Network

A Bayesian network (BN) is a directed acyclic graph (DAG) consisting of nodes that represent system variables and arcs and that shows the dependencies or the cause-

effect relationship between the variables. It has been used in the field of dependability, risk analysis, and maintenance areas for quite some time now [1]. It allows merging of various kinds of data, including expert opinion and missing data. It is a probable model that can be used for cumulative risk assessment.

Local conditional dependencies can be handled in a BN since nodes directly connect causes that influence an effect. It can be used for both predictive as well as diagnostic analysis [37].

Popularity of BN lies in its ability to address complex systems with dependencies and common cause failure among its components. It allows modeling of multi-state variables and can represent several system failure possibilities, which are not possible in a FT. Bobbio *et al.* showed how FT can be mapped onto a BN while maintaining its Boolean properties to incorporate multi-state variables and dependencies [38]. Further efforts have been made successfully to map the various logical gates in a dynamic fault tree into discrete time Bayesian network (DTBN) [41, 63, 64]. Bearfield *et. al.* showed a method for mapping an ET onto a BN [39] and later on Khakzad *et al.* carried out dynamic safety analysis by mapping a bow-tie into a BN [41]. Barua *et. al.* further showed how DBN can be used to model dependent failures of a system[64].

To allow determination of uncertainty in parameter estimation, there has been a shift from discrete variable to continuous distributions in recent times. Analytical method for computation of continuous distribution limits the number of distribution types that can be used. Hence, numerical approaches are preferred, though they are computationally demanding. Software has been developed that use various methods such

as Markov Chain Monte Carlo (MCMC) simulation or dynamic discretization to reduce the computational load and allow modeling in BN with continuous variables [65-68]. The programs allow use of equations that can reflect how each variable interacts with each other, giving the modeler greater flexibility in developing a network and minimizes the trouble of handling large number of Boolean data to fill the conditional probability tables.

With the development of such software, greater advantages of BN are being realized through the application of Hierarchical Bayesian Analysis. These enable probability updating of generic data using plant-specific data or observed data, thus minimizing source-to-source data uncertainty. Past data are fed as evidence/likelihood to determine posterior probabilities in the first stage of Bayesian analysis and then these posterior are used as priors to fit the evidence from the plant in question, giving rise to plant specific data[69]. This stage-by-stage updating is the reason behind the naming. Khakzad *et al.* showed a two-step Bayesian updating to develop a case specific posterior distribution for an initiating event using generic and case specific precursor data [41]. Real time updating of data will be possible with BN and has been shown by many researchers [70].

2.3.5. Petri Nets

Petri Nets are directed bipartite graphs consisting of two types of nodes called places (P) and transitions (T) in which places are connected to transitions and transitions to places via arcs. Places represent condition of a local state while transitions represent

an event that changes the state of a system. A place may contain one or more tokens each of which represents the status of the place. Movement of token from one state (place) to another occurs through the 'firing' of transitions and captures the dynamic behavior of a system.

PN is a powerful modeling formalism that allows cyclic processes to be modeled, unlike the BN or the ET. Thus, components undergoing failure-repair cycles can be well modeled in PN. Analytical methods are possible only for small Markov systems but for large ones (and non-Markovian ones) simulation such as Monte Carlo is used. Stochastic Petri Nets (SPN) are based on simulating the dynamic behavior of a system via movement of tokens through various states (places) and then obtaining probabilistic values by statistical analysis.

Liu *et al*. described how every logic gate, including AND and OR gates of a Fault Tree can be modeled in Petri Nets [71]. Bobbio *et al*. developed the Parametric Fault Tree that he used for modeling in PN and Nyvlt *et. al.* developed a PN-based model of a complex event tree [37, 44]. Application of PN has been limited by their long simulation time which occurs due to the massive number of states that can occur even for a small system and by their weakness in handling low frequency events which is crucial while performing risk analysis of rare events [1].

2.3.6. Summary of learnings from literature

An analysis of each of the tools and a case study was conducted for this research to compare the application and outcomes of FT, ET, BN and PN in an attempt to outline

the benefit and difficulty of using each of them [43]. The results obtained from FT, ET and BN were the same with the values obtained from PN varying slightly due to the randomness of Monte Carlo simulation. ET and FT were found to be simple, graphical and easy to use, but by themselves they allowed only static models to be developed. However, they can be mapped onto BN to be made dynamic and to consider dependencies and uncertainties of parameters. The BN required smaller number of nodes than PN which made it easier to use and understand.

A setback for discrete BN was the large number of input values required in its conditional probability tables (CPT) when the number of parent nodes increased. This setback can be greatly minimized through the use of continuous distribution nodes that allows each child node to be described as a function of its parent nodes through an equation [66]. Nodes with different distribution functions can be inferred in the same network. This convolution can increase the required computational time since the process now requires sampling of the data through simulation embedded in the software. However, it still requires much less time than Petri Nets.

For larger system, due to the large number of place and transition nodes, PN can lose its transparency and become less explicable. An advantage of PN was its ability to properly model an order of events and handle firing delays which may be immediate, deterministic, exponential, or Poisson in a single model. This means any action that requires a certain sojourn time till execution are well modelled by Petri Nets, thus giving a more realistic model. Developing such a model is possible in some existing BN

software, but it requires more careful consideration of how the network is developed and may not be as explicit.

BN readily allows incorporation of expert judgement and handling of different sorts of data. For PN, this is still in the development phase. Some recent work utilizes fuzzy sets in Generalized Stochastic Petri Nets (GSPN) to handle uncertainty associated with expert opinion while another brings together condition monitoring data and expert opinion together through a Plausible Petri Net (PPN) model [72, 73].

Perhaps the greatest advantage offered by BN for our purpose is that, being based on Bayes theorem, it allows past data to be used with new data to get a more informative understanding of risk. Hierarchical Bayesian analysis reduces source-to source variability of data for more plant-specific assessments. PN lags this provision

BN attains results by probabilistic inference of connected nodes whereas for PN, probabilistic values are obtained by statistical analysis of the behavior of process via simulation. In that context, these two tools achieve their common goal through different approaches which gives rise to different pros and cons of each method. Selection of whether to use BN or PN should depend on the intended application and the way one wants to view the system.

In order to carry out cumulative risk assessment, both methods have provisions for modeling the interaction of various deviations. However, BN allows consideration of dependencies and updating of probabilities, and if a BN is copied and run at a different time slice (as in a DBN), it allows for a quantified dynamic risk assessment. Although PN allows modeling of cyclic processes which are essential for a feedback system, the

explosion of the number of nodes in a PN for even a simple system and the required computation time as a result of this makes utilization of BN more preferable.

2.4. Quantification of human and organizational factors (HOF)

Incidents such as the Long Island disaster led to the realization that risk assessment should consider the impact of human and management decision on system failure. In 1992, Embrey noted that failure data collected from the field were not intrinsic properties but were much influenced by management of these components in the system [74]. He provided a generic model called MACHINE (Model of Accident Causation using Hierarchical Influence Network) where he showed that human error and hardware failures were affected by multiple levels of causal influences that were related to organization and management.

Most methods rely on expert opinions to express the level of impact management has had on system failure. We look at the various attempts to that has been made in the past in this regard.

The MANAGER method was developed in the early 90s through analysis of 921 incidents to provide generic failure frequencies (historical average) of contributing factors behind the incidents [75, 76]. These generic frequencies were then made plant-specific by multiplication with a single score of Management Factor (MF):

$F_{Estimate} = (MF) \times (F_{Generic})$

Values for MFs were obtained through a scoring system that involved experts answering 114 questions on critical technical barriers and process safety management

aspects within their facility on a three-point scale (good, average, bad). A ternary graph was developed to determine the value of MF from the scores obtained through the questionnaire. Line drawn on the ternary diagram to determine value of MF from the scores were also obtained from expert opinion and were site-specific.

Davoudian *et al*. suggested the Work Process Analysis Model (WPAM), modifying it to WPAM-II to consider dependencies among organizational factors that affected the failure of systems [77, 78]. Organizational culture (including safety culture, time urgency, ownership) were shown to indirectly influence the failure rate of equipment and human operation. WPAM used a three-step procedure that used task analysis and expert opinion to defined the relative importance of organizational factors for each process. Logical combinations of minimal cut sets (MSC) allowed bringing basic events such as hardware failure, human error, common cause failure together to determine incident frequencies. WPAM II offered a modification to this method by suggesting that organizational factors (such as inadequate training, improper maintenance procedure) could induce failure of dissimilar equipment as well [78]. For the quantification, WPAM II stated that changes in frequencies due to organizational factors were second order effects and used the success likelihood index (SLI) procedure to update the MCS frequencies.

$$f_{MCS} = f_{IE}.p_1.p_{2|1}$$

where p_1 is the probability of the first event and the $p_{2|1}$ is the probability of the second event given the first has occurred and is determined from the success likelihood index:

$$SLI_{2|1} = \sum_i R_j W_j$$

R_j and W_j represent the rating and the weight of organizational factors that are determined from expert judgement using the Analytical Hierarchy Process (AHP) [78].

The System-Action-Management (SAM) framework, published by Pate-Cornell *et al.* in 1996, suggested that incidents had organizational factors at their roots which influenced the management decisions and actions. These in turn influenced the basic events of system's failure [8]. SAM provided an analytical approach to consider the probability of a system failure under a given set of management factors. The physical system's failure probability was given as

$$p(F|M_k) = \sum_i \sum_j p\left(F\middle|IE_i, DA_j\right) p\left(IE_i\middle|DA_j\right) p(DA_j|M_k)$$

where F represented a physical failure or a loss level, IE represented the initiating events that led to failure and DA were the decisions and actions that contributed to the initiating event and the failure. This meant that the management affected a physical system's failure probability through a set of human actions and decisions. Expert opinion and physical system failure statistics were used for the analysis [8].

Papazoglou *et. al.* carried out an analysis of observed incidents in chemical facilities and identified eight (out of a total of 54) major underlying failure causes that appeared frequently in those incidents [79]. The work was based on the Process Risk Management Audit (PRIMA) system developed by Hurst *et al.* to give a quantitative measure of process safety management system (PSMS) for direct use in quantitative risk assessment (QRA) calculations [80]. Audits were conducted on these eight areas, called

Main Audit Areas (MAA), to provide subjective expert judgement and the results were assessed and converted to a single score a_i. The generic failure frequency f_{md}, taken from the RIDDOR database was then updated to get a modified frequency f_{mod} using the following equation:

$$\log f_{mod} = \log f_{md} + \sum_{i=1}^{8} a_i x_i$$

where x_i can attain values of -1,0 and +1 depending on whether the audit judges the plant safety management system as 'good', 'average' or 'bad' respectively.

Due to the presence of large number of equipment and human, operational and organizational factors to consider, a more structured approach was required. The previous work was extended to carry out assessment of safety indicators using audit. The project was termed I-Risk. It used audit to quantify the quality of the safety management system which was then used to update the base events of its fault free. The frequency was modified using the following relation [49, 81]:

$$\ln f_j = lnf_l + \frac{(lnf_u - lnf_l)}{10} m_j$$

where f_j is the modified parameter, f_l is the lower value and f_u is the upper value of each parameter for an installation with the best safety management system in the industry. These values were based on expert elicitation. I-Risk was different from PRIMA or MANAGER because while the latter attempted to find a single score as a modifying factor for updating failure rates, I-Risk linked management factors (termed 'delivery systems') to the base events of fault trees generated during QRAs. By applying the notion that the delivery systems were common to various events in the fault trees, I-Risk was able to reduce the number of links required for consideration in QRAs. However,

the link between the audit findings and the events of the fault tree were not well established and the required analysis and audit were not very practical [82].

Building upon the I-Risk project with an addition of an indicator on safety culture, the Accidental Risk Assessment Methodology for IndustrieS (ARAMIS) project was developed. This project aimed to put a chain of methods that led to determination of the impact a particular facility will have on its surrounding, given the current condition of its safety barriers [83, 84]. It tried to change the link from the delivery systems to the events of the fault tree in I-Risk to link between the delivery system and safety barriers. Duijm *et al*. provided a barrier-oriented quantification method for the ARAMIS project [82], basing the probability of failure on demand (PFD) of a SIL on the design value and suggesting that in reality, the value will be less because of deficiencies in safety management system.

$$LC_{operational,k} = (1 - \sum_{i=0}^{7}(1 - S_i)B_{i,k})LC_{design,k}$$

LC (level of confidence) refers to the reliability of a SIL system, *Si* is the audit rating for the management factor (delivery system) corresponding to structural element *i* and *Bi*,*k* is an array of weight factors linking the importance of the delivery system linked to *i* to the barrier type *k* affected.

Mosleh *et al.* provided a parametric model for incorporating the influence of organizational factors using the ω-factor model [85]. The total failure rate was

$\lambda_{Total} = \lambda_I + \lambda_o$

where the 'inherent' failure rate λ_I is usually determined through testing of an equipment by the manufacturer (beyond the influence of the plant) or can be seen as the individual characteristic of an operator (in case of human performance reliability). The rate of failure due to organizational factors λ_o increased the total failure rate. The factor $\omega = {\lambda_o}/{\lambda_I}$ represented this increase. For failure being affected by maintenance, the component reliability and operator performance were modeled as

$$\lambda_{Total} = \frac{n_I}{T} + \frac{\hat{P} N_{maint}}{T}$$

Where $\hat{P}$ is the probability of a worker's performance being adversely affected by organizational factors (for maintenance, $\hat{P}$ can be the ratio of the number of maintenance-caused failures to the total number of maintenance activities conducted N_{maint}) and T is the operating time. In this model the consideration of time and hence rate added a dynamic aspect to the assessment. Most of the conditional probabilities of influences are estimated from expert opinion, but provisions are made for incorporation of field data if available, making the ω-factor model more data-driven than others.

The impact of human and organizational factors on SIL were studied by Schönbeck et al. [86]. This group suggested the use of a factor θ that represents the sensitivity of safety instrumented systems to human and organizational factors and proposed using the following equation to determine the existing SIL level.

$$SIL_{operational} = (\theta \sum_{i=1}^{8} R_i W_i - 1) log PDF_{design}$$

Here the rating R_i and W_i were to be obtained from expert opinion again. It was noted that although weights could be obtained from accident data analysis, due to the rarity of incidents, it was better to seek expert elicitation for values. Values obtained indicated if the operational SIL level was the same as designed and did not update the existing failure rate of the instruments.

Organizational Risk Influence Model (ORIM) were proposed by Øien to be used as a tool for monitoring risk in offshore installation [50]. The author used Bayesian Network to tackle the possibility of multistate representation and the intuitive connection between the organizational factors with the technical ones. Each organizational factor could be assessed by multiple indicators. The measured value of each indicator was converted to a rating value and were brought together using weights (determined from expert opinion) to obtain the rating for the organizational factor being assessed. The weightage used for bringing the factors together could be obtained from experts or could be data driven. Bayesian network propagation algorithm was used to take account of the rating of the organizational factors as well as previously observed leak events. For the weightage of how each organizational factor contributed to the failure rate, a rather complex process was developed utilizing concepts of Hidden Markov Model, Markov Chain Monte Carlo simulations, expert judgment, Maximum Likelihood Estimation and Cox Model of Proportional Hazards. The values had basis on analysis of 92 previous leak incidents and the process attempted to estimate the conditions that existed in the plant prior to the incidents to understand how each factor contributed to each incident.

The number of times each factor contributed to incident were assumed to be Poisson distributed.

An easy method to make data more plant specific to account for local operating conditions is outlined in the CCPS Guideline [87] . The method is straight forward and uses correction factors based on judgement. When company practices vary, this method can provide uncertain outcomes [75]. The MIL-HDBK-217F also offers constant values called π factors that modify the base failure rate. These are, however, constant values and organization influences the failure rate in a linear manner [88].

The API RP 581, published in 2000, provides a simpler methodology to modify generic equipment failure rates through use of 'modification factors' based on design data and site inspection. It was developed to be a better version of that suggested by CCPS [89]. It provides look-up tables based on the number and category of inspection for estimation of the probability of failures due to corrosion, erosion *etc*. As Pitblado *et. al*. mentions, this method was developed based on findings about 20 years ago. Management systems have changed significantly, values have changed and this method is no longer valid for application [75].

With the development of the bowtie method formed from a combination of event trees and fault trees, the barrier concept became more accepted. Barriers were capable of addressing operational risks and the bowtie made clear what barriers were in place, what factors affected their effectiveness and how they can be managed [75]. Studies were conducted to identify what barriers were present in upstream facilities and methods were developed to allow quantification to understand their effectiveness [11, 12, 48, 75]. The

Barrier and Operational Risk Assessment (BORA) method [11, 90] used the similar scoring method to compare 'risk influencing factors (RIF)' with industry average P_{ave} to modify values for operational factors that could affect barrier conditions.

$P_{rev}(A) = P_{ave}(A)\sum_{i=1}^{n} w_i Q_i$

A modification to this method, called Risk_OMT, came with the development of the Hybrid Causal Logic (HCL), discussed in Section 1.3.1.1. The HCL allowed the RIFs to be integrated with the basic events of the fault tree and be mapped onto a Bayesian Belief Network (BBN) [12, 45, 46]. The RIFs were obtained by the same scoring method and was applied for evaluating risk in an offshore installation.

The TEC2O considers an improved version of API 581 as the Technical Modification Factor (TMF) and multiplies it with the Management Modification Factor (MMF) to obtain an overall modification factor for generic failure frequencies [91]. For TMF, indicators covering aspects of ageing, environment, construction and process are considered, whereas for MMF, aspects of operation and organization are included [92]. The equation used is

$f = f_b \times TMF \times MMF$

where f_b is the baseline frequency or generic frequency. Values for TMF and MMF are obtained through the scoring of specific indicators (S) and application of weights (wt) obtained from expert opinion (or all scores are assumed to carry equal weights). The score and the weights are combined as

$\varepsilon = \sum_{i=1}^{n} S_{i,j} wt_i$

This combined value is used to obtain TMF and MMF from a relationship graph. How the relationship graph was obtained was not clearly explained.

2.4.1. Summary of findings

Where the scoring method is used, a complete reliance on expert judgement is required. The number of questions that the experts are required to answer are also very large, usually being more than one hundred. Expert opinions may vary, and though may methods have been suggested for eliciting and analyzing the results, they may not reflect the exact plant conditions [17, 93]. The expertise of the expert himself may be questioned too. Also, it is not possible to gather up experts to redo the questionnaire whenever an operation is undertaken. Thus, the dynamic risk assessment may become a static one with risk values indicating plant situation many months back.

2.5. Techniques for updating risk with time

One of the challenges for assessing cumulative risk is to keep data used for the assessment updated and precise. Most of the data used in the industry and by other researchers are either obtained from generic failure data, from manufacturers' recommendations or through expert opinions. Updating the data allows for incorporation of changes in the system over time and also makes the data plant specific.

Bayesian Network has been widely used for this purpose due to its capability of updating beliefs based on new information as they became available, i.e. as new failures were reported in the facility.

Meel *et. al.* showed how incident database from a chemical facility could be utilized to provide likelihood data for a Bayesian updating of current failure probabilities to obtain a posterior/updated one [94, 95]. Kalantarnia *et. al.* developed a method based on the work by Meel *et. al*. to develop a predictive model for probability of an incident based on 'accident precursor data' (which are events that are not incidents, but indicate an increased likelihood of one) from expert feedback and plant specific data [96].

Later, Rathnayaka *et. al*. developed the System Hazard Identification, Prediction and Prevention (SHIPP) model using the concept of Bayesian updating to use near-misses and incident information to predict the number of incidents in a future and update the failure probabilities of different barriers [97, 98]. They adapted the failure tree model developed by Kujath *et. al.* that showed the different factors that contributed to barrier conditions in offshore installations and converted each to fault trees [99]. The model was modified to include human and management barriers as well. Event tree analysis was used to depict the consequences for failure of different barriers with severities defined as near miss, mishap, incident and accident. While the fault trees showed how failure of a factor contributed to failure of a barrier, the event tree showed how failure of each barrier gave rise to various severities of consequences. Information regarding the number of scenarios in each severity were obtained from analysis of various abnormal scenarios in an offshore facility. This information was used to determine the likelihood of those abnormal incidents (taken as Poisson distribution of failure frequency λ which is a prior gamma distribution). Based on conjugate property, the posterior was a gamma distribution whose parameters were easily derived to

determine the probability distribution of the number of abnormal events in the next time interval given observed data y_i, as shown below:

$$p(y_{t+1}|data) = \frac{\lambda_p^{y_{t+1}} e^{\lambda_p}}{y_{t+1}}$$

Further, the likelihood data was used to update the failure frequencies of each barrier assuming each severity to be due to failure of a particular set of barrier failure and taking failure frequency of each barrier failure to be an independent random variable.

Hierarchical Bayesian Analysis (HBA) has been used frequently in recent times to update generic data with plant specific data. HBA is so called because it utilizes a hierarchy of prior distributions. Generally, a two-stage updating of the prior is utilized whereby a population variability curve is generated in the first stage and a plant-specific data is used to update the variability curve in the second stage.

If θ id the unknown parameter of interest, the Bayes Theorem gives

$$\pi_1(\theta|x) = \frac{f(x|\theta)\pi_0(\theta)}{\int_\Theta f(x|\theta)\pi_0(\theta)d\theta}$$

Where $\pi_0(\theta)$ is the prior distribution of θ, f(x|θ) is the likelihood function, or the aleatory model of x given values of θ and $\pi_1(\theta)$ is the posterior distribution of θ [69, 100]. Observed data are fed to the equation via the likelihood function.

In HBA, we first use a prior to represent the population variability (the variability in the data sources) and then specify a second prior to represent the epistemic uncertainty associated with the parameters of the first-stage prior [68]. The prior distribution for a parameter of interest θ is denoted as π(θ) where

$\pi(\theta)=\int_{\Phi} \pi_1(\theta|\varphi)\pi_2(\varphi)d\varphi$

Here, $\pi_1(\theta|\varphi)$ is the first-stage prior distribution of θ conditioned upon φ and represents the variation in θ in the population. $\pi_2(\varphi)$ is the hyperprior representing the uncertainty in φ or the prior knowledge and its components are termed hyperparameters [69]. Various methods have been proposed using HBA to update probability distributions with new data [101, 102]

Mohaghegh *et. al*. outlines a socio-technical safety causal model SoTeRiA that brings organizational factors with technical ones using big data analytics in Bayesian Belief Network [103-106]. The method suggests using investigation reports, developed models and various other documents handled in a facility to update the risk assessment model. However, though what needs to be done is suggested, implementation method and obtaining risk values are yet to be shown. The relations among the various factors have not been shown, and hence the model is still incomplete.

2.5.1. Summary of learnings from literature

Although it is suggested that if barriers are updated, then by the diagnosis capability of Bayesian networks, one may update probabilities of basic events, these basic events are actually conditioned on the barrier failure and does not reflect true probabilities [107]. In a dynamic system, changes in the values of probabilities may make some contributing factors to have more effect on the barrier than previously determined. Thus, this suggestion of updating probabilities of basic events from updated probabilities of barrier failure may lead to wrong conclusions. However, the concept of

learning from incidents and incorporating the learning into the risk assessment model may be the best way to understand how the system changes and what changes cause failures.

2.6. Gap identification

From the past approaches that have been developed to assess overall risk in a plant, we identify that it is essential to develop a model that captures the non-linear interaction of various factors and also provides a feedback loop whereby the actions resulting from decisions or changes can be understood. On the other hand, simple models such as fault tree and event trees are preferred to maintain the transparency of the risk assessment. There does not exist a model that can do both.

In terms of the tool to use for risk assessment, fault trees and event trees mapped onto BN and BN by itself appear to be the best choice to move forward.

As noted from the literature review, quantification methods to incorporate the effect of human and organizational behavior not only gives the overall value of risk, it also allows for making generic data plant specific. Most of the methods developed however rely on expert opinion. The use of the expert opinion or scoring method has its limitations for dynamic risk assessment: the only way it can capture the dynamic nature of a changing system is by asking for experts' updated opinion, which is difficult since the process of gather opinions is lengthy and accumulating reliable opinion from multiple experts is not always feasible. There has been attempts to utilize past incident records to learn how organization has influenced system failure, but incidents were

gathered from various facilities and to make the data plant-specific, expert opinion had been reverted to again.

The use of Bayesian Network to update failure frequencies of barriers is a fairly new concept and hierarchical Bayesian analysis allows learning from incidents to be absorbed into risk assessment method. Since catastrophic events are very rare in the industry, the concept allows information from the more frequent near- misses and smaller incidents as well as incidents in other facilities to be utilized to update knowledge about barrier conditions so that we can predict the probability of large incidents. However, the method applied in the SHIPP model allows updating only the barrier failure probabilities from near-misses and small incidents but does not tell us what contributing factors are more likely to cause the failure. Using information about various types of incidents may allow updating barriers, but what contributed to the barrier failure can only be understood if the failure probabilities of the basic events or contributing factors behind the barriers are updated.

Risk assessments should be up to date and frequently done to be aware of any factors contributing to barrier failures and to take necessary measures whenever needed. The use of Bayesian network and learning from incidents and other available data from the facility to update the network seems to be a better approach than seeking expert elicitation every time a risk assessment is needed. The use of Dynamic Bayesian Network would provide an easy way to assess dynamic risk. Visualization of the changes in risk with time can be obtained, which is not possible by any other method found. To update the risk, the knowledge about basic events can be obtained from

incidents, via investigation. Findings from investigations can then be applied to update the basic events or contributing factors and these will show the present barrier health condition. This can be further extended to bring information from other sources such as maintenance and inspection databases, making the model more dynamic and cumulative.

3. METHODOLOGY*

3.1. The Reflected-Pyramid Concept

For plant-specific and dynamic risk assessment, we need to utilize information generated within the facility itself over time. As mentioned above, one of the starting points for extracting site-specific information to understand existing risk situations is to learn from failures that have occurred in the past to reveal the dynamic patterns behind them. Experimental determination of failures is not always feasible: equipment failures are largely dependent on their operating environment and how they are maintained, while organizational failures are impossible to experiment with. As Coze mentions, it is rather difficult to determine ahead of time what will go organizationally wrong due to the large amount of information [34]. He also states that organizational studies focusing on normal operations are extremely difficult since what can go wrong is not as clear as it is after an incident. Also, it is difficult to learn from incidents since large scale incidents are rare. If the idea behind Heinrich's Safety Pyramid is extended, much more information can be generated through analysis of near misses as well as minor incidents that occur within the facility [26, 108]. Figure 1 depicts how information from various incidents and near misses can be used to constantly update our knowledge about the management system of a facility [109].

---

* Parts of this section are reprinted with permission from "A journey to excellence in process safety management" by SZ Halim and MS Mannan, 2018. Journal of Loss Prevention in the Process Industries, 55,71-79, Copyright [2018] by Elsevier.

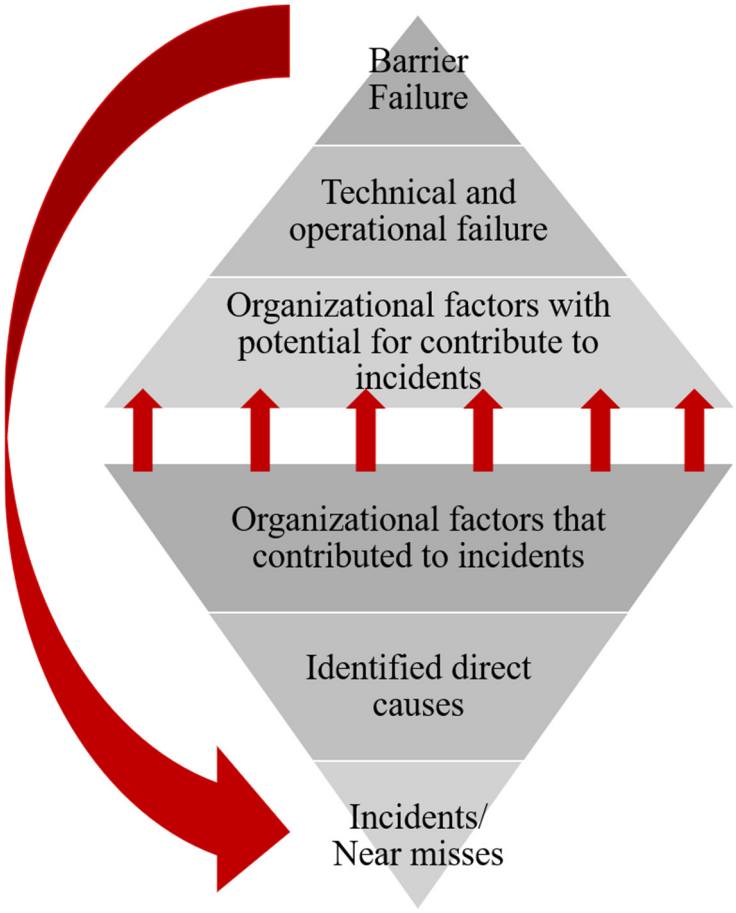


Figure 1: The Reflected-Pyramid Concept: Learning and Extracting Mechanism *Reprinted with permission from "A journey to excellence in process safety management" by SZ Halim and MS Mannan, 2018. Journal of Loss Prevention in the Process Industries, 55,71-79, Copyright [2018] by Elsevier.

Near-misses (where the last line of defense is challenged) and incidents, as shown at the bottom of the triangle, can be investigated to identify the direct/immediate causes that led to their occurrence. These will usually emerge as technical or operational factors, such as equipment failure or human error, respectively. These technical/operational factors should be analyzed further (for example by asking more

questions such as why an equipment failed, or why there was operational error). This will usually help identify a larger number of organizational or managerial issues (such as maintenance backlog, understaffing, lack of training) which contributed to the direct causes. In this manner, investigation of near misses and incidents can eventually lead to a better understanding of the organizational limitations which reside within the system and may play a role behind future incidents. This information can be used to update failure data of the system. Extraction of data from these incidents will be independent of the investigation process. In Figure 1, the smaller red arrows in between the pyramids indicate that information about organizational factors extracted from investigation reports from the lower triangle can be applied to the bottom part of the upper triangle.

The upper triangle in Figure 1 represents predicting the risk of future barrier failure. Here, organizational or managerial limitations are seen to contribute towards technical or operational failure, ultimately causing barrier failure. Failure of barriers can lead to a near-miss or incident. Information about any barrier failure (with or without an incident) can be used to re-update information about the organizational factors by again starting from the bottom part of the lower triangle (via the larger red arrow) creating a feedback loop.

In this way, it is possible to keep updating information about the management system through continual investigation of barrier failures and keeping the risk assessment dynamic. Barrier failures act as a feedback to the way the facility is managed and allows completion of a learning loop. This model can be further applied to all technical and operational failures but would require larger resource for investigation.

Development of a simple mechanism for extracting data from all failures can provide an easy pathway to continually update information to provide a more dynamic look at risk.

3.2. Framework for Cumulative Risk Assessment

The reflected-pyramid concept shown in Figure 1 forms the basis for assessment of the plant-specific and dynamic health condition of barriers to predict cumulative risk. This concept allows identification of organizational limitations from past incidents, recognition of previously unknown combination of causes that led to failure, and extracting relevant information from data sources to quantify non-technical factors for assessing cumulative risk.

Figure 2 shows the framework for cumulative risk assessment to assess barrier health. When a significant amount of data from the past incidents and operation of a facility is available, the risk assessment model can be established. Past data provides a prior knowledge about the way barriers have failed in the past. As new data becomes available, this knowledge is updated to determine the current condition of a barrier (through the use of Bayesian analysis). In the absence of sufficient data, generic or industry-averaged data can be used to begin with, which can later be updated with plant-specific data as they become available.

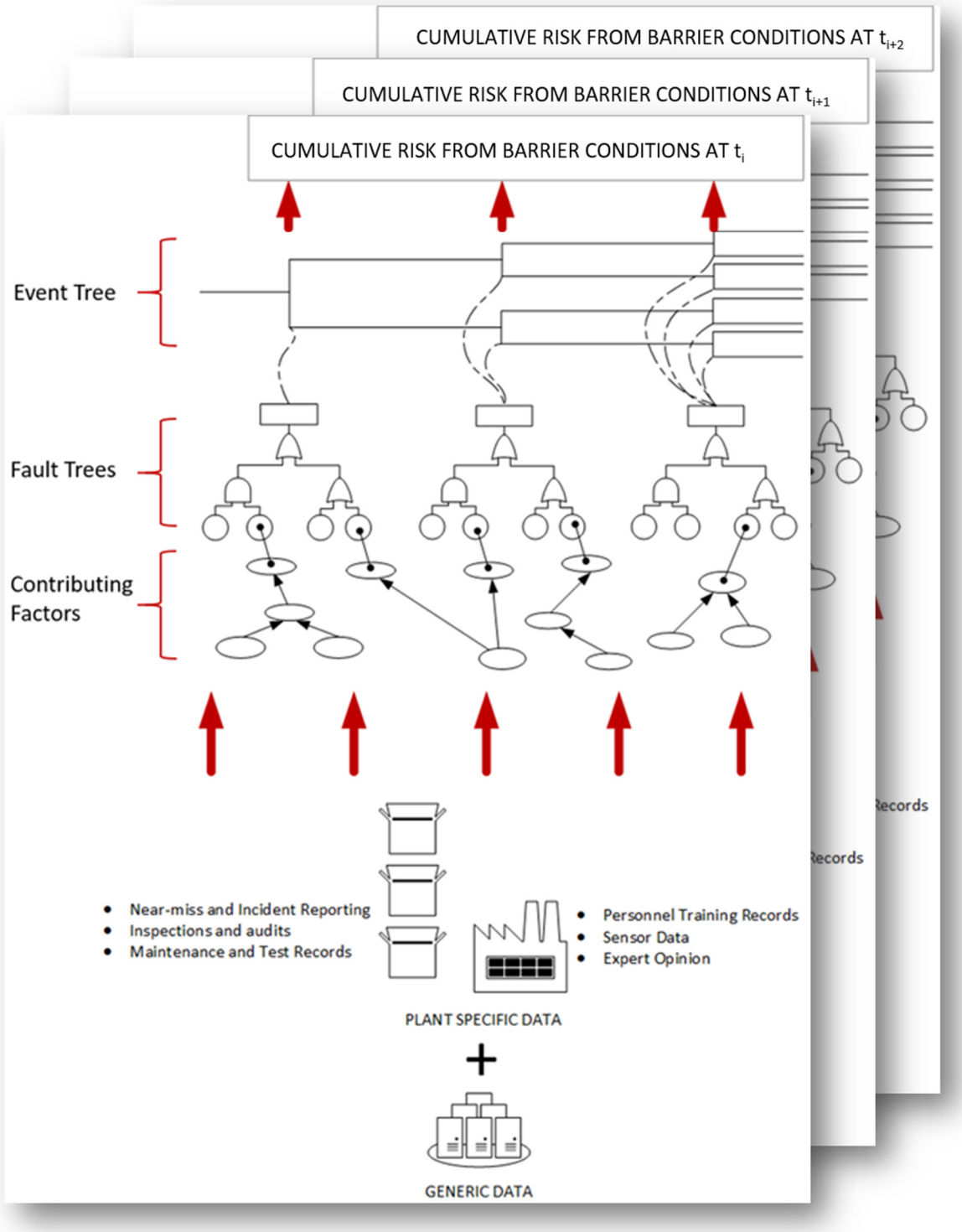


Figure 2: Framework for Cumulative Risk Assessment

The following chapters provide step-by-step guide on how this framework is to be established. It begins with analysis of past incidents and moves on to answer the following questions:

- What are the factors that contribute to an incident?
- What is the rate at which each factor has been occurring in the past and how can they be used to estimate future failure probabilities?
- How do these factors interact with each other to increase the risk?

Due to the novelty of this work, this thesis first establishes the methodology for generation of generic data, showing how non-technical factors are identified, quantified and used for developing a risk assessment model based on learnings. Through a case study, it also shows how the model can be updated with time to capture the dynamic changes in risk in a facility. Bayesian network is used for development of the framework.

3.3. Step-by-step method for CRA

3.3.1. Step 1: Learning and extracting information from incidents

For any near miss or incident reported, an investigation has to be conducted and a report must be presented. This investigation report is used to obtain information to assess barrier conditions. For this research, we apply this step to investigation reports of US OCS offshore facilities.

This step is performed by breaking it down into the following tasks:

- Establish a methodology for extraction of information from investigation reports.

- Use developed methodology to analyze incident investigation reports to identify contributing factors behind each incident

This constitutes Chapter 4.

3.3.2. Step 2: Generation of generic and plant-specific failure data to estimate frequency/probability of occurrence

Step 2 looks at using data generated in Step 1 (Chapter 4) for updating the technical and non-technical failure rates and probabilities to capture the dynamicity of the system. Mathematical formulations for updating technical factors from generic data are readily available in literature [110, 111] and are adopted. In this work, this step will focus on showing how generic data can be generated for non-technical factors and can be updated as plant data becomes available. Step 2 includes the following tasks:

- Adopt a mathematical formulation for updating failure rates of equipment
- Propose a method for determining prior quantity about failure chances of non-technical factors (estimation of generic data)
- Modify generic information using plant-specific data

This constitutes Chapter 5.

3.3.3. Step 3: Estimation of how various factors combine to increase risk

Step 3 uses the learning from Step 1 (Chapter 4) to determine all possible path by which each contributing factor can interact with each other to cause the incident.

Importance of each path is expressed by assigning weightage that is calculated from the analysis in Step 1. Step 3 performs the following task:

- Estimate the weightage of various combinations of contributing factors from previous incidents

This constitutes Chapter 6.

3.3.4. Step 4: Dynamic Barrier Health: Estimating cumulative probabilistic risk

With an understanding from Step 1 and quantitative results from Steps 2 and 3, the risk assessment model is developed to merge all technical and non-technical factors in Step 4. To assess the risk of barrier failure in the future the following tasks are performed:

- Construct a model for barrier analysis, based on contributing factors identified in Step 1.
- Using values of failure probabilities determined in Step 2 and weightage of their combination in Step 3, conduct the probabilistic risk assessment to analyze dynamic cumulative risk.

This constitutes Chapter 7.

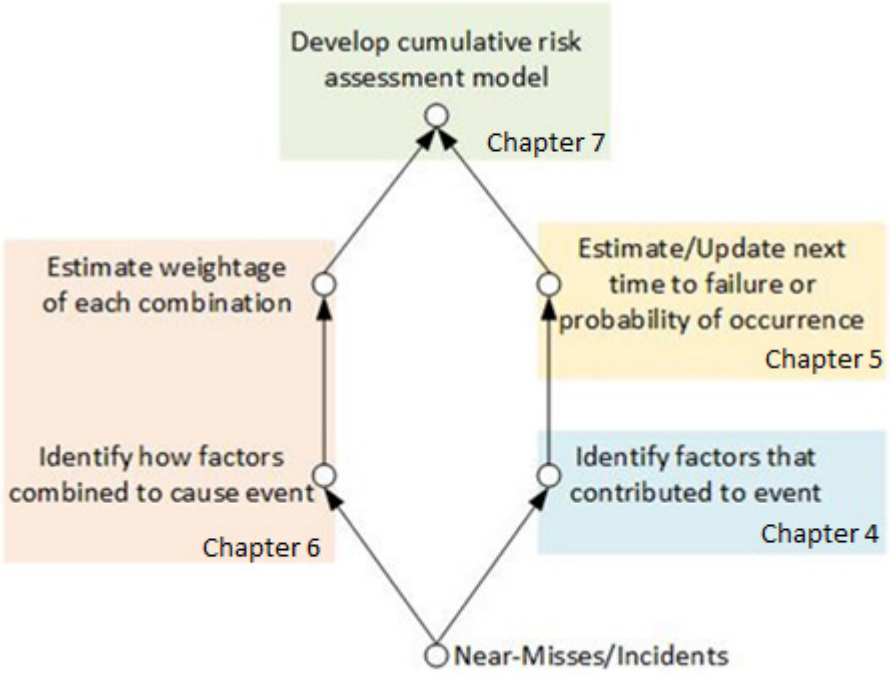


Figure 3: Methodology for a cumulative risk assessment showing how the task performed in each step lead to the development of the model.

Figure 3 shows the steps to be followed for cumulative risk assessment and hence outlines the organization of the thesis. Each of the steps are covered by the subsequent chapters. We basically start at the bottom of the inverted pyramid and work our way upwards.

4. LEARNING AND EXTRACTING INFORMATION FROM INCIDENTS[†]

4.1. Background

Offshore platforms are generally characterized by a high degree of congestion created by a network of pipelines and other equipment essential for the operations. Also, the rigs have limited ventilation and difficult escape routes, which increase the risk of working in these environments. Under these circumstances, a minor event can quickly accelerate into a catastrophe. Many such incidents have occurred in the past that have led to large loss of assets and human life and tremendous damage to the environment in terms of pollution. The Deepwater Horizon oil spill in the Macondo oil well and the Piper Alpha disaster in the North Sea are a few examples of events that had far-reaching effects on the society and regulatory infrastructure. Some of the known incident scenarios in offshore facilities include blowouts, liquid and vapor leaks, fires and explosions, vessel collisions, dropped objects and structural failures [112, 113]. It is thus essential to understand why these incidents occur in order to develop an awareness of conditions that have the potential to lead to disasters. This will enable timely measures to be taken to prevent them from occurring.

