RISK BASED FRAMEWORK FOR CRITICAL DECISION MAKING

by

© Mark van Staalduinen

A Thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Engineering

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

October, 2016

St. John’s, Newfoundland and Labrador

ABSTRACT

Risk analysis is a science of understanding and quantifying the probability of the occurrence(s) of undesirable event(s). Traditionally, risk assessments have been concerned with the management of safety based incidents. Recent attacks on chemical facilities in the Middle East and Northern Africa illustrate the need to broaden the risk management mindset. This body of work proposes quantitative barrier-based methodologies to assist management of broad-based decision-making processes. This research began by exploiting concepts from security-based research accompanied with a barrier-based methodology from safety research through both fault and event trees. This work expands into mapping the trees onto Bayesian Networks to manipulate the conditional probability table of intermediate variables. This manipulation allows for the implementation of various relaxation assumptions. Case studies accompany each proposed approach to illustrate its execution. The goal of this work is to raise awareness of quantitative security based methodologies and to assist in critical decision-making.

ACKNOWLEDGEMENTS

I would like to recognize my gratitude towards my supervisors Dr. Faisal Khan and Dr. Veeresh Gadag for their comments, mentorship, and guidance through the learning process of this master thesis. Furthermore, I would like to thank them for their insightful support and constructive criticism to endlessly push me to become a better engineer, researcher, and person. To them, I am eternally thankful.

I am grateful for Dr. Genserik Reniers, who assisted and provided remarks in completion of the Chapter 3 manuscript.

Additionally, I would like to thank my parents and immediate family members for their undying support, constant source of love, and encouragement to pursue higher education. I would also like to thank my fiancée, Jennifer, who helped me to stay focused on my graduate studies. Without their help, I would not be the person I am today.

Table of Contents

List of Tables

List of Figures

List of Symbols, Nomenclature or Abbreviations

α – gamma distribution shape parameter

β – gamma distribution scale parameter

θ – unknown parameter

λ – prior distribution

λ_p – mean value of posterior distribution

c_i – causation probability

c_L – leaky parameter

k – consequence severity level

$N_{F,i}$ – number of failures at barrier i

$N_{S,i}$ – number of success at barrier i

P(E) – basic event failure

P(T) – threat probability

q_i – inhibitor probability

SB_k – security barrier associated with level k

s_i – substitution probability

t – time interval

x_i – child node

y_n – likelihood distribution data

z – discrete random variable

ACC – American Chemistry Council

ANSI – American National Standards Institute

APCI – Air Products and Chemicals Inc.

API – Ameircan Petroleum Institute

ASME – American Society of Mechanical Engineers

AVM – Asset Vulnerability Model

BN – Bayesian Network

BT – Bow Tie

C – Communication

CCPS – Center for Chemical Process Safety

CFATS – Chemical Facility Anti-Terrorism Standards

CPT – Conditional Probability Table

DHS – Department of Homeland Security

F – Fortification

FRT – Facility Response Team

FTA – Fault Tree Analysis

LNG – Liquefied Natural Gas

NRC – National Research Council

P&ID – Piping and Instrumentation Diagram

PRA – Probabilistic Risk Assessment

QSRA – Quantitative Security Risk Assessment

RAMCAP – Risk Analysis and Management for Critical Asset Protection

SHIPP – System Hazard Identification, Prevention and Prediction

SRA – Security Risk Assessment

SRFT- Security Risk Factor Table

SVA – Security Vulnerability Assessment

SVAPP – Security Vulnerability Assessment, Prevention and Prediction

TA – Threat Analysis/Assessment

VA – Vulnerability Analysis

Introduction and Overview

Risk analysis is a science of understanding and quantifying the probability of the occurrence of undesired events and associated outcomes. It aims to demystify uncertainty connected with these undesired events and outcomes. The chemical process industry encourages the application of Probabilistic Risk Assessment (PRA) as a risk analysis method to study the occurrence of low probability – high consequence accidents. Through implementation of the methodologies, these accidents and their outcomes can be mitigated. Risk analysis in the area of chemical safety is focused on unintentional acts whereas, in chemical security, risk analysis focuses on intentional acts. Following the attacks on September 11, 2001, the Department of Homeland Security (DHS) was granted the authority to manage security risk in chemical plants within the United States (U.S.) (DHS, 2003). The goal of the DHS was to regulate security of chemical plants involving high risk chemicals (DHS, 2003). This goal led to the development of PRA as a risk analysis method by using estimates of different components of risk, based on opinions of experts in the industry (Sadiq 2013). Furthermore, the development of Chemical Facility Anti-Terrorism Standards (CFATS) imposed federal regulations on chemical facilities considered to be at high risk (DHS, 2007). Later, Sadiq (2013) recognized that CFATS still needed improvements and implored researchers to further investigate how enhancements could be made in PRA technique.