Over the years, researchers have indicated the need to investigate incidents and near misses to harness the information to prevent recurrences [114-116]. Many authors

---

[†] Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier

have been involved in examining the causes behind past industrial incidents. Kidam et. al. analyzed 364 chemical process industry (CPI)-related incidents that occurred from 1964-2003 [117]. They used a database that contained extensive information to determine the frequency and importance of various contributing factors behind the incidents. They found that human and organizational factors were the largest contributors (19%). Okoh et al. analyzed major incidents caused by maintenance and related activities in various process industries [118, 119]. The main objective of the study was to understand how maintenance influenced the occurrence of incidents to facilitate an understanding of the required measures to prevent them. They classified the causes based on their Work and Accident Process (WAP) classification scheme. The work was based on the investigation of incidents with maintenance related issues only. Kannan et al. collected and analyzed 96 incidents from across the world in a one-year period in order to identify deficiencies in safety management systems [120]. The incidents were classified based on the geographic zone, type of industry (upstream, midstream, downstream), incident category (fire, explosion, release) and substance involved. The analysis used the 20 elements of risk-based process safety management approach. Some of the most important factors that contributed to the incidents were: deficiency of safe work practices, operating procedures and conduct of operations. Mannan et. al analyzed 5 years of United States Environmental Protection Agency (EPA)'s accidental release information program database to identify common primary and contributing causes that led to chemical releases [121]. Their study found that maintenance activities, upset conditions, inappropriate operating procedures, improper

training, by-pass conditions, unsuitable equipment, faulty process design, weather conditions, unknown conditions and others were the contributing factors behind incidents. They concluded that issues such as data integrity, taxonomy of the database, and differences among facilities may present certain drawbacks when analyzing these databases.

Although many researchers have analyzed past incidents, most of these are limited to specific sectors of industry or the chemical industry in general. Very limited work has been done that are focused on the offshore oil and gas industry specifically. Operation in different industries vary by the type of equipment used, the environment, the required skills of personnel involved, the material handled and so on. Thus, a generalized analysis encompassing various chemical industries may not be suitable to identifying causes behind offshore incidents.

Hare et. al. developed a report, which provided details regarding the underlying causes of offshore incidents [122]. The document is based on the analysis of 67 offshore incidents obtained through UK Health and Safety Executive (HSE) Offshore Safety Division (OSD) and RIDDOR (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations) investigation reports. The study only deals with incidents that took place between 2004 and 2008 and considered only those incidents that resulted in fatalities or major injuries or both. However, to gain a better understanding of the causes behind offshore incidents, it is important to not only consider major incidents, but also minor ones, as well as near misses if possible. Information about many incidents that

occur in offshore facilities are not always readily available and this can pose a challenge towards learning about the contributing factors behind them.

Offshore operators operating within the US Outer Continental Shelf (OCS) are required to report certain incidents to the Bureau of Safety and Environmental Enforcement (BSEE) District Manager according to the US Code of Federal Regulations (30 CFR 250.188) [123, 124]. Their website on offshore incident statistics show that the number of incidents reported vary by type (fatalities, injuries, loss of well control, fires/explosions, collisions, spills >50 bbls, lifting, gas releases, evacuation musters), and by number ranging from 475 to 783 incidents each year between 2009-2016 (fiscal year) [125]. This indicates that incidents still keep happening! BSEE conducts investigation of these incidents and has taken steps to make some investigation reports publicly available through their website [126, 127]. The investigation reports are constantly being added to the system as they are generated and hence can aid in providing a good database for analyzing causes behind recent offshore incidents. With this view, a study was undertaken to analyze 137 fire-related incident investigation reports obtained from the BSEE website to provide a more comprehensive statistical summary of various underlying technical, operational, human and organizational factors behind these offshore incidents in the US OCS [127].

The remaining part of this chapter provides details about what information was available in these reports and how they have been analyzed, followed by a discussion about the findings and the measures required to reduce future incidents.

4.2. BSEE incident investigation report

4.2.1. Incident Investigation by BSEE

Based on the incident reported, BSEE determines the type of investigation that is to be conducted by their personnel. Usually incidents that involve fatality, serious injury or a major pollution event are investigated in details by a panel that includes investigators from BSEE's Safety and Incident Investigations Division, Regional Office of Incident Investigations and also from other agencies when needed [123]. These are termed Panel Investigation Reports. Some investigations that require less resources are conducted by BSEE's district personnel and are delivered as District Investigation Reports [123]. All investigations are usually conducted via a combination of witness interviews, testing and analysis of involved equipment, and a review of the operators' and contractors' documentation [123].

4.2.2. BSEE's List and Status of Incident Investigations

BSEE has listed information about the investigated incidents in their website and as of October 31, 2017, the list showed a total of 1617 panel and district investigations conducted from January 4, 1995 till October 31, 2017 in the US OCS (reports prior to formation of BSEE in October 2011 had been developed by Minerals Management Service (MMS))[128]. This list of status and investigation has been termed as the "Investigation Reports Listed" shown in Table 2. Some of these reports are still pending completion and not all of the reports are publicly available via the website. The numbers that we were able to download are listed under "Investigation Reports Available" in

Table 2. The table also shows the time range of the incidents whose reports are listed or available.

Table 2: Table showing number and time range of district investigation reports and panel investigation reports listed and available via BSEE website (as of October 31, 2017). *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

	Investigation Reports Listed [16]		**Investigation Reports Available [14,15]**	
	Time Covered	**No. of Reports**	**Time Covered**	**No. of Reports**
Panel Investigations	01/04/1995-09/19/2017	70	07/20/1983-03/10/2016	101
District Investigations	01/04/1995-09/19/2017	1547	04/11/2003-09/11/2017	859
Total Investigations		1617		960

All investigation reports listed have been categorized according to their type and are identified as follows: required evacuation, LTA (1-3 days), LTA (>3 days), RW/JT (1-3 days), RW/JT (>3 days), injuries, fatality, pollution, fire, explosion, loss of well control, collision, structural damage, crane, other lifting device, damaged/disabled system, incident >25K, H_2S release, required muster, shutdown from gas release and others (LTA refers to Lost Time Accident and RW/JT refers to Restricted Work/Job

Transfer) [128]. Figure 4 shows the numbers in each category as provided in the BSEE investigation list. Each incident may include several categories (*e.g.* a blowout incident may also include fire and other injuries). For clarity, only the types investigated in greater numbers are shown here.

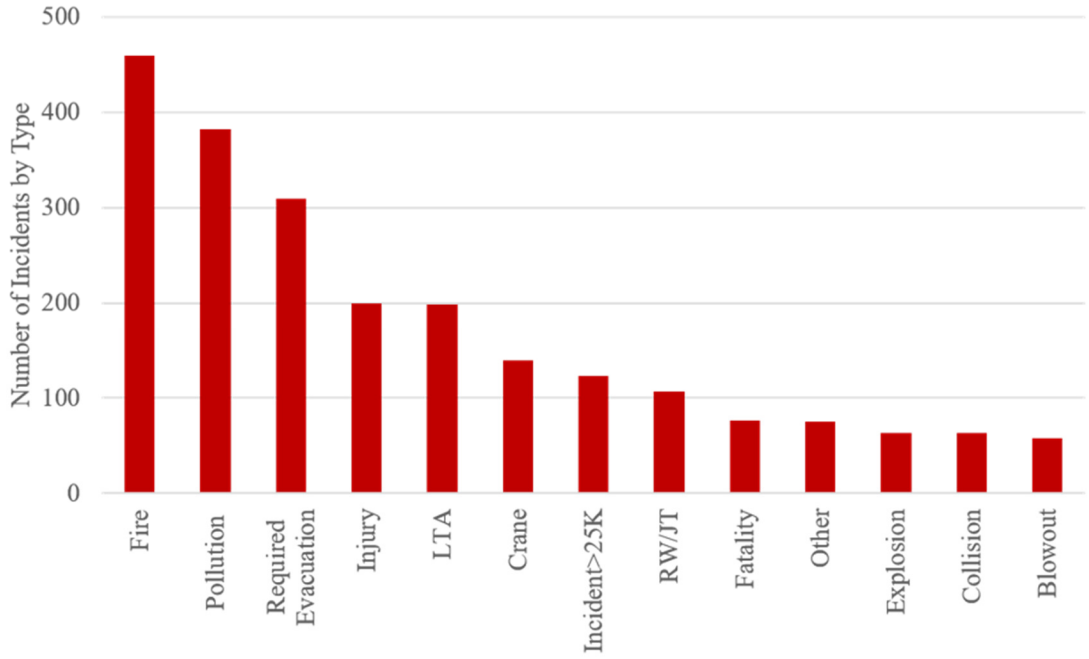


Figure 4: Figure shows the top-most type of incidents present in the investigation reports listed (in the time range 01/04/1995-09/19/2017) *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

Based on the above findings, it can be seen that over the given period, fire incidents have been investigated the most (28.4%). From a process safety point of view, fire incidents can indeed bring major catastrophe on an offshore oil/gas facility. This paper analyzes 137 fire-related district investigation reports obtained from BSEE's website to identify the contributing factors behind them [127]. The sample reports used

in this study covered incidents that had occurred between calendar years 2004 and 2016. Since the panel investigation reports differed significantly from the general format of the district investigation report, the analysis was restricted only to the latter.

4.2.3. BSEE District Investigation Reports:

The district investigation reports are short reports prepared by BSEE investigators. All reports have a fixed format whereby different information are filled under various sections/categories. The first page has a format similar to that shown in Table 3a: it is concise, information about the offshore facility and type of incident and causes are indicated under 16 sections.

Although the general format of all reports remains more or less the same (some reports were found to have no information disclosed on certain topics), individual investigation reports mainly vary starting from the second page (Table 3b) where the investigation findings are diverse and have different lengths of narration. Based on the incident occurrences, identified causes and the overall narration, the district investigation reports also vary in size. In addition to the first page, or Page 1 (Table 3a), the following pages of the reports provide information under various other headings as given in Table 3b.

4.2.4. BSEE Incident Information

Some of the sections shown in Tables 3a and 3b provided specific and concise information about the facility. This information was collected from all 137 fire incidents.

Table 3a Table showing the general information presented in the first page (Page 1) of district investigation reports. *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

1. Occurred a. Date b. Time 2. Operator: a. Representative b. Telephone Contractor a. Representative b. Telephone 3. Operator/ Contractor Representative/ Supervisor on site at time of incident 4. Lease: a. Area c. Latitude b. Block d. Longitude 5. Platform Rig Name 6. Activity o Exploration	o External Damage o Fire o Explosion LWC o Historic Blowout o Underground o Surface o Diverter o Surface Equipment Failure or Procedures Collision o Historic >$25K <=$25K o Structural Damage o Crane o Other Lifting Device o Damaged/Disabled Safety Sys. o Incident >$25K o H2S/15Min./20ppm o Required Muster

Table 3a: Continued

○ Development/Production (DOCD/POD) Operation ○ Production ○ Drilling ○ Workover ○ Completion ○ Helicopter ○ Motor Vessel ○ Pipeline Segment No. ○ Other 7. Type ○ Historic Injury ○ Required Evacuation ○ LTA (1-3 days) ○ LTA (>3 days) ○ RW/JT (1-3 days) ○ Other Injury ○ Fatality ○ Pollution ○ Human Error	○ Shutdown From Gas Release ○ Other Cause ○ Equipment Failure ○ Slip/Trip/Fall ○ Weather Related ○ Leak ○ Upset H2O Treating ○ Overboard Drilling Fluid ○ Other 8. Water Depth 9. Distance From Shore 10. Wind Direction Speed 11. Current Direction Speed 12. Sea State 13. Pictures Taken 14. Statement Taken 15. Operator Representative/ Supervisor on site at time of incident

Table 3b Table showing information presented in the remaining pages of the district investigation reports *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

17. Investigation Findings
18. List the Probable Cause(s) of Accident
19. List the Contributing Cause(s) of Accident
20. List of Additional Information
21. Property Damaged, Nature of Damage and Estimated Amount (Total)
22. Recommendations to Prevent Recurrence
23. Possible OCS Violations Related to Accident
24. Specify Violations Directly or Indirectly Contributing
25. Date of Onsite Investigation
26. Onsite Team Members
27. Operator Report on File
28.Accident Classification
29. Accident Investigation Panel Formed, OCS Report
30. District Supervisor/Approved Date

The data collected indicated that most of the incidents occurred Production Operations (68%), followed by Others which include Plugging and Abandoning Operations, Construction, Maintenance *etc*. (from section 6 of Table 3a). A significant number of incidents also occur during Drilling (Figure 5).

By comparing the information about the depths of offshore facilities provided (from section 9 of Table 3a), it was found that 6% of fire incidents occurred in ultra-deepwater facilities (>1500 m), 20% in deepwater facilities (125m-1500 m) and the remaining 74% occurred in the shelf (<125 m).

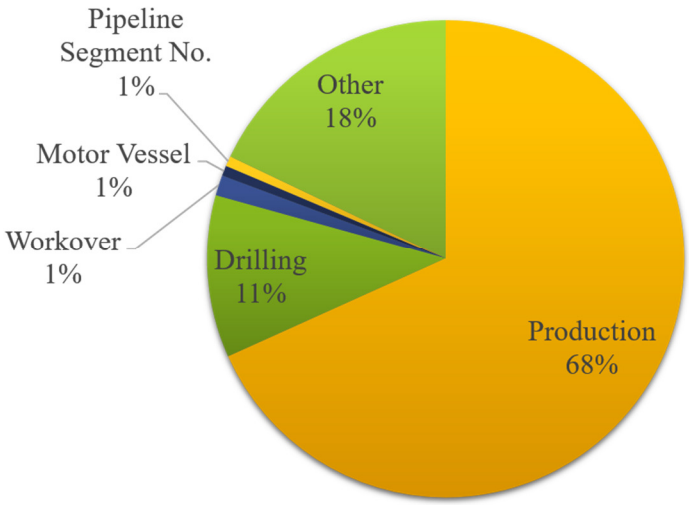


Figure 5: Figure showing type of operation being conducted when fire occurred *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

From the property damages reported in the 137 fire incidents (from section 21 of Table 3b), the total cost incurred was close to $20 million, averaging to a little more than

$142,000 property lost in each fire incident (including incidents where no damage was reported). There were 56 violations found in these incidents, most of which (54%) were G-110 violations (related to unsafe and/or unworkmanlike practices, procedures, or operations).

BSEE identifies the causes of incidents into 9 general categories: Equipment Failure, Human Error, External Damage, Slip/Trip/Fall, Weather Related, Leak, Upset H2O Treating, Overboard Drilling Fluid and Other as seen in Section 8 of Table 3a. Data collected on these cause categories from the 137 reports are shown in Figure 6.

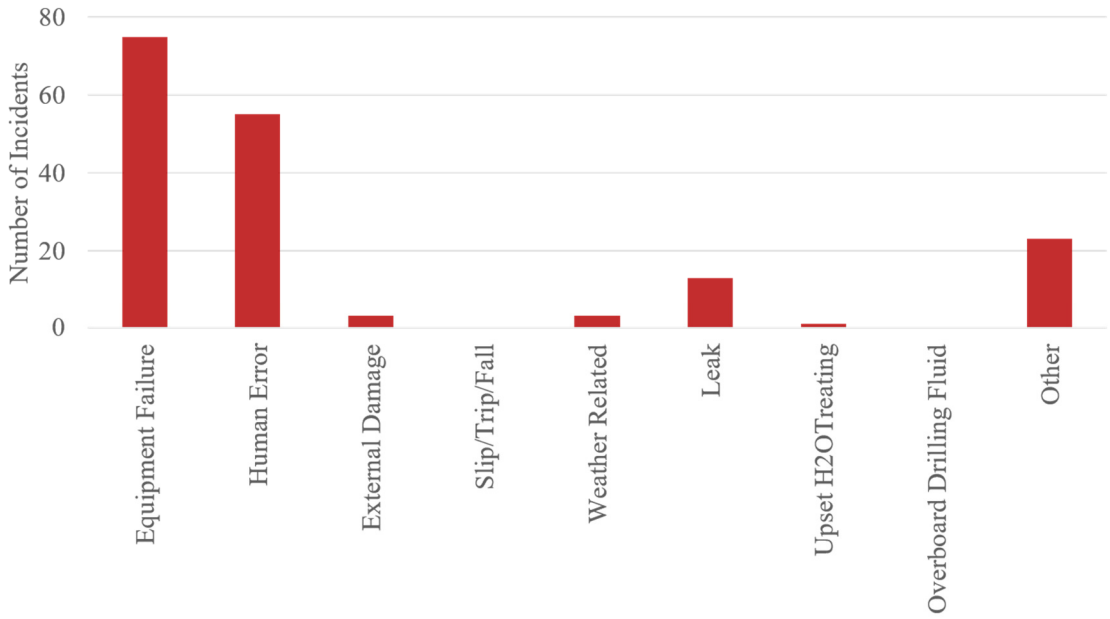


Figure 6: Figure showing the number of times each of the 9 causes were identified by BSEE in the sample 137 fire incidents (2004-2016). *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

Here, Equipment Failure (56%) and Human Error (40%) appeared to have been the leading causes behind fires in offshore facilities. This was followed by Others (17%), where the causes varied significantly.

However, the investigation findings in Table 3b, Sections 17, 18 and 19 had more information narrated than projected concisely as causes in the first page of the reports. In addition, identifying issues like leak as a cause did not seem appropriate (a leak is usually a consequence of other factors). Thus, the current work digs deeper into the incident investigation reports by analyzing the findings in Table 3b to identify the common contributing causes behind the fire incidents.

4.3. Methodology for extraction of information from incidents

For the purpose of this study, each investigation report was studied individually by the team members to identify the causes behind offshore fire incidents. The work did not follow any particular classification scheme since the intention was to be all inclusive and identify all factors that contributed without trying to make the incidents fall in predefined buckets of causes.

Prior to the analysis, attempts were taken to minimize differences in opinion among team members so that all reports were treated in the same manner. Initially several reports were studied in an attempt to identify how the analysis will be done. Team members met several times and developed a list of factors (in addition to the ones BSEE already had) that could have contributed to the incidents studied. Once a preliminary list was made, the team members randomly selected several incidents which

they discussed and reviewed together to identify the factors that influenced the incident. This ensured that all members were on the same ground and inconsistencies were minimized between different incident analysis. To ensure clarity among members, a question was developed for each factor which, if answered affirmative, would help confirm that the factor had contributed to the incident occurrence (Appendix B). Sections under Headings 17, 18 and 19 of Table 3b were studied to identify causes. Identified causes were only limited to what was mentioned in these sections and team members were not allowed to draw their own conclusions. Once all members began to agree on the analysis of individual incidents, the work was divided.

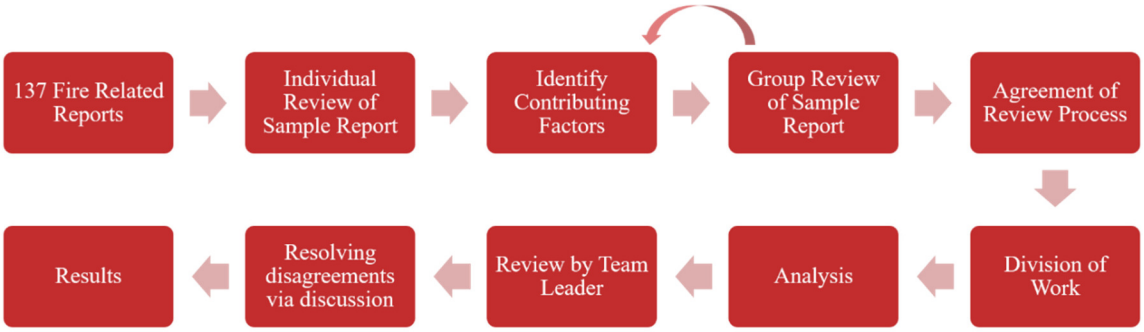


Figure 7: Figure summarizing the methodology followed in the analysis *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

A spreadsheet was developed where the factors were listed and the presence of a factor in an incident were marked as 1, absence being marked as 0. A provision was kept for adding suggestions for factors that contributed to an incident but had not been listed

in the spreadsheet. As work progressed, if these factors recurred again and again, they were added to the list in the spreadsheet, otherwise, if their occurrence was uncommon, they were kept noted under a common heading titled 'Others'. In the end, all incidents were reviewed by the team leader and discrepancies were noted, discussed and resolved. Midway through the work, the work was presented to subject matter experts and their feedback and comments were incorporated in this work.

It is to be noted that the methodology applied analyzed the contributing factors that led to the fire incidents from the reports and does not/may not reflect the root causes behind the incidents. Also, many of the investigations included accounts of actions/occurrences that took place once the fire had already initiated and allowed keeping a minor fire from becoming a major one. There actions/occurrences were considered as consequences and these post-fire activities have not been included in the current analysis.

4.4. Analysis of offshore incident investigation reports and identification of contributing factors

Current analysis found 26 contributing factors apart from the 9 causes already identified by BSEE. Appendix B shows a list of terms that were used for each contributing factor and provides a definition for each that were identified (in addition to the list of causes in BSEE's reports) along with their definitions. The last five terms in the list (marked with *) were found to be consequences of fire and hence has not been included in the present analysis.

Figure 8 shows the number of times each contributing factor was identified in the analysis of the 137 incidents. Each incident involved multiple contributing factors. Equipment failure and human error, which had been identified as top causes in the 137 reports, appeared to have been influenced by other factors. The study thus analyzed the other contributing factors that appeared in conjunction with equipment failure and human error to get an insight of the causes behind the fires.

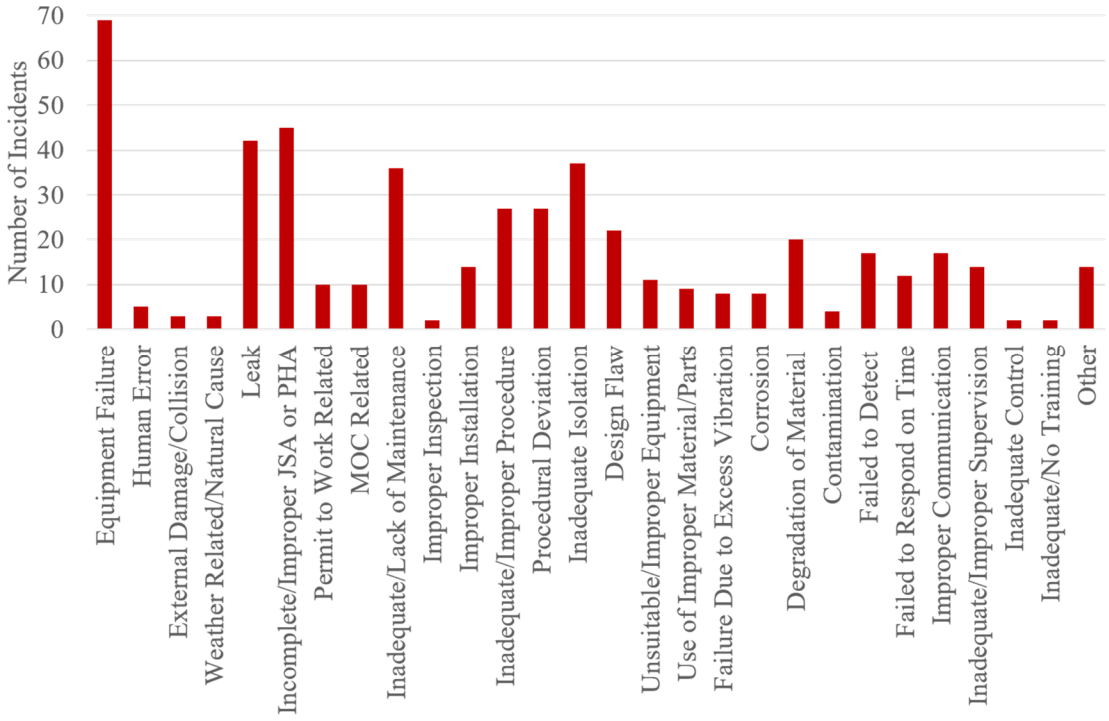


Figure 8: Figure showing factors that were identified in the analysis of 137 offshore fire incidents' investigation reports. Factors that were considered but did not appear in the investigation reports are not shown here. (JSA refers to Job Safety Analysis, PHA refers to Process Hazard Analysis and MOC refers to Management of Change) *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

4.4.1. Equipment Failure

Of the 77 incidents that BSEE marked as being caused by equipment failure, there were several where BSEE had identified fires initiating from leaks in pipes/hoses connected to a tank as equipment failure. However, according to the working teams' understanding, these were taken as leak incidents rather than equipment failures. Also, it was found that use of wrong size of parts of equipment that had led to failure, leak and fire had been identified as equipment failure in some cases, but were not in others. Similarly, some incidents involving equipment failure were marked as being 'other' causes with different causes or equipment name written next to it. Such inconsistencies in reporting contributed to the differences between the BSEE identified equipment failures (77) and the team's analysis (68).

The analysis of the 68 incidents where equipment failures were identified is shown in Figure 9 along with other important factors that seemed to have contributed to the failures. These appeared mostly to reflect laggings in measures which could have prevented the failures and hence can be seen as deeper causes behind a single surface cause.

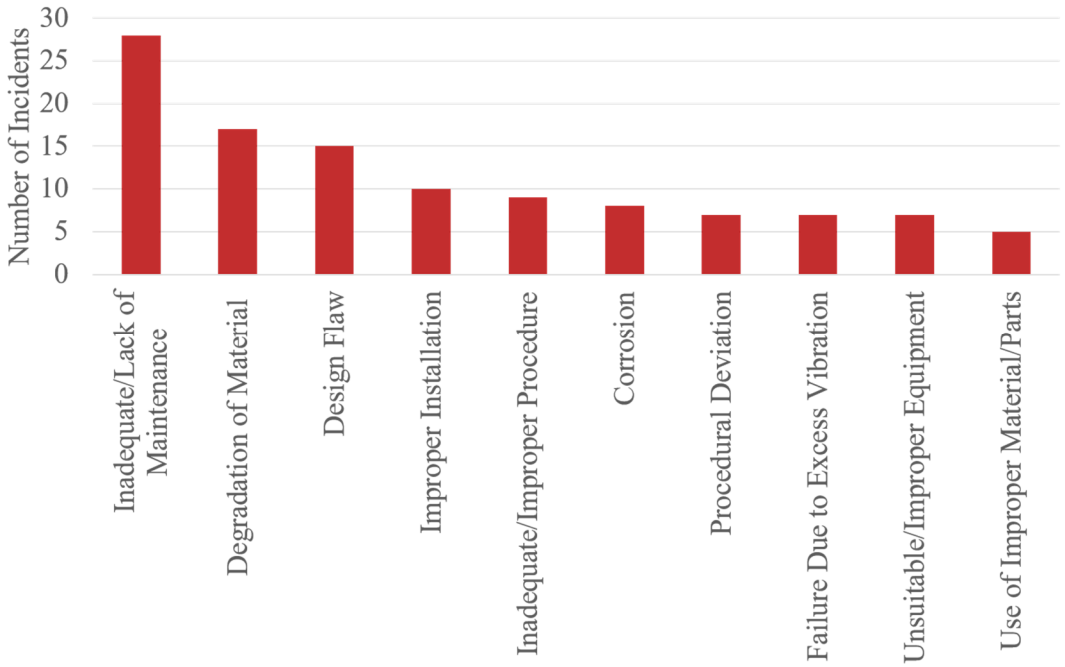


Figure 9: Figure showing factors that appeared in conjunction with "Equipment Failure" incidents identified in the analysis. *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

Much of the equipment failure can be attributed to maintenance (41%) which was inadequate or not done properly. Thus, maintenance program is important to prevent equipment failures leading to fires. Another important factor was degradation of parts (25%) or whole equipment either due to excess heat, abrasion, vibration or corrosion. Why these occurred may be contributed to factors such as design flaw (22%), improper installation (14%), use of equipment/parts (10%) or material (7%) not suited for the function or due to lack of maintenance itself. It is interesting how procedure impacted the equipment failure (inadequate procedure 13% and procedural deviation 10%). In

most incidents where these two (equipment failure and procedure) were common, an improper or inadequate way of conducting a task had initiated an equipment failure that eventually led to the fire. This shows that procedure-related issues are playing an important role behind failure of equipment. The investigation reports did not provide further information that would have allowed to find the deeper causes as to why these factors surfaced.

4.4.2. Human Error

There was a significant difference between the number of incidents with human error identified by BSEE (55) and the numbers identified in our analysis (5). This difference can be attributed to the fact that the analysis team believed strongly that what had been taken as human error were actually actions that were influenced by other factors in the system and hence should not blame an individual in that context. As Sidney Dekker mentions, the point of investigation is not to find where people went wrong, it is to understand why their assessment and actions seemed right at the time [129]. Through the analysis of the 55 human-error related incidents that BSEE identified, it was found that there were multiple factors in almost every incident that could have influenced the human performance and hence cause error. In other cases, there were limitations in measures that led to unwanted deviations, which were then blamed on the human operator.

From Figure 10, it can be seen that incidents where human error was identified had arisen largely from a lack of proper Job Safety Analysis (JSA)/ Process Hazard

Analysis (PHA) (56%). Although the larger portion of these incidents were related to improper JSAs, in overall, it shows that there was an incomplete realization of hazards associated with a task or process. Incidents related to Permit to Work were also mostly due to this lack of realization of hazards (15%). Although it may be criticized that this lack of realization was an error on part of the human, the large number of incomplete/improper Job Safety Analysis (JSA) conducted should raise one question: why are the JSAs failing? A look at factors behind faulty JSAs should identify causes of human error. Incident reports should not stop only at 'human error' but look beyond.

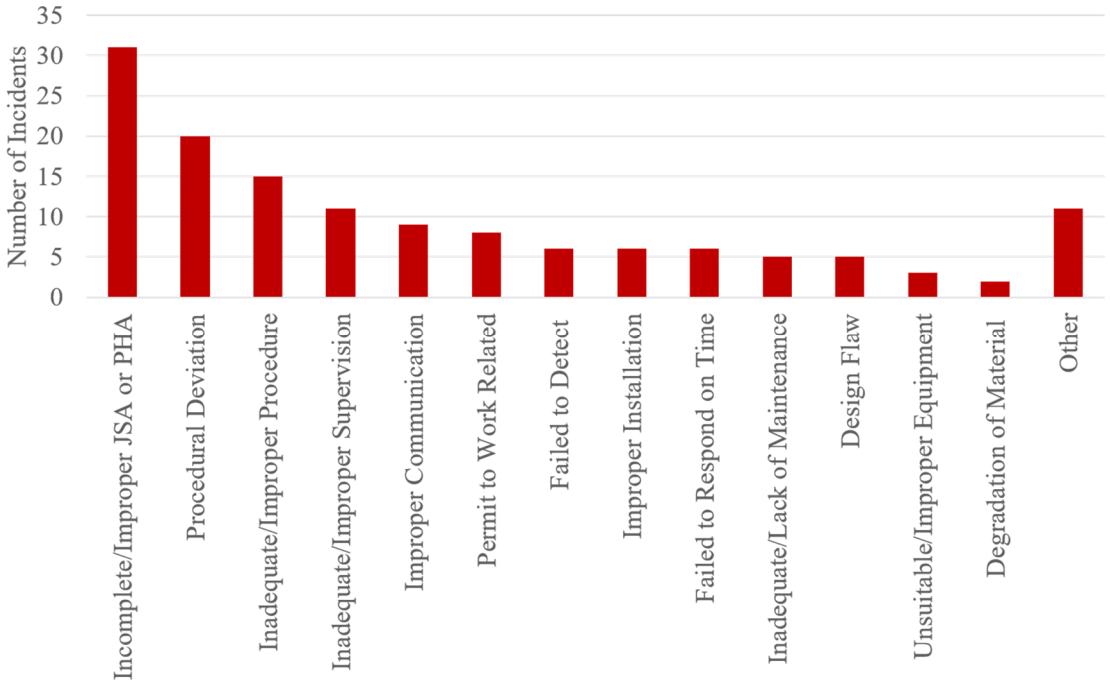


Figure 10: Figure showing factors that appeared in conjunction with "Human Error" identified by BSEE *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

The second and third largest factors are both related to procedure (36% Procedural Deviation and 27% Inadequate Procedure). Upon analysis of incidents where procedure-issues appeared, it was found that deviation or failure to adhere to procedures occurred due to problems such as inadequacy of the procedure itself, ergonomic issues and operator busy doing other work and thus failing to pay full attention (multi-tasking). There were many investigations that stopped at reporting that the procedure was violated, but did not ask further, such as asking the person why he had deviated. This would have revealed some important information about the causes that led to human error.

In 20% of these cases, a supervisor had not been present during the job or had not provided proper guidance. In one incident, a supervisor had left the facility in a helicopter while the work he was supervising was still ongoing. Such factors should be looked from an organizational behavior perspective and one needs to ask: why did he leave, or why was he allowed to leave? For incidents where supervisors had misguided his subordinates, leading them to making errors in a task, it should be asked if the supervisor was informed and competent enough to lead the task. Blaming his/her subordinates for human error does not capture the whole picture, neither does blaming the individual supervisor as making human error help identify causes behind incidents. Improper communication showed up in 16% of incidents where BSEE had identified human error as a cause. If an operator is not made aware of the hazards through proper communication, his actions can lead to unwanted deviations. In this analysis, communication also included providing sufficient warning signs and providing proper

identification of hazardous materials. In one case where a crane operator had rigged up a gas line instead of an air pipeline, it was found that the pipelines were not properly labelled. The contract crane operator would not have known he was rigging up a wrong pipe unless it was properly communicated to him. Similar incidents were found where the welder was not informed about hazards associated with presence of fuel gas in the vicinity of his work.

'Failed to detect' (11%) occurred usually due to cases where an adequate sensor was not present or where the JSA was improper and the presence of flammable material were not checked, rendering a false blame on the human for error.

Incidents where operators had 'failure to respond on time/delayed response' (11%) had been identified as human error, but analysis shows that these failures arose from issues such as operator not being able to reach/find the proper valve/button on time, or operator multi-tasking; the previous one being related to ergonomics and the latter one being organizational safety culture issue.

Factors 'inadequate/lack of maintenance', 'degradation of materials' and 'improper inspection' appeared several times in conjunction with human errors, though in much less numbers than those discussed previously. One incident involved inadequate tightening of a bolt that led to a leak of flammable fuel. Although at first look it appeared as human error, questions about proper procedure, inspection, fool-proofing a system arose. Lack of proper maintenance, inspection and their backlog should be tackled from a management level as should ensuring that systems are kept fool-proof and

operators are given proper procedures. Similarly, as can be seen, incidents where design flaw had led to fire, human error has been blamed.

The term ‘other’ factors appeared significantly with ‘human error’ but the individual factors under ‘other’ are different from each other. Even then, it needs to be mentioned that some of the factors included not utilizing stop work authority (SWA) when it was needed, smoking in non-designated areas, leaving workstation unattended when needed *etc*. These factors usually reflect the safety culture of the organization and the subsequent behavior of the agents in this organization. Blaming an individual for such actions will not help eliminate the cause.

Analysis of BSEE identified human error appeared mostly related to organizational laggings that were not tackled on time. As Sydney Dekker mentioned: “Underneath every simple, obvious story about ‘human error,’ there is a deeper, more complex story.” [129].

4.4.3. Other significant findings

In the analysis, it was found that the most common equipment where fire initiated were compressors, which related in 18% of the incidents. Pipelines and hoses conducting hydrocarbons appeared next in 16%, and generators and engines followed in 15% of the incidents. Compressors and pipes usually provided the fuel source whereas engines and generators were the most common ignition sources, their hot surfaces providing energy for initiation of the fires. Energy due to hot work was the next common ignition source.

Almost 33% of the fire incidents occurred during maintenance work, suggesting more precautions being required during this time. 24% of all incidents involved hot work. Although it is understandable that performing hot work which provides high heat/energy in a flammable area of the facility is more prone to fires, Figure 11 indicates that inadequate measures usually caused these incidents.

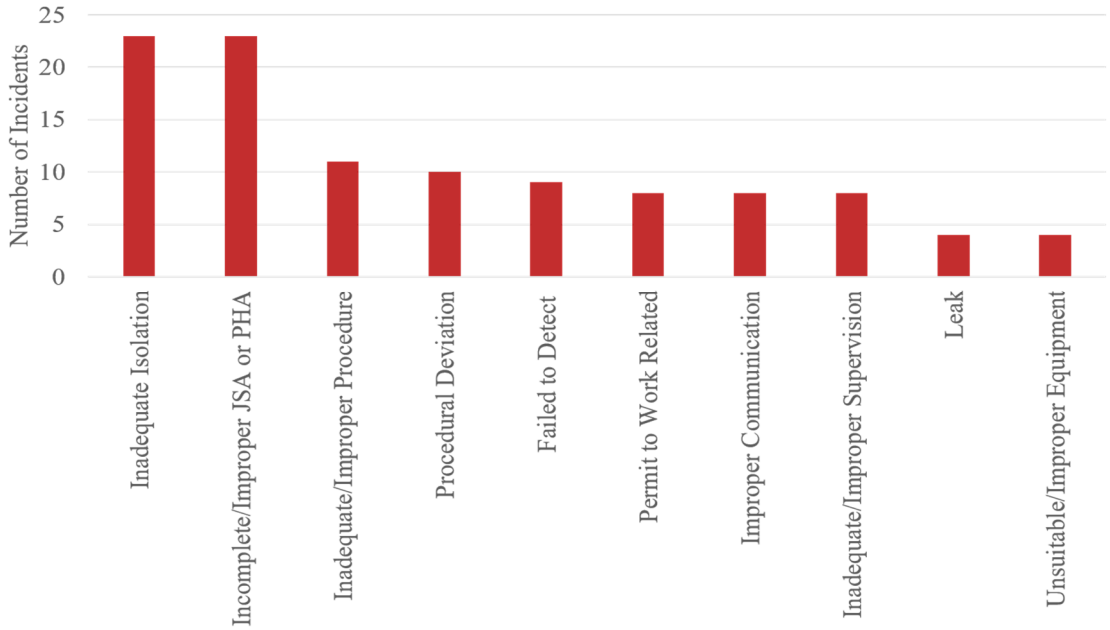


Figure 11: Figure showing the most common factors that appeared in incidents related to Hot Work. *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

70% of all hot-work related incidents lacked proper isolation, which led to the fire. These incidents either involved a loss of containment of flammables or slags or embers that caused the fire. Lack of proper understanding of hazards reflected via

improper JSA led to fire in 70% of cases and mostly influenced why proper barriers were not placed to ensure isolation. Inadequate procedure was found in 33% and procedural deviation were found in 30% of cases where hot-work was involved, indicating the influence of procedure in hot-work related fires. Many of the incidents involved welders deviating from the procedure determined during the JSA because the procedure appeared inconvenient at that time. In such cases, the proper method would have been to stop work and reevaluate the process. Proper guidance or supervision would also have prevented further progression of work when the appropriate procedure was being deviated from. However, almost none of the investigation reports mentioned how lack of such measures could have contributed to the incident. Hence, issues such as improper communication and improper supervision appear in smaller numbers (both 24%) in Figure 11. The graph also reflects how failure to detect flammables had led to fire (27%). Use of unsuitable equipment and the fact that procedures did not include proper guidance to 'smell' for flammables contributed to this factor too. Thus, when there had been leaks, the undetected flammables along with the heat of hot-work led to the fire incidents.