There has been much controversy over which technique is best suited to conduct a risk analysis associated with terrorism. The National Research Council (NRC) (2008) highlighted the difficulty in assessing the proper risk probability as techniques are based solely on expert opinion. However, Ezell et al. (2010) argued that while there are shortcomings in PRA technique, this methodology can still be utilized effectively to understand terrorism risk. The methodologies presented in this thesis go one step further in addressing the concern of the NRC. Within this research, we obtain the initial risk estimates based on the use of existing PRA method. We then use these values as prior probabilities in the Bayesian analysis techniques to continually update the security risk probabilities based on real data on incidents as they unfold over time and provide estimates of realistic risk probabilities in real time.

The methodologies presented in the subsequent chapters are based on barrier approach methods known as epidemiological accident models. Epidemiological accident models can easily be understood through Reason's "Swiss Cheese" model (1990). Reason's model proposes that each "slice of cheese" acts as a barrier and an accident occurs when holes in the barriers align. The hole in a barrier can be a failure or a weakness of the system which then illustrates that an accident is a process of multiple causalities. To better depict the complete accident process, Kujath et al. (2010) combined Reason (1990) and Bird and Germain (1996) to develop a conceptual model for an offshore environment. This qualitative barrier approach with five mechanical barriers used both fault trees and an event trees to illustrate the escalation of an accident if a particular barrier was to fail.

Rathnayaka et al. (2011) further enhanced the conceptual model proposed by Kujath et al. (2010) to expand the model to all process industries. System hazard identification, prevention and prediction (SHIPP) methodology added the dimension of event tree analysis and basic probability failure to transform the approach into a probabilistic risk assessment (PRA). In addition, the authors added two more barriers that account for human interaction within the system. The quantitative component was executed through event tree analysis (ETA) and determineed the likelihood of various types of accidents. Rathanayaka et al. (2011) introduced an updating mechanism and predictive component which minimized uncertainties. The predictive component used past history data to determine the expected future events in the subsequent time interval. Meanwhile, the updating mechanism utilized new information and data based on the number of events that occurred as they occur to update the likelihood of each consequence.

Probabilistic risk assessments can be executed through the use of fault and event trees, Bayesian Networks (BN), and Bow-Tie models. Fault and event tree analysis is widely used and is a common approach to determine the failure probability of a system. A top event or system failure can be broken down into further sub systems and components linked through Boolean logic gates. At the base of each fault tree are the basic events, typically failures, that may trigger the gate above it based on the logic assigned. Basic event probability can be found through historical data, literature, or where needed, expert judgment. Event tree analysis is utilized to show the sequence of failures that lead to the various consequences. The top event probability, which can be represented by a barrier or system failure, helps to calculate the occurrence probabilities for each consequence. Delvosalle et al. (2005) described a Bow-Tie model as a fault tree that ties directly into an event tree. The basic events are on the left side and consequences are on the right side. Furthermore, both the fault and event trees can be mapped into Bayesian Networks (BN) (Bobbio et al. 2001). BN are graphical method used to illustrate relationships between events and outcomes. A parent node (event) will have a direct arc to a child node (outcome), where the arc denotes a direct relationship between the two nodes. A BN has the ability to combine any finite number of variables into one joint probability distribution (Díez and Druzdel 2007). Through the graphical presentation, BN have the ability to aid decision makers as they perceive the direction of casual influence of one variable over another. Additionally, BN allows for the conditional probability table (CPT) to be manipulated. Pearl (1988) first introduced the concept of Noisy-OR, where a probability exists that may inhibit the parent node to cause the child node even if the parent node is still active. Other CPT manipulations have been developed such as, the Leaky Noisy-OR and the Noisy-AND (Díez and Druzdel 2007). The Leaky Noisy-OR is a similar cause to the Noisy-OR however, it adds a leak parameter that accounts for causes that could not be explicitly modelled (Adedigba et al. 2016; Abimbola et al. 2016). Meanwhile, the Noisy-AND adds a substitution probability that is replaced when a node is not active. Therefore, in the Noisy-AND technique, a parent node will either have a substitution or inhibitor probability.