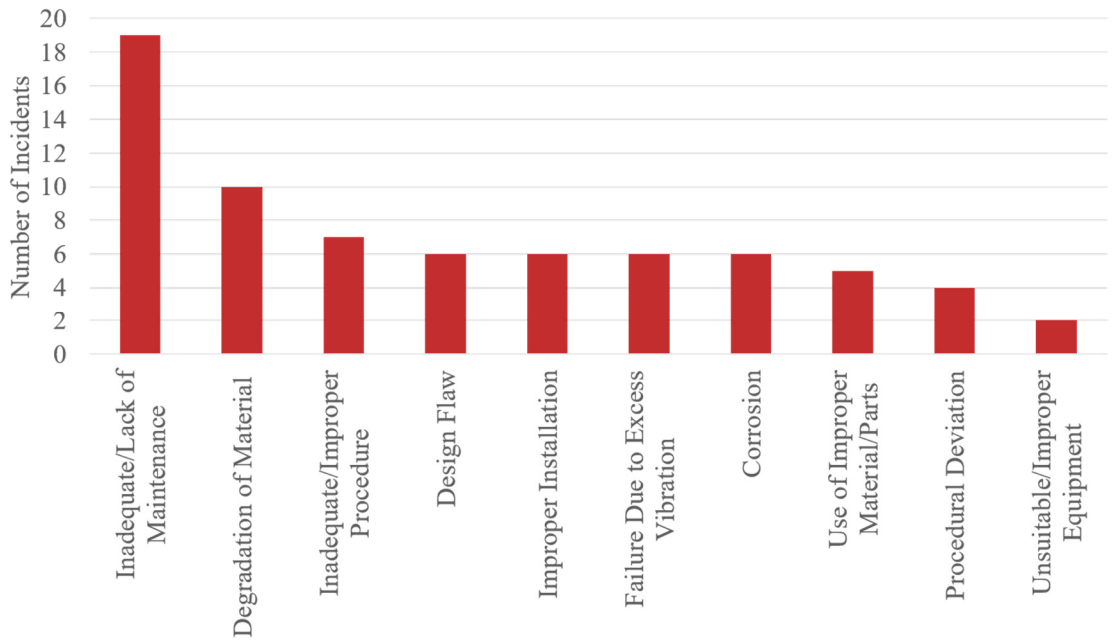


Figure 12: Figure showing the different factors that appeared in conjunction with leaks. *Reprinted with permission from "In search of causes behind offshore incidents: Fire in offshore oil and gas facilities" by S.Z. Halim, S. Janardanan, T. Flechas, and M.S. Mannan, 2018. Journal of Loss Prevention in the Process Industries, 54, 254-265, Copyright [2018] by Elsevier.

Figure 12 shows factors that appeared in conjunction with leaks found in the analysis. BSEE had identified leak as cause of fire in 11 of the 137 incidents. Our analysis found 42 such incidents. This was mostly because some incidents that involved leak as well as equipment failure were marked on the reports as having only equipment failure in section 8 of table 3a. As can be seen, inadequate/lack of maintenance (45%) and degradation of material (24%) play the most influencing factors similar to the analysis of equipment failure. Also, in a similar fashion, procedures occur as an important factor, appearing in 26% of incidents with leaks.

4.4.4. Limitations to the analysis

At this point, it is essential to mention the sources of error and limitations in the final outcome of the analysis. The three main sources of error in the analysis can arise from the following [4]:

1. Errors of Non-observation: Not all incidents reported to BSEE were investigated, and not all investigations were available in the BSEE website for public access. Only available District Investigation Reports were analyzed. Hence, the result of the analysis is limited only to these investigations. Even then, analysis of 137 fire incidents is a fairly large number.
2. Errors of Observation: As the reports were analyzed, it was observed that the quality of the reports varied from one to the other. Some reports were very elaborate, others were not. Also, identification of the probable and contributing causes for similar incidents also varied. This may have been due to investigations being conducted by different team with different set of minds, or due to the difference in their approach or may depend on the amount of information they had been able to gather from the operators. Hence, the analysis is only as in-depth as BSEE's investigation findings.
3. Errors of Processing: In order to avoid inconsistencies that may arise in analysis of investigation reports by different team members, the methodology discussed in Section 4.3 was adapted. In the end, the analysis was limited only to the information that was made available through the reports and the information that

was obtained from the analysis is only as in depth as the investigation findings allowed.

4.5. Summary

It can be seen from the analysis provided in this paper that the 9 categories of causes identified by BSEE are quite broad and do not aid in an in-depth analysis about what led to an incident or where focus should be given to develop measures to prevent future ones from occurring. Although it is quite easy to state that an equipment failure, leak or a human error led to a fire, the numerous factors that contributed to equipment failure or led the human to err will remain unidentified and misunderstood if not properly analyzed. However, the investigation reports provided by BSEE, though not detailed enough to identify root causes, does provide an outline of common contributing factors that led to mishaps. These causes are rather concealed or out of sight, but surface over and over again. Such factors that recurred a greater number of times include: inadequate JSA/PHA (33%), inadequate isolation (27%), inadequate maintenance (26%), improper/inadequate procedure (20%), procedural deviation (20%). Others such as design flaw (16%), degradation of material (15%), failure to detect (12%), improper communication (12%), improper installation (10%) and inadequate supervision (10%) occurred less frequently.

Job safety analysis: In many cases, human (operator or supervisor) has been blamed for not conducting a proper JSA. However, questions as to what was lagging in the JSA or why a hazard was not identified (even though similar incidents seemed to

occur over and over again) needs to be queried. The large percentage of incidents with inadequate JSAs raises one question: why are JSAs failing so much? Companies need to re-evaluate how they are doing their hazard analysis and how JSAs are being conducted during frontline operation to find a solution to the question.

Procedure: Almost twenty percent of incidents had occurred due to inadequate procedures and an equal percentage due to deviation from an outlined one. Together, procedures contribute the most behind offshore incidents. In 5% of incidents, both had occurred, explaining that operators had deviated because they had realized the problem with the procedure, but had taken a wrong action to correct it. What the reports do not answer precisely is why operators deviated in the remaining 15% incidents. From the analysis of reports, in some cases it appeared that either the procedure had failed to mention the required action for a particular situation, or that the procedure outlined was simply not convenient at the time. In most cases however, the reports lack explanation about this. At times, it appeared that many of the operators were not well supervised, or the related hazards of their task were not communicated well enough. In a smaller number of cases of procedural deviations, sudden mistakes in operation had appeared. However, it should be realized that human error will occur and hence there is a need to design systems that are not error-prone. Multiple barriers can help in this regard. One incident for example involved operator opening a wrong valve that led to a fire. There were other mitigative measures in place to prevent accidental release of flammables, but all of them had been turned off removing the “fool-proof” aspect of the system.

Investigation should find what caused the human to err, or why a system failed instead of blaming anyone.

Inadequate isolation: This mostly occurred during hot work (62%) and in conjunction with inadequate hazard identification (62%) and procedure related issues (46%). However, in 38% of the incidents with inadequate isolation, human error has been identified by BSEE as the cause of fire incident.

Inadequate/Lack of maintenance: The effect of lack of maintenance are profound when it comes to equipment failure and leaks. Further analysis as to why there was inadequate maintenance, or a backlog could not be identified. Although the investigation findings allowed us to find contributing factors behind the surface causes, the analysis team agreed that in most reports, further questions and queries would have enabled finding the deeper causes behind the incidents. For example, many incidents where degradation of material led to fire, the reports do not state why the material degraded in the first place. Was there a lack of inspection or maintenance, was there a use of improper material of construction, or something else? Many reports indicate degradation due to excess heat, others just state that the material developed a leak without recognizing the deeper cause.

Blaming human (as an individual) for the shortcomings in maintenance, isolation, procedure or JSA does not solve the problem. The analysis team did not agree with many cases where BSEE had identified "Human Error" as the cause. For instance, maintenance work remaining in backlog and thus leading to wires arcing and igniting a fire should not be blamed on an individual, but the whole inspection and maintenance

system of the organization. Also, further analysis as to why an individual failed to perform a task as required or why he/she deviated needs to be conducted. Most reports tagging human error as causes of fire showed problems with JSA, procedure, supervision and communication to be the leading contributing factors that affected the human performance. Investigations should have probed more into the matter by asking questions such as “what was the problem with the JSA, or procedure”, “why was there a problem of communication” and henceforth.

Even with the limitations mentioned above, it is clear that causes behind offshore incidents mostly involve lack of proper hazard analysis, laggings in procedure, and lack of steps to eliminate human error. Fire incidents have deeper roots than reported and only proper investigations can bring forth the proper mitigative measures required. If an organization investigates all incidents (and near misses) and implements the learnings over time, then it is possible to significantly reduce future incidents and ensure safer operation. Capturing the learning via implementation is crucial but prior to that, a proper investigation to understand what went wrong must be conducted. As the study finds, terms such as human error, equipment failure *etc.* may indicate superficial causes for an incident, but the underlying factors need to be addressed to take adequate measures to prevent incidents.

The work also shows how information from various investigations can be utilized to understand the safety culture or safety awareness of the industry in general. If similar approach is used to investigate major, minor as well as near miss incidents for a particular company, then the laggings in that organization will also be found and can

thus be eliminated. In that context, a proper investigation method should be developed. As seen mentioned before, many of the investigation reports were not detailed, and the analysis team felt that many questions had remained unanswered. A proper investigation methodology, that is easy to use, yet effective to find the root causes and a reporting system that will provide information for a larger scale analysis like the one presented here will be the next step to implementing learnings from failure.

5. QUANTIFICATION OF CONTRIBUTING FACTORS TO DETERMINE GENERIC AND PLANT SPECIFIC FAILURE DATA

5.1. Background

The failure trend of a component is assessed by using the following information: a. the past performance data of the specific component, b. performance data of similar components in similar installations or, c. engineering knowledge of design and construction of the component [130].

For any equipment, in the absence of information a, information b and c can be obtained from manufacturer specifications or from generic data (failure data of a specific component accumulated from various facilities and averaged) and used for failure. As the equipment operates, its performance data (a) can then be used to update the information from b and c to provide plant-specific and current data.

Generic reliability data for offshore equipment failure are readily available in multiple data sources such as the OREDA database, WellMaster RMS or the PDS Handbook [131-133]. Data are provided with variance to incorporate the uncertainties in their estimation. Methodologies exist for collection of data from similar facilities to develop generic failure trends of equipment [97, 102].

Although a lot of work has been published in this field, almost all such work encompasses only technical factors, *i.e*. they are concerned with equipment reliability. The remaining are focused on estimating human error, whereby an operator's task completion probabilities are estimated [134]. Methods for regular updating of non-

technical factors are almost non-existent. Audits and expert opinions are used most frequently for incorporating the effect of organization on failure of a system. Generic data that reflect the frequency of occurrence of contributing factors leading to an incident are missing.

In order to merge technical and non-technical factors, both need to be expressed in similar terms of failure tendencies. In here, we develop a method similar to equipment reliability to represent non-technical factors. These can be seen as components of organizational reliability.

In this chapter, a frequently used method based on Hierarchical Bayesian inference for updating equipment failure rates (and hence failure probabilities) by combining generic and past performance data of equipment with current data is shown. Next, a methodology for quantification of failure occurrences of non-technical factors is provided. A method for estimation of generic data and for updating the generic data using plant-specific data for the non-technical factors is proposed. Assumptions for the methodology are also provided.

Before discussing the mathematical formulation for determining the failure rates, a general background about counting processes is discussed. These processes help determine the failure tendencies of a system by using information about the failures and failure times.

5.1.1. Homogenous Poisson Process vs. Renewal vs. Non-homogenous Poisson Process

Taking the failure process as being failure points located randomly in the time space, the Poisson processes can be used to define the failure of a component/factor. The three common types of counting processes are

- Homogenous Poisson processes (HPP)
- Renewal processes (RP)
- Nonhomogenous Poisson processes (NHPP)

An HPP is a regular counting process with independent and stationary increments. A point process is said to have independent increments if the number of failures or events in mutually exclusive time intervals are independent random variables and is said to be stationary if the distribution of the number of events in any time interval depends only on the length of the time interval only and not on the distance of the interval from the origin [110, 111]. The cumulative intensity function W(t) is the expected number of failures N(t) observed in the time interval (0, t] and its derivative is w(t), the rate of occurrence of failure (ROCOF).

For an HPP, ROCOF is a constant (λ) which is independent of time. The number of failures is Poisson distributed with the mean and is expressed as:

$\Pr(N(t_2)-N(t_1)=n) = \frac{[\lambda(t_2-t_1)]^n}{n!} e^{-\lambda(t_2-t_1)}$ for all $t_2 > t_1 > 0$

The interarrival times between failures are independent and identically distributed exponential random variables [110]. The arrival of the r^{th} failure has a Gamma distribution with the probability density function:

$f(t)=\frac{(\lambda t)^{r-1}}{(r-1)!}\lambda e^{-\lambda t}$

The HPP is generally applicable for systems where components are not repaired or where they are replaced with another one.

In a RP the components are put into function at time t=0 and are renewed or repaired to 'as good as new' condition upon failure [110]. When the renewal period is identical to the life length of components, the renewal density is identical to λ and RP provides a generalization of the HPP. The times between failures (interarrival times) are independently and identically distributed.

An HPP is generalized by assuming that the intensity of the failure process is a function of time. This is a NHPP where the repair reverts the system to 'as same as old' condition. The expected number of failures or the cumulative intensity function is given as:

$W(t)=\int_0^t w(u)du$

In NHPP, the failures do not require stationary increments, that is, failures are more likely to occur at certain times than others and the time between failures are generally neither independently nor identically distributed [110]. The ROCOF varies with time. NHPP can model ageing of a system reflecting its improvement or deterioration of the system through decreasing or increasing ROCOF respectively. Following repair, the system's reliability is assumed to remain the same as it was right before it failed. For a large and complex system, if only a small part of it is replaced or repaired, the system's reliability remains the same as before failure and the assumption of minimal repair of the NHPP becomes valid. For the NHPP, one has to construct a

likelihood function based on the fact that each failure time after the first is dependent on the preceding failure time [68].

5.2. Adopted mathematical formulation for estimation of failure rates of equipment

Methodologies for estimation and updating equipment failure rates using plant-specific data are abundant in literature and here we adopt a methodology that uses the Bayes theorem for reliability calculations [110, 111, 135].

Generic failure rates of equipment are readily available, as mentioned before. It is important to recognize that equipment failure rates change with time due to various issues ranging from environmental factors to organizational factors. For example, equipment used in offshore marine environment are more susceptible to failure arising from corrosion than those in dry non-corrosive environment. The maintenance program in one facility may vary significantly from that in another facility. Subsequently, the failure rate of a system kept under negligence due to a maintenance backlog is more prone to failure with time than one that is regularly maintained properly.

Equipment/technical failures are usually modelled as following an HPP. Although the exponential distribution finds the widest application in equipment reliability (or failure probability) estimation due to its simplicity, the memoryless property of the distribution mean that it cannot capture the aging nature of an equipment [110]. Many suggest using Bayes theorem to update the failure rates by assuming the uncertainty to be modelled by Gamma distribution with parameters α and γ. Prior knowledge of failure rates are taken from OREDA database [131] and plant failure data

provide the likelihood to determine the posterior failure rates in the following way, adopted from Hauge[135]:

Equation 1 $\boldsymbol{\gamma = \frac{\lambda_0}{(\lambda_0^* - \lambda_0)^2}}$

and,

Equation 2 $\boldsymbol{\alpha = \gamma \times \lambda_0}$

where, λ_0 = prior failure rate of equipment obtained from database, and λ^*_0= Either of the three following alternatives:

i. An analyst specifies a particular value based on his knowledge of the process and/or other source of data.

ii. In case an analyst cannot make such estimate, the OREDA database is used to make a conservative estimate by taking $\lambda^*_0 = 2 \times \lambda_0$ since the standard deviation of many failure rates are found to be twice that of the mean failure rate [131].

iii. In either of the two estimates, the conservative estimate should not exceed 5×10^{-7} failures/hour. This value has been adopted for practical reasons.

Then, if the recorded number of failures is x over an aggregated time t in service, then the posterior failure rate is estimated as:

Equation 3 $\boldsymbol{\lambda_1 = \frac{\alpha + x}{\gamma + t}}$

5.2.1. Example problem

Suppose an automatic fire detection system, consists of installed detectors throughout the operational area of a facility. According to the OREDA database, the failure rate is given as follows [131]:

Fail to function on demand = λ_0= 0.97×10^{-6} /hr

Suppose plant records indicate that in between inspections, it was noted that 3 detectors had failed (x) over a period of 6 months (t). Then according to equation (1) and (2), assuming that all detectors failed at the end of 6 months service:

$$\gamma = \frac{0.97\times10^{-6}}{\left((2*0.97\times10^{-6})-0.97\times10^{-6}\right)^2} = 1030927$$

$$\alpha = 1030927 \times 0.97 \times 10^{-6}=1$$

$$\lambda_1 = \frac{1+3}{1030927+(6\times30\times24\times3)}=0.0000038=3.8\times10^{-6}/\text{hr}$$

The result above indicates that the having 3 detector failures every 6 months is worse than the industry average as indicated by the OREDA database.

If, in between each updating, failure rates are assumed to remain constant, then the probability of failure of a detector with time is given by:

Pr(Detector failure)= $1-e^{-\lambda t}$

Figure 13 shows how updating of failure rate causes a significant change in probability of failure estimation as time passes by.

Failure rates of other equipment can be updated in a similar manner. Failure information of equipment can also be extracted from maintenance database, inspection database, audits and other sources or data historian. Thus, updating failure rates should not be strictly restricted only to near misses and incident, but also other databases.

As shown in Figure 13, the probability of failure, based on plant data, could be far more than that estimated when a constant industry average value is used throughout

the life of the plant. Thus, it is essential to update failure rates for a more dynamic risk assessment.

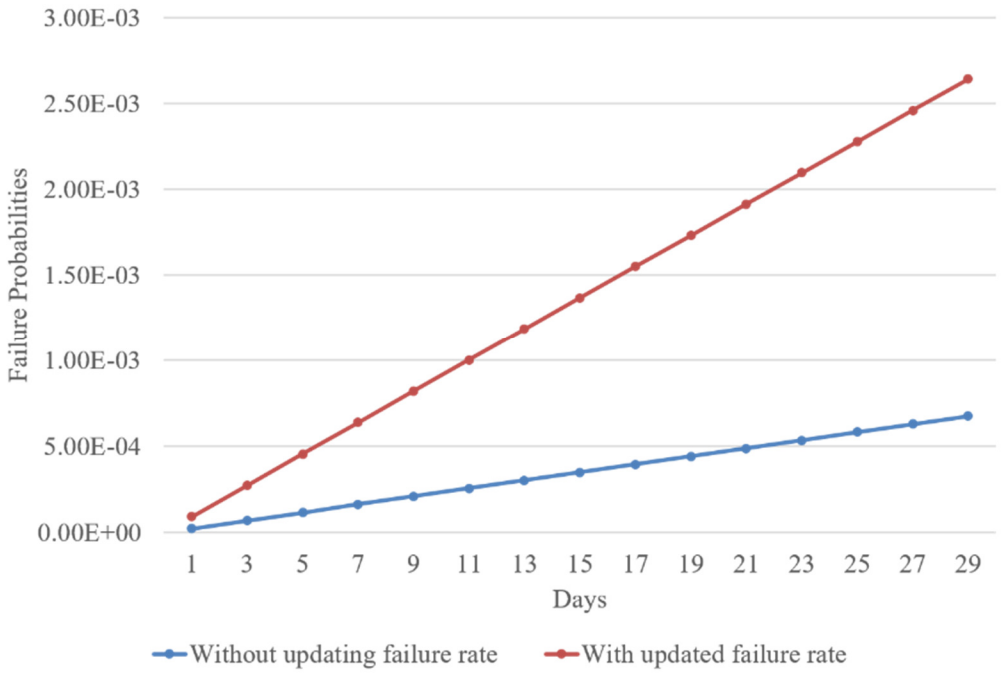


Figure 13: Graph shows how updating failure rates can vary our understanding of the probability of failure of an equipment

5.3. Proposed mathematical formulation for quantified estimation and updating of failure time of non-technical factors

As a first step to merging non-technical factors with technical ones, it is essential to express failure of non-technical factors in reliability terms like equipment failure. In other words, express organizational or operational failures in terms of number of failures in a given time. For determination of failure rates of non-technical factors, we opt for a

methodology similar to that mentioned for technical factor/equipment reliability. Since this methodology development is the novelty of this thesis, detailed explanation for the method is provided.

5.3.1. Data format for quantifying contributing/non-technical factors

In order to keep a dynamic aspect to risk assessment, time is a crucial factor and thus, failures are observed over a given time. In the analysis provided in Chapter 4, the date of each incident was noted along with the specification of the facility in which the incident occurred. A sample screenshot is shown in Figure 14.

	Date Occurred	Incomplete/Improper ISA or PHA	Inadequate Isolation	Inadequate/Lack of Maintenance	Inadequate/Improper Procedure	Procedural Deviation	Design Flaw	Degradation of Material	Failed to Detect	Improper Communication	Improper Installation	Inadequate/Improper Supervision	Failed to Respond on Time	Unsuitable/Improper Equipment
1	12/23/2016													
2	12/10/2016						1							
3	7/22/2016	1				1								
4	4/13/2016						1		1					
5	3/12/2016		1				1					1	1	
6	2/13/2016		1	1									1	
7	12/13/2015													

Figure 14: A screenshot of the spreadsheet used for analysis in Chapter 4, showing recorded occurrence time of some contributing factors over a period of time

The dataset consisted of the exact date and time of occurrence of a fire scenario. Through this, the amount of time elapsed between each appearance of a particular contributing factor (say, procedural deviation), was available. This can be viewed in a manner similar to reliability calculations performed for various equipment where the interarrival times are known and the reliability of the equipment can be measured henceforth. Such information will enable us to determine the reliability of both technical and non-technical factors contributing to the risk of fire in an offshore facility.

Before we proceed to quantification of non-technical factors using this data, we mention a few assumptions that needs to be made.

5.3.2. Assumptions for quantification

The novelty of this dissertation lies in developing a procedure for quantifying reliability of non-technical factors using time between failure of various contributing factors identified from the study of fire incident reports generated by BSEE for offshore facilities in the US OCS. For developing mathematical formulation for generation of generic data and for updating it, the following assumptions are made applicable to these factors:

1. Laggings or failure of non-technical factors can exist without occurrence of an incident. Only at random times do these failures show-up as 'critical' and lead to an incident. The term 'critical' for an individual contributing factor will be used henceforth to refer to the particular factor's subset of occurrence time when that factor contributed to an incident. For example, procedural deviation has been

found as a commonly occurring contributing factor behind fire incidents. This assumption states that procedural deviation may occur more frequently than the observed incidents but it does not always contribute to an incident. Only when procedural deviation is 'critical' do we get an incident (such as a fire). In this study, such 'critical' events have led to the incidents and these are termed as the 'failure' of that factor.

2. The number of failures N(t) is taken as a random variable in the time interval (0, t]. All failures are taken as random stochastic events. A stochastic process is used to define a mathematical model of a system that behaves in a random non-predictable manner and when the number of failures N(t) is observed over a time interval [0,t] it is also called a counting process [110, 111]. The contributing factors identified in Chapter 4 can be taken as failures of those factors.
3. The occurrence of 'critical' non-technical failures may vary over time. For example, at times of budget cut or a slump in the economy there can be a loss of competent workforce, inadequate training, or understaffing within an organization, all of which can have an influence on the overall system, and contribute to an incident. Number of occurrences can be more in certain times than in others.
4. Organizations can be taken as repairable systems and all contributing factors or non-technical factors influencing an incident can be taken to be repairable. That is to say that any issue that leads to an incident could have been repaired prior to its failure, had adequate measures been taken on time.

5. Once a factor has occurred/failed, the time to repair to a functioning state are taken as negligible. This allows us to treat the failure counting process as point process. This assumption is valid when repair times are short compared to operational time or when we are concerned only with operational times and repair times are modelled separately [68]. From a realistic point of view, in most cases companies/ organizations will continue operation following any occurrence of non-technical failures even if it leads to near misses or minor incidents. Only in rare cases will there be a major incident that will require complete shutdown and reorganization. Recommendations made following an incident usually takes some time to implement, but the organization continues its operation in the meantime. Changes made to organization will be reflected by changes in the occurrence rate of critical failures and thus will be incorporated whenever the model is updated.
6. The data available to us comes from the overall US OCS, with reported fire incidents from various facilities. This data can be taken to represent a sample of a larger population of incidents and near misses that are not required to be reported or are not included in the study.
7. The reliability of the contributing factors that have been developed here forth in this study can be taken as being generated under the same conditions. This assumption makes sense given that the regulatory policies and other external factors that each facility is exposed to are all similar to a certain extent. They

differ by conduct of operations and the operational discipline outlined by individual company's policy and also by the design and operation of the facility.

As mentioned before, ROCOF of non-technical factors are expected to vary with time and hence, the assumption that they follow the HPP is not applicable. A perfect repair assumption is also not valid for technical factors since an organization cannot revert to a new condition whenever there is a failure of a contributing factor. Thus, the RP is not applicable for such factors.

NHPP is applicable for modeling non-technical factors because it allows modeling of 'same-as-old' repair which are more applicable for organizations than a 'good-as-new' assumption. The best option would be to select a repair situation that is in between same-as-old and 'good-as-new' or an imperfect repair that leaves the system in a condition worse than old, but such models are still not well developed and require determination of the extent of repair which is quite impossible to measure for non-technical factors. Also, as mentioned in Chapter 4, the identified contributing factors are generally not the root causes behind the incidents. Such factors usually have contribution from multiple other issues that lead to its failure. For example, procedural deviation can have contributions from operator's stress level, inadequate procedure, lack of training, inadequate supervision and so on. Similarly, an incident also occurs by contribution of multiple factors. When multiple issues contribute to a failure, then the assumption of repair as good as old is more appropriate. Thus, the assumption of a NHPP for failure is valid for components of complex systems like organizations and its components.

5.3.3. Methodology for quantification of non-technical factors following a NHPP

5.3.3.1. The Power Law (for modeling non-technical factors)

The ROCOF (rate of occurrence of failure) of a NHPP (nonhomogenous Poisson process) has been described in literature by several parametric models [69, 110, 111] including the power law model, the linear model and the log-linear model. Of these, the statistical models for the power law model is the most developed and it can subsume other models such as the linear model under certain conditions [69]. For this reason, we use the power law model for modeling failure of non-technical factors.

In the power law model, the ROCOF is defined as

$$w(t) = \frac{\beta}{\alpha}(\frac{t}{\alpha})^{\beta-1}$$

where α is the scale parameter (that sets the units with which time is measured) and β is the shape parameter (that determines how the ROCOF changes over time).

For β=1, the power law reverts to an HPP. If β<1, reliability growth is occurring (smaller frequency of failures as time increases) and if β>1, ageing is occurring (failures are occurring more frequently as time increases). The time to first failure for the power law process follows a Weibull distribution as given by the density function:

$$f(t_1) = \frac{\beta}{\alpha}(\frac{t_1}{\alpha})^{\beta-1}\exp[-\left(\frac{t_1}{\alpha}\right)^{\beta}]$$

It should be noted that this is applicable only for first time to failures. If data of interarrival times are fitted to a Weibull distribution, it would be misleading since this would mean that the data are from a renewal process (where a repair as-good-as-new reverts the system back to a new condition).

The parameters α and β will have to be estimated to determine the ROCOF of a non-technical factor at a given t. Expert opinion can be utilized for this, but from our literature review, we learnt that using available data to determine the values of the parameters would be more precise.

5.3.3.2. Bayesian Analysis (for learning from past incidents)

We have data that is obtained from analysis of incidents [136]. We want to make inference about the process that produced this data.

Two candidates, widely used for determination of α and β from data, are the Maximum Likelihood Estimate (MLE) and Bayesian analysis. The MLE method is widely known and straightforward to apply. A limitation for application of MLE in our case is that it does not work well when the number of data points is small and does not allow incorporation of any prior beliefs or opinions. With reliance on small number of incident data, MLE is likely to give results that offshoot the actual estimation by a large range. Epistemic uncertainty of the parameters α and β is not incorporated in the MLE method [100].

On the contrary, Bayesian analysis can allow prior information or opinion to be incorporated in the estimation, allowing the small data generated from a facility to 'fine-tune' this prior information to make the estimate plant-specific. Hierarchical Bayesian Analysis (HBA) discussed in Section 2.5 is best suited for this purpose. The prior information can come as evidence of failures in other facilities and its distribution is used for uncertainty propagation. Information about rare incidents (which may not have

yet occurred in the facility of interest) can be incorporated into the model through the use of such prior distributions.

HBA particularly allows evidence from other sources/facilities to be used for estimation of a prior which can then be used to update failure likelihood of a specific facility using the facility's own data. It should also be noted that other methods (such as MLE) use lumped data to yield results that generate a relatively narrow posterior distribution. But such results are population averaged and do not adequately reflect the full range of uncertainty associated with source-to-source variability of the data. HBA can explicitly address this variability [69, 100].

5.3.3.3. WinBUGS/ OpenBUGS (for computation of Bayesian inference)

Although the Bayesian equation is straightforward, its normalizing constant (the denominator) can prove to be computationally challenging [137]. Conjugate distributions are preferred to enable tractable analytic solutions for estimation of the joint posterior in continuous Bayesian networks. However, this limits the power of Bayesian inference only to a few known distributions. Using the power law distribution to model time to failure will not be possible analytically. An alternate to this is a developed numerical method whereby Markov Chain Monte Carlo (MCMC) method is used for deriving complicated distributions [67]. WinBUGS and OpenBUGS are publicly available software that enable such calculations to be performed [138]. They enable stochastic sampling from given distributions and follow certain rules whereby repetitive iterations allow the posterior to be estimated [67, 68, 139]. Since how the

calculation is performed is beyond the scope of this work, we will only provide the developed algorithm that were used for HBA.

5.4. Generating generic data for non-technical factors

Utilization of generic data provides a prior knowledge about population variability of a parameter of interest that can then be combined with case-specific data to determine the distribution particular to a facility. Generic data can be determined using HBA in which it is calculated in the first stage using data from various facilities.

In order to generate a generic data for the non-technical factors, we turn our attention back to the data generated from the BSEE incident investigation report analysis in Chapter 4. There we obtained the dates on which a particular non-technical factor contributed to a fire incident. We use that data to determine the interarrival time of the critical failures of the non-technical factors. In the absence of data available from various facilities, we utilize this data which encompasses the overall US OCS.

Measurement of failure rates are made in terms of number of failures and units of operation time. Data of BSEE fire incidents encompass information from all facilities in the US OCS and amount of operation can vary from time to time. Thus, a simple measurement of number of days elapsed between failures will not reflect the actual amount of operational time. It is essential to consider the sum of days of operation in each existing/working facilities within that time period in between failures.

Following provides the steps followed for determination of the total operating time in the US OCS in between the observed occurrence of each non-technical factors.

5.4.1. Determination of operating times between failures:

Data of offshore structures located in the US OCS were obtained from the BSEE Data Center [140]. This spreadsheet contained various data about the platform structures located in the US OCS including their installation and removal dates. As of January 19, 2019, there is data about 7151 platform structures to ever operate in the US OCS.

The following steps were followed to calculate the time of operation in between incidents:

1. Data of the structures belonging to the same complex were eliminated, except for the structure with the oldest installation date in that complex. It was assumed that each of these remaining structures represented each facility and a separate organization.
2. Since incidents observed in Chapter 4 were from 01/01/2014 up to 12/31/2016, platforms that were removed from operation prior to 01/01/2014 or installed after 12/31/2016 were eliminated from the calculation of operation time. This reduced the number of platform structures to 3985 only.
3. Of the remaining platforms, those that were installed prior to 01/01/2004 but continued operation after this date had their installation dates set to 01/01/2004. This was done solely for simplification of computation. Similarly, platforms removed after 12/31/2016 but installed before this date had their removal dates set to 12/31/2016.
4. Next, a Matlab file was developed to determine the total time of operation from 01/01/2004 upto an incident date (here, an incident date refers to the date of the

incident in which the particular non-technical factor being considered was found to fail critically).

If Installation date < Incident date < Removal date,

Time of operation of installation i= Incident date – Installation date

If Installation date >Incident date

Time of operation of installation i = 0

If Incident date > Removal date

Time of operation of installation i= 0

Total time of operation (from 01/01/2004 up to incident date) =

$$\sum_i Time\ of\ operation\ of\ installation\ i$$

Time in between incidents =

Total time of operation of $(j+1)^{th}$ incident – Total time of operation of j^{th} incident

Time of operation in between incidents for each non-technical factor were calculated in this manner and data for several factors are provided in Table 4.

Table 4: Table showing cumulative operating time (years) upto failure of different non-technical factors as identified from the analysis of past offshore fire incident reports.

Number of incidents	Procedural Deviation	Inadequate Job Safety Analysis	Inadequate Supervision	Inadequate Communication	Inadequate Isolation	Inadequate Maintenance	Inadequate Procedure	Design Flaw	Degradation	Failed to Detect
1	1934	248	3128	2861	2010	1249	1951	1917	1787	812
2	3548	1631	7083	5511	2258	1824	2598	2118	2881	1715
3	4014	1741	7789	10358	3429	4111	2926	3239	3036	8991
4	4363	2043	8303	11435	3641	4660	3492	4971	9927	10274
5	6182	2208	9052	14960	4053	4669	4613	5694	10583	12745
6	6529	3904	9060	14960	4218	5245	12809	6617	10995	13235
7	7325	4014	12107	16046	4865	5318	12818	7146	13707	14078
8	8357	4870	12577	16629	5385	6844	13877	9099	14249	18128
9	11034	6182	13662	16972	9152	6971	14060	9511	14641	21133
10	11097	6365	21571	17114	10367`	8141	14531	10199	15536	21589

Table 4: Continued

Number of incidents	Procedural Deviation	Inadequate Job Safety Analysis	Inadequate Supervision	Inadequate Communication	Inadequate Isolation	Inadequate Maintenance	Inadequate Procedure	Design Flaw	Degradation	Failed to Detect
11	11803	6602	22472	18017	11059	8796	15865	10350	15552	21825
12	11989	7142	23376	21545	13044	9163	18003	13647	17070	23199
13	13066	8357	27336	21961	14035	9208	18346	14068	19948	24443
14	14317	11034		22002	14327	9727	18441	15396	19956	28459
15	17027	11830		28080	15076	10383	19391	20932	23848	28748
16	18603	12317		28780	15085	11474	20076	27060	26298	29473
17	19718	13066			16144	11920	22919	28080	26775	
18	23176	13075			16798	12462	23376	28337	27243	
19	23211	14134			17288	13345	23612	29719	29821	
20	23592	14317			18074	13749	25328	29886		

Table 4: Continued

Number of incidents	Procedural Deviation	Inadequate Job Safety Analysis	Inadequate Supervision	Inadequate Communication	Inadequate Isolation	Inadequate Maintenance	Inadequate Procedure	Design Flaw	Degradation	Failed to Detect
21	23633	15799			18132	13882	26229	31091		
22	25585	15816			18601	17062	26289			
23	26486	16064			18601	17715	27275			
24	27650	16591			18947	18169	28434			
25	30411	16591			19037	18628	29454			
26	32031	16937			19350	20474	30245			
27		17340			20676	21658				
28		17381			20708	21935				
29		17677			20755	24976				
30		18603			22343	24988				

Table 4: Continued

Number of incidents	Procedural Deviation	Inadequate Job Safety Analysis	Inadequate Supervision	Inadequate Communication	Inadequate Isolation	Inadequate Maintenance	Inadequate Procedure	Design Flaw	Degradation	Failed to Detect
31		18666			27252	25456				
32		18698			27595	25598				
33		18745			32422	26668				
34		19718			32802	27777				
35		20333			33214	29270				
36		22563			33360					
37		23176								
38		23211								
39		23869								
40		25242								

Table 4: Continued

Number of incidents	Procedural Deviation	Inadequate Job Safety Analysis	Inadequate Supervision	Inadequate Communication	Inadequate Isolation	Inadequate Maintenance	Inadequate Procedure	Design Flaw	Degradation	Failed to Detect
41		25585								
42		26486								
43		30502								
44		32031								

With the data on the total operating time between failures, we can make visual examination of the failure trend of the contributing factors with elapsed time. In Figures 15 and 16, we show graphs of the number of failures against the cumulative operating times calculated in Table 4. Only graphs for contributing factors Procedural Deviation and Inadequate Supervision are shown respectively.

From the graphs of number of incidents against cumulative time, we see that failure occurs at irregular times and some failures are more cluttered in certain time periods than in during other periods, indicating that the failure rates are different over these periods and the interarrival times seem to be not independent or identically distributed as we had assumed for a single facility. Thus, using this data obtained from the US OCS and treating it as coming from a single organization is justified.

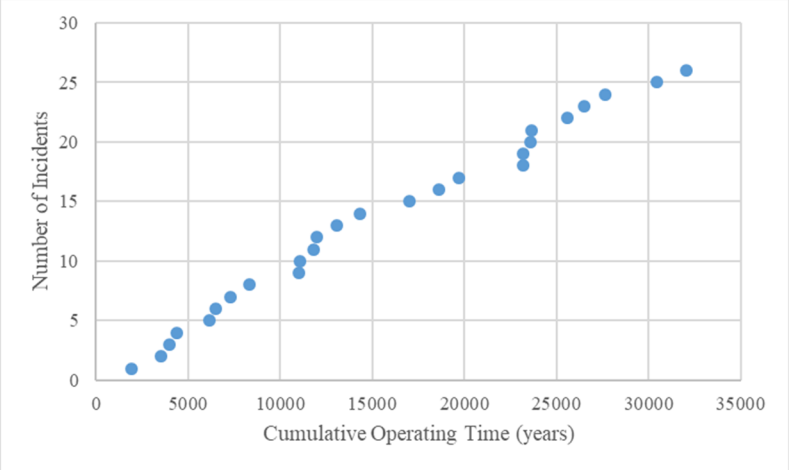


Figure 15: The number of failures and the hazard function against cumulative operating time graphs for Procedural Deviation showing that the assumption of failure following a non-homogenous failure process is valid for this data.

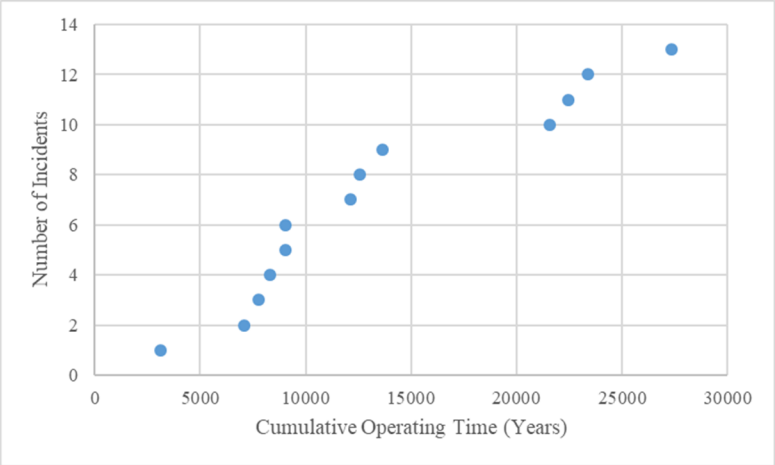


Figure 16: The number of failures and the hazard function against cumulative operating time graphs for Inadequate Supervision showing that the assumption of failure following a non-homogenous failure process is valid for this data

5.4.2. Application of Power Law for determination of hyperparameters

The power law is given by

$$w(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1}$$

We analyze the data for a failure-truncated case where we stop our observation after the last failure is seen. If t_i is the cumulative time until the i^{th} failure, then the likelihood function can be derived using the fact that the time to first failure is Weibull distributed and the succeeding times to failure follow a left truncated Weibull distribution at the preceding failure times [68, 69]. Thus, the likelihood function becomes:

$$f(t_1, t_2, \ldots t_n|\alpha,\beta) = \frac{\beta^n}{\alpha^{n\beta}} \prod_{i=1}^{n} t_i^{\beta-1} \exp\left[-\left(\frac{t_n}{\beta}\right)^{\beta}\right]$$

The first incident is used as a starting point for the estimation of cumulative failure times described in the previous section. Each of the time to failure is loaded as 'data' (evidence) to the likelihood function in OpenBUGS.

We are required to specify prior distributions which will reflect our prior knowledge of the times to failure. Here, expert opinion can be applied which will make it a 'informative' prior. Non-informative priors are studied to develop priors that mathematically represent complete uncertainty: they contain little or no information about the parameter of interest. Using them enables a wide range of α and β values to be generated making the inference envelope all possible data. Such priors have little influence on the posterior, thus making the inference completely reliant on the data inserted through the likelihood function.

One of the most widely used non-informative priors is the Jeffrey's prior [141]. However, these do not work well for multi-parameter problems and hence are not suitable for the power law process. An alternate use is the uniform distribution whereby equal probability is assigned to all values of a parameter within a range. However, opinions state that defining the range makes the prior informative and uniform distribution is not invariant, thereby generating different posteriors under different reparameterization [102]. Utilization of diffused gamma distributions as non-informative priors have been proposed in multiple sources [68, 69, 102]. This work adopts diffused gamma distribution as non-informative priors, defining α and β as

We utilize OpenBUGS to perform MCMC sampling to generate the joint posterior distribution of α and β and the marginal posterior distribution in a manner

similar to that proposed by Kelly *et al*. and Rodionov *et al*. [68, 69]. Since the likelihood function is not pre-programmed into OpenBUGS, the 'zero-trick' method is utilized as described by Rodionov et al. and Kelly et al. [68, 69].

Because OpenBUGS can have difficulty in generating initial values from the priors, initial values for α and β are provided. These initial values are just estimated values for starting the sampling. For complicated models, two chains are run in parallel, starting at two different points to understand when convergence to posterior has been achieved [68]. If the history plots of these two chains indicate show mixing, then convergence has been achieved. An alternate is to use the BGR (Brooks-Gelman-Rubin) convergence diagnostic [68]. We will not discuss how this works since it if beyond the scope of our work. If the red line (representing BGR ratio) in the BGR diagnostic becomes 1 and if the blue line (estimate of with-in chain variance) is stable, then convergence is said to have been achieved. The iterations following convergence point are then used for the real estimation of the posterior probabilities.

The MCMC sampling provides us with statistics of α and β. We are also interested in determining the next time to failure as well as the probability of failure with a given time interval after the last incident where a given non-technical factor failed. To obtain the uncertainty associated with the estimation of time to next failure, its value is modelled as being extracted from a gamma distribution. All known times to failure data are loaded into the algorithm along with an additional data entry coded as NA to signify that the value of this data point is not known. Initial values are given as NA for each chain (since exact values are already provided), and the initial value of the extra data

entry are given as a value slightly more (+1) than the value of the last measured time to failure.

Distribution of the probability of failure are also determined from the cumulative distribution function and is given by

$$F(t) = 1 - \exp\{-\lambda((T+t)^{\beta} - T^{\beta})\}$$

Where T is the cumulative time of the last failure and t is the cumulative time of the next predicted failure and $\lambda=\alpha^{-\beta}$ [68].

Two types of probabilities are estimated: one for failure in the US OCS in the next 3,6,9 and 12 months and one for a single facility in the next 6 months, 1 year, 1.5 year and 2 years. The calculated operation times upto failures have units in years. With the large number of facilities operating in the US OCS, each day the sum of operating time was found to be equivalent to 7.73 years of operation in a single facility. It was calculated that, on average, the sum of three months of operation time in the US OCS was equivalent to an operation time of 695 years. Thus, the algorithm calculates the probability of failure in the next 695,1390, 2085 and 2780 years respectively to determine the probability distribution of failure in the US OCS bimonthly. The algorithm also calculated the probability of the next failure being in the next 6,12,18,24 months by setting t as 0.5,1,1.5,2 respectively. This would be operation time of a single faclity. The algorithm is provided in Appendix B.

We next provide a sample estimation of the failure data of the non-technical factor “Procedural Deviation”. Only the results obtained from other non-technical factors are given after the example.

5.4.2.1. Procedural Deviation: Example

Data for likelihood function: Data is obtained from the second column of Table 4 and entered with an additional data given as NA. This tell OpenBUGS that we do not know the value of this node so that we can monitor its value as the time to next failure.

Priors: α ~ gamma (0.0001, 0.0001), β ~ gamma (0.0001, 0.0001)

Initial values:

Chain 1: α=1500, β=0.5, t=c (NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, 32032)

Chain 2: α=1500,β=1.5, t=c (NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, NA, 32032)

Two chains were run simultaneously to determine if convergence has been achieved. The program was iterated 40000 times and the BGR statistics were observed for α and β as shown in Figure 17. As can been seen, convergence has been achieved (red line is close to 1.0 and blue line is stable).

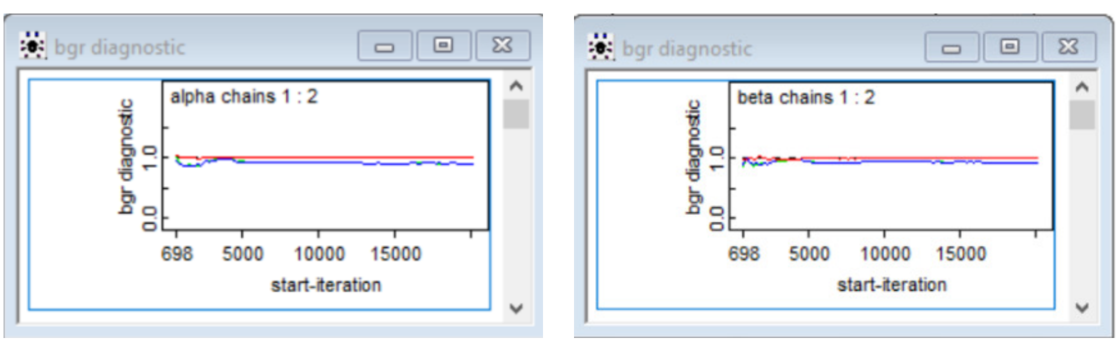
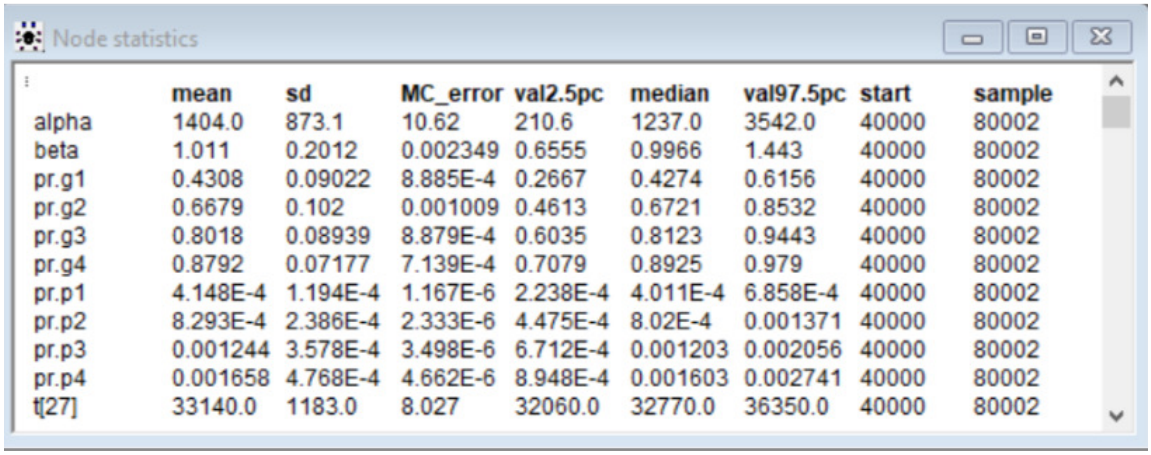


Figure 17: BGR statistics of hyperparameters α and β showing convergence

The program was run for another 40000 iterations (took 25 sec) to compute the values of the parameters. The data are shown in figure 18.



	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1404.0	873.1	10.62	210.6	1237.0	3542.0	40000	80002
beta	1.011	0.2012	0.002349	0.6555	0.9966	1.443	40000	80002
pr.g1	0.4308	0.09022	8.885E-4	0.2667	0.4274	0.6156	40000	80002
pr.g2	0.6679	0.102	0.001009	0.4613	0.6721	0.8532	40000	80002
pr.g3	0.8018	0.08939	8.879E-4	0.6035	0.8123	0.9443	40000	80002
pr.g4	0.8792	0.07177	7.139E-4	0.7079	0.8925	0.979	40000	80002
pr.p1	4.148E-4	1.194E-4	1.167E-6	2.238E-4	4.011E-4	6.858E-4	40000	80002
pr.p2	8.293E-4	2.386E-4	2.333E-6	4.475E-4	8.02E-4	0.001371	40000	80002
pr.p3	0.001244	3.578E-4	3.498E-6	6.712E-4	0.001203	0.002056	40000	80002
pr.p4	0.001658	4.768E-4	4.662E-6	8.948E-4	0.001603	0.002741	40000	80002
t[27]	33140.0	1183.0	8.027	32060.0	32770.0	36350.0	40000	80002

Figure 18: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Procedural deviation

Here pr.g1=probability of next failure within the next 3 calendar months, pr.g2=probability of next failure within the next 6 calendar months, pr.g3=probability of next failure within the next 9 calendar months and, pr.g4=probability of next failure within the next 12 calendar months of operation in the US OCS. pr.p1=probability of next failure within the next six months (0.5 years of operating time) in a single facility, pr.p2=probability of next failure within the next 1 year in a single facility, pr.p3=probability of next failure within the next 1.5 years in a single facility, pr.p4=probability of next failure within the next 2 years of operation in a single facility.

OpenBUGS guidelines suggest that the value of Monte Carlo (MC) error should be no more than 5% of the standard deviation. If it is more, then more iterations would

be carried out to ensure convergence. As can be seen from the values provided in the table, this condition is satisfied and the chains have converged.

Values of estimates for 2.5 and 97.5 percent confidence intervals are also provided along with the median.

Distribution graphs obtained are provided below in Figures 17-20. The last graph (Figure 20) provides the distribution of the predicted next time to failure, with the x axis showing the number of years of operating time in the US OCS.

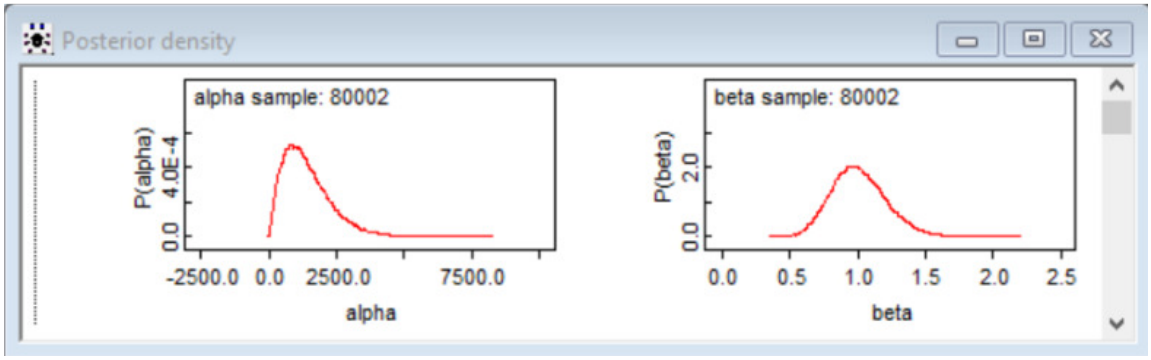


Figure 19 : Figure showing the obtained distribution of the parameters of the power law from the iterations carried out after convergence in OpenBUGS

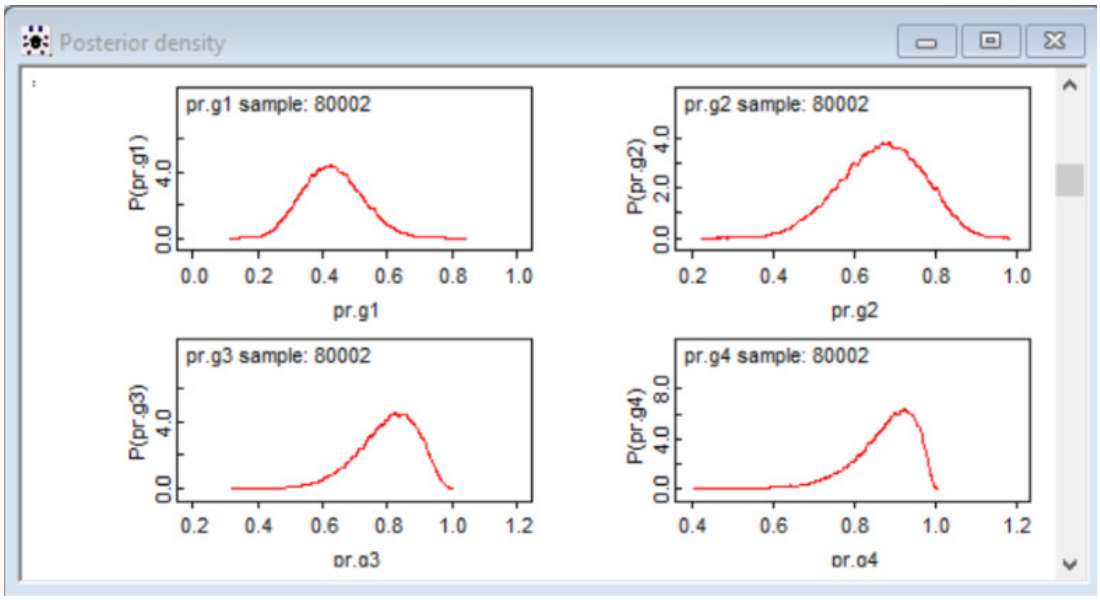


Figure 20: The probability distribution of the next critical failure of Procedural Deviation occurring in the US OCS within the next 3 months (pr.g1), 6 months (pr.g2), 9 months (pr.g3) and 12 months (pr.g4) are shown here.

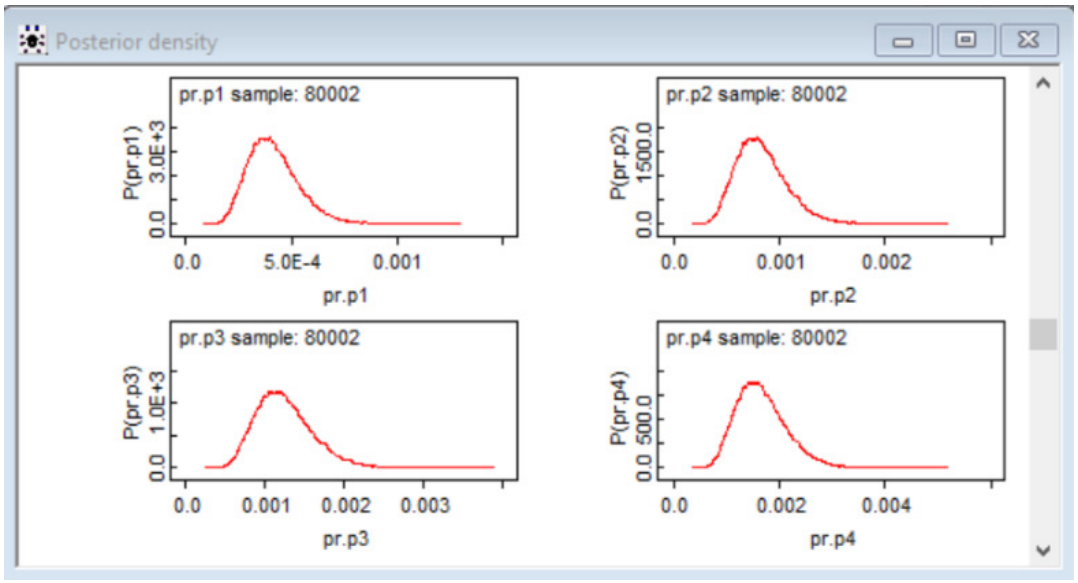


Figure 21: The probability distribution of the next critical failure of Procedural Deviation occurring with a single facility located in the US OCS within the next 6 months (pr.p1), 1 year (pr.p2), 1.5 years (pr.p3) and 2 years (pr.p4) are shown here. Notice the shift in the mean value as time elapses, indicating an increased probability of the next failure as time goes by.

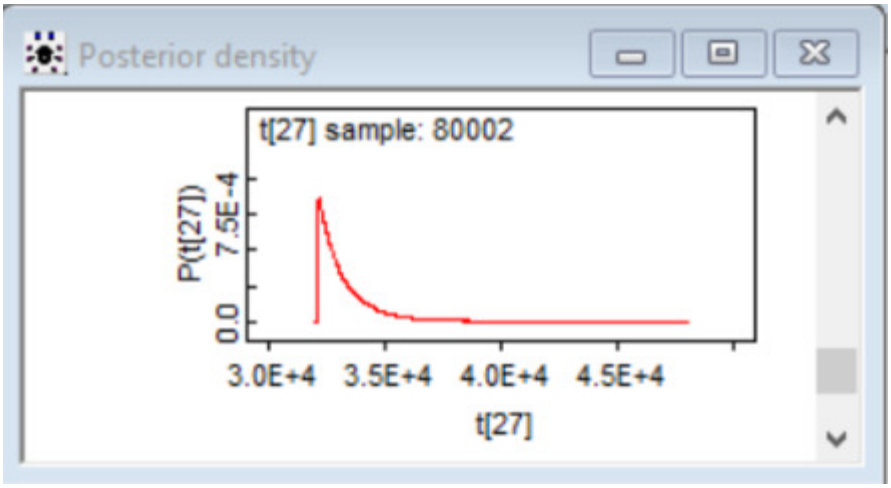


Figure 22: The probability distribution of the predicted next time to failure with contribution from Procedural Deviation in the US OCS

For the probability distributions in Figure 20 and 21, notice the shift in the mean value as time elapses, indicating an increased probability of the next failure as time goes by.

With the last time to failure occurring at 32031 years of operation (from Table 4), the next time to failure is expected to occur after 33140 years of operation, with a standard deviation of 1183 years of operation. This means that the next time to failure is 1109 years after the last incident was noted in the US OCS. With an average of 2780 years of operation time every calendar year, the next incident is expected to occur approximately 4.8 calendar months after the last one.

As shown for Procedural Deviation, results obtained for some of the other non-technical factors are also provided below. Data used for these computations were those given in Table 4. BGR graphs and history was checked (graphs of convergence are not shown) and a further 40000 iterations were conducted to obtain sample results.

5.4.2.2. Design Flaw:

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1191.0	841.4	14.55	130.4	1002.0	3328.0	40001	40000
beta	0.8979	0.1935	0.003295	0.5673	0.8834	1.321	40001	40000
pr.g1	0.341	0.08419	0.001357	0.1933	0.3356	0.5194	40001	40000
pr.g2	0.5583	0.1093	0.001765	0.3483	0.5582	0.7697	40001	40000
pr.g3	0.6992	0.1089	0.00176	0.4726	0.7059	0.89	40001	40000
pr.g4	0.7922	0.09867	0.001593	0.5728	0.804	0.9476	40001	40000
pr.p1	3.064E-4	9.594E-5	1.538E-6	1.55E-4	2.945E-4	5.258E-4	40001	40000
pr.p2	6.127E-4	1.918E-4	3.074E-6	3.101E-4	5.889E-4	0.001051	40001	40000
pr.p3	9.188E-4	2.876E-4	4.61E-6	4.651E-4	8.832E-4	0.001577	40001	40000
pr.p4	0.001225	3.834E-4	6.144E-6	6.201E-4	0.001177	0.002102	40001	40000
t[22]	32520.0	1552.0	15.17	31130.0	32040.0	36680.0	40001	40000

Figure 23: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Design Flaw

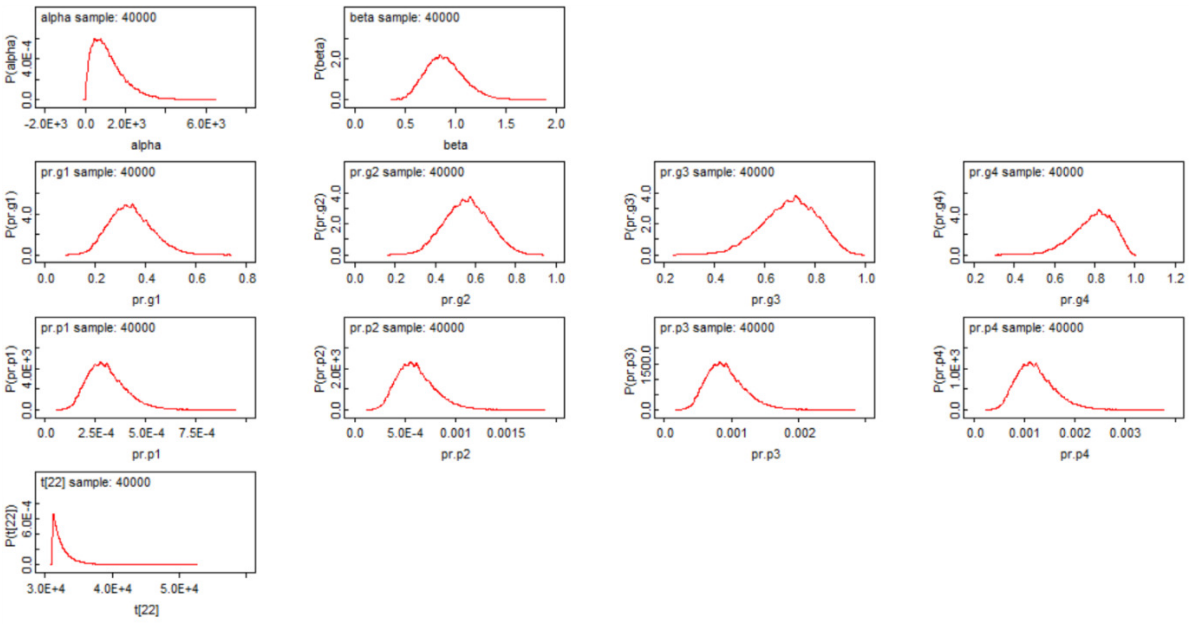


Figure 24: Distributions obtained for hyperparameters α and β, probabilities and time to next failure for Design Flaw

5.4.2.3. Degradation of Material

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	2201.0	1320.0	18.99	316.5	1980.0	5279.0	40001	40000
beta	1.099	0.255	0.003673	0.6598	1.079	1.647	40001	40000
pr.g1	0.3838	0.0969	0.001345	0.2097	0.3788	0.5863	40001	40000
pr.g2	0.6114	0.1179	0.001643	0.3747	0.6144	0.8305	40001	40000
pr.g3	0.7495	0.1113	0.001558	0.5046	0.761	0.9311	40001	40000
pr.g4	0.8353	0.09612	0.001354	0.607	0.852	0.9723	40001	40000
pr.p1	3.573E-4	1.192E-4	1.65E-6	1.695E-4	3.421E-4	6.311E-4	40001	40000
pr.p2	7.144E-4	2.383E-4	3.299E-6	3.39E-4	6.84E-4	0.001262	40001	40000
pr.p3	0.001071	3.573E-4	4.946E-6	5.085E-4	0.001026	0.001892	40001	40000
pr.p4	0.001428	4.763E-4	6.592E-6	6.779E-4	0.001368	0.002522	40001	40000
t[20]	31090.0	1374.0	13.6	29850.0	30650.0	34800.0	40001	40000

Figure 25: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Degradation of Material

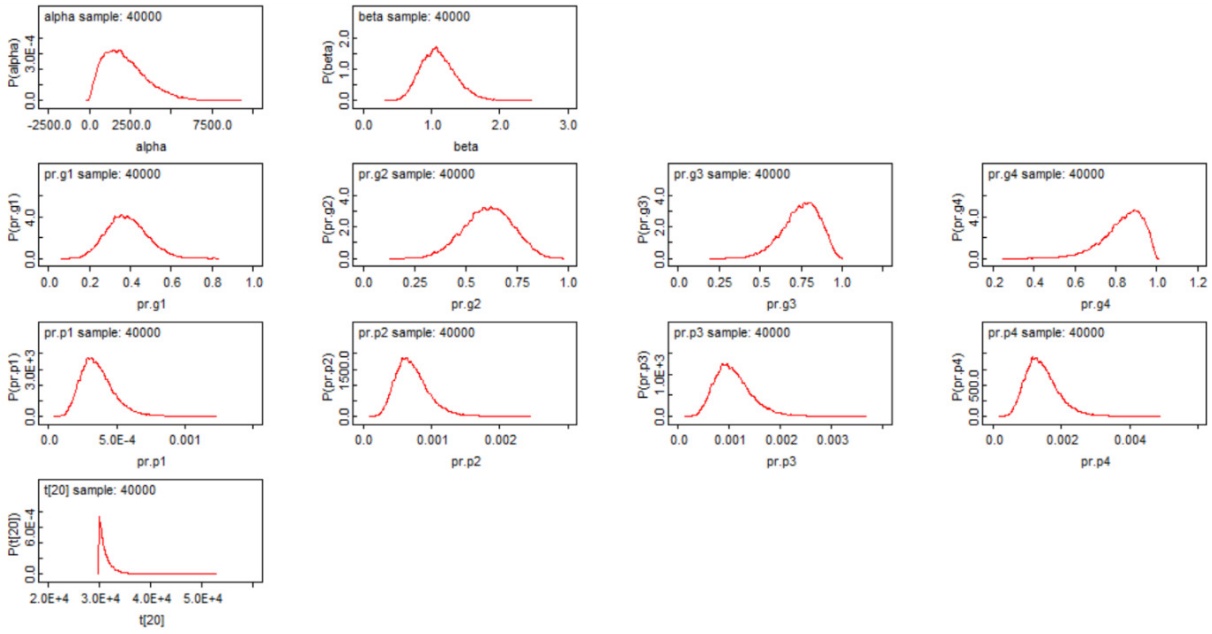


Figure 26: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Degradation of Material

5.4.2.4. Inadequate/Lack of Maintenance

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	960.0	566.6	9.447	171.4	855.5	2343.0	40001	40000
beta	1.013	0.1735	0.002858	0.6999	1.003	1.378	40001	40000
pr.g1	0.5627	0.08654	0.001311	0.3937	0.5627	0.7292	40001	40000
pr.g2	0.8012	0.07683	0.00118	0.6316	0.8088	0.9272	40001	40000
pr.g3	0.9064	0.05382	8.353E-4	0.7755	0.9164	0.9806	40001	40000
pr.g4	0.9545	0.03506	5.486E-4	0.863	0.9635	0.9948	40001	40000
pr.p1	6.094E-4	1.485E-4	2.214E-6	3.608E-4	5.948E-4	9.367E-4	40001	40000
pr.p2	0.001218	2.967E-4	4.424E-6	7.215E-4	0.001189	0.001873	40001	40000
pr.p3	0.001827	4.448E-4	6.632E-6	0.001082	0.001783	0.002807	40001	40000
pr.p4	0.002435	5.927E-4	8.837E-6	0.001442	0.002377	0.003742	40001	40000
t[36]	30050.0	809.3	8.511	29290.0	29800.0	32220.0	40001	40000

Figure 27: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate/Lack of Maintenance

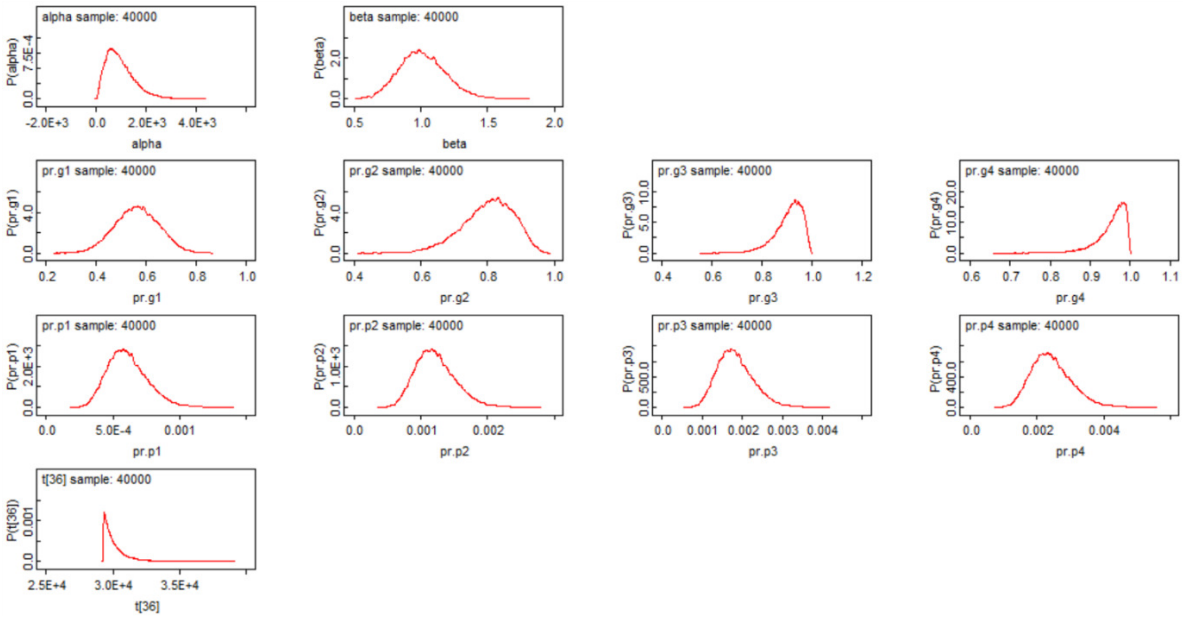


Figure 28: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate/Lack of Maintenance

5.4.2.5. Improper Procedure

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	2237.0	1137.0	16.31	504.8	2093.0	4853.0	40001	40000
beta	1.229	0.2399	0.003386	0.8031	1.216	1.734	40001	40000
pr.g1	0.5175	0.09742	0.001401	0.3294	0.5164	0.7075	40001	40000
pr.g2	0.7585	0.09504	0.001371	0.5499	0.767	0.9158	40001	40000
pr.g3	0.8749	0.07313	0.001057	0.6976	0.888	0.9762	40001	40000
pr.g4	0.9331	0.05232	7.566E-4	0.7968	0.9464	0.9934	40001	40000
pr.p1	5.382E-4	1.521E-4	2.176E-6	2.877E-4	5.213E-4	8.783E-4	40001	40000
pr.p2	0.001076	3.041E-4	4.349E-6	5.753E-4	0.001042	0.001756	40001	40000
pr.p3	0.001614	4.559E-4	6.52E-6	8.629E-4	0.001563	0.002633	40001	40000
pr.p4	0.002151	6.075E-4	8.688E-6	0.00115	0.002083	0.003508	40001	40000
t[27]	31130.0	947.4	8.664	30270.0	30820.0	33710.0	40001	40000

Figure 29: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Improper Procedure

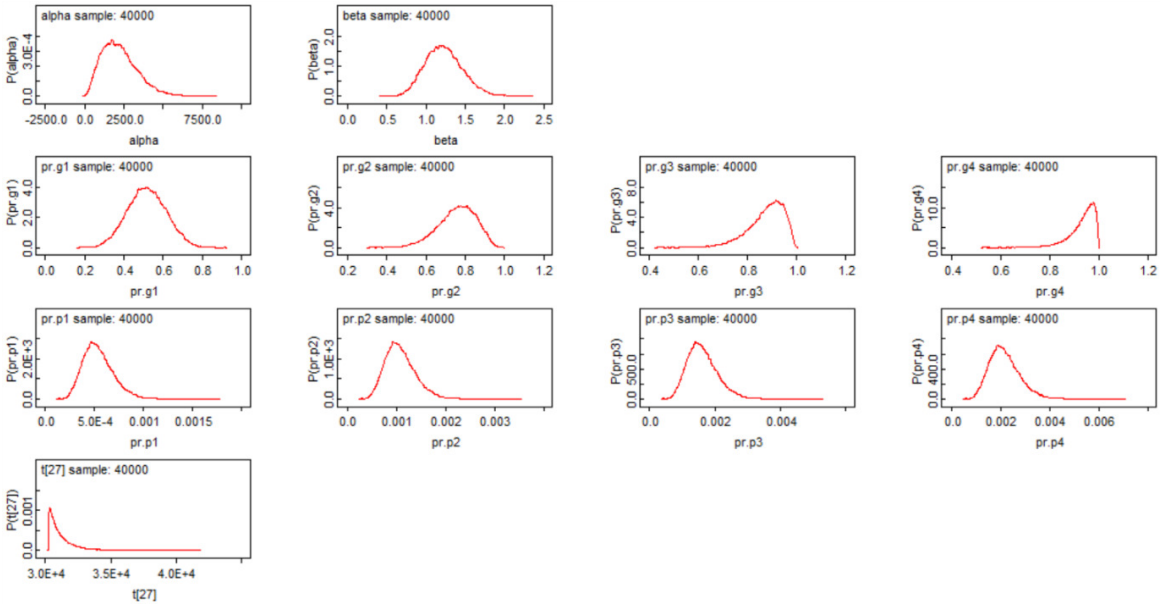


Figure 30: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Improper Procedure

5.4.2.6. Inadequate Supervision

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	2532.0	1673.0	26.79	237.4	2241.0	6515.0	40001	40000
beta	1.045	0.2929	0.004365	0.5529	1.02	1.689	40001	40000
pr.g1	0.294	0.09641	0.001378	0.1317	0.2854	0.5079	40001	40000
pr.g2	0.4926	0.1326	0.00189	0.2452	0.4895	0.7599	40001	40000
pr.g3	0.6293	0.1405	0.001992	0.3429	0.6353	0.884	40001	40000
pr.g4	0.7251	0.1354	0.001907	0.4278	0.7396	0.9443	40001	40000
pr.p1	2.573E-4	1.04E-4	1.485E-6	1.019E-4	2.416E-4	5.07E-4	40001	40000
pr.p2	5.146E-4	2.08E-4	2.97E-6	2.039E-4	4.832E-4	0.001014	40001	40000
pr.p3	7.717E-4	3.119E-4	4.453E-6	3.058E-4	7.247E-4	0.00152	40001	40000
pr.p4	0.001029	4.157E-4	5.936E-6	4.077E-4	9.661E-4	0.002026	40001	40000
t[14]	29050.0	1882.0	17.9	27380.0	28460.0	34120.0	40001	40000

Figure 31: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Supervision

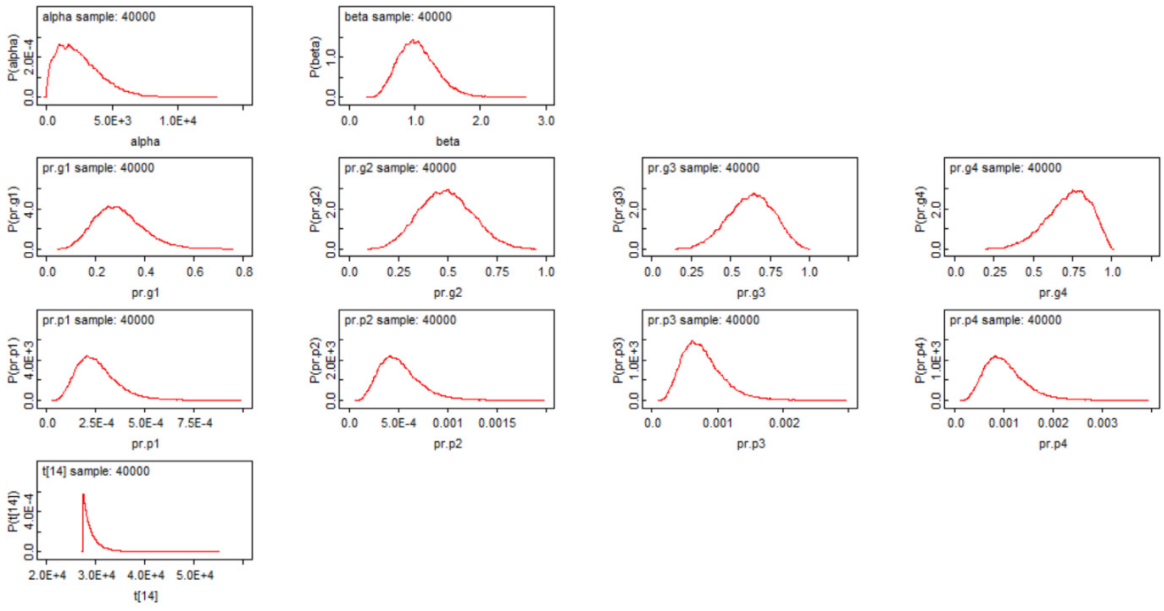


Figure 32: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Supervision

5.4.2.7. Inadequate Communication

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	3732.0	1919.0	29.27	697.6	3519.0	8055.0	40001	40000
beta	1.342	0.3394	0.005066	0.7587	1.31	2.087	40001	40000
pr.g1	0.4073	0.1085	0.001497	0.2151	0.4012	0.6359	40001	40000
pr.g2	0.6383	0.1268	0.001719	0.3835	0.6428	0.8699	40001	40000
pr.g3	0.7733	0.1159	0.001546	0.5155	0.7877	0.9546	40001	40000
pr.g4	0.8545	0.09755	0.001281	0.6192	0.8743	0.9845	40001	40000
pr.p1	3.876E-4	1.407E-4	1.977E-6	1.745E-4	3.675E-4	7.183E-4	40001	40000
pr.p2	7.75E-4	2.814E-4	3.952E-6	3.489E-4	7.349E-4	0.001436	40001	40000
pr.p3	0.001162	4.218E-4	5.925E-6	5.233E-4	0.001102	0.002153	40001	40000
pr.p4	0.001549	5.622E-4	7.896E-6	6.977E-4	0.001469	0.00287	40001	40000
t[17]	3.0E+4	1323.0	13.42	28810.0	29580.0	33610.0	40001	40000

Figure 33: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Communication

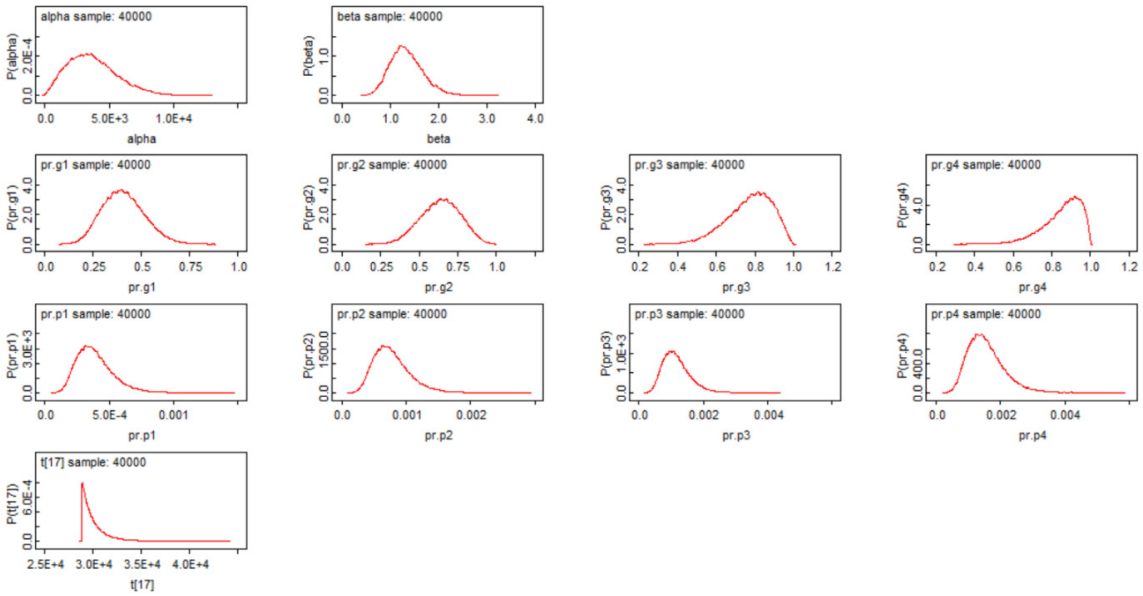


Figure 34: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Communication

5.4.2.8. Improper Job Safety Analysis (JSA)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	555.4	346.0	6.432	93.27	485.3	1416.0	40001	40000
beta	0.9073	0.1378	0.002475	0.6536	0.9007	1.199	40001	40000
pr.g1	0.5723	0.07812	0.001209	0.4194	0.5729	0.7239	40001	40000
pr.g2	0.8106	0.06788	0.001053	0.6619	0.8172	0.924	40001	40000
pr.g3	0.9134	0.04632	7.161E-4	0.8025	0.9217	0.9792	40001	40000
pr.g4	0.9592	0.02929	4.496E-4	0.8842	0.9664	0.9943	40001	40000
pr.p1	6.239E-4	1.361E-4	2.091E-6	3.922E-4	6.126E-4	9.245E-4	40001	40000
pr.p2	0.001247	2.72E-4	4.18E-6	7.843E-4	0.001225	0.001848	40001	40000
pr.p3	0.00187	4.077E-4	6.266E-6	0.001176	0.001837	0.002771	40001	40000
pr.p4	0.002493	5.432E-4	8.349E-6	0.001568	0.002448	0.003693	40001	40000
t[45]	32790.0	794.8	7.4	32050.0	32540.0	34920.0	40001	40000