While chemical safety risk assessments focus on natural-unintentional events, chemical security risk assessments concentrate on unnatural-intentional acts. Chemical processing facilities are targets for both criminal and terrorist acts as they contain hazardous, expensive materials in large quantities which may cause substantial causalities, economic loss, and have an environmental impact. In 2003, the Center for Chemical Process Safety (CCPS, 2003) released a document that outlined a Security Vulnerability Assessment (SVA) that discussed physical security analysis for a chemical site including management and prevention strategies. The CCPS (2003) described multiple concepts and defined numerous terms such as, rings of protection. Rings of protection is a concept whereby, the most valuable assets are located in the center and each ring has increasing security measures to further protect the asset. An intruder must penetrate numerous rings to reach the asset. The SVA methodology (CCPS, 2003) is broken down into five [5] steps which are: (1) Project Planning, (2) Facility Characterization, (3) Threat Assessment, (4) Vulnerability Analysis, and (5) Identify Countermeasures. The goal of project planning is to outline the objectives and scope developed by a multifaceted team. Facility characterization identifies critical assets, attractiveness of a target, and the possible consequences. Threat assessment defines the threats which may be internal, external, or a combination of an internal source colluding with an external source. The vulnerability analysis step combines an asset with a threat to evaluate the degree of vulnerability through either an asset-based approach and/or a scenario-based approach. Lastly, countermeasures are identified to provide improvements that would meet the security standards designated by the SVA team.

Within this thesis, we combined quantitative measures found in the safety discipline with the qualitative components of the security approach. Through this amalgamation, separate methodologies have been developed and demonstrated through case studies in the subsequent chapters. Chapter 1, entitled '*A Barrier Based Methodology to Asses Site Security Risk'*, builds the basis for the subsequent two chapters entitled '*SVAPP Methodology: A Predictive Security Vulnerability Assessment Modelling Method'* (Chapter 2) and '*Functional Quantitative Security Risk Analysis (QSRA) to Assist in Protecting Critical Process Infrastructure'* (Chapter 3).

In Chapter 1, the initial fault trees for each barrier are developed and the event tree is established. Furthermore, each fault and event tree are mapped into BN and each

CPT manipulation technique mentioned is explored. Chapter 2 proposes a Security Vulnerability Assessment, Prevention and Prediction (SVAPP) methodology that builds upon the foundations of Chapter 1 and continues to explore the relationships among the separate mapped barriers. The SVAPP, similar to SHIPP, executes an updating mechanism to continually obtain more accurate estimates of uncertainty (risk). It also has a prediction component to predict the total number of incidents that can be expected for the next time frame.

Chapter 3 is an independent methodology that utilizes the Bow-Tie concept to determine the overall attack probability and the subsequent consequence occurrence probabilities. The mapped fault tree to determine the attack probability adds more to detail the political barrier that was illustrated in Chapter 1. Additionally, the probabilities are altered depending on the various type of attacks that could be orchestrated on a chemical processing plant. If the risk is deemed not acceptable, the QSRA methodology allows for reassessment through a cost analysis of risk reduction strategies. The proposed QSRA approach contains a risk monitoring and tracking component through the use of key indicators, to ensure a re-assessment of the security program if an indicator changes.

As illustrated through the subsequent chapters, the goal of this manuscript is to raise awareness for the need of quantitative security methodologies to assist in an overall risk analysis of a chemical processing plant.

Co-authorship Statement

I hereby declare that the manuscript titled A Barrier Based Methodology to Assess Site Security Risk (van Staalduinen M, Khan F. *A Barrier Based Methodology to Assess Site Security Risk*. In: SPE E&P Health, Safety, Security, and Environmental Conference – Americas; 2015 Mar 16 – Mar 18, 2015; Denver, USA. Copy of the document available from Department of Process Engineering, Memorial University, St John's, Canada). As primary author, I led the development of the framework, its implementation, and analysis of the results with the help of co-author, Dr. Faisal Khan. I have drafted the initial manuscript, which was reviewed and commented by co-authors. Their suggestions were later incorporated in the final manuscript. As co-author, Faisal Khan helped developing the framework, and supported in finalizing the methodology to implement the framework. He also contributed in reviewing and revising the manuscript.

For the manuscript titled *SVAPP Methodology: A Predictive Security Vulnerability Assessment Modelling Method* (van Staalduinen MA, Khan FI, Gadag V. SVAPP Methodology: A Predictive Security Vulnerability Assessment Modelling Method. Loss Prevention in the Process Industries. 2016; 43: 397-413), I declare it was a joint research collaboration between: primary author, Dr. Faisal Khan, and Dr. Veeresh Gadag. I am the lead on this work. With the assistance of co-authors (Dr. Faisal Khan and Dr. Veersah Gadag) I developed the framework and implemented, analyzed and compiled the results. I have drafted the initial manuscript, which was reviewed and commented by co-authors. Their suggestions were later incorporated in the final manuscript. Co-authors (Dr. Faisal Khan and Dr. Veersah Gadag) helped developing the framework and supported in finalizing the methodology to implement the framework. They have also contributed in reviewing and revising the manuscript.

Finally, the third manuscript titled *Functional Quantitative Security Risk Analysis (QSRA) to Assist in Protecting Critical Process Infrastructure* (van Staalduinen MA, Khan FI, Gadag V, Reniers G. Functional Quantitative Security Risk Analysis (QSRA) to Assist in Protecting Critical Process Infrastructure. Reliability Engineering and System Safety. 2017; 157: 23-34). I declare it was a joint research collaboration between: primary author, Dr. Faisal Khan, Dr. Veeresh Gadag and Dr. Genserik Reniers. I am the lead on this work. With the assistance of co-authors (Dr. Faisal Khan, Dr. Veeresh Gadag, and Dr. Genserik Reniers) I developed the framework and implemented, analyzed and compiled the results. I have drafted the initial manuscript, which was reviewed and commented by co-authors. Their suggestions were later incorporated in the final manuscript. Co-authors (Dr. Faisal Khan Dr. Veeresh Gadag, and Dr. Genserik Reniers) helped developing the framework, and supported in finalizing the methodology to implement the framework. They have also contributed in reviewing and revising the manuscript.

Chapter 1: A Barrier Based Methodology to Assess Site Security Risk

1.0 Abstract

The recent attacks on petroleum plants in various countries such as Algeria, Nigeria, and Iraq have greatly changed the risk mindset of the chemical industry (Johnson and Gilbert, 2013; Nordland and Al-Sahy, 2014). Risk assessments and management traditionally are conducted on unintended (safety related) incidents and not on intentional acts. These intentional acts could either be from an internal or external source. This paper extends the probabilistic risk assessment methodology (generally focus on safety unintended) to the security facet (focusing on intended incidents) of a processing facility. The methodology is based on the barrier approach. Five security barriers are proposed throughout the facility to help deter an attack. These security barriers are external, internal, interior, critical, and the fail-safe barrier, which are implemented at various stages of a plant with varying objectives. For example, the fail-safe barrier aims to bring the plant to safe shutdown mode, once it observes breach of the barrier. Breach of each barrier is modeled using fault tree approach. A number of monitoring parameters are proposed to track the effectiveness of the barrier, which are modeled as basic events in the fault tree. The occurrence of each basic event is modeled using two failure modes: i) natural, and ii) forced failure. Conditional probability with soft computing theory is used to model occurrence probability. The proposed methodology also takes into account effectiveness of the management, and political parameters in an impeding attack.

In addition, the fault trees modeled are mapped into respective Bayesian Networks. Bayesian networks allow for manipulation of the conditional probability table. There are three relaxation assumptions that manipulate the conditional probability table

that is explored in this paper. In order to eliminate uncertainty developed in the data, an updating mechanism is used along with a predictive component to make the model dynamic. This is significant as the model can be become dynamic to reflect any changes that may have occurred.

Finally, a case study of a typical processing facility is presented to demonstrate the effectiveness of the model and to indicate areas of further improvement. This paper aspires to bring awareness to security risk assessments and the need to create a database for security related failures.

1.1 Introduction

Prior to the attacks of September 11, 2001, risk assessments completed for chemical facilities focused primarily on safety incidents or natural events. Through risk analysis, the facilities were able to plan for not only the high frequency-low consequence accidents but also the low frequency-high consequence events. In the years immediately following 9/11, both the American Chemistry Council (ACC) and the American Petroleum Institute (API) released documents to aid chemical companies in conducting site security vulnerability assessments (SVAs) to help prevent attacks.