Figure 35: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Improper JSA

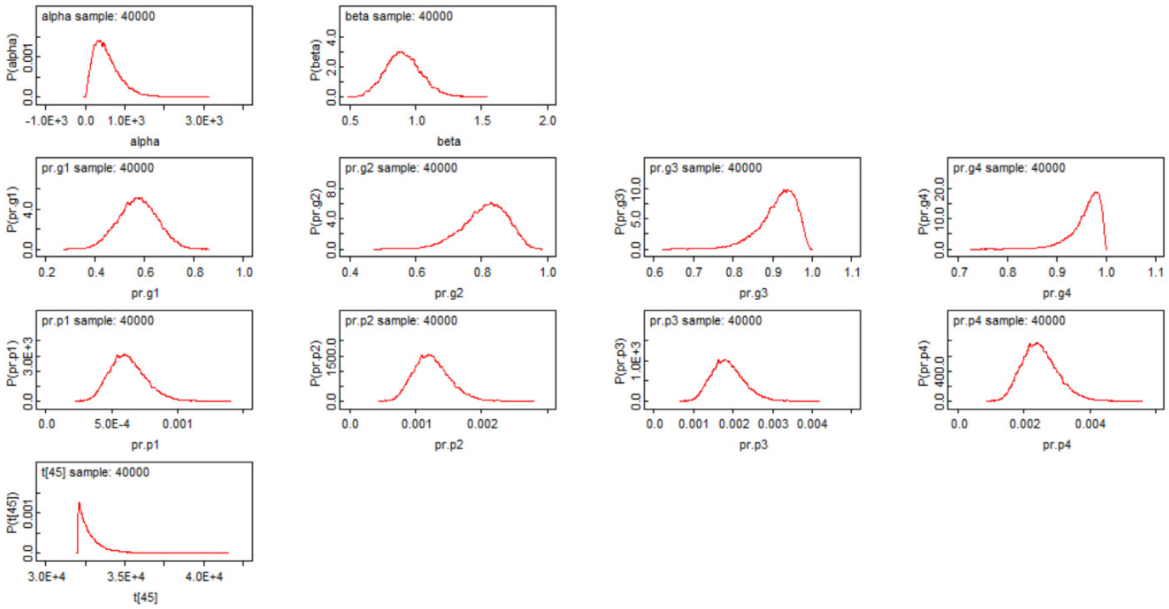


Figure 36: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Improper JSA

5.4.2.9. Failed to Detect

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	2628.0	1581.0	24.34	375.8	2367.0	6296.0	40001	40000
beta	1.119	0.278	0.004243	0.6534	1.096	1.738	40001	40000
pr.g1	0.3463	0.09672	0.001395	0.1789	0.3402	0.5544	40001	40000
pr.g2	0.5638	0.124	0.001778	0.3251	0.565	0.8032	40001	40000
pr.g3	0.7034	0.1229	0.001749	0.4446	0.7136	0.9139	40001	40000
pr.g4	0.7948	0.1111	0.001567	0.5428	0.8115	0.9627	40001	40000
pr.p1	3.136E-4	1.124E-4	1.625E-6	1.422E-4	2.988E-4	5.776E-4	40001	40000
pr.p2	6.27E-4	2.247E-4	3.249E-6	2.843E-4	5.975E-4	0.001155	40001	40000
pr.p3	9.404E-4	3.37E-4	4.872E-6	4.264E-4	8.961E-4	0.001732	40001	40000
pr.p4	0.001254	4.491E-4	6.494E-6	5.685E-4	0.001195	0.002308	40001	40000
t[17]	30890.0	1531.0	13.52	29510.0	30410.0	35060.0	40001	40000

Figure 37: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Failed to Detect

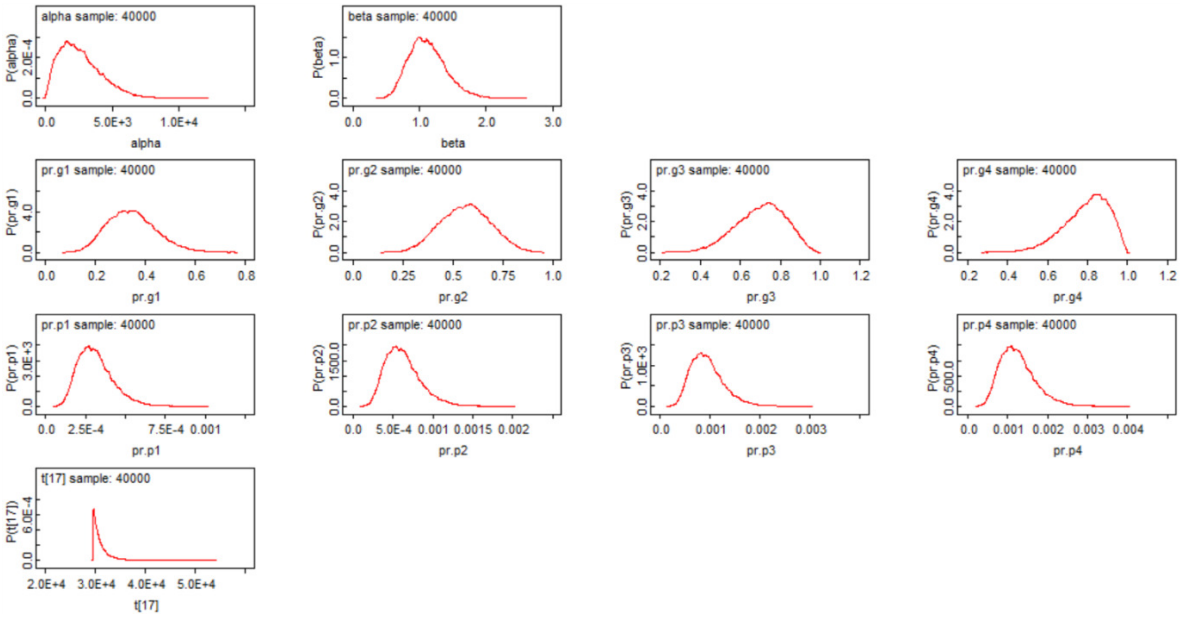


Figure 38: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Failed to Detect

5.4.2.10. Inadequate Isolation

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1084.0	636.4	10.78	203.8	970.0	2621.0	40001	40000
beta	1.019	0.172	0.002723	0.7088	1.01	1.386	40001	40000
pr.g1	0.5289	0.08341	0.001173	0.3707	0.5274	0.6936	40001	40000
pr.g2	0.7711	0.07911	0.001126	0.6032	0.7767	0.9067	40001	40000
pr.g3	0.8856	0.05864	8.439E-4	0.7493	0.8946	0.9718	40001	40000
pr.g4	0.9412	0.0401	5.83E-4	0.8412	0.9502	0.9915	40001	40000
pr.p1	5.529E-4	1.325E-4	1.836E-6	3.339E-4	5.389E-4	8.483E-4	40001	40000
pr.p2	0.001106	2.647E-4	3.669E-6	6.678E-4	0.001078	0.001696	40001	40000
pr.p3	0.001658	3.969E-4	5.5E-6	0.001001	0.001616	0.002543	40001	40000
pr.p4	0.00221	5.289E-4	7.33E-6	0.001335	0.002154	0.003389	40001	40000
t[37]	34220.0	886.1	8.865	33380.0	33940.0	36590.0	40001	40000

Figure 39: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Isolation

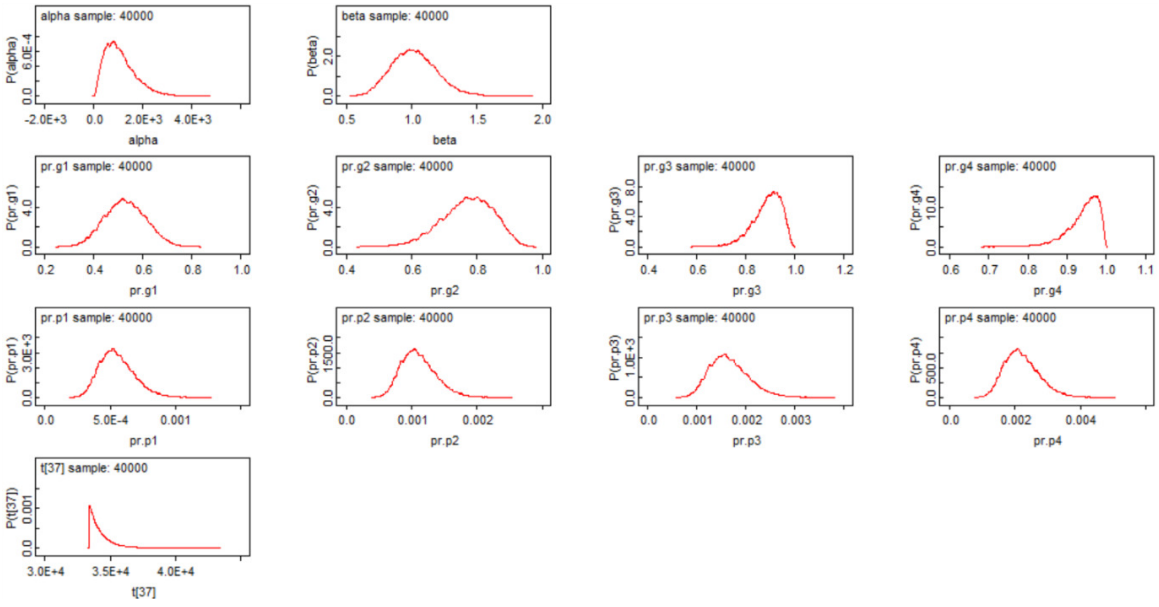


Figure 40: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Inadequate Isolation

5.4.2.11. Contact with Hot Surface (Ignition source)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	842.5	409.4	6.67	239.8	776.4	1803.0	40001	40000
beta	1.071	0.1376	0.002167	0.8206	1.065	1.36	40001	40000
pr.g1	0.7041	0.06581	9.175E-4	0.5706	0.7056	0.8265	40001	40000
pr.g2	0.9082	0.04025	5.596E-4	0.8153	0.9135	0.9702	40001	40000
pr.g3	0.9702	0.01964	2.707E-4	0.9204	0.9746	0.9949	40001	40000
pr.g4	0.99	0.008996	1.223E-4	0.9657	0.9926	0.9991	40001	40000
pr.p1	8.935E-4	1.658E-4	2.305E-6	6.087E-4	8.789E-4	0.001256	40001	40000
pr.p2	0.001786	3.314E-4	4.606E-6	0.001217	0.001757	0.002511	40001	40000
pr.p3	0.002678	4.966E-4	6.903E-6	0.001825	0.002634	0.003764	40001	40000
pr.p4	0.003569	6.615E-4	9.196E-6	0.002432	0.003511	0.005015	40001	40000
t[60]	36170.0	554.3	5.02	35650.0	35990.0	37680.0	40001	40000

Figure 41: Computed data showing various values of the hyperparameters α and β, probabilities and time to next failure for Contact with Hot Surface

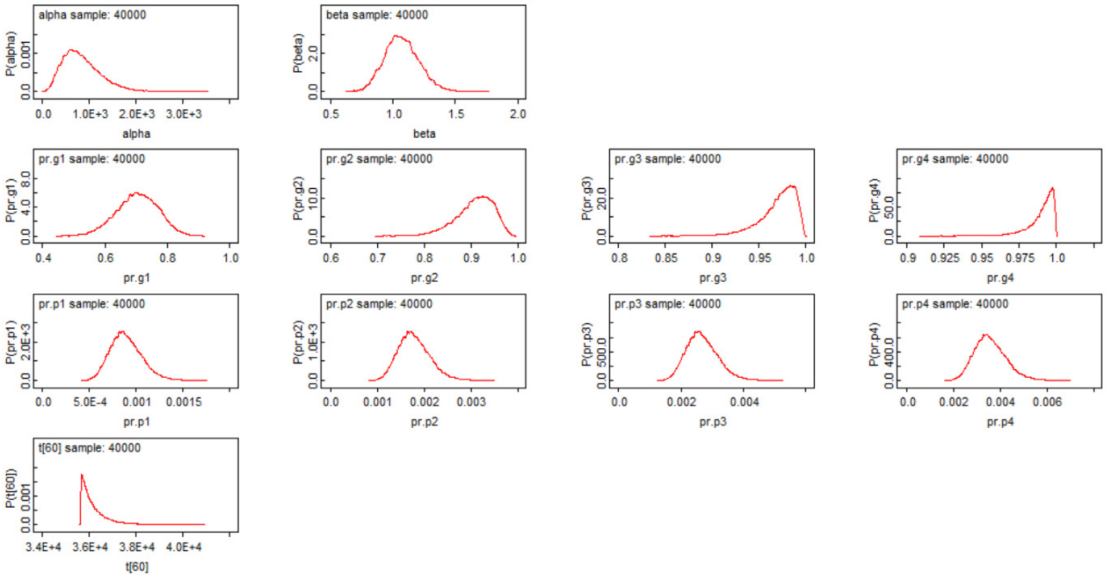


Figure 42: Distributions obtained for various values of the hyperparameters α and β, probabilities and time to next failure for Contact with Hot Surface

Figures 23, 25, 27, 29, 31, 33, 35, 37,39 and 41 provides the results obtained from the MCMC sampling obtained using the data for various contributing factors from Table 4. They show the various parameters such as mean, standard deviation, median

and the boundaries for the 95% confidence interval. Figures 26, 28, 30, 32, 34, 36, 38, 40 and 42 shows the distribution of the hyperparameters, the probabilities of failures based on operation time in the overall US OCS, and in a single facility. The distribution of the predicted time to next failure is also shown. As discussed before the probability distribution is seen to change over time, as the probability of failure increases as time elapses.

5.5. Updating to Plant Specific Data

If past plant data is available, that data can be used to determine the current failure probability distributions of each factor using the methodology described in the previous section. In the absence of such data, aggregated data from other facilities or the entire US OCS can be used as shown. The parameters α and β for each non-technical factor describe the distribution of this generic data. As the facility keeps operating and new data becomes available, we will have to update the probability distributions using the new data. This will enable the generic data to be made plant-specific.

The posterior parameters estimated from the generic data are fed as priors to the algorithm of the plant-specific data. This forms the second stage of the Hierarchical Bayesian analysis. That is to say that we learnt and have a general idea about the distribution of α and β from the data of the US OCS and we will now use that knowledge to modify the parameters α and β using our plant specific failure data. The algorithm basically remains the same but we replace the prior of the algorithm with the posterior

parameters α and β estimated from the generic data. Cumulative time to failure of a factor in the facility is fed as evidence.

Since we have values of α and β expressed as mean and standard deviations from the first stage of the HBA and we want to use these values as priors in the second stage, we use a truncated normal distribution. OpenBUGS provides compete dataset that represents the distribution of α and β but we simplify this using only the mean and standard deviation. OpenBUGS parameterizes the normal distribution with mean and precision (which is 1/variance). So, the mean and standard deviation of the posterior α and are converted to mean and precision and fed as priors to the plant-specific algorithm. The program is run in the similar manner as shown before.

5.5.1. Updating Procedural Deviation: Example

Suppose we find 3 occurrences of Procedural deviation from past plant data. These deviations are assumed to have occurred 200, 300 and 520 days from the last incident.

The prior distributions were written as truncated normal distributions in terms of (mean,precision) as

alpha ~ dnorm(1404,0.00000335)T(0,1500)

beta ~ dnorm(1.011,24)T(0,2)

Initial values taken were

list(alpha=2,beta=0.5,t=c(NA,NA,NA,1.4445))

list(alpha=2,beta=1.5,t=c(NA,NA,NA,1.4445))

Data were converted from days to years since the parameters α and β (priors) were obtained for years of operation. Thus, the data was fed as .55556,.83333, 1.4444 (corresponding to 200, 300 and 520 days).

As usual, iterations were initially conducted to allow for convergence. The BGR statistics was used to check for convergence.

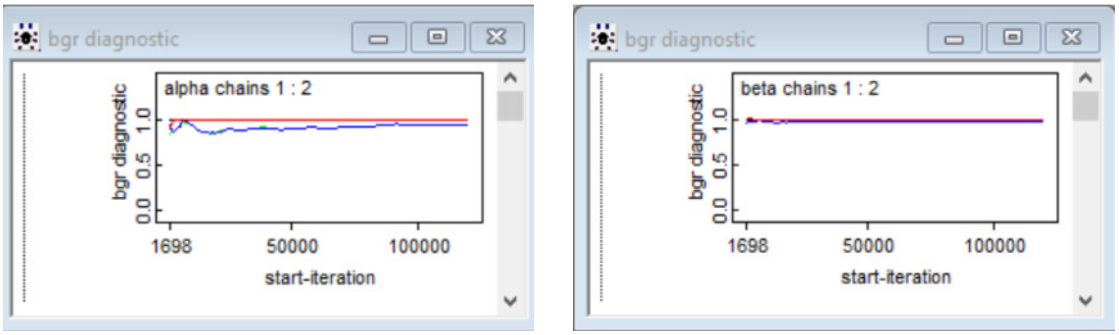


Figure 43: BGR statistics of updated hyperparameters α and β showing convergence

This time it took 240,000 iterations to achieve convergence. We run 80000 more iterations to obtained the parameters.

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1.061	1.167	0.02988	0.234	0.766	3.638	240000	80002
beta	1.065	0.1905	0.00245	0.6982	1.062	1.448	240000	80002
pr.p1	0.5193	0.22	0.002789	0.1181	0.5193	0.9188	240000	80002
pr.p2	0.7219	0.2194	0.003136	0.2212	0.7714	0.9944	240000	80002
pr.p3	0.8202	0.1936	0.003009	0.3104	0.8918	0.9997	240000	80002
pr.p4	0.8748	0.1681	0.00279	0.3887	0.9492	1.0	240000	80002
t[4]	2.125	1.115	0.01257	1.456	1.795	4.818	240000	80002

Figure 44: Computed data showing updated values of the hyperparameters α and β, probabilities and time to next failure for Procedural Deviation

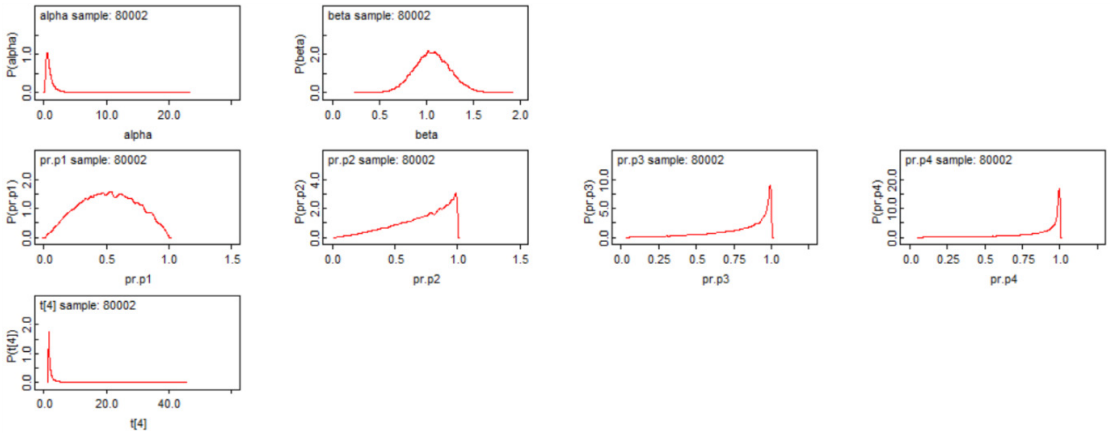


Figure 45: Distributions obtained for updated values of the hyperparameters α and β, probabilities and time to next failure for Procedural Deviation

From the data obtained, the next time to failure due to procedural deviation is expected to be (2.125×365)-520= 256 days after the last incident. We also note that as we make out data plant-specific, the parameter α changes drastically (from 1404 to 1.061), bringing the scale of the distribution in alignment with that of the facility itself. We assumed that we observed 3 procedural incidents in only 1.44 years of operation. This time between failures is extremely small compared to the thousands of years of operation we observed in the US OCS before an incident takes place. Hence, we have observed these incidents occurring way more frequently than is actually noticed in reality. The shape factor is also changed (from 1.011 to 1.065) indicating a worn out system where the procedural deviation is occurring within lesser time gap than before (frequency of failure is increasing). Thus, the management should focus on how to reduce procedural deviation.

Other factors can also be updated by this method.

5.5.2. Conversion to Near Miss data

As mentioned, our assumed observed data for updating Procedural deviation was a little offset because we were considering 3 major fire incidents occurring in a facility in a short period of time (1.44 years). Here the challenge arises that fire incidents are quite rare in offshore facilities and hence collecting data to update non-technical factors so that they reflect the condition of the organization would not be possible frequently. Just to provide an idea about the rarity of major incidents, we find that there were 86 fire and explosion incidents in 2016 in the US OCS out of 1900 facilities that were in operation during that time. A straightforward average gives a probability of fire incidents as 0.045 in a facility per year (equivalent to 1 fire incident in 22 years of operation). Thus, it becomes very difficult to assess changes in non-technical factors and requires a catastrophe to understand the change (which completely defies the purpose of a risk assessment). It becomes essential to find sources other than incidents to update our estimation.

A study of 1.75 million incidents reports from 297 organizations in 21 different industries found that for every major incident, there were 10 minor incidnts,30 property damage incidents and 600 no-loss incidents or near misses [142]. This forms the basis of Bird's triangle or Heinrich's triangle. For individual organizations or for regulators, it may be possible to collect data of near misses (incidents where the last barrier was challenged) and to conduct a complete and accurate analysis. For the purpose of this thesis, since we do not have the data of near misses, we assume that each major incident has 600 near miss incidents behind it.

The values estimated for each non-technical factor in the previous section were based on only those 137 fire incidents who investigation reports were available to us. We have assumed that data from these available reports are sample data from a larger population that encompasses all fire incidents that occur in the US OCS and that BSEE only investigates 'major' fire incidents. Then, each of these incidents will have approximately 600 near misses and the cumulative operational time before each failure are averaged to be 600 times less than computed in the previous section.

Below, the modified generic data used cumulative operation times to failures that lead to near-misses are provided for an example with Procedural Deviation.

5.5.2.1. Procedural Deviation with near miss data: Example

Data for near miss incident was obtained by diving the cumulative time to major incidents by 600 using Heinrich's major accident to near miss ratio. For convenience, the time was then converted to days from years.

Table 5: Assumed near miss data obtained for Procedural Deviation by taking ration of near miss to major incident as 600.

Incident number from the first incident noted after 01/01/2004	Cumulative time for procedural deviation to contribute to a near miss incident (days)
1	1176
2	2158
3	2442

Table 5: Continued

Incident number from the first incident noted after 01/01/2004	Cumulative time for procedural deviation to contribute to a near miss incident (days)
4	2654
5	3761
6	3972
7	4456
8	5084
9	6713
10	6751
11	7180
12	7294
13	7948
14	8710
15	10358
16	11317
17	11995
18	14099
19	14120
20	14352
21	14376

Table 5: Continued

Incident number from the first incident noted after 01/01/2004	Cumulative time for procedural deviation to contribute to a near miss incident (days)
22	15564
23	16113
24	16820
25	18500
26	19486

As before, the BGR statistics was checked and it was observed that using 40000 iterations for convergence was sufficient, as shown in Figure 46.

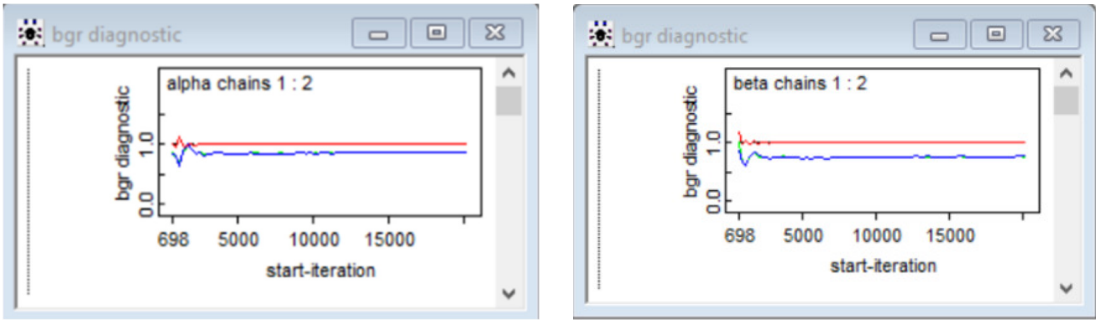


Figure 46: BGR statistics of hyperparameters α and β for near miss data showing convergence

Another 40000 iterations were run again for sampling data shown in Figures 47 and 48.

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	880.8	546.2	6.404	138.2	778.2	2200.0	40001	80000
beta	1.02	0.2027	0.002363	0.6622	1.007	1.449	40001	80000
pr.p1	0.2165	0.05381	5.764E-4	0.1229	0.2126	0.3318	40001	80000
pr.p2	0.3833	0.08332	8.983E-4	0.2306	0.38	0.554	40001	80000
pr.p3	0.5124	0.09745	0.001057	0.3247	0.5118	0.7029	40001	80000
pr.p4	0.6128	0.102	0.001111	0.4073	0.6156	0.8023	40001	80000
t[27]	20190.0	752.0	5.382	19500.0	19950.0	22220.0	40001	80000

Figure 47: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Procedural Deviation

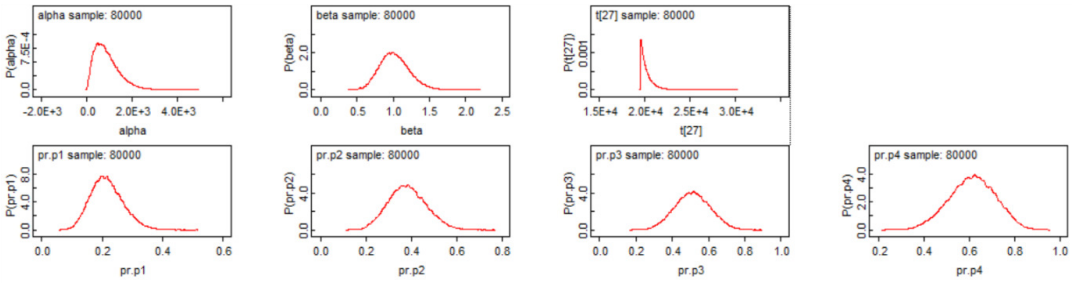


Figure 48: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Procedural Deviation

As can be seen in Figure 48, the shapes of the curves remain the same but the values have altered. Probability of failure leading to a near miss within the next 1 year (given by pr.p2) has a mean of 0.3833 whereas it was 0.2566 before when we were considering only the chances of a major incident where procedural deviation would be a contributor. This is in alignment with our assumptions that non-technical failures like that of procedural deviation occur frequently and although not all lead to major incidents, the probability value estimated is that of near miss where barriers have failed. Thus, using probability of non-technical failures from near miss data gives us more information about barrier conditions.

Results for other non-technical factors leading to near misses are provided next.

5.5.2.2. Design Flaw (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	744.5	542.3	10.47	64.02	625.6	2097.0	40001	40000
beta	0.9012	0.2018	0.003885	0.5473	0.8873	1.336	40001	40000
pr.p1	0.164	0.04766	7.405E-4	0.08452	0.1594	0.2695	40001	40000
pr.p2	0.2988	0.07863	0.00123	0.1617	0.2932	0.4667	40001	40000
pr.p3	0.4099	0.0978	0.001539	0.232	0.4057	0.6109	40001	40000
pr.p4	0.5019	0.1086	0.001721	0.2964	0.5001	0.7163	40001	40000
t[22]	19850.0	1031.0	10.78	18940.0	19530.0	22640.0	40001	40000

Figure 49: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Design Flaw

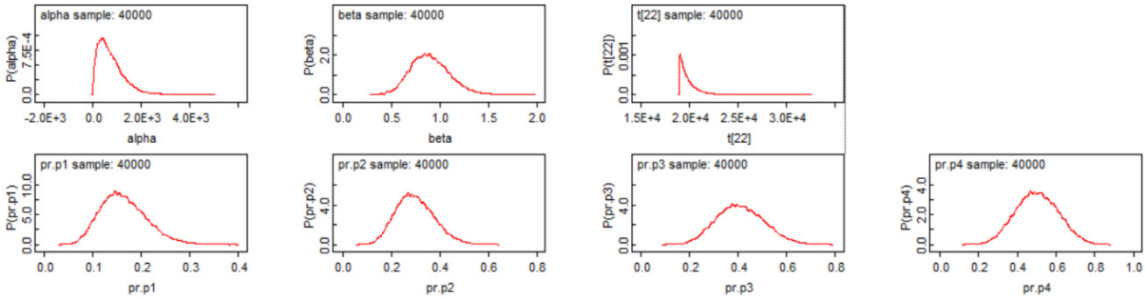


Figure 50: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Design Flaw

5.5.2.3. Degradation of Material (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1376.0	828.9	13.28	207.6	1239.0	3345.0	40001	40000
beta	1.112	0.2607	0.004019	0.6646	1.091	1.683	40001	40000
pr.p1	0.1913	0.05731	7.899E-4	0.09598	0.1859	0.3176	40001	40000
pr.p2	0.3428	0.09117	0.00126	0.1826	0.3375	0.5353	40001	40000
pr.p3	0.4636	0.1096	0.001519	0.2607	0.4608	0.6839	40001	40000
pr.p4	0.5602	0.118	0.001638	0.3312	0.5613	0.7854	40001	40000
t[20]	18950.0	889.9	8.779	18160.0	18670.0	21310.0	40001	40000

Figure 51: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Degradation of Material

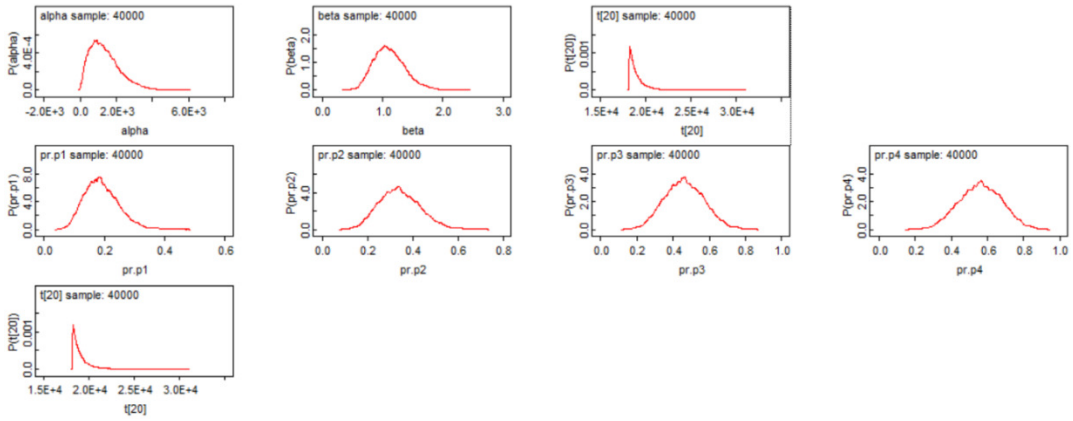


Figure 52: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Degradation of Material

5.5.2.4. Inadequate/Lack of Maintenance (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	582.3	334.5	5.616	116.7	518.4	1372.0	40001	40000
beta	1.014	0.1692	0.002815	0.7145	1.003	1.37	40001	40000
pr.p1	0.3012	0.06011	8.4E-4	0.1934	0.2976	0.4314	40001	40000
pr.p2	0.5081	0.08303	0.001166	0.3492	0.5067	0.6773	40001	40000
pr.p3	0.6513	0.08698	0.001227	0.4747	0.6535	0.8172	40001	40000
pr.p4	0.7511	0.08183	0.001159	0.5758	0.7566	0.8966	40001	40000
t[36]	18290.0	512.3	4.38	17820.0	18130.0	19670.0	40001	40000

Figure 53: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate/Lack of Maintenance

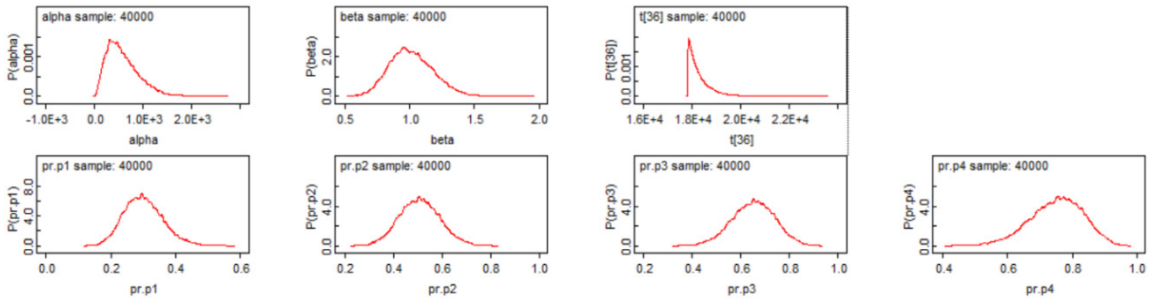


Figure 54: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate/Lack of Maintenance

5.5.2.5. Improper Procedure (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1402.0	720.7	11.42	309.2	1300.0	3039.0	40001	40000
beta	1.24	0.2458	0.003716	0.8066	1.223	1.766	40001	40000
pr.p1	0.2709	0.06447	8.684E-4	0.1577	0.2664	0.4077	40001	40000
pr.p2	0.4646	0.09286	0.001253	0.2906	0.4622	0.6502	40001	40000
pr.p3	0.6042	0.1014	0.001369	0.4023	0.606	0.794	40001	40000
pr.p4	0.7054	0.0994	0.001343	0.4963	0.7116	0.8791	40001	40000
t[27]	18950.0	599.0	5.738	18410.0	18760.0	20560.0	40001	40000

Figure 55: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Improper Procedure

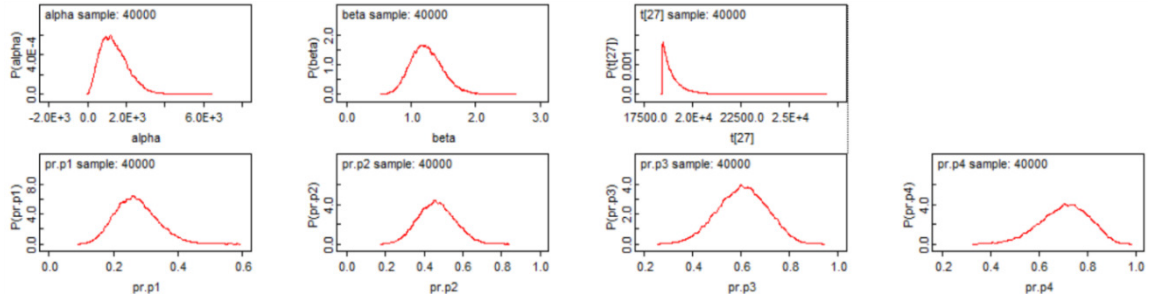


Figure 56: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Improper Procedure

5.5.2.6. Inadequate Supervision (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1647.0	1061.0	18.57	170.3	1469.0	4139.0	40001	40000
beta	1.073	0.3006	0.005266	0.5726	1.046	1.731	40001	40000
pr.p1	0.1418	0.05295	8.567E-4	0.05931	0.1351	0.2628	40001	40000
pr.p2	0.2609	0.08911	0.001449	0.1149	0.252	0.4573	40001	40000
pr.p3	0.3612	0.1131	0.001847	0.1671	0.3531	0.6012	40001	40000
pr.p4	0.4461	0.1284	0.002102	0.2161	0.4405	0.7076	40001	40000
t[14]	17730.0	1251.0	13.09	16650.0	17340.0	21090.0	40001	40000

Figure 57: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Supervision

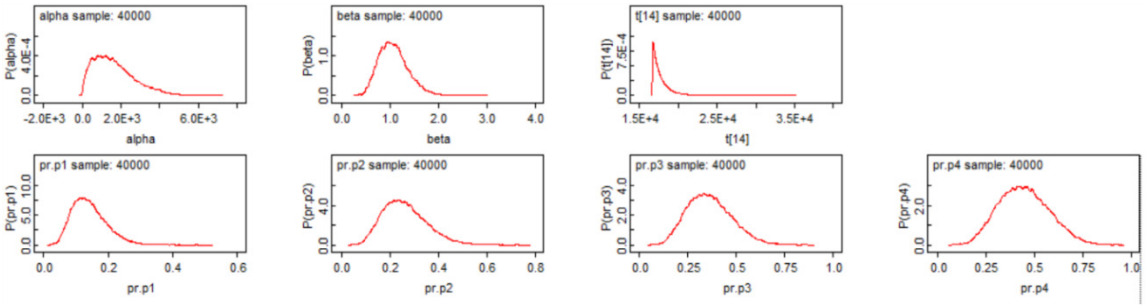


Figure 58: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Supervision

5.5.2.7. Inadequate Communication (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	2368.0	1208.0	19.23	458.8	2235.0	5084.0	40001	40000
beta	1.37	0.3526	0.005586	0.7714	1.338	2.147	40001	40000
pr.p1	0.2062	0.06679	9.735E-4	0.09646	0.1991	0.3587	40001	40000
pr.p2	0.3659	0.1037	0.001499	0.1835	0.3591	0.5903	40001	40000
pr.p3	0.4906	0.1221	0.001751	0.2621	0.4876	0.7392	40001	40000
pr.p4	0.5885	0.129	0.001838	0.3333	0.5906	0.8347	40001	40000
t[17]	18270.0	823.4	7.895	17520.0	1.8E+4	20520.0	40001	40000

Figure 59: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Communication

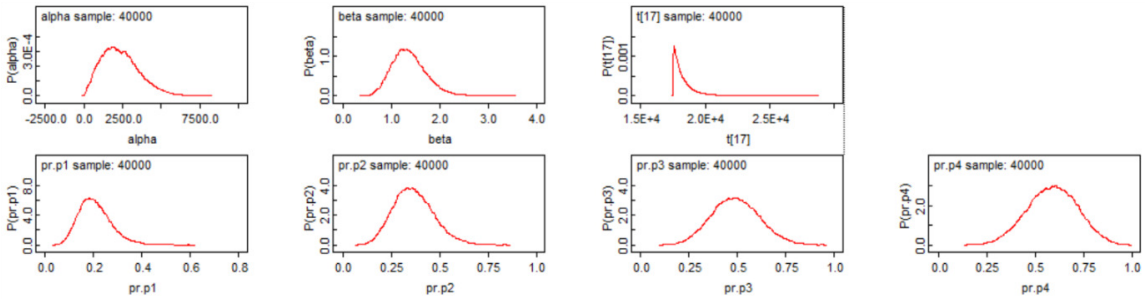


Figure 60: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Communication

5.5.2.8. Improper JSA (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	339.9	212.5	3.999	60.75	296.7	864.0	40001	40000
beta	0.9091	0.1371	0.00241	0.6607	0.9024	1.198	40001	40000
pr.p1	0.3071	0.05459	8.358E-4	0.2079	0.3053	0.4211	40001	40000
pr.p2	0.5168	0.07513	0.001156	0.3722	0.5172	0.665	40001	40000
pr.p3	0.6609	0.07827	0.00121	0.502	0.6645	0.8062	40001	40000
pr.p4	0.7606	0.07311	0.001135	0.6048	0.7667	0.888	40001	40000
t[45]	19960.0	494.1	4.712	19500.0	19810.0	21270.0	40001	40000

Figure 61: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Improper JSA

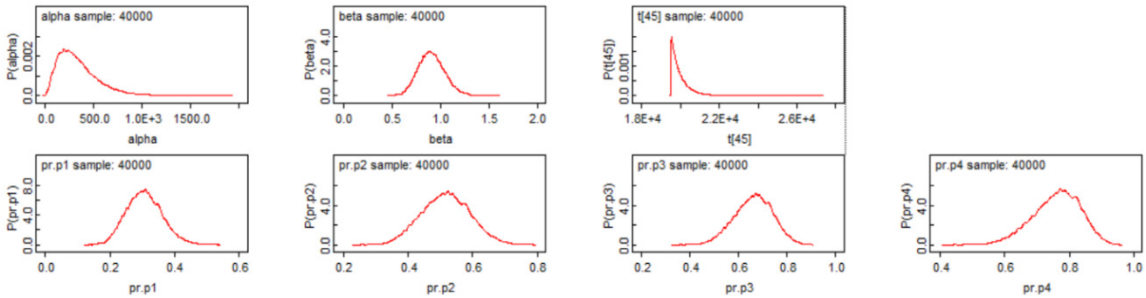


Figure 62: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Improper JSA

5.5.2.9. Failed to Detect (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	1669.0	1004.0	17.84	228.2	1496.0	4005.0	40001	40000
beta	1.136	0.2887	0.004804	0.6485	1.112	1.763	40001	40000
pr.p1	0.1686	0.05554	7.658E-4	0.0787	0.1627	0.2941	40001	40000
pr.p2	0.306	0.09072	0.001258	0.151	0.2992	0.5025	40001	40000
pr.p3	0.4183	0.1119	0.001559	0.2176	0.4135	0.65	40001	40000
pr.p4	0.5106	0.1234	0.001727	0.2789	0.5092	0.7541	40001	40000
t[17]	18860.0	1019.0	9.73	17950.0	18540.0	21630.0	40001	40000

Figure 63: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Failed to Detect

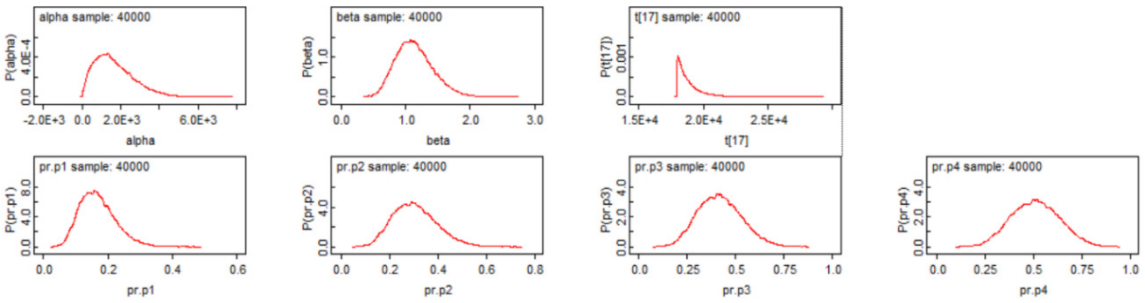


Figure 64: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Failed to Detect

5.5.2.10. Inadequate Isolation (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	658.8	377.1	6.912	133.4	589.4	1579.0	40001	40000
beta	1.02	0.1687	0.003009	0.7174	1.009	1.38	40001	40000
pr.p1	0.2772	0.05516	8.076E-4	0.1786	0.2736	0.3943	40001	40000
pr.p2	0.4746	0.07899	0.001161	0.3251	0.4724	0.6335	40001	40000
pr.p3	0.6159	0.08557	0.001262	0.4453	0.6168	0.7784	40001	40000
pr.p4	0.7177	0.08307	0.001228	0.5439	0.7216	0.8662	40001	40000
t[37]	20820.0	555.4	5.581	20310.0	20650.0	22330.0	40001	40000

Figure 65: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Isolation

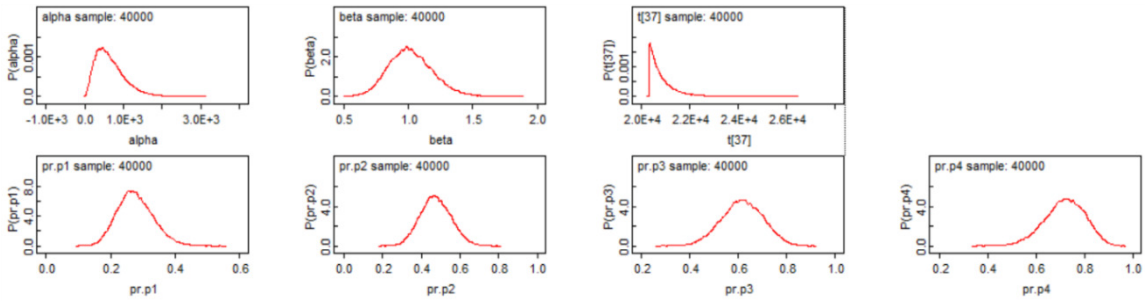


Figure 66: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Inadequate Isolation

5.5.2.11. Contact with Hot Surface (Ignition source) (leading to near miss)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	528.5	259.4	3.939	145.3	489.3	1151.0	40001	40000
beta	1.078	0.1413	0.002029	0.8202	1.072	1.372	40001	40000
pr.p1	0.4084	0.057	7.231E-4	0.3013	0.4072	0.5245	40001	40000
pr.p2	0.6469	0.06734	8.646E-4	0.5116	0.6487	0.7743	40001	40000
pr.p3	0.7874	0.06047	7.862E-4	0.6585	0.7919	0.8931	40001	40000
pr.p4	0.8709	0.04889	6.441E-4	0.7611	0.8767	0.9494	40001	40000
t[60]	22010.0	343.4	3.146	21690.0	21900.0	22950.0	40001	40000

Figure 67: Computed data showing values of the hyperparameters α and β, probabilities and time to next failure using near miss data for Contact with Hot Surface

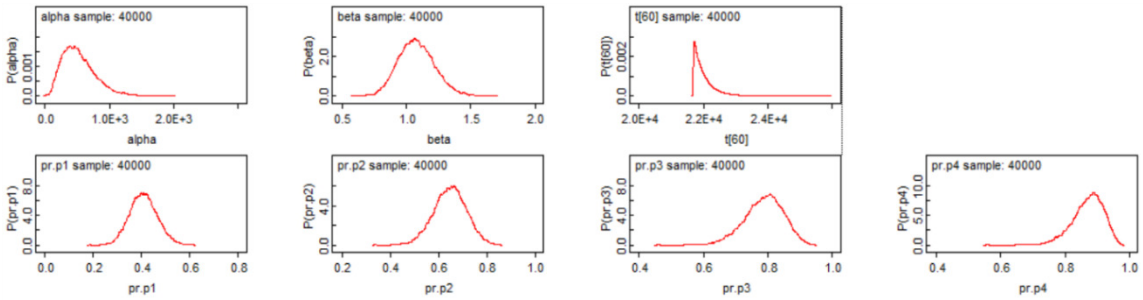


Figure 68: Distributions obtained for hyperparameters α and β, probabilities and time to next failure using near miss data for Contact with Hot Surface

Figures 49, 51, 53, 55, 57, 59, 61, 63, 65 and 67 provides the results obtained from the MCMC sampling obtained using the data for various contributing factors from Table 5. They show the various parameters such as mean, standard deviation, median and the boundaries for the 95% confidence interval. Figures 50, 52, 54, 56, 58, 60, 62, 64, 66 and 68 shows the distribution of the hyperparameters and the probabilities of failures based on near miss data for a facility. The distribution of the predicted time to next failure is also shown.