With current available security methodology, the need for continual improvement will always exist. In late February of 2006, the Abqaiq refinery in Saudi Arabia went under a terrorist attack from Islamic militants (BBC 2006). Vehicles with explosives attempted to gain access and cause damage to the world's largest refinery. At the cost of two security guard fatalities, the refinery was able to foil the attack and prevent any disruption. Almost three years after this attack, Iraq's largest oil refinery was shut down for several weeks due to a terrorist bombing (Al-Bazee 2011). Not only was the production of 150,000 barrels per day halted but four workers lost their lives. The most recent incident was the attack on the In Amenas gas refinery on January 16, 2013 that lasted three days (Hagen 2013). In total, forty [40] workers were killed throughout the duration of the attack. The above examples verify that security failures led to financial loss, material loss and most importantly loss of human life. Therefore, the need to create a proper security risk assessment is crucial.

Existing security risk methodologies are qualitative and based on SVAs that include a threat and vulnerability analysis. There is a need to develop a quantitative model and respective data. Through this quantification, models will have the ability to become more accurate and thus expose the weak points in a security management system. With this knowledge the appropriate measures can be taken to further deter and/or prevent attacks from happening.

The first methodology for modeling a safety incident was developed by Heinrich (1941). He proposed that accidents happen in chain of events or a sequence, and removal of any one element could therefore prevent the accident from occurring. Later, Reason (1990) developed the infamous "Swiss Cheese" model shown in Figure 1-1 below. This model proposed that each slice was a relevant barrier and each hole represented a weakness or a failure the system. An accident occurs when all of the holes align, otherwise it does not occur.

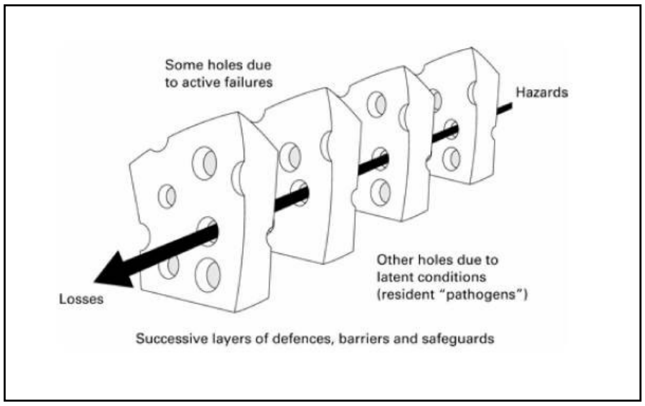

Figure 1 - 1: Swiss Cheese Model: Swiss Cheese Model (Adapted from Reason, 2000)

Further building upon this idea, was Kujath et al. (2010) who showed that each barrier could be described using fault tree analysis (FTA). Based in an offshore environment, the authors illustrated how basic event failures would lead to a barrier failure and thus an eventual accident. To provide a more holistic view, Rathnayaka et al. (2011) developed system hazard identification, prevention, and prediction (SHIPP) methodology based on the Kujath conceptual model. The conceptual accident model of SHIPP is shown Figure 1-2 and similar to Kujath, each barrier is built using FTA. Through the use of reliability data handbooks and expert judgment, the SHIPP method is able to assess and manage risk as well as represent the process accident sequence.

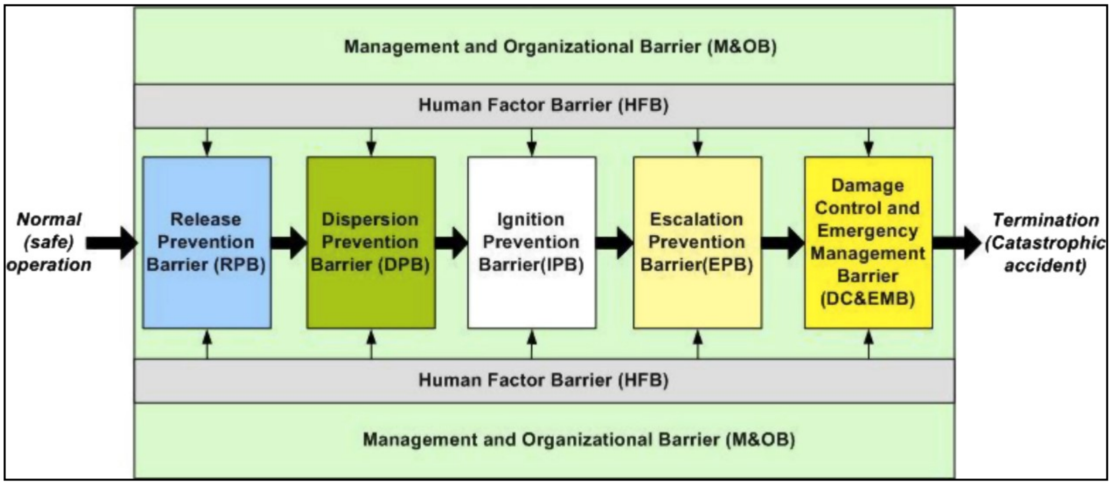
Management and Organizational Barrier (M&OB)
Human Factor Barrier (HFB)
Normal (safe) operation
Release Prevention Barrier (RPB)
Dispersion Prevention Barrier (DPB)
Ignition Prevention Barrier(IPB)
Escalation Prevention Barrier(EPB)
Damage Control and Emergency Management Barrier (DC&EMB)
Termination (Catastrophic accident)
Human Factor Barrier (HFB)
Management and Organizational Barrier (M&OB)