5.5.3. Updating Near Miss data with Plant-Specific data

The values (mean and standard deviation) of α and β obtained as posterior in the generic data are now used as prior for updating with evidence specific to the plant. We apply same methodology we showed before in Section 5.5.1, except that we use the posteriors we obtained from using near miss data in days. Near misses are to be investigated to determine the contribution from non-technical factors.

5.5.3.1. Updating non-technical factor (Procedural Deviation) using generic near miss data: Example

Like before, we assume that we observed Procedural Deviation in investigated near-misses and/or incidents in the following cumulative times since the last failure: 200, 300 and 520 days.

The posterior values of (mean, standard deviation) of α and β were (880.8,546.2) and (1.011,.2012) respectively. The standard deviations were converted to precision.

Input:

alpha ~ dnorm(880,0.000003352)T(10,1000)

beta ~ dnorm(1.02,24)T(0,10)

Initial values:

list(alpha=15,beta=0.5,t=c(NA,NA,NA,521))

list(alpha=15,beta=1.5,t=c(NA,NA,NA, 521))

Convergence was achieved within 40000 iterations. A further 40000 iterations were run to obtain sample data:

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	376.8	211.9	3.605	97.53	325.2	890.1	40001	40000
beta	1.082	0.1897	0.002466	0.714	1.081	1.463	40001	40000
pr.p1	0.4893	0.2066	0.003242	0.1708	0.4681	0.9011	40001	40000
pr.p2	0.6986	0.204	0.003321	0.3097	0.7212	0.9914	40001	40000
pr.p3	0.8064	0.174	0.002871	0.4227	0.855	0.9993	40001	40000
pr.p4	0.8686	0.144	0.002387	0.5148	0.9252	1.0	40001	40000
t[4]	759.2	326.7	3.945	524.5	655.0	1634.0	40001	40000

Figure 69: Updated data showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Procedural deviation occurred

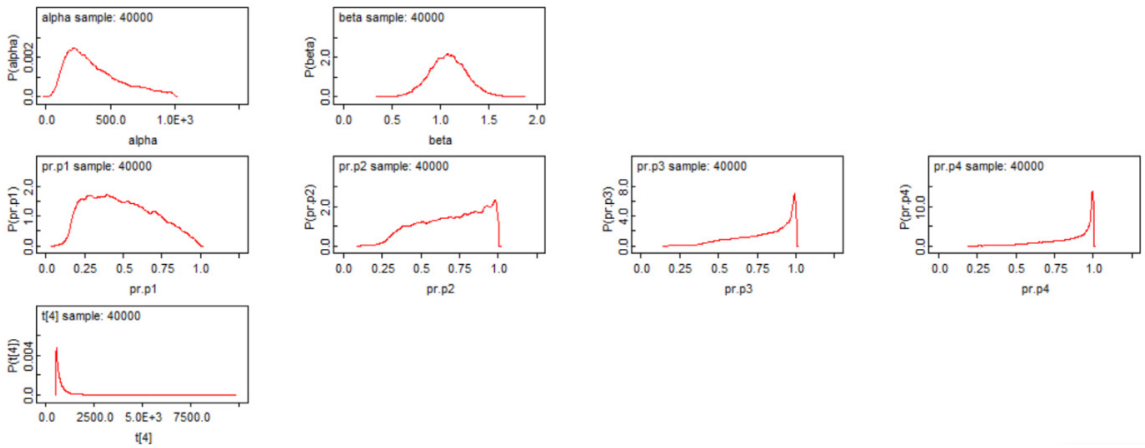


Figure 70: Distributions showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Procedural deviation occurred

Time to next failure was predicted to be 759-520=239 days after the last recorded near-miss/incident. Compared to Figure 47, this is lesser than the generic time to failure which was 20190-19486= 704 days. This is in accordance with what the value of β indicates. If β>1, it indicates a worn-out system where incidents are occurring more

frequently. A decrease in the time to next failure is due to this. Based on procedural deviation, this organization's performance is worse than the industry average.

5.6. Summary

This chapter provides methodologies for generation of generic data for non-technical factors and for subsequent updating of the data to make it plant specific. An interesting find in this section is that in the development of generic data, since total operation time in the entire US OCS is considered, it gives a good estimate about the overall performance of the facilities over time in this region. Since the total number of facilities vary with time, year by year, so does the total operation time. Because number of incidents have been expressed in terms of number of calendar years, it has always been a challenge to understand the trend of incidents. The total operation time, in contrast to calendar time, provides a normalization based on the amount of operation conducted in this region and thus provides a better understanding of whether any particular non-technical factor has an increasing or a decreasing trend. The trend can be understood from the value of β.

- If $\beta<1$, the factor is seeing 'reliability growth', meaning that time between failures are growing with time, indicating better performance.
- If $\beta>1$, it indicates a worn-out or an 'ageing' system, meaning that the performance had gotten worse with time and failures are being more frequent with passage of time.

From the analysis of the data, we see that factors Design flaw and Improper JSA are the only two factors for which $\beta<1$. This indicates that with time, flaws in design has reduced and that identification of hazards in job safety analysis have gotten better. As for the other factors, measures need to be taken to identify how to improve them.

The mean values of β obtained from the data can thus indicate which factors are leading to more fire incident in the US OCS and which factors have improved over time, giving the regulatory body an indication of where to focus their efforts.

BSEE conducts a large number of incident investigations every year. Proper data collection from these investigations can allow generation of precise generic data for non-technical factors. Facilities can make use of it and update their data to have a better understanding of their own system. Operating companies themselves can develop methods to investigate near misses to identify failure of the non-technical factors and assess their own risks. Several companies can join hands to share their experience and data to develop their own generic data that each company can update and have precise understanding of their laggings.

6. ESTIMATION OF THE IMPORTANCE OF EACH COMBINATION OF NON-TECHNICAL FACTORS

6.1. Background

In order to predict the risk of fire in a facility, it is important to understand the condition or failure probability of each individual factor and also to determine their interdependency to understand how their individual failures interact with each other. One of the greatest challenges of incorporating non-technical factors into risk assessment models is to establish how these factors are to be brought together for computation of risk. Some may be influenced by a common cause; some factors may have a stronger influence on causing system failures than others and so on. Traditional fault trees only consider linear interaction of the failures but where non-technical factors are involved in a complex system, their interaction may well be non-linear [143].

In this chapter we establish a method by which the learning from past incident analysis is utilized to determine how multiple factors interacted with each other that led to a fire incident. For this we consider all possible combinations of the factors, and determine weightage of each combination by counting the number of incidents that occurred due to each combination.

6.2. Determining weightage of each combination of factors

Fire incidents analyzed in Chapter 4 varied from each other in the combination of the different contributing factors that led to the incident. Some combinations were more common than others. All possible combinations of contributing factors and a relative probability of their occurrence to each other can be determined from the analysis conducted. This relative probability, or weightage provides a comparison of the importance of each combination in a risk assessment. As shown in Figure 14, for each incident analyzed, we had marked occurrence of contributing factors as 1 and its absence as 0 (making their occurrences Boolean). In the end, we could sum up to get the number of occurrences of each combination. This, divided by the total number of incidents studied gives us the weightage of each combination.

Thus, if A and B are the only two contributing factors considered, weightage is given by

$$w(A=a, B=b) = \frac{Number\ of\ incidents\ where\ A=a\ and\ B=b}{total\ number\ of\ incidents}$$

where a and b are Boolean (can be either 1 or 0). For n number of non-technical factors, we can have 2^n combinations (since their occurrences are Boolean).

For our case study to be developed in the next chapter, we will consider only a few of the contributing factors for simplicity. As shown in Chapter 4, multiple factors occur in conjunction with equipment failure. We consider only the top three factors, which are Inadequate/Lack of Maintenance, Degradation of Material and Design flaw. With 3 contributing factors, we get 2^3= 8 combinations. We ignore those incidents where other factors contributed, so the combination where the three factors considered do not

appear are taken to be zero. We note that there were in total 69 incidents where Equipment failure was found, out of which 44 had one or more of the three non-technical factors considered. Among these 44 incidents, the counts of the various combinations are provided in Table 6 with the respective computed weights.

Table 6: Counts and weights for various combinations of three non-technical factors contributing to equipment failure are shown.

Combination No.	Inadequate/Lack of Maintenance	Degradation	Design Flaw	Count	Weight
1	1	1	1	2	0.045
2	1	0	1	2	0.045
3	1	1	0	8	0.182
4	1	0	0	16	0.364
5	0	1	1	2	0.045
6	0	0	1	9	0.205
7	0	1	0	5	0.114
8	0	0	0	0	0.000
Total				44	1.000

From the analysis in Chapter 4, it was also noted that in a large portion of the incidents, non-routine tasks led to fire incidents. Risk assessment models should consider their contribution apart from just equipment failure during routine operations.

For the case study, we will consider Procedural deviation, Inadequate/Improper Procedure, Inadequate supervision and Improper job safety analysis (JSA) as the contributing factors only. The factors Procedural deviation and Inadequate/Improper procedure are combined together as Procedure related for sake of simplicity. The weights of these factors in the 137 fire incidents are provided below in Table 7. We ignore those incidents where none of the considered factors occurred (others did) for simplification.

Table 7: Counts and weights for various combinations of four non-technical factors contributing to incidents during non-routine operations are shown

Combi-nation No.	Procedure Related	Improper JSA	Inadequate Communi-cation	Inadequate Supervision	Count	Weight
1	1	1	1	1	1	0.018
2	1	1	1	0	1	0.018
3	1	1	0	1	4	0.070
4	1	1	0	0	15	0.263
5	1	0	1	1	0	0.000
6	1	0	1	0	5	0.088
7	1	0	0	1	2	0.035
8	1	0	0	0	10	0.175
9	0	1	1	1	3	0.053

Table 7: Continued

Combi-nation No.	Procedure Related	Improper JSA	Inadequate Communi-cation	Inadequate Supervision	Count	Weight
10	0	1	1	0	2	0.035
11	0	1	0	1	1	0.018
12	0	1	0	0	12	0.211
13	0	0	1	1	0	0.000
14	0	0	1	0	0	0.000
15	0	0	0	1	1	0.018
16	0	0	0	0	0	0.000
Total					57	1

Hot work operations provided a significant ignition source that led to a large number of incidents. Other non-technical factors were seen to contribute to this. The top three factors were Inadequate Isolations, Improper JSA and Procedural Deviation. We determined the weights of the various combinations of these factors where hot work was a source of ignition (Table 8).

Table 8: Counts and weights for various combinations of three non-technical factors contributing to ignition during hot work are shown

Combination Number	Inadequate Isolation	Improper JSA	Procedural Deviation	Count	Weights
1	1	1	1	3	0.094
2	1	1	0	13	0.406
3	1	0	1	1	0.031
4	1	0	0	6	0.188
5	0	1	1	4	0.125
6	0	1	0	3	0.094
7	0	0	1	2	0.063
8	0	0	0	0	0.000
Total				32	1.000

6.3. Summary

The various ways contributing factors can interact with each other and lead to an incident have been addressed in this chapter. The weights represent the non-linear interaction that can arise from such interaction.

Certain combinations have 0 weight, meaning they did not appear in any incident observed. For non-routine operations, we found 26 incidents where none of the factors considered contributed. For equipment failure, there were 25. If we were to consider more and more contributing factors, this number would have eventually reduced to zero.

The combinations and corresponding weights obtained can now be used to merge all factors for a cumulative risk assessment.

7. DEVELOPMENT OF BARRIER ANALYSIS MODEL TO ASSESS CUMULATIVE RISK

7.1. Background

We have determined the individual probabilities of failure of non-technical factors (Chapter 5) and determined the way they depend on or combine with each other to lead to an incident (Chapter 6). We now use this information to merge all factors to assess the cumulative risk of barrier failure.

AND-gates and OR-gates a for continuous probability distributions are computed using the equations shown in Table 9 [144].

Table 9: Table showing equations for calculating probabilities of factors connected by AND-gate and OR-gate.

AND-gate	$P_N = P_{N1-1} \cdot P_{N2-1} \cdot \ldots P_{Ni-1}$
OR-gate	$P_N = 1- (1- P_{N1-1}) \cdot (1-P_{N2-1}) \cdot \ldots (1- P_{Ni-1})$ (Approximated as $P_N = P_{N1-1}+P_{N2-1}+\ldots P_{Ni-1}$)

where N1, N2…Ni are the parent nodes of the child node N.

The factors present in any particular combination are to be combined as -AND gate (their probabilities are multiplied) as shown:

$$P_{ANDj}=P_1.P_2\ldots P_i \quad (1)$$

where i is the number of factors contributing in the combination j. This gives the probability of occurrence of a particular combination.

Each combination is then merged with another through an -OR gate with weightage of each combination. The weightage gives an estimate of the averaged probability that a particular combination may cause the incident:

$$P_{\text{System Failure}} = 1 - \prod_1^j [1 - \omega(j) P_{ANDj}] \quad (2)$$

where i is the number of combinations, and ω is the weight of combination j.

An approximation of Equation (2) is given as

$$P_{\text{System Failure}} \sim \sum_j [\omega(j) P_{ANDj}] \quad (3)$$

The utilization of weights is similar to that proposed in the BORA model, except that in that case, the weights were determined by experts and the probabilities were replaced by the score of the risk influencing factors (RIFs) which were also obtained from aggregated expert opinion [11, 90].

An -OR gate and the -AND gate can be modelled in OpenBUGS, but using the free Bayesian Network software GeNIE proved much simpler [66] .

An analysis of barrier failure probabilities would require development of a method to assess all conditions that lead to failure of each barrier and how failure of individual barrier then leads to a consequence. For this purpose, an example of a release scenario from an offshore separator has been adopted from literature and the details are provided below.

7.2. Case Study

An offshore oil/gas separator is considered for the case study. Failure of the separator can cause release of hydrocarbons, which, if not detected, can find an ignition source and lead to fire. For simplicity, only three barriers are considered:

- Release Prevention Barrier: Its failure causes loss of containment for the flammables from the separator
- Detection Barrier: This enables early detection of the loss of containment/release of hydrocarbon, and
- Ignition Prevention barrier: This ensures no ignition source is present when the loss of containment occurs so that the released flammables may not ignite.

An event tree was developed with each fault tree connected to its pivotal points. The consequences for the failure of each barrier were categorized according to severity.

7.2.1. Release Prevention Barrier:

In an offshore production platform, gas from wellhead manifold are processed in two identical separators to separate out the condensate before being passed through a gas compressor manifold [110]. One of the separators are shown in Figure 71. Pressure buildup within the separator can cause the separator to rupture, releasing hazardous flammable gases onto the platform. Valves are installed to prevent such a situation and hazards must be analyzed to understand how failure of these valves may lead to a release.

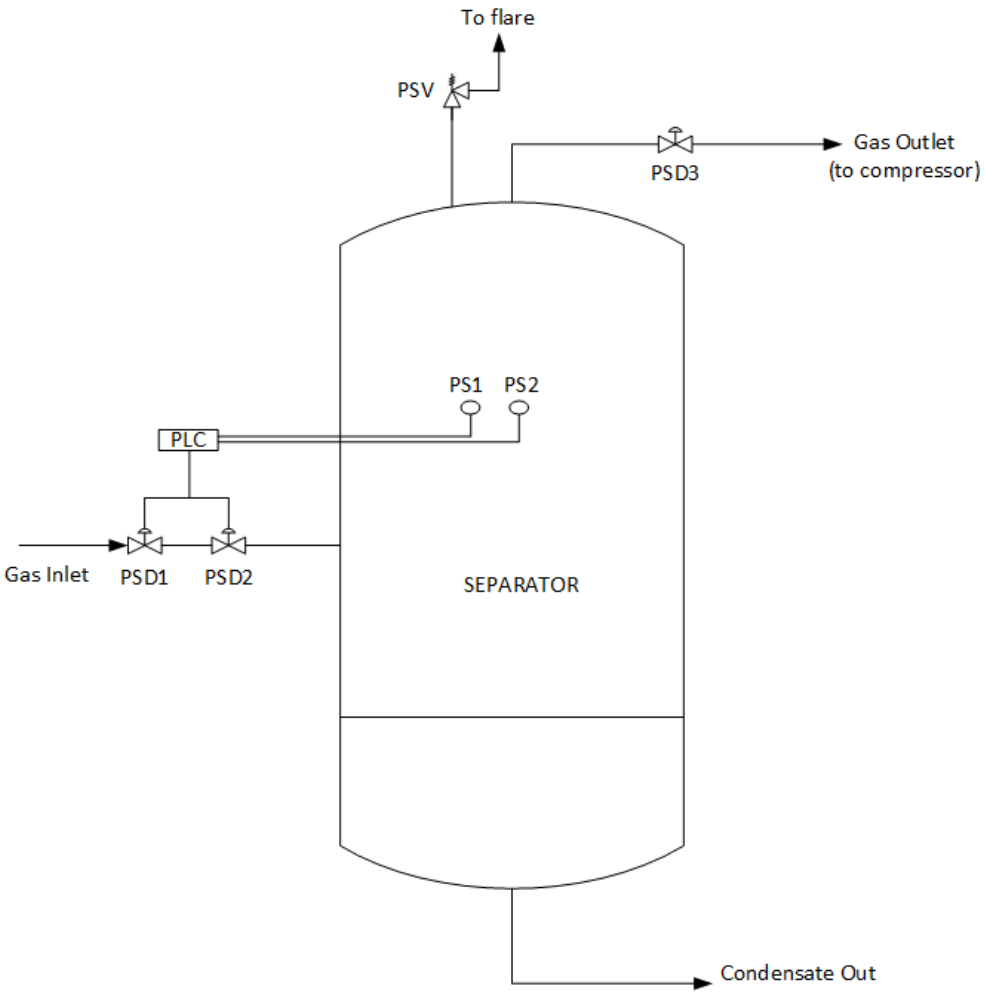


Figure 71: A simplified schematic diagram of an offshore oil-gas separator (Figure adopted from Rausand, M. and H. Arnljot, *System reliability theory: models, statistical methods, and applications*. Vol. 396. 2004: John Wiley & Sons)

As shown in the Figure 71, the gas inlet pipe coming from the wellhead has two process shutdown valves PSD1 and PSD2 installed in series. These valves are held open by hydrostatic pressure and are designed to fail close in case of emergency. Another similar valve PSD3 is installed at the outlet pipe from the separator. A pressure safety

valve, PSV is installed to relieve any excess pressure buildup within the separator and is designed to open if this pressure goes beyond a set point p.

Due to the fail close design of the PSDs, they may close spuriously. If PSD3 fails close spuriously, this may lead to a rapid rise in pressure within the separator. Pressure switches, PS1 and PS2 are installed to independently monitor the pressure within the separator and in case the pressure rises to p_1, which is less than p, the switches will send a signal to the Programmable Logic Controller, PLC, which uses as 1-out-of-2 voting logic to close the valves PSD1 and PSD2. Hazard may also increase if the PSD1 and PSD2 fails to close on command. If all control system fails and the pressure in the separator exceed p, the PSV may activate to relieve off the pressure. If the PSV fails, then the separator is subject to overpressure and may rupture and release flammable gases.

Apart from the inherent failure tendency of the individual components, failure probabilities are also influenced by the extent of maintenance conducted. There can be a lack of maintenance, or the maintenance work done may have not been completed properly. At the same time, degradation of material also influences the failure probabilities of the equipment or its connections. There have been many incidents where design flaw has led to early failure of a component and thus a release was noted. These factors are taken to directly influence the failure probabilities of the components along with their inherent failure tendency. Weights give an idea of the extent to which each factor influences the overall system failure probability.

As a further modification to the hazard analysis, it is noted that release of hydrocarbons from the separator may not occur solely due to overpressure, but may also be caused by a structural failure or due to mistakes made during non-routine operations such as maintenance. The fault tree shown in Figure 72 provides a graphical representation of this. Structural failure may arise due to degradation of the wall arising from say, corrosion. It may also occur due to impact that may lead to a sudden release. In our analysis of incidents, such causes of structural failure were not seen and will not be considered in our risk assessment (hence they have been drawn in a lighter shade). We only consider failure from non-routine operations such as maintenance work, including hot work because they were frequently found to lead to hydrocarbon releases. Determination of the weights of combinations in Chapter 6 provided a background for understanding which factors were more likely to cause failure and hence were incorporated in the fault tree.

Connection to the non-technical factors are shown with gray-dotted lines to represent influence on component, and not direct failures.

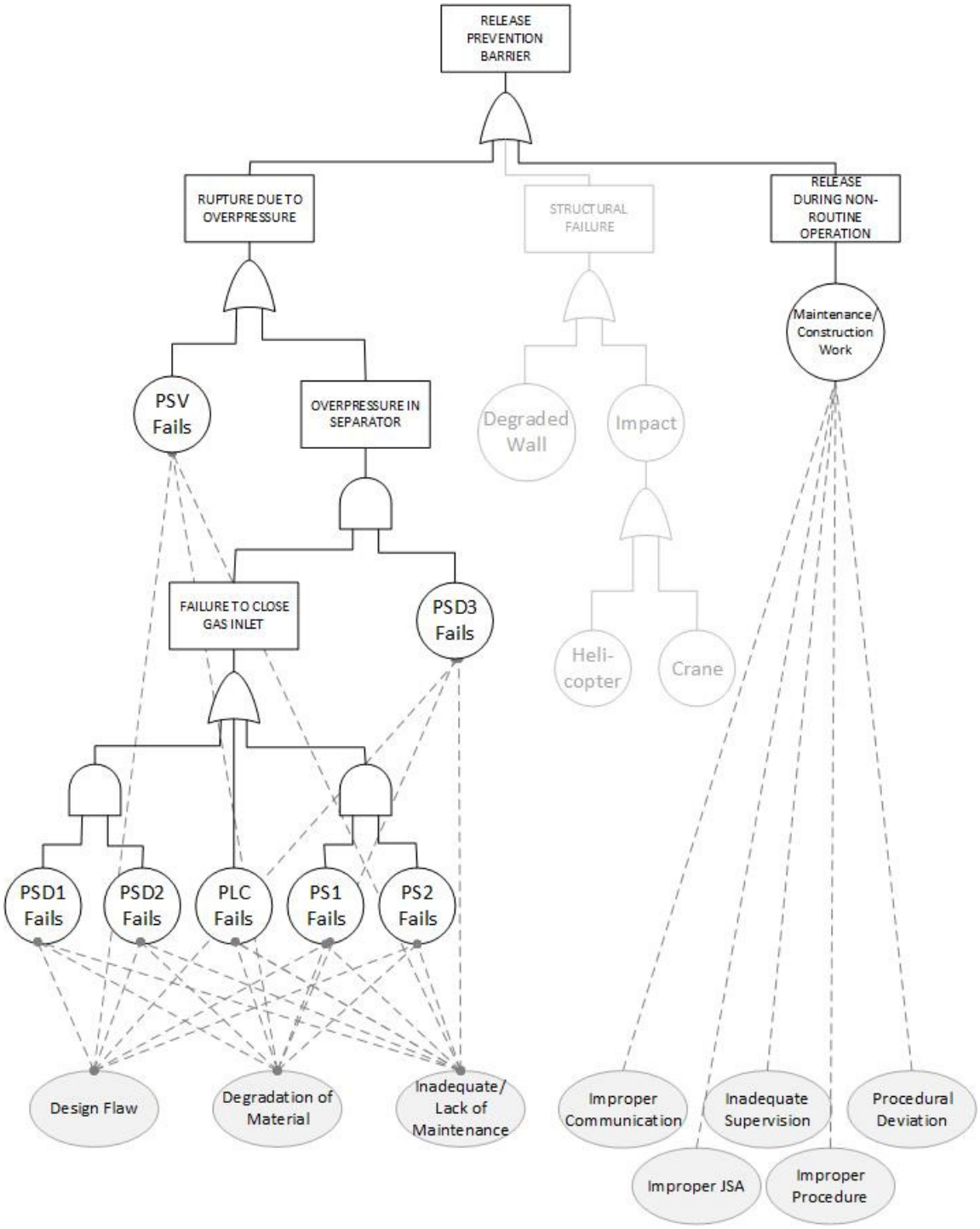


Figure 72: Release Prevention Barrier with influence from non-technical factors

7.2.2. Detection Barrier:

A detection system is likely to be available on an offshore gas production platform to detect any unwanted release of flammable gases before it ignites. The fault tree for an offshore gas detection system is shown below in Figure 73 along with the non-technical factors. Inadequate maintenance of detectors, improper placement etc. contributed to their failure. During non-routine operations, it was found that operators failed to detect the release of hydrocarbons. That too was considered in this barrier.

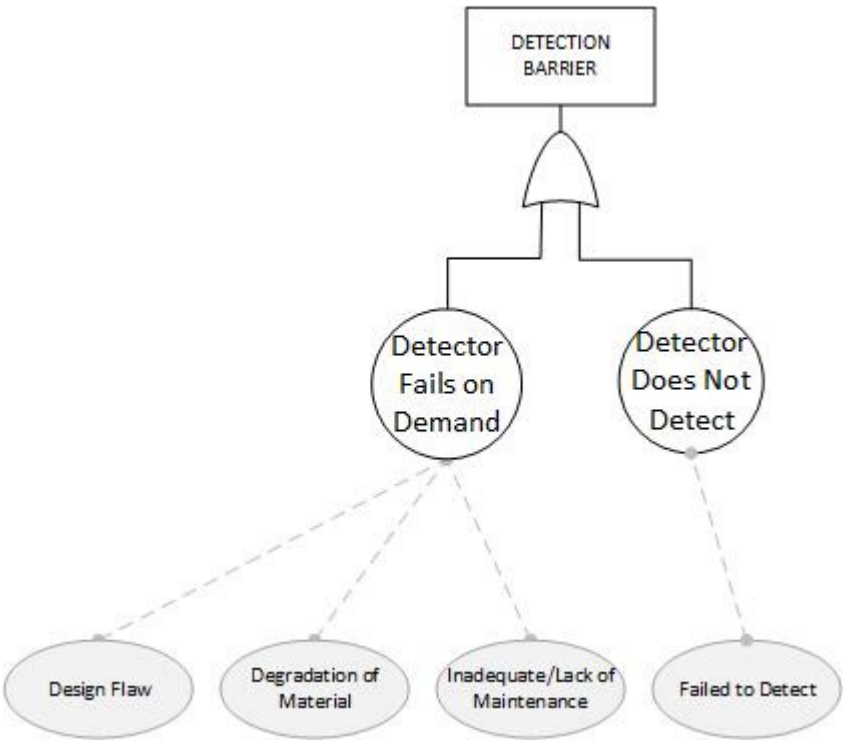


Figure 73: Hydrocarbon Detection Barrier with influence from non-technical factors

7.2.3. Ignition Prevention Barrier:

Several common ignition sources were identified from the investigation report analysis. These included heat sources from hot work, heated equipment surface, static electricity, lightening and electric arcs due to equipment malfunction. Only the hot work and the heated surface sources are considered in the failure of the ignition barrier. As shown in Figure 74, inadequate isolation along with inadequate JSA and procedural deviation play a crucial role in this barrier's success.

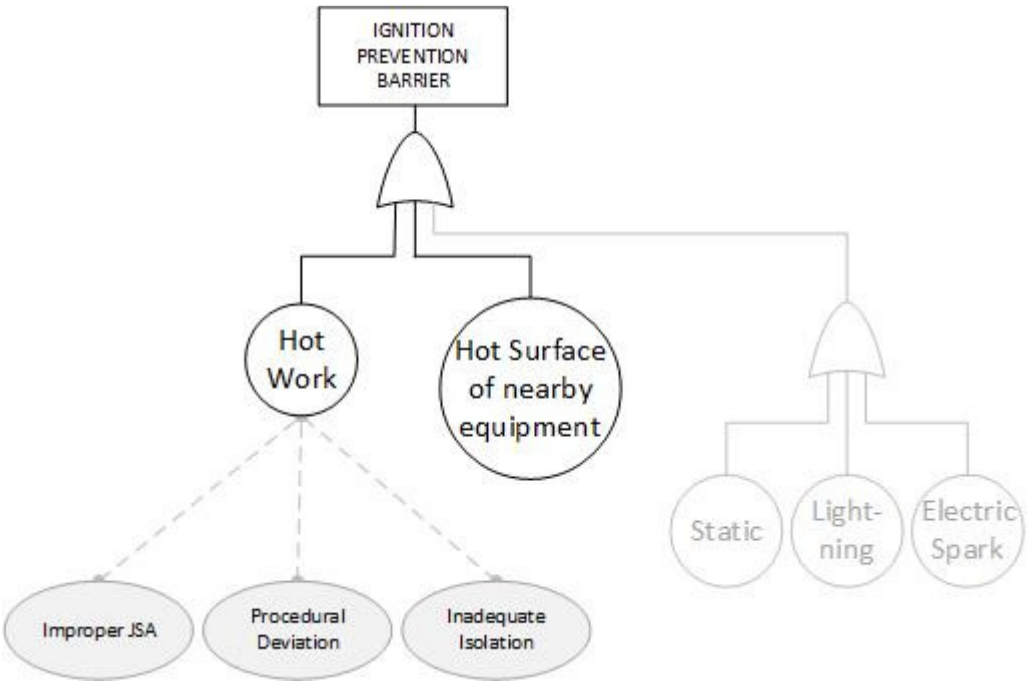


Figure 74: Ignition Prevention Barrier showing influence from non-technical factors

7.2.4. Event Tree:

In the event tree, each pivotal point is taken as a barrier as shown in Figure 75. Initiating event frequencies are not required since we are monitoring only the barriers health conditions (the top event of each fault tree), but if it can be assigned, then the event tree will allow determination of the probabilities of each consequence which are defined next. When all three barriers fail, it is termed a catastrophe. In case only one barrier is safe, and the remaining fails, it is termed a near miss (near-miss can be defined as 'only one barrier did not fail and was challenged'). In case only one barrier failed and the others functioned, it is termed an event. If all the barrier is functioning, then it is a safe operation.

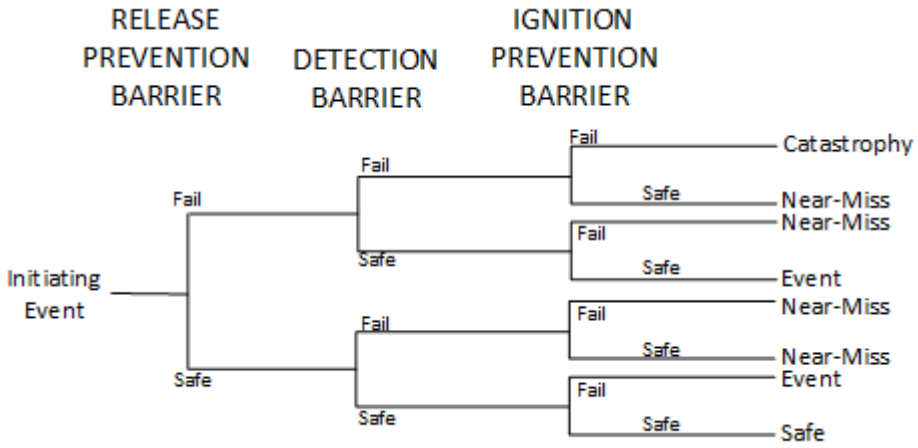


Figure 75: Event tree for separator

7.2.5. Mapping fault trees and event trees into Bayesian Network

The fault trees and event trees developed in the previous sections were combined and mapped into a Bayesian Network in GeNIe [66] as shown in Figure 76.

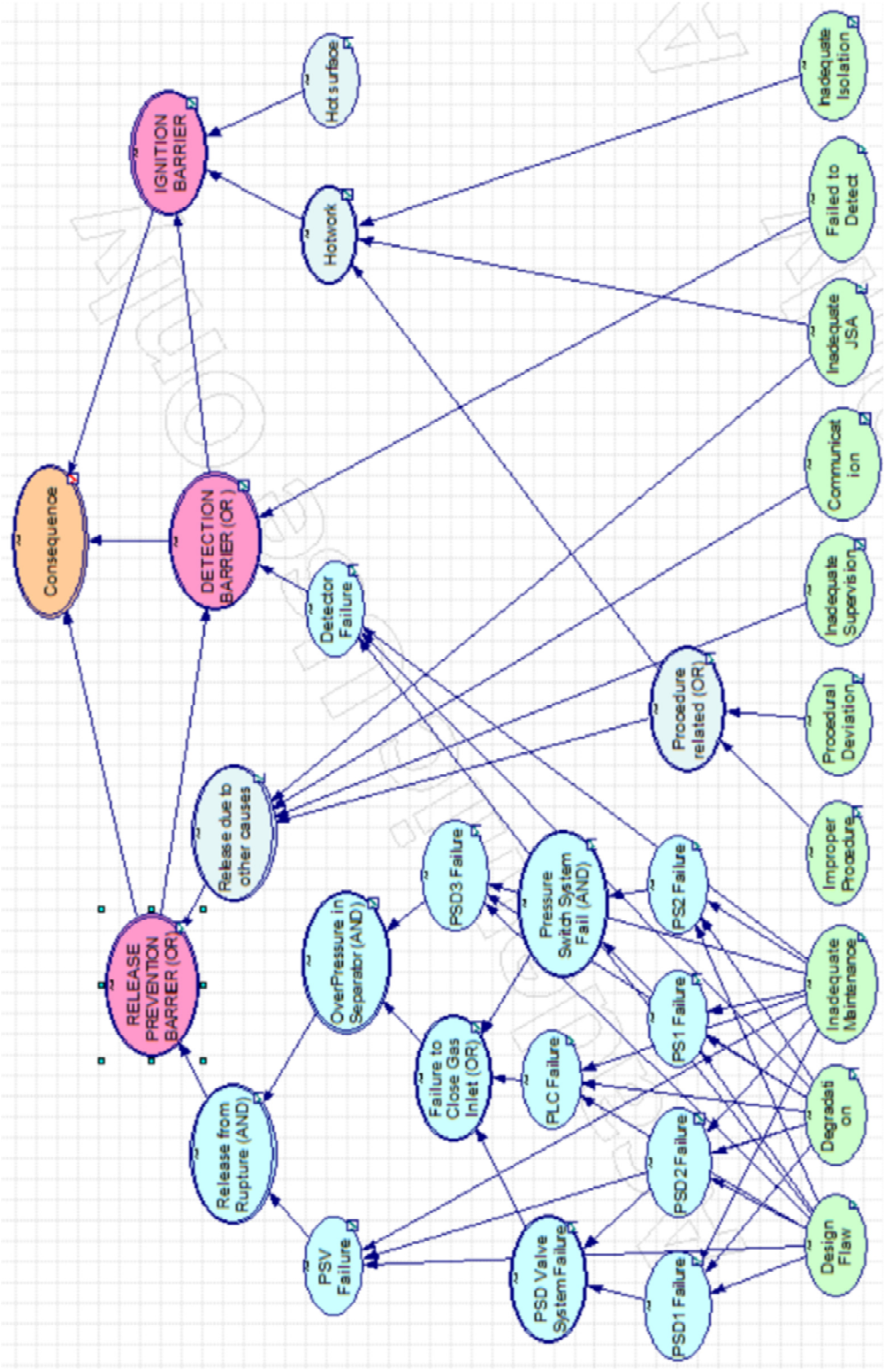


Figure 76: Bayesian Network for assessing cumulative risk of fire in Case Study

For the non-technical factors, values of 'pr.p2' were taken for near miss data of each factor. This value was taken since it corresponded to failure probability at the end of next year. Nodes for non-technical factors were modelled in GeNIE with truncated normal distributions.

Data for equipment failure rates were taken from the OREDA Database Handbook [131]. Failure rates were converted to failure probabilities with time set to 1 year.

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

Thus, we were able to obtain the distribution of the failure probability of an equipment component using the mean and thee standard deviation provided.

Table 10: Mean and standard deviation of probability of failure of various equipment described in the Case Study

	Mean probability of failure in the next 1 year	**Standard deviation of the probability of failure in the next 1 year**
PSD Valve (PSD1)	2.275E-01	1.867E-01
PS System (PS1)	2.926E-02	2.286E-02
PSV	1.901E-02	2.365E-02
PLC	4.073E-02	2.137E-02
Detector	9.636E-03	2.935E-02

Equipment failure probabilities were modeled in GeNIE with truncated normal distributions also.

Equations (1) and (2) were used to determine the failure probabilities of the child nodes where non-technical factors were the parent nodes. These child nodes were PDS1, PSD2, PSD3, PS1, PS2, PLC, PSV, Detector, Non-routine Operations, and Hot Work nodes.

For non-technical factors influencing failure of equipment, equations were written using the weights given in Table 6. For example, the equation for the node of PDS1 failure was:

PSD1_Failure=1-(1-TruncNormal(0.2275,0.1867,0))*(1-(0.045*D*M*DG+0.045*D*M+0.182*M*DG+0.364*M+0.045*D*DG+0.205*D+0.114*DG))

Here D, M and DG represent the nodes Design Flaw, Inadequate/Lack of Maintenance and Degradation of Material respectively.

System failure arising from the contributing non-technical factors are added using respective weights to the generic failure data of the equipment. This is done because the equipment can fail due to its inherent properties or due to contributions from non-technical factors. Thus, their probabilities are added.

Using weights from Table 7, the node for Release from Non-routine Operation was written as:

Release_due_to_other_causes_=(0.0175*P*S*J*C)+(0.0175*P*J*C)+(0.07*P*J*S)+(0.263*P*J)+(0.088*P*C)+(0.035*P*S)+(0.175*P)+(0.053*S*J*C)+(0.035*J*C)+(0.018*S*J)+(0.211*J)+(0.018*S)

Here, P, J, S, C refers to Procedure Related, Improper JSA, Inadequate Supervision, Inadequate Communication respectively. The node Procedure Related is an OR-gate that brings together the nodes Procedural Deviation and Improper Procedure.

The equation for node Hot Work was written using Table 8 in a similar manner:

Hotwork=(0.09375*I*J*P)+(0.406*I*J)+(0.03125*I*P)+(0.1875*I)+(0.125*J*P)+(0.09375*J+0.0625*P)

The purpose of the work is to analyze each of the barriers. We also add a consequence node to determine the probability of an incident occurring when all barriers fail. This is given by and AND-gate:

Consequence=RPB*DB*IB

where RPB, DB and IB refers to the release prevention barrier, the detection barrier and the ignition barrier respectively.

Once the Bayesian Network was developed it was run to generate results.

7.2.5.1. Result of Case Study

The resulting probability distributions of each node is shown in Figure 77. Closer view of the probability distribution and parameter information of each barrier and the consequence is provided in Figures 78,79,80 and 81.

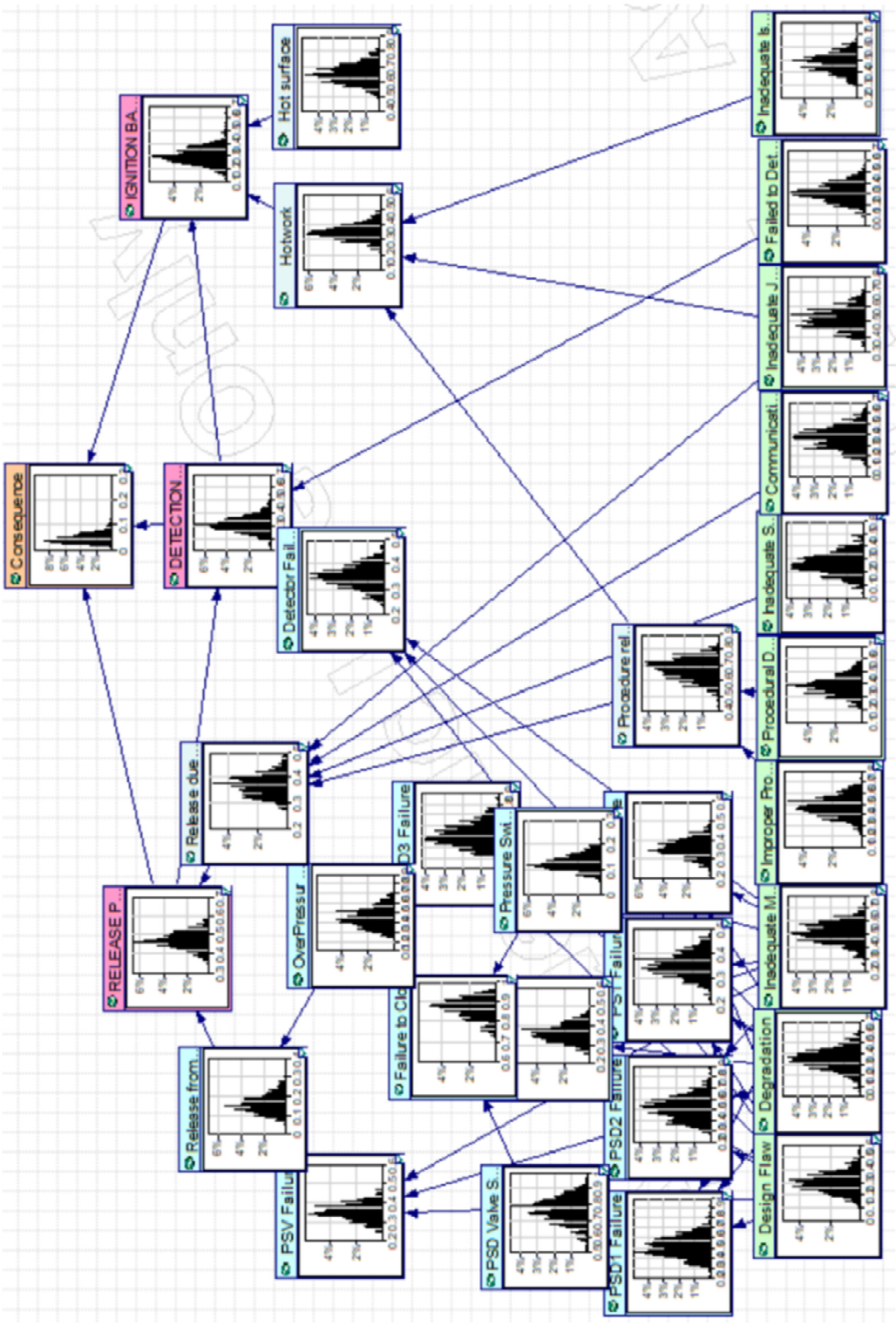
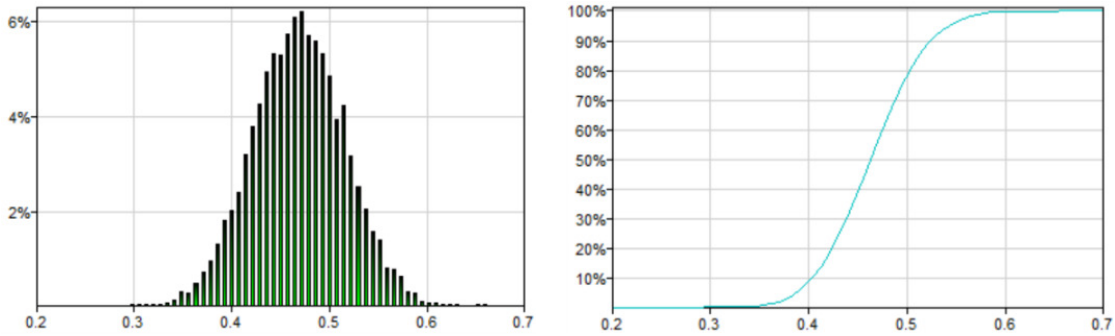


Figure 77: Results obtained by running the Bayesian Network in GeNIE gave distributions of all the nodes

7.2.5.1.1. Release Prevention Barrier

a. b.



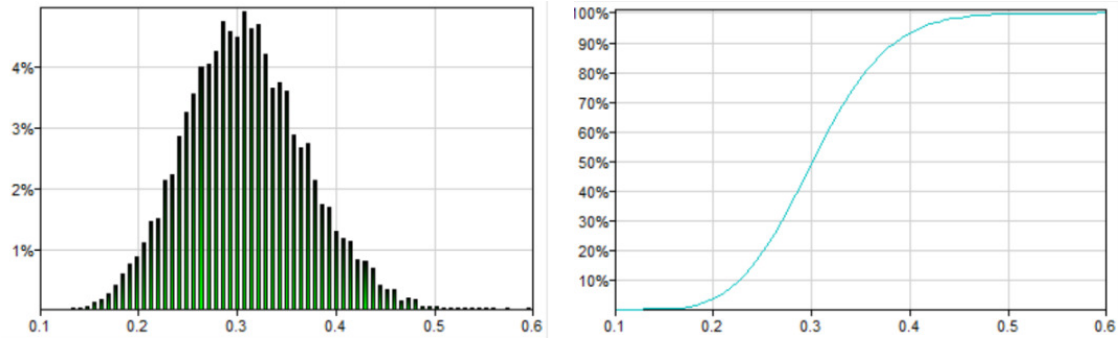
Mean: 0.4683 Minimum: 0.2947

Standard Deviation:0.0475 Maximum: 0.6606

Figure 78: a. Probability density function (PDF) and b. Cumulative density function (CDF) of the Release Prevention Barrier. The mean, standard deviation and the minimum and maximum values obtained are also provided.

7.2.5.1.2. Detection Barrier

a. b.



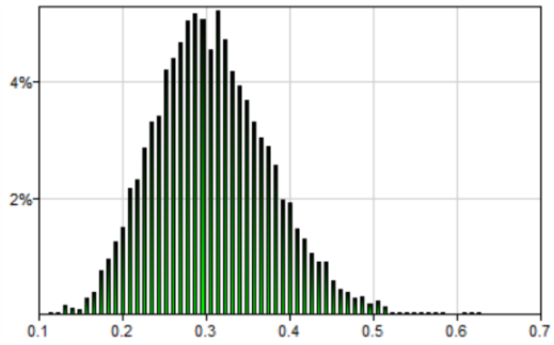
Mean=0.3084 Minimum=0.1299

Standard Deviation=0.0622 Maximum=0.5944

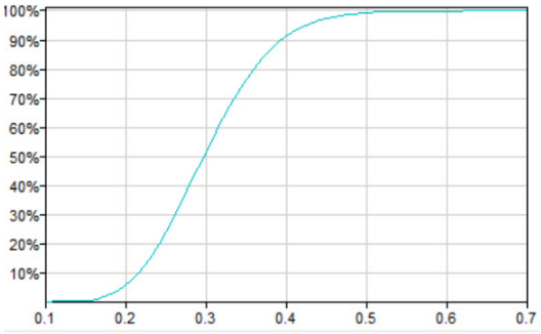
Figure 79: a. Probability density function (PDF) and b. Cumulative density function (CDF) of the Hydrocarbon Detection Barrier. The mean, standard deviation and the minimum and maximum values obtained are also provided.

7.2.5.1.3. Ignition Prevention Barrier

a.



b.



Mean=0.3072

Standard Deviation=0.0699

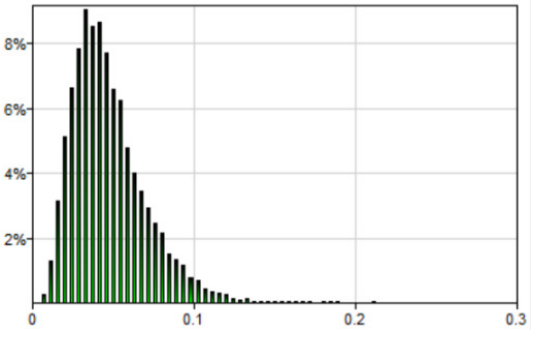
Minimum=0.1115

Maximum=0.6231

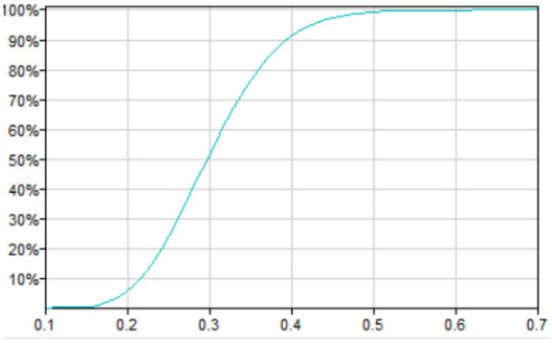
Figure 80: a. Probability density function (PDF) and b. Cumulative density function (CDF) of the Ignition Prevention Barrier. The mean, standard deviation and the minimum and maximum values obtained are also provided.

7.2.5.1.4. Consequences

a.



b.



Mean=0.0476

Standard Deviation=0.0238

Minimum=0.0055

Maximum=0.2115

Figure 81: a. Probability density function (PDF) and b. Cumulative density function (CDF) of the Consequences node. The mean, standard deviation and the minimum and maximum values obtained are also provided.

7.2.5.2. Updating case study with plant specific data

We assume that we observe 5 near misses/incidents over a period of 2 years in a facility and we investigate and analyze the incidents to find contributions from non-technical factors as those shown in Table 11.

Table 11: Assumed data for incidents and their analysis results showing occurrence of 3 non-technical factors

Near Miss/Incident	Cumulative time since last incident (days)	Procedural deviation count	Improper JSA count	Inadequate/Lack of maintenance count
1	200	1		
2	300	1		1
3	450			1
4	520	1	1	
5	680		1	1

Equipment failure probabilities may also be updated by taking data from maintenance and inspection databases which can provide information about the number of times the equipment had failed. The data can be used to update the reliability information of the equipment and compute the failure probability. For simplification we focus only on the failure of non-technical factors for now.

Updating the Procedural deviation was shown in Chapter 5 and repeated in Figures 82 and 83. Improper JSA and Inadequate/Lack of maintenance are updated in the same way and the results are shown in Figures 84-87.

7.2.5.2.1. Procedural Deviation (updated)

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	376.8	211.9	3.605	97.53	325.2	890.1	40001	40000
beta	1.082	0.1897	0.002466	0.714	1.081	1.463	40001	40000
pr.p1	0.4893	0.2066	0.003242	0.1708	0.4681	0.9011	40001	40000
pr.p2	0.6986	0.204	0.003321	0.3097	0.7212	0.9914	40001	40000
pr.p3	0.8064	0.174	0.002871	0.4227	0.855	0.9993	40001	40000
pr.p4	0.8686	0.144	0.002387	0.5148	0.9252	1.0	40001	40000
t[4]	759.2	326.7	3.945	524.5	655.0	1634.0	40001	40000

Figure 82: Updated data showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Procedural deviation occurred

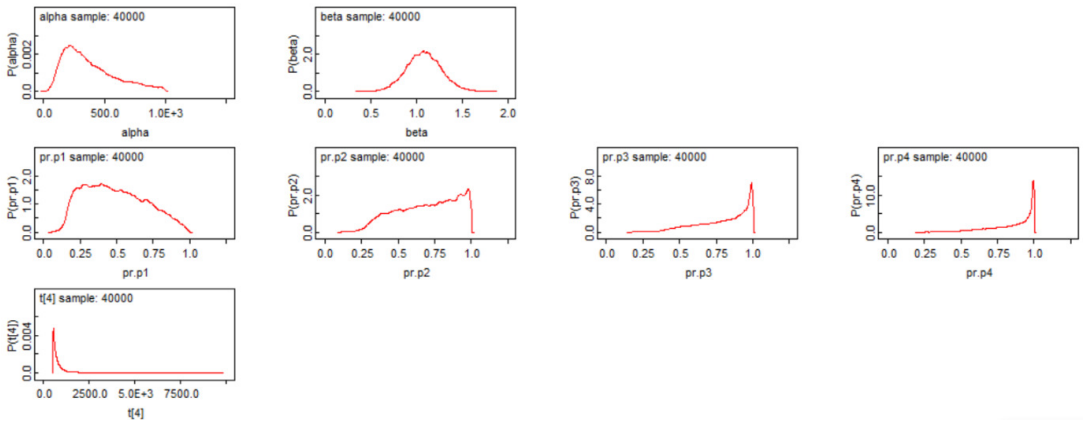


Figure 83: Distributions showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Procedural deviation occurred

7.2.5.2.2. Improper JSA

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	376.6	150.4	2.154	135.7	361.0	710.0	40001	40000
beta	0.9459	0.1324	0.001803	0.6914	0.945	1.208	40001	40000
pr.p1	0.3801	0.1359	0.001927	0.1788	0.3582	0.699	40001	40000
pr.p2	0.5959	0.1576	0.002282	0.3217	0.587	0.9103	40001	40000
pr.p3	0.7264	0.1474	0.002161	0.4366	0.7333	0.9736	40001	40000
pr.p4	0.8091	0.129	0.001903	0.5299	0.8274	0.9923	40001	40000
t[3]	976.5	362.8	3.384	686.4	861.4	1952.0	40001	40000

Figure 84: Updated data showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Improper JSA occurred

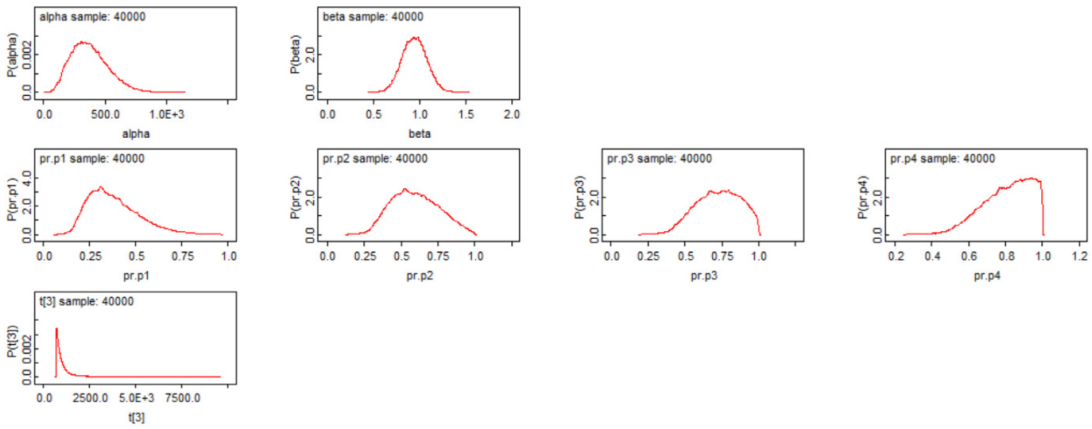


Figure 85: Distributions showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Improper JSA occurred

7.2.5.2.3. Inadequate/Lack of Maintenance

Node statistics

	mean	sd	MC_error	val2.5pc	median	val97.5pc	start	sample
alpha	433.6	213.3	3.017	134.4	393.9	940.6	40001	40000
beta	1.073	0.161	0.002088	0.7595	1.072	1.394	40001	40000
pr.p1	0.43	0.1751	0.002169	0.1635	0.4054	0.8127	40001	40000
pr.p2	0.6463	0.1883	0.002453	0.2983	0.6491	0.9668	40001	40000
pr.p3	0.7676	0.1682	0.00227	0.41	0.7943	0.9945	40001	40000
pr.p4	0.8408	0.1431	0.00198	0.5028	0.88	0.9991	40001	40000
t[4]	966.9	365.4	3.987	685.4	850.4	1948.0	40001	40000

Figure 86: Updated data showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Inadequate/Lack of maintenance occurred

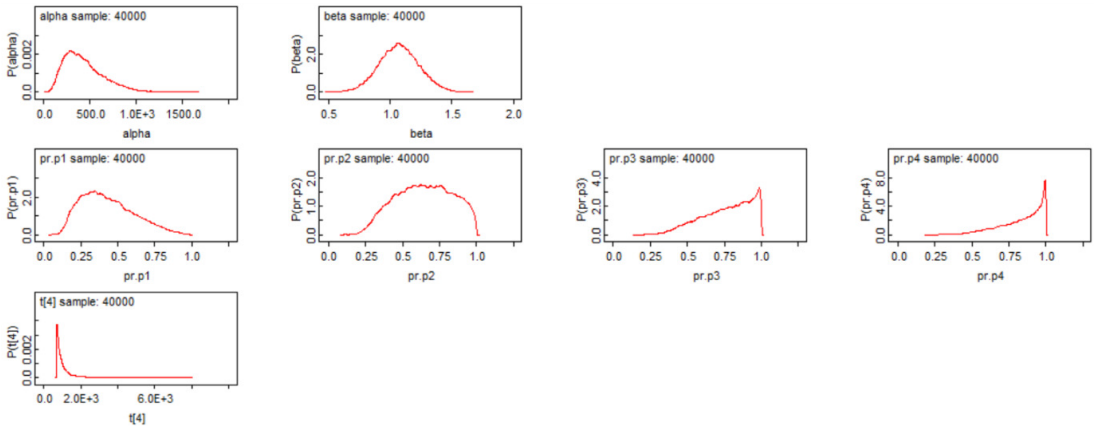


Figure 87: Distributions showing new values of the hyperparameters α and β, probabilities and time to next failure for 3 plant incidents where Inadequate/Lack of maintenance occurred

As before, the mean and standard deviation of 'pr.p2' is inserted into the GeNIE model to provide an updated information about the barrier conditions and the overall probabilistic risk.

7.2.5.3. Results after updating data with new information

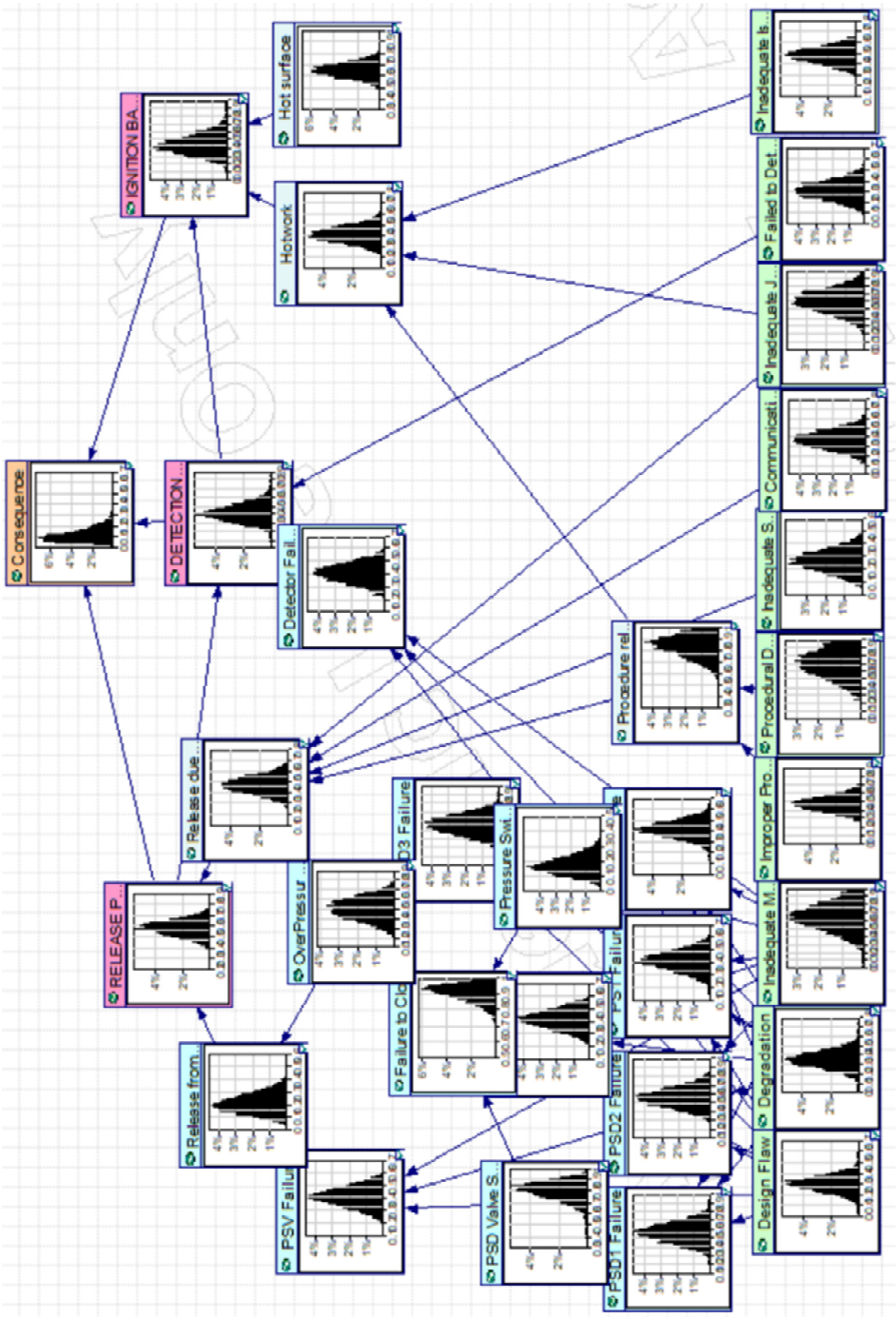
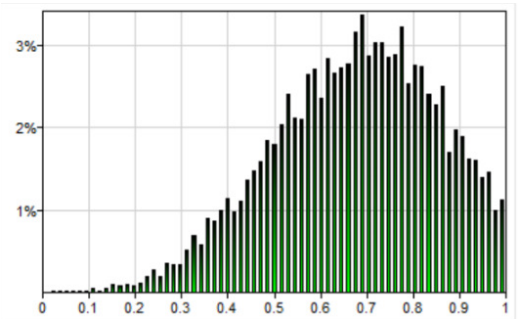


Figure 88: Updated Bayesian Network, made plant specific with data about failure of 3 non-technical factors from past plant operation

7.2.5.3.1. Release Prevention Barrier (updated)

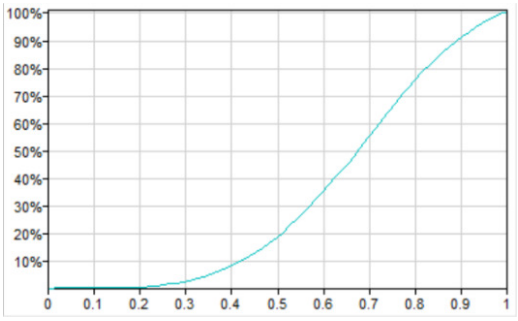
a.



Mean=0.6700

Standard Deviation=0.1787

b.



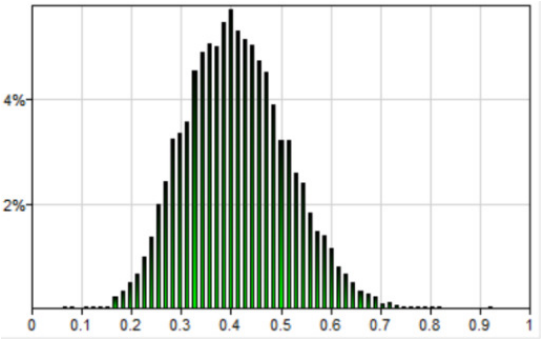
Minimum=0.0246

Maximum=1.0000

Figure 89: Updated a. PDF and b. CDF of Release Prevention Barrier with mean and standard deviation of the probability of failure

7.2.5.3.2. Hydrocarbon Detection Barrier (updated)

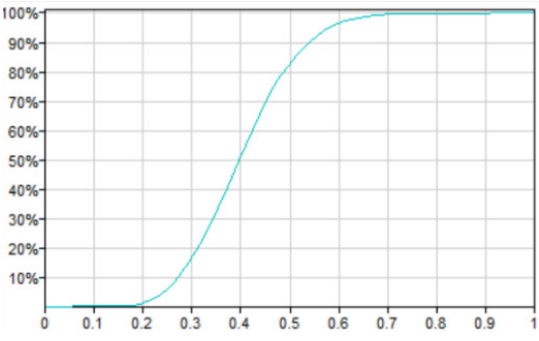
a.



Mean=0.4109

Standard Deviation=0.1037

b.



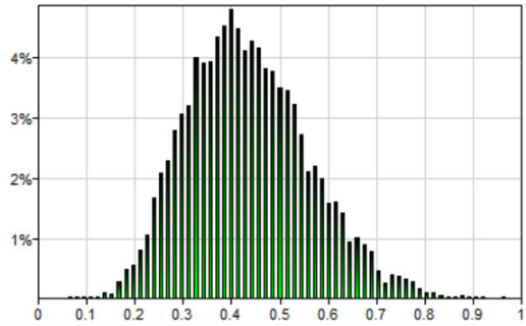
Minimum=0.0719

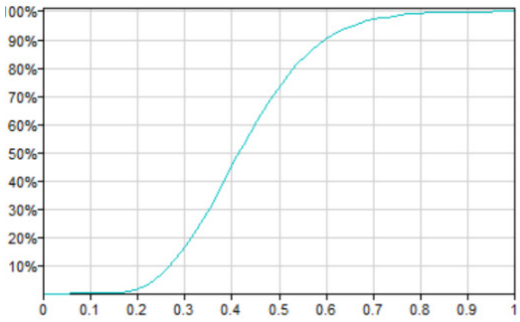
Maximum=0.9267

Figure 90: Updated a. PDF and b. CDF of Hydrocarbon Detection Barrier with mean and standard deviation of the probability of failure

7.2.5.3.3. Ignition Prevention Barrier (updated)

a. b.





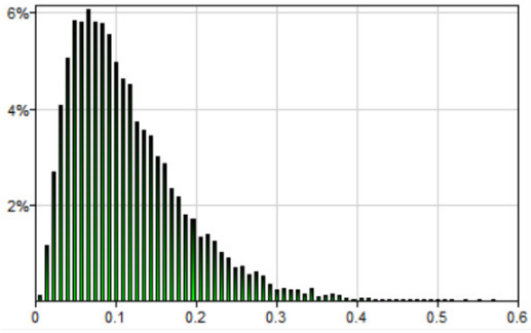
Mean=0.4351 Minimum=0.0624

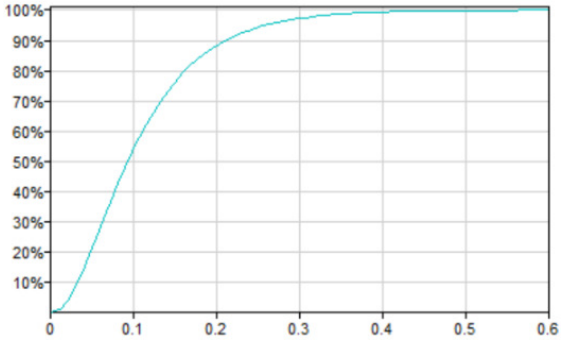
Standard Deviation=0.1285 Maximum=0.9635

Figure 91: Updated a. PDF and b. CDF of Ignition Prevention Barrier with mean and standard deviation of the probability of failure

7.2.5.3.4. Consequence (updated)

a. b.





Mean=0.1160 Minimum=0.0016

Standard Deviation=0.0754 Maximum=0.5697

Figure 92: Updated a. PDF and b. CDF of Consequence node with mean and standard deviation of the probability of failure

From Figures 88-92, we get the distribution and the parameters of the barriers and the consequence nodes that were updated with plant data. We note that there is an increase in the mean or an increase in the trend of failure probability. This indicates that the facility in consideration has a performance that is worse than the industry average, *i.e.* the US OCS.

If desired, values of pr.p1, pr.p3 and pr.p4 can also be used to determine the probabilities at various time periods. The graph in Figure 93 shows how the probability increases as time elapses for the consequence node, depicting an increasing chance of fire as time elapses. Also, if the updated probabilities are higher, then the probability of a fire also increases.

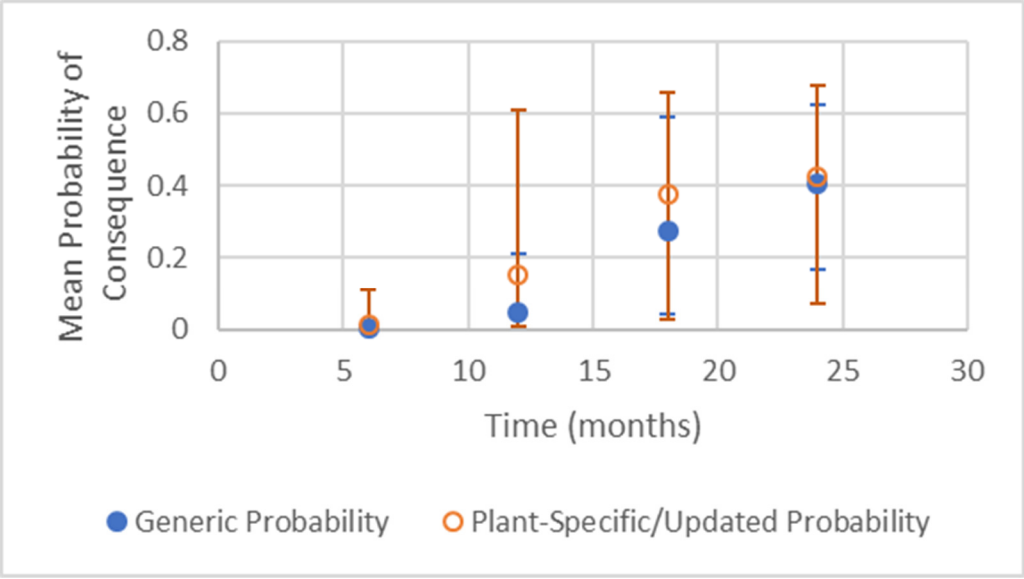


Figure 93: Graph showing how the probability of the consequence node changes over calendar time (months). The generic failure probability is shown with a X and the updated probabilities are shown with box markers.

7.2.6. Financial Analysis using estimated cumulative risk

The cumulative risk estimated so far only looks at the probabilistic part. Risk is the product of the frequency (probability in a given time) of an incident and its consequence. Hence, we need to consider the impact a fire incident may have given that all its barriers fail. Consequence modelling is beyond the scope of this work. But we can provide a probabilistic consequence from the analysis of the BSEE incident investigation reports.

As shown in Table 3a, BSEE incident investigation reports provided records of the estimated financial damage that was caused by the outbreak of fire. We clustered the collected data of financial loss into 4 categories as shown in Table 12 and counted the number of incidents in each cluster. As expected, the number of incidents increases with decrease of the consequence. These are however not exact values since these do not include financial losses incurred due to compensation provided due to any fatality or injury. They were mostly covered in Panel Investigations which have not been included in this study. The Macondo disaster is also not included in this list. However, the method suggested here provides an outline of how financial losses can be predicted when sufficient and proper data is made available.

On the right most column of Table 12, the number of incidents in each cluster has been normalized with the total count of 137 incidents. This gives an average chance that damage from a fire outbreak will be in the given range.

Table 12: Table showing the count of incidents in different categories of disaster based on the amount of financial loss incurred due to the incident

Incident type	**Range of estimated loss ($)**	**Count of incidents**	**Percent Chance (%)**
Catastrophe	>1 Billion	1	0.7
Disaster	1 Million- 1 Billion	5	3.6
Major Incident	100,001-999,999	28	20.4
Minor Incident	0-100,000	103	75.2
	Total	137	100

As we found before (Section 7.2.5.1.4), the probability of a fire (consequence node) at the end of 1 year was 0.0476. And, if there is a fire outbreak, the probability that it will be a catastrophe (>$1 billion damage) is 0.0476×0.007= 0.00033. Then, the risk of a catastrophe (more than $1 billion damage) is estimated to be greater than 0.00033*$1 billion=$333,200. Thus, the company should be willing to spend more than this amount of money per facility annually to overcome the chances of a catastrophe. Risk of major and minor incidents will add to this cost.

Figure 94 summarizes the flow path followed in the current research.

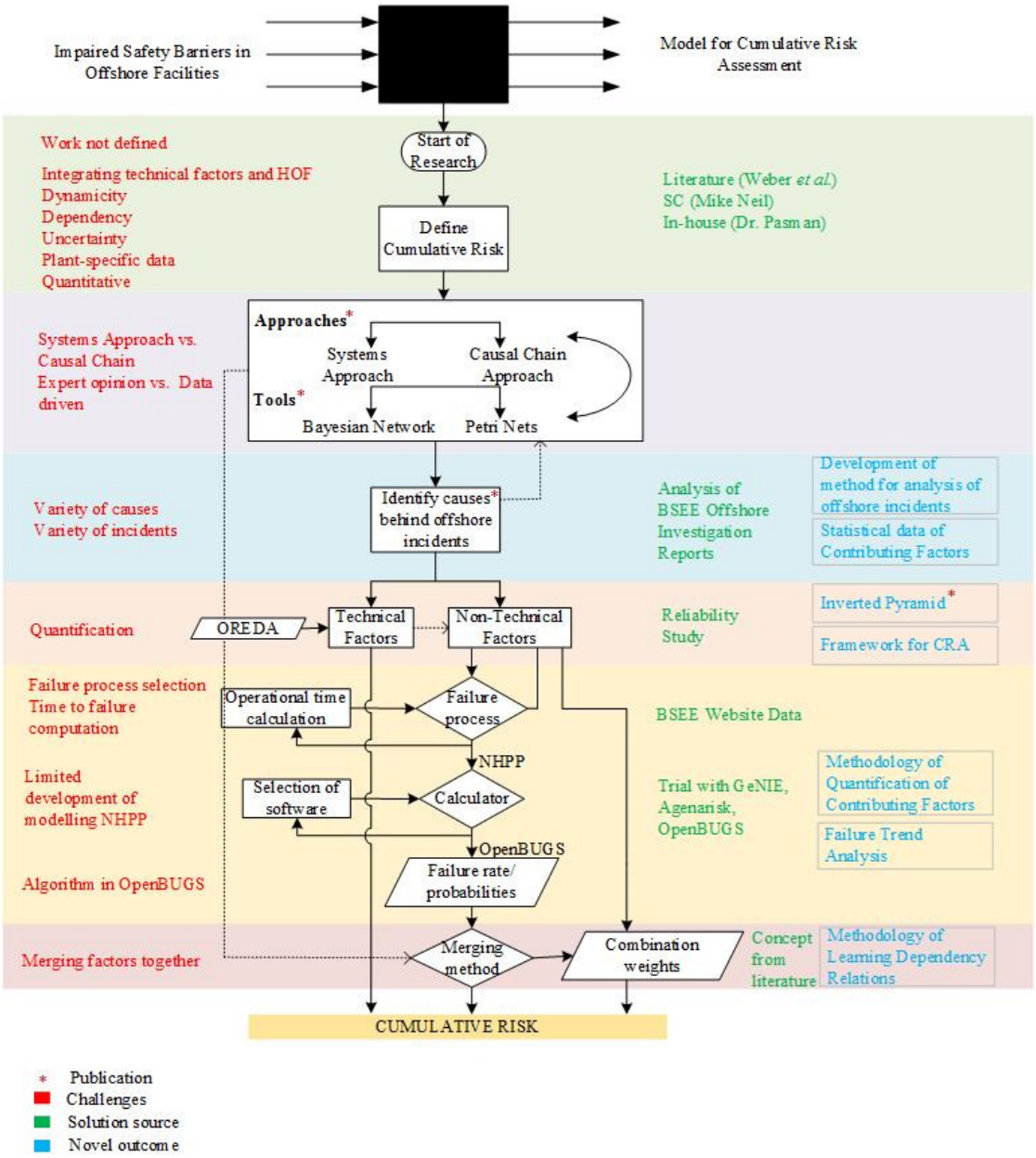


Figure 94: The various flow paths followed during the research to arrive at the goal for developing a methodology for cumulative risk assessment is shown.

We began with establishing a definition for cumulative risk assessment as *achieving an updated information about the dynamic risk through merging of technical, operational, human and organizational deviations existing within a facility using data that is specific to that facility and current in time.* The definition was established based on literature review, discussion with industry experts and in-house support and identified several key challenges associated with merging of technical, operational, human and organizational factors with their dynamicity, inter-dependencies and uncertainties.
A further and more extensive literature review was conducted to understand how all the challenges of cumulative risk assessment can be met and the pros and cons of various past efforts were studied. The review found that a standalone model for cumulative risk that met all the requisites was still missing and that the current practices do not extensively incorporate human and organizational factors into the risk assessment due to the difficulty of measuring and merging them with technical factors. It was concluded that development of a data-centric approach would allow overcoming the limitations of expert opinion used for merging various factors and would also make the model more dynamic.

In the first step, a methodology was developed to analyze 137 incident investigation reports prepared by BSEE from 2004 to 2016 to identify causes behind fire incidents in the US OCS. This methodology provided a statistical representation of contributing factors that led to the incidents. This new methodology shows how incident investigation reports can be harnessed for statistical data about non-technical factors (human and organizational aspects). Although direct causes such as equipment failure

and human error have been generally taken as reasons behind incidents in the investigation report, the deeper study revealed contribution from organizational deviations as deeper causes.

Results showed that inadequate maintenance, degradation of material and design flaw were the leading contributors that occurred in conjunction with equipment failure, improper JSA, procedural deviation and improper procedure contributed most with human error and inadequate isolation, improper JSA and improper procedure occurred most in hot work incidents. These findings formed the basis of development of the Inverted Pyramid Concept and the subsequent CRA Framework from which the next steps were then defined. The statistical data obtained in this step allowed it to be used for quantification in the next step.

In the second step, it was proposed that reliability assessment methods could be utilized to quantify the contributing factors using the generic dataset obtained in the first step. This allowed expressing non-technical factors in terms equivalent to the technical factors. Since the number of facilities in the offshore region change over time, a normalizing method was shown whereby the total operation time in a given calendar time between failures was calculated. Results showed that the rate of occurrence of non-technical failure were non-constant and a non-homogenous Poisson process should be used for modeling such failures. The Power Law process was used in Hierarchical Bayesian analysis whereby the generic dataset was used as evidence to generate probability distributions for failure trend of contributing factors. 11 contributing factors were modelled in this manner and results showed that for the US OCS, failure rates of

'design flaw' and 'inadequate/improper JSA' have been decreasing over time although for the other 9 factors, deterioration was observed. Also, the time to next occurrence was also computed. For example, it was predicted that the next time of occurrence of an incident due to a procedural deviation was 1109 years of total operating time in the US OCS after the last observed incident. Due to the rarity of occurrence of major incidents, the concept of Heinrich's Pyramid was used to convert the incident dataset to that of near-misses and computation of an updated probability using mock data about contributing factors from a particular facility was shown. Results showing changes in the probability of failure indicated how changes within a dynamic facility can be captured over time. When there is lack of data, generic data can be used for assessment and the failure probabilities and the next time to failure of non-technical factors can be estimated.

Once the probability of failure of the individual factors were determined and updated, the next step involved proposing a method of merging them. This was done through counting of the number of times each combination of multiple factors was observed. This step thus developed a data-centric method of learning relationships among various contributors, reducing the need to depend solely on expert opinion.

In the last step, all the information computed in the previous steps were brought in together for the case of an offshore hydrocarbon separator. Three barrier fault trees (release prevention, detection and ignition prevention) constituting of both system instruments and contributing factors were mapped onto Bayesian network. Probability of occurrence of failure determined previously were integrated into the model. A case

study considering several observed near miss incidents in a facility was used to show how the generic data estimated could be updated to show the changes in the barrier health conditions over time. This model merged technical, operational, human and organizational factors together and could be updated in time as plant data became available. It contained information from past incident records as well as current condition, thus giving a holistic look at risk.

The novelty of this research lies in the development of a framework which enables a complex system to be broken down and assessed in simple steps to enable a better understanding of the dynamicity of the contributing factors on the overall risk. In the process, the following novel methods were developed:

- Identifying contributing factors and harnessing their data from investigation reports
- Quantifying contributing factors and assessing their reliability dynamically
- Estimating dependencies of contributing factors through learning from past incidents
- Merging contributing factors and updating understanding of the risk along with the uncertainty associated with its estimation

While conducting this research, certain limitations were realized, some as arising from the assumptions made while some were due to the quality of the information used. These limitations are noted next and recommendations for future work are made to overcome them:

- In the analysis of incident investigation reports, we observed that our work was limited by non-observation, since not all incidents were reported, and by observation, since the analysis was based only on what was reported. Added to these were limitations in our analysis. Although we had developed a methodology for analysis of investigation reports, there was still some subjectivity involved in the analysis. With better investigation and reporting process, this might be reduced, but where there will be non-technical factors involved, a certain degree of subjectivity can be expected.
- There is a lot of scope for improvement in investigation methods and subsequent reporting. Some incident reports were found to be very detailed while others were the opposite. An in-depth and consistent investigation method will enable better identification of root causes. However, an in-depth investigation requires time and resources, which sets another limitation.
- Since investigation of near misses will allow generation of more data, attempts should be taken in the future to develop a quick investigation method to identify the causes behind then. This however, would again require a quick investigation and reporting methodology.
- Attempt can be made to either develop a taxonomy for reporting or to develop natural language processing methods to analyze investigation reports so that machine learning from incidents becomes possible.
- We provided justification for assuming non-technical factors as following a non-homogenous Poisson process for failure. This was based on the reasoning that their failure rate may not be constant with time due to dynamicity of the organization. If a

large amount of data is available for successive failure incidents, then the validity of this assumption can be checked.

- All cumulative operating times were counted from the first incident date on record (after 1/1/2004). During this time, it was assumed that all facilities were in similar operating conditions, which most likely may not be true. This limitation can be overcome in the future if data of all incidents from the installation date of the respective facilities are available.
- The analysis did not categorize incidents in terms of severity of the consequences. In the future, new reports can be analyzed with categorization in mind.
- Regulators and operators need to work together for better results in assessing cumulative risk. All incidents should be reported and investigation and analyzed. This will help operators in terms of obtaining generic data and understanding of how to merge factors through use of weights. Thus, by reporting incidents, they will in return be able to assess barrier conditions better. Only then will the feedback loop of the inverted pyramid be complete.
- This research provides a ground for development of a dashboard model whereby all contributors to risk can be viewed in current time and the effect of altering the probability of occurrence of a contributor can be better understood. Such model will allow management to visually understand how to optimize their resources among the highest contributors so that the risk of barrier failure can be brought down to ALARP.
- This approach can be extended to other area of practice such as pipeline where interacting contributing factors play an important role in risk assessment.

In conclusion, the methodology developed in this research tackled all the identified challenges associated with cumulative risk assessment. Because the contributors to risk are precisely understood, the risk can now be controlled better. When applied, this method will enable management to optimize resource allocation in a manner that provides the greatest return while keeping risks to a minimal. A data-centered model has been developed that reduces the reliance on expert opinion and makes the risk assessment more dynamic and accurate.

REFERENCES

1. Weber, P., G. Medina-Oliva, C. Simon, and B. Iung, *Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas.* Engineering Applications of Artificial Intelligence, 2012. **25**(4): p. 671-682.
2. Chemical Safety and Hazard Investigation Board (CSB), *Investigation Report: Refinery Explosion and Fire*. 2007.
3. Chemical Safety and Hazard Investigation Board (CSB), *Investigation Report Executive Summary: Drilling Rig Explosion and Fire at Macondo Well*. 2016.
4. Haquet, C., *Macondo: The Disaster that Changed the Rules*. 2014, Scor Global P&C.
5. Hosseini, S.H. and M. Takahashi. *Combining static/dynamic fault trees and event trees using Bayesian networks*. in International Conference on Computer Safety, Reliability, and Security. 2007. Springer.
6. Reason, J., E. Hollnagel, and J. Paries, *Revisiting the Swiss cheese model of accidents.* Journal of Clinical Engineering, 2006. **27**: p. 110-115.
7. Neill, M. *Improving risk-based decision making by connecting PSM systems to day-to-day plant operations*. in 2015 AIChE National Spring Meeting, 11th Global Congress on Process Safety. 2015.
8. Pate-Cornell, M.E. and D.M. Murphy, *Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications.* Reliability Engineering & System Safety, 1996. **53**(2): p. 115-126.
9. Sklet, S., *Safety barriers: Definition, classification, and performance.* Journal of Loss Prevention in the Process Industries, 2006. **19**(5): p. 494-506.
10. Pitblado, R., M. Fisher, B. Nelson, H. Fløtaker, K. Molazemi, and A. Stokke, *Concepts for dynamic barrier management.* Journal of Loss Prevention in the Process Industries, 2016. **43**: p. 741-746.
11. Sklet, S., J.E. Vinnem, and T. Aven, *Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part II: Results from a case study.* Journal of Hazardous Materials, 2006. **137**(2): p. 692-708.
12. Gran, B., R. Bye, O. Nyheim, E. Okstad, J. Seljelid, S. Sklet, J. Vatn, and J. Vinnem, *Evaluation of the risk OMT model for maintenance work on major offshore process equipment.* Journal of Loss Prevention in the Process Industries, 2012. **25**(3): p. 582-593.
13. Siu, N., *Risk assessment for dynamic systems: an overview.* Reliability Engineering & System Safety, 1994. **43**(1): p. 43-73.
14. Skogdalen, J.E. and J.E. Vinnem, *Quantitative risk analysis offshore—Human and organizational factors.* Reliability Engineering & System Safety, 2011. **96**(4): p. 468-479.
15. Murthy, M. and N. Serikova, *Selection of failure frequency and its impact on risk assessment–A case study from plot plan optimisation.* Journal of Loss Prevention in the Process Industries, 2016. **44**: p. 690-698.

16. Anderson, M. *European state-of-the-art research: Integrating technical and management/organisational factors in major hazard risk assessment*. in Institution of Chemical Engineers Symposium Series. 1999. Hemisphere Publishing Corporation.
17. Mosleh, A., V.M. Bier, and G. Apostolakis, *A critique of current practice for the use of expert opinions in probabilistic risk assessment.* Reliability Engineering & System Safety, 1988. **20**(1): p. 63-85.
18. Labeau, P.-E., C. Smidts, and S. Swaminathan, *Dynamic reliability: towards an integrated platform for probabilistic risk assessment.* Reliability Engineering & System Safety, 2000. **68**(3): p. 219-254.
19. Covello, V.T. and J. Mumpower, *Risk analysis and risk management: an historical perspective.* Risk analysis, 1985. **5**(2): p. 103-120.
20. Bernstein, P.L. and P.L. Bernstein, *Against the gods: The remarkable story of risk*. 1996: Wiley New York.
21. Bernoulli, J., *Ars conjectandi*. 1713: Impensis Thurnisiorum, fratrum.
22. Shafer, G., *The significance of Jacob Bernoulli's Ars Conjectandi for the philosophy of probability today.* Journal of Econometrics, 1996. **75**(1): p. 15-32.
23. Wald, M.L. *Chauncey Starr, 95, Pioneer in Nuclear Energy, Dies*. 2007; Available from: https://www.nytimes.com/2007/04/19/obituaries/19starr.html.
24. Starr, C., *Social benefit versus technological risk.* Science, 1969. **165**(3899): p. 1232-1238.
25. Amburgey, T.L., D. Kelly, and W.P. Barnett. *Resetting the clock: The dynamics of organizational change and failure*. in Academy of Management Proceedings. 1990. Academy of Management Briarcliff Manor, NY 10510.
26. Heinrich, H.W., *Industrial Accident Prevention. A Scientific Approach, 2nd Edition*. 1941: New York & London : McGraw-Hill Book Company, Inc.
27. Rasmussen, J., *Risk management in a dynamic society: a modelling problem.* Safety Science, 1997. **27**(2-3): p. 183-213.
28. Aven, T., *Risk assessment and risk management: Review of recent advances on their foundation.* European Journal of Operational Research, 2016. **253**(1): p. 1-13.
29. Cooke, R.M. *A brief history of quantitative risk assessment*. 2009; Available from: http://www.rff.org/files/sharepoint/WorkImages/Download/RFF-Resources-172_Risk_Assessment.pdf.
30. Perrow, C., *Normal Accidents: Living with High Risk Technologies-Updated Edition*. 2011: Princeton university press.
31. Khan, F., S. Rathnayaka, and S. Ahmed, *Methods and models in process safety and risk management: past, present and future.* Process Safety and Environmental Protection, 2015. **98**: p. 116-147.
32. Halim, S.Z., Y. Koirala, and M.S. Mannan. *A Look into Cumulative Risk Assessment: Past, Present and Future*. in AIChE Spring Meeting and Global Congress on Process Safety. 2017. San Antonio, TX: Center for Chemical Process Safety.

33. Tixier, J., G. Dusserre, O. Salvi, and D. Gaston, *Review of 62 risk analysis methodologies of industrial plants.* Journal of Loss Prevention in the process industries, 2002. **15**(4): p. 291-303.
34. Coze, J.-C.L., *Are organisations too complex to be integrated in technical risk assessment and current safety auditing?* Safety Science, 2005. **43**(8): p. 613-638.
35. Pasman, H.J., *Risk analysis and control for industrial processes-gas, oil and chemicals: A system perspective for assessing and avoiding low-probability, high-consequence events*. 2015: Butterworth-Heinemann.
36. Dugan, J.B., S.J. Bavuso, and M.A. Boyd, *Dynamic fault-tree models for fault-tolerant computer systems.* IEEE Transactions on Reliability, 1992. **41**(3): p. 363-377.
37. Bobbio, A., E. Ciancamerla, G. Franceschinis, R. Gaeta, M. Minichino, and L. Portinale, *Sequential application of heterogeneous models for the safetyanalysis of a control system: a case study.* Reliability Engineering & System Safety, 2003. **81**(3): p. 269-280.
38. Bobbio, A., L. Portinale, M. Minichino, and E. Ciancamerla, *Improving the analysis of dependable systems by mapping fault trees into Bayesian networks.* Reliability Engineering & System Safety, 2001. **71**(3): p. 249-260.
39. Bearfield, G. and W. Marsh. *Generalising event trees using Bayesian networks with a case study of train derailment*. in International Conference on Computer Safety, Reliability, and Security. 2005. Springer.
40. Khakzad, N., F. Khan, and P. Amyotte, *Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network.* Process Safety and Environmental Protection, 2013. **91**(1): p. 46-53.
41. Khakzad, N., F. Khan, and P. Amyotte, *Risk-based design of process systems using discrete-time Bayesian networks.* Reliability Engineering & System Safety, 2013. **109**: p. 5-17.
42. Nývlt, O. and M. Rausand, *Dependencies in event trees analyzed by Petri nets.* Reliability Engineering & System Safety, 2012. **104**: p. 45-57.
43. Halim, S.Z., H.J. Pasman, and M.S. Mannan. *Probabilistic methods of quantitative risk analysis: A case study with Bayesian Network and Petri Nets approaches*. in Mary Kay O'Connor International Process Safety Symposium. 2016. College Station, TX.
44. Nývlt, O., L. Ferkl, and S. Haugen, *Stochastic Coloured Petri Nets as a modelling language for complex Event Trees.* Nutritional Care of the Patient with Gastrointestinal Disease, 2015: p. 201.
45. Wang, C., *PhD Dissertation: Hybrid causal logic methodology for risk assessment*. 2007: University of Maryland, College Park.
46. Røed, W., A. Mosleh, J.E. Vinnem, and T. Aven, *On the use of the hybrid causal logic method in offshore risk analysis.* Reliability Engineering & System Safety, 2009. **94**(2): p. 445-455.
47. Vinnem, J., R. Bye, B. Gran, T. Kongsvik, O. Nyheim, E. Okstad, J. Seljelid, and J. Vatn, *Risk modelling of maintenance work on major process equipment on*

offshore petroleum installations. Journal of Loss Prevention in the Process Industries, 2012. **25**(2): p. 274-292.
48. Vinnem, J., J. Seljelid, S. Haugen, S. Sklet, and T. Aven, *Generalized methodology for operational risk analysis of offshore installations.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2009. **223**(1): p. 87-97.
49. Papazoglou, I., L. Bellamy, A. Hale, O. Aneziris, B. Ale, J. Post, and J. Oh, *I-Risk: development of an integrated technical and management risk methodology for chemical installations.* Journal of Loss Prevention in Process Industries, 2003. **16**(6): p. 575-591.
50. Øien, K., *A framework for the establishment of organizational risk indicators.* Reliability Engineering & System Safety, 2001. **74**(2): p. 147-167.
51. Rasmussen, J. and I. Suedung, *Proactive risk management in a dynamic society*. 2000: Swedish Rescue Services Agency.
52. Svedung, I. and J. Rasmussen, *Graphic representation of accidentscenarios: mapping system structure and the causation of accidents.* Safety Science, 2002. **40**(5): p. 397-417.
53. Salmon, P.M., M. Cornelissen, and M.J. Trotter, *Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP.* Safety Science, 2012. **50**(4): p. 1158-1170.
54. Leveson, N., *Engineering a safer world: Systems thinking applied to safety*. 2011: MIT press.
55. Leveson, N., *A systems approach to risk management through leading safety indicators.* Reliability Engineering & System Safety, 2015. **136**: p. 17-34.
56. Altabbakh, H., M.A. AlKazimi, S. Murray, and K. Grantham, *STAMP–Holistic system safety approach or just another risk model?* Journal of Loss Prevention in the Process Industries, 2014. **32**: p. 109-119.
57. Thomas, J. and D. Suo, *STPA-based method to identify and control feature interactions in large complex systems.* Procedia Engineering, 2015. **128**: p. 12-14.
58. Hollnagel, E. and J. Speziali, *Study on Developments in Accident Investigation Methods: A Survey of the" State-of-the-Art*. 2008, CRC - Centre de recherche sur les Risques et les Crises.
59. Hollnagel, E., *An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change*. 2013, Strålsäkerhetsmyndigheten (Swedish Radiation Safety Authority).
60. Hollnagel, E., *FRAM: the functional resonance analysis method: modelling complex socio-technical systems*. 2017: CRC Press.
61. Aven, T., *Trends in quantitative risk assessments.* International Journal of Performability Engineering, 2009. **5**(5): p. 447.
62. Kulkarni, V.G., *Modeling and analysis of stochastic systems*. 2016: CRC Press.
63. Boudali, H. and J.B. Dugan, *A discrete-time Bayesian network reliability modeling and analysis framework.* Reliability Engineering & System Safety, 2005. **87**(3): p. 337-349.

64. Barua, S., X. Gao, H. Pasman, and M.S. Mannan, *Bayesian network based dynamic operational risk assessment.* Journal of Loss Prevention in the Process Industries, 2016. **41**: p. 399-410.
65. Fenton, N. and M. Neil, *Risk assessment and decision analysis with Bayesian networks*. 2012: CRC Press.
66. BayesFusion, L. *GeNIe Modeler: Complete Modeling Freedom*. 2015-2018 [cited 2018.
67. Lunn, D.J., A. Thomas, N. Best, and D. Spiegelhalter, *WinBUGS-a Bayesian modelling framework: concepts, structure, and extensibility.* Statistics and computing, 2000. **10**(4): p. 325-337.
68. Rodionov, A., D. Kelly, and J. Uwe-Klügel, *Guidelines for analysis of data related to ageing of nuclear power plant components and systems.* JRC Scientific and Technical Reports, EUR, 2009. **23954**: p. 88-90.
69. Kelly, D.L. and C.L. Smith, *Bayesian inference in probabilistic risk assessment—the current state of the art.* Reliability Engineering & System Safety, 2009. **94**(2): p. 628-643.
70. Hu, J., L. Zhang, Z. Cai, Y. Wang, and A. Wang, *Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework.* Process Safety and Environmental Protection, 2015. **97**: p. 25-36.
71. Liu, T. and S. Chiou, *The application of Petri nets to failure analysis.* Reliability Engineering & System Safety, 1997. **57**(2): p. 129-142.
72. Chiachío, M., J. Chiachío, D. Prescott, and J. Andrews, *A new paradigm for uncertain knowledge representation by Plausible Petri nets.* Information Sciences, 2018. **453**: p. 323-345.
73. Snene, W., W. Mechri, and K.B. Othman, *Uncertainty analysis in the unavailability assessment using Generalized Stochastic Petri Net with fuzzy parameters.* International Journal of Applied Engineering Research, 2017. **12**(10): p. 2150-2161.
74. Embrey, D.E., *Incorporating management and organisational factors into probabilistic safety assessment.* Reliability Engineering & System Safety, 1992. **38**(1-2): p. 199-208.
75. Pitblado, R., B. Bain, A. Falck, K. Litland, and C. Spitzenberger, *Frequency data and modification factors used in QRA studies.* Journal of Loss Prevention in the Process Industries, 2011. **24**(3): p. 249-258.
76. Pitblado, R., J. Williams, and D. Slater, *Quantitative assessment of process safety programs.* Process Safety Progress, 1990. **9**(3): p. 169-175.
77. Davoudian, K., J.-S. Wu, and G. Apostolakis, *Incorporating organizational factors into risk assessment through the analysis of work processes.* Reliability Engineering & System Safety, 1994. **45**(1): p. 85-105.
78. Davoudian, K., J.-S. Wu, and G. Apostolakis, *The work process analysis model (WPAM).* Reliability Engineering & System Safety, 1994. **45**(1): p. 107-125.
79. Papazoglou, I.A. and O. Aneziris, *On the quantification of the effects of organizational and management factors in chemical installations.* Reliability Engineering & System Safety, 1999. **63**(1): p. 33-45.

80. Hurst, N.W., S. Young, I. Donald, H. Gibson, and A. Muyselaar, *Measures of safety management performance and attitudes to safety at major hazard sites.* Journal of Loss Prevention in the Process Industries, 1996. **9**(2): p. 161-172.
81. Papazoglou, I., O. Aneziris, J. Post, and B. Ale, *Technical modeling in integrated risk assessment of chemical installations.* Journal of Loss Prevention in the Process Industries, 2002. **15**(6): p. 545-554.
82. Duijm, N.J. and L. Goossens, *Quantifying the influence of safety management on the reliability of safety barriers.* Journal of Hazardous Materials, 2006. **130**(3): p. 284-292.
83. Guldenmund, F., A. Hale, L. Goossens, J. Betten, and N.J. Duijm, *The development of an audit technique to assess the quality of safety barrier management.* Journal of hazardous materials, 2006. **130**(3): p. 234-241.
84. Delvosalle, C., C. Fievez, A. Pipart, and B. Debray, *ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries.* Journal of Hazardous Materials, 2006. **130**(3): p. 200-219.
85. Mosleh, A., E. Goldfeiz, and S. Shen. *The/spl omega/-factor approach for modeling the influence of organizational factors in probabilistic safety assessment*. in Human Factors and Power Plants, 1997. Global Perspectives of Human Factors in Power Generation., Proceedings of the 1997 IEEE Sixth Conference on. 1997. IEEE.
86. Schönbeck, M., M. Rausand, and J. Rouvroye, *Human and organisational factors in the operational phase of safety instrumented systems: A new approach.* Safety Science, 2010. **48**(3): p. 310-318.
87. Center for Chemical Process Safety, *Guidelines for chemical process quantitative risk analysis*. 2000: Center for Chemical Process Safety/AIChE.
88. Jin, H., M. Rausand, A. Mosleh, and S. Haugen. *Quantification of organizational influences on failure rate: A Bayesian approach*. in Industrial Engineering and Engineering Management (IEEM), 2012 IEEE International Conference on. 2012. IEEE.
89. American Petroleum Institute (API), *API RP 581 Risk-Based Inspection Technology, 3rd Edition*. 2008.
90. Aven, T., S. Sklet, and J.E. Vinnem, *Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description.* Journal of Hazardous Materials, 2006. **137**(2): p. 681-691.
91. Landucci, G. and N. Paltrinieri, *Accident frequency evaluation to support dynamic risk studies.* Chemical Engineering Transactions, 2016. **48**: p. 685-690.
92. Landucci, G. and N. Paltrinieri, *Dynamic evaluation of risk: From safety indicators to proactive techniques.* Chemical Engineering Transactions, 2016. **53**: p. 169-174.
93. Kerkering, J.C., *Eliciting and analyzing expert judgment, a practical guide*. 2002, Taylor & Francis.
94. Meel, A. and W.D. Seider, *Plant-specific dynamic failure assessment using Bayesian theory.* Chemical Engineering Science, 2006. **61**(21): p. 7036-7056.

95. Meel, A., L. O'neill, J. Levin, W.D. Seider, U. Oktem, and N. Keren, *Operational risk assessment of chemical industries by exploiting accident databases.* Journal of Loss Prevention in the Process Industries, 2007. **20**(2): p. 113-127.
96. Kalantarnia, M., F. Khan, and K. Hawboldt, *Dynamic risk assessment using failure assessment and Bayesian theory.* Journal of Loss Prevention in the Process Industries, 2009. **22**(5): p. 600-606.
97. Rathnayaka, S., F. Khan, and P. Amyotte, *SHIPP methodology: Predictive accident modeling approach. Part I: Methodology and model description.* Process Safety and Environmental Protection, 2011. **89**(3): p. 151-164.
98. Rathnayaka, S., F. Khan, and P. Amyotte, *SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study.* Process Safety and Environmental Protection, 2011. **89**(2): p. 75-88.
99. Kujath, M., P. Amyotte, and F. Khan, *A conceptual offshore oil and gas process accident model.* Journal of Loss Prevention in the Process Industries, 2010. **23**(2): p. 323-330.
100. Siu, N.O. and D.L. Kelly, *Bayesian parameter estimation in probabilistic risk assessment1.* Reliability Engineering & System Safety, 1998. **62**(1-2): p. 89-116.
101. Khakzad, N., F. Khan, and N. Paltrinieri, *On the application of near accident data to risk analysis of major accidents.* Reliability Engineering & System Safety, 2014. **126**: p. 116-125.
102. Yu, H., F. Khan, and B. Veitch, *A flexible hierarchical Bayesian modeling technique for risk analysis of major accidents.* Risk analysis, 2017. **37**(9): p. 1668-1682.
103. Mohaghegh, Z. *Combining system dynamics and Bayesian belief networks for socio-technical risk analysis*. in Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on. 2010. IEEE.
104. Mohaghegh, Z., R. Kazemi, and A. Mosleh, *Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization.* Reliability Engineering & System Safety, 2009. **94**(5): p. 1000-1018.
105. Mohaghegh, Z. and A. Mosleh, *Incorporating organizational factors into probabilistic risk assessment of complex socio-technical systems: Principles and theoretical foundations.* Safety Science, 2009. **47**(8): p. 1139-1158.
106. Pence, J., Z. Mohaghegh, C. Ostroff, E. Kee, G. Yilmaz, R. Grantom, and D. Johnson, *Toward monitoring organizational safety indicators by integrating probabilistic risk assessment, socio-technical systems theory, and big data analytics*, in *2th International Probabilistic Safety Assessment and Management Conference, PSAM 2014*. 2014.
107. Meng, X., G. Chen, G. Zhu, and Y. Zhu, *Dynamic quantitative risk assessment of accidents induced by leakage on offshore platforms using DEMATEL-BN.* International Journal of Naval Architecture and Ocean Engineering, 2018.
108. Radvanska, A., *Accident losses elimination by means of safety pyramid analysis.* Annals of Faculty Engineering Hunedoara. Int J Eng. 2010; 8 (1): 73, 2010. **6**.

109. Halim, S.Z. and M.S. Mannan, *A journey to excellence in process safety management.* Journal of Loss Prevention in the Process Industries, 2018. **55**: p. 71-79.
110. Rausand, M. and H. Arnljot, *System reliability theory: models, statistical methods, and applications*. Vol. 396. 2004: John Wiley & Sons.
111. Modarres, M., M.P. Kaminskiy, and V. Krivtsov, *Reliability engineering and risk analysis: a practical guide*. 2016: CRC press.
112. Pula, R., F.I. Khan, B. Veitch, and P.R. Amyotte, *Revised fire consequence models for offshore quantitative risk assessment.* Journal of Loss Prevention in the Process Industries, 2005. **18**(4): p. 443-454.
113. Tamim, N., D.M. Laboureur, R.A. Mentzer, A.R. Hasan, and M.S. Mannan, *A framework for developing leading indicators for offshore drillwell blowout incidents.* Process Safety and Environmental Protection, 2017. **106**: p. 256-262.
114. Mannan, M.S., R.A. Mentzer, and J. Zhang, *Framework for creating a Best-in-Class safety culture.* Journal of Loss Prevention in the Process Industries, 2013. **26**(6): p. 1423-1432.
115. Mannan, M.S., H.H. West, K. Krishna, A.A. Aldeeb, N. Keren, S.R. Saraf, Y.-S. Liu, and M. Gentile, *The legacy of Bhopal: the impact over the last 20 years and future direction.* Journal of Loss Prevention in the Process Industries, 2005. **18**(4): p. 218-224.
116. Heinrich, H.W., *Industrial Accident Prevention. A Scientific Approach.* Industrial Accident Prevention. A Scientific Approach., 1941(Second Edition).
117. Kidam, K. and M. Hurme, *Statistical analysis of contributors to chemical process accidents.* Chemical Engineering & Technology, 2013. **36**(1): p. 167-176.
118. Okoh, P. and S. Haugen, *Maintenance-related major accidents: classification of causes and case study.* Journal of Loss Prevention in the Process Industries, 2013. **26**(6): p. 1060-1070.
119. Okoh, P. and S. Haugen, *A study of maintenance-related major accident cases in the 21st century.* Process Safety and Environmental Protection, 2014. **92**(4): p. 346-356.
120. Kannan, P., T. Flechas, E. Mendez, L. Angarita, P. Chaudhari, Y. Hong, and M.S. Mannan, *A web-based collection and analysis of process safety incidents.* Journal of Loss Prevention in the Process Industries, 2016. **44**: p. 171-192.
121. Mannan, M.S., T.M. O'Connor, and H.H. West, *Accident history database: An opportunity.* Environmental Progress & Sustainable Energy, 1999. **18**(1): p. 1-6.
122. Hare, J. and M. Johnson, *Underlying Causes of Offshore Incidents.* Health and Safety Executive, published May, 2009. **15**.
123. Bureau of Safety and Environmental Enforcement (BSEE). *Offshore Incidents Investigations*. https://www.bsee.gov/what-we-do/incident-investigations/offshore-incident-investigations (Accessed 02/14/2019).
124. U.S. Government Publishing Office, *Electronic Code of Federal Regulations: 30 CFR 250.188*. 2019: https://www.gpo.gov/fdsys/browse/collectionCfr.action?collectionCode=CFR&s

earchPath=Title+30%2FChapter+II%2FSubchapter+B%2FPart+250%2FSubpart+A%2FSubjgrp&oldPath=Title+30%2FChapter+II%2FSubchapter+B%2FPart+250%2FSubpart+A&isCollapsed=true&selectedYearFrom=2017&ycord=1480.6666259765625 (Accessed 12/14/2017).
125. Bureau of Safety and Environmental Enforcement (BSEE). *Offshore Incident Statistics*. https://www.bsee.gov/stats-facts/offshore-incident-statistics (Accessed 02/14/2019).
126. Bureau of Safety and Environmental Enforcement (BSEE). *Panel Investigation Reports*. https://www.bsee.gov/what-we-do/incident-investigations/offshore-incident-investigations/panel-investigation-reports (Accessed 02/14/2019); Available from: https://www.bsee.gov/what-we-do/incident-investigations/offshore-incident-investigations/panel-investigation-reports.
127. Bureau of Safety and Environmental Enforcement (BSEE). *District Investigation Reports*. https://www.bsee.gov/what-we-do/incident-investigations/offshore-incident-investigations /district-investigation-reports (Accessed 02/14/2019).
128. Bureau of Safety and Environmental Enforcement (BSEE). *Listing and Status of Incident Investigations*. https://www.data.bsee.gov/Other/DataTables/IncidentInvestigations.aspx (Accessed 02/14/2019).
129. Dekker, S., *The field guide to understanding'human error'*. 2014: Ashgate Publishing, Ltd.
130. Kaplan, S., *On a" Two-Stage" Bayesian Procedure for Determining ailure Rates from Experimental Data.* IEEE Transactions on Power Apparatus and Systems, 1983(1): p. 195-202.
131. SINTEF Industrial Management, *Offshore Reliability Data Handbook, 4th Edition*. 2002, OREDA Participants and Det Norske Veritas (DNV).
132. Hauge, S. and T. Onshus, *Reliability Data for Safety Instrumented Systems: PDS Data Handbook*. 2010: SINTEF Technology and Society.
133. Wellmaster. *Well integrity and reliability analytics for increased well uptime*. https://www.exprosoft.com/ (Accessed 03/03/2019) 2019.
134. Bell, J. and J. Holroyd, *Review of human reliability assessment methods.* Health and Safety Laboratory, 2009.
135. Hauge, S., M. Lundteigen, and M. Rausand. *Updating failure rates and test intervals in the operational phase: A practical implementation of IEC 61511 and IEC 61508*. in Reliability, Risk and Safety-Theory and Applications, Proceedings of the European Safety and Reliability Conference, ESREL. 2009.
136. Halim, S.Z., S. Janardanan, T. Flechas, and M.S. Mannan, *In search of causes behind offshore incidents: Fire in offshore oil and gas facilities.* Journal of Loss Prevention in the Process Industries, 2018. **54**: p. 254-265.
137. Fink, D. *A Compendium of Conjugate Priors*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.157.5540&rep=rep1&type=pdf (Accessed 02/14/2019), 1997.

138. University of Cambridge: MRC Biostatistics Unit. *OpenBUGS*. https://www.mrc-bsu.cam.ac.uk/software/bugs/openbugs/ (Accessed 03/03/2019) 2019.
139. Song, G., F. Khan, M. Yang, and H. Wang, *Predictive Abnormal Events Analysis Using Continuous Bayesian Network.* ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering, 2017. **3**(4): p. 041004.
140. Bureau of Safety and Environmental Enforcement (BSEE). *BSEE Data Center: Platform Structures*. https://www.data.bsee.gov/ (Accessed on 02/14/2019), 2019.
141. Datta, G.S. and M. Ghosh, *On the invariance of noninformative priors.* The annals of Statistics, 1996. **24**(1): p. 141-159.
142. Williamsen, M., *Near-miss reporting: A missing link in safety culture.* Professional Safety, 2013. **58**(05): p. 46-50.
143. Adedigba, S.A., F. Khan, and M. Yang, *Process accident model considering dependency among contributory factors.* Process Safety and Environmental Protection, 2016. **102**: p. 633-647.
144. Pasman, H. and W. Rogers, *How can we use the information provided by process safety performance indicators? Possibilities and limitations.* Journal of Loss Prevention in the Process Industries, 2014. **30**: p. 197-206.

APPENDIX A

DEFINITION OF CONTRIBUTING FACTORS AS USED IN THE INCIDENT INVESTIGATION REPORT ANALYSIS [136]

For each incident, the following questions were asked. Terms for which the answers came 'yes' were noted as a factor for the incident.

	Term	**Definition of term as used in analysis**
1.	Equipment Failure	Did the incident initiate due to failure of a particular equipment?
2.	Human error	Did the incident occur due to a mistake/violation/attention failure/memory failure of an operator/supervisor?
3.	External damage/collision	Did the incident occur due to any large impact (such as between helicopter and rig/platform) from outside? Note that this is different from point 4 which refers to impact within a platform
4.	Impact/dropped object	Did the incident occur because there was an impact between two objects inside the rig/platform? (See point 3 also)
5.	Weather related/ natural cause	Did the incident involve a natural calamity (*e.g.* storm)
6.	Leak	Did the incident occur due to a leak?

	Term	**Definition of term as used in analysis**
7.	Incomplete/improper JSA or PHA	Was the Job Safety Analysis (JSA) or Process Hazard Analysis (PHA) missing or inadequate? Did the JSA/PHA fail to identify all the hazards?
8.	Permit to work	Was there a problem with the permit to work? Was the permit to work missing?
9.	MOC related	Was there a missing MOC (Management of Change)? Was the MOC wrong?
10.	Inadequate/lack of maintenance	Was there negligence in the maintenance? Was the maintenance in backlog? Was the maintenance done in a way that later led to the incident?
11.	Improper inspection	Was there a failure to find the flaw during an inspection? Was inspection not done when needed?
12.	Improper installation	Did improper installation (*e.g*. a missing gasket at a previous maintenance work) of equipment or parts lead to the incident?
13.	Inadequate/improper procedure	Was the method of task completion not clearly defined or not defined at all through documentation? Was there a flaw in the procedure?

	Term	Definition of term as used in analysis
14.	Procedural Deviation	Did a person deviate in action from the procedure or from steps outlined in the Job Safety Analysis (JSA) ? (This includes both deliberate and non-deliberate actions)
15.	Inadequate isolation	Was there a missing physical barrier, or were there improper measures/lack of measures taken to isolate a system in case of a loss of containment?
16.	Design flaw	Did the incident initiate because there was a design flaw or there was a mistake made in the way the system had been designed?
17.	Unsuitable/improper equipment	Was the equipment/tool being used for the task not the right one to fulfil the function? Was the equipment/tool expected to function beyond its design criteria/range?
18.	Improper material/parts	Did the equipment involved in the incident have a wrong material of construction or a wrong part inserted?
19.	Failure due to excess vibration	Did the incident occur due to a failure that resulted from excessive vibration?
20.	Corrosion	Did the incident arise due to a corrosion problem?
21.	Degradation of material	Did the incident occur due to degradation of a material caused by any reason apart from corrosion (such as

	Term	Definition of term as used in analysis
		abrasion, heat or too much stress applied to a material that caused it to fail)?
22.	Contamination	Did the incident involve any contamination or addition of impurities?
23.	Failed to detect	Did the incident occur because of occurrences that went undetected or unnoticed?
24.	Failed to respond on time	Did a human/equipment fail to carry out an action on time when it was supposed to be done that led to the incident?
25.	Improper communication	Was there a missing information between any two entities (e.g. between two operators or between operator and management/supervisor)?
26.	Inadequate/improper supervision	Was the supervisor giving wrong instructions, no instructions, absent before the incident occurred?
27.	Inadequate control	Did the incident occur because the system/task could not be controlled properly?
28.	Inadequate/no training	Was appropriate training given to the operator at the correct time?
29.	Improper storage and handling	Was something stored in a manner it was not supposed to be that led to the incident?

	Term	Definition of term as used in analysis
30.	Improper Mud Weight	Did improper mud weight in the column lead to loss of containment that caused the incident?
31.	Hot work related	Was hot work being performed that led to the incident?
32.	Cementing Problem/Improper cementing	(Related to drilling): Did the incident occur because of improper cementing inside the well?
33.	*Unsuitable PPE	Was any person injured in the incident wearing a wrong Personal Protective Equipment (PPE), or not wearing a PPE at all?
34.	*Slip/Trip/Fall	Did someone slip, trip or fall during the incident?
35.	*Flawed emergency preparedness	Was the emergency response flawed?
36.	*Overboard Drilling Fluid	(Related to pollution incidents) Was any drilling fluid spilled overboard?
37.	*Lack of equipment	Did the incident propagate due to lack of equipment (such as fire detectors, extinguishers)?
38.	Other	Are there any other factor that has not been considered in this questionnaire?

* These factors were on consequences of the fire incident analyzed and hence were not considered in the analysis.

APPENDIX B

OPENBUGS ALGORITHM TO DETERMINE POSTERIOR PARAMETERS, FAILURE PROBABILITY IN GIVEN TIMES AND TIME TO NEXT FAILURE

```
model {
for(i in 1:N) {
zeros[i] <- 0
zeros[i] ~ dpois(phi[i])
#phi[i] = -log(likelihood)
}
#Power-law model (failure-truncated)
phi[1] <- -log(beta) + beta*log(alpha) - (beta-1)*log(t[1]) + pow(t[1]/alpha, beta)
t[N] ~ dgamma(0.0001, 0.0001)I(t[N-1],) #Monitor node t[N] for time to next failure
for(j in 2:N) {
phi[j] <- -log(beta) + beta*log(alpha) - (beta-1)*log(t[j]) + pow(t[j]/alpha, beta) -
pow(t[j-1]/alpha,
beta)
}
lambda <- pow(alpha, -beta)
t.GOM1 <- 695 #Average years of operation in 3 calendar months in US OCS
t.window1 <- t[N] + t.GOM1
```

```
pr.g1 <- 1 - exp(-lambda*(pow(t.window1, beta) - pow(t[N], beta))) #Mean will give
probability of failure in the next 0.25 real year in GOM
t.GOM2 <- 1390 #Average years of operation in 6 calendar months in US OCS
t.window2 <- t[N] + t.GOM2
pr.g2<- 1 - exp(-lambda*(pow(t.window2, beta) - pow(t[N], beta))) #Mean will give
probability of failure in the next 0.5 real year in GOM
t.GOM3 <- 2085 #Average years of operation in 9 calendar months in US OCS
t.window3 <- t[N] + t.GOM3
pr.g3 <- 1 - exp(-lambda*(pow(t.window3, beta) - pow(t[N], beta))) #Mean will give
probability of failure in the next 0.75 real year in GOM
t.GOM4<- 2780 #Average years of operation in 12 calendar months in US OCS
t.window4 <- t[N] + t.GOM4
pr.g4 <- 1 - exp(-lambda*(pow(t.window4, beta) - pow(t[N], beta)))

t.p1<- .5 # 6 months of plant operation
t.w1<- t[N] + t.p1
pr.p1<- 1 - exp(-lambda*(pow(t.w1, beta) - pow(t[N], beta)))
t.p2<- 1 # 1yr of plant operation
t.w2<- t[N] + t.p2
pr.p2<- 1 - exp(-lambda*(pow(t.w2, beta) - pow(t[N], beta)))
t.p3<- 1.5 # 1.5 yr of plant operation
t.w3<- t[N] + t.p3
```

```
pr.p3<- 1 - exp(-lambda*(pow(t.w3, beta) - pow(t[N], beta)))

t.p4<- 2 #2 yrs of plant operation

t.w4<- t[N] + t.p4

pr.p4<- 1 - exp(-lambda*(pow(t.w4, beta) - pow(t[N], beta)))


alpha ~ dgamma(0.0001, 0.0001) #Prior

beta ~ dgamma(0.0001, 0.0001) #Prior

}
```