Figure 1 - 2: SHIPP Conceptual Accident Model (adapted from Rathnayaka et. al, 2011)

This current work is an extension of probabilistic risk assessment that previously focused on unintended or safety incidents. These events could be categorized as natural events, as they are expected to happen without the interference of human occupancy. Security incidents are characterized as intentional or unnatural events. The reason for this simply is that these incidents would not occur unless there is human interaction with the process. Security related accidents can stem from two main sources, internal or external. The American Petroleum Institute (API) recognizes three main threats to a chemical processing facility, which are (API 2003):

- Internal
- External
- Internal working with an external

Baybutt and Reddy (2003) indicate that an internal threat can come from either current or former employees or contractors. These threats frequently are intended to inflict economic damage through disruption of the process. An external threat however has a much more serious purpose with intentions to inflict casualties rather than economic damages. However, the most serious circumstance is the combination of an internal and external threat. With an inside knowledge of the facility, a terrorist group or criminal could extort a weakness and cause a major catastrophe.

Chemical sites are major targets for criminals and terrorists because of their hazardous materials and operating conditions. These sites are already at risk with natural events and the chance of an intentional act only increases the likelihood of incident to occur. Since the terrorist attacks on September 11, 2001, companies have begun to include security in their overall site risk assessment. The security culture first began to change with new releases of security guidelines for the chemical industry. One such document, from the American Chemistry Council (ACC 2001) discussed risk assessment, prevention strategies, management issues and physical security for a chemical site. An additional document was released by the Center for Chemical Process Safety (CCPS 2003), which introduced the idea of rings of protection that are shown in Figure 1-3, along with appropriate security countermeasures.

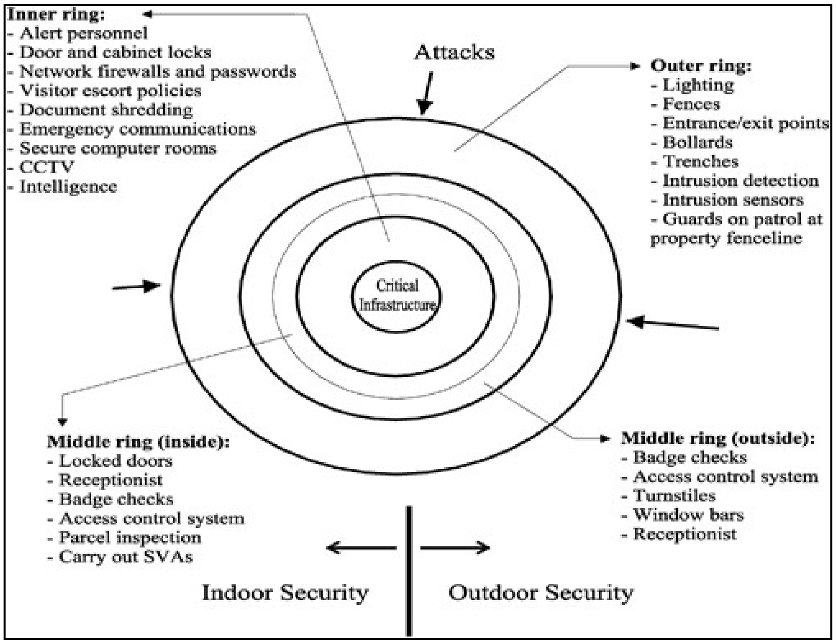

Figure 1 - 3: Rings of Protection from CCPS (2003)

Later, Bajpai and Gupta (2005) completed a work intended to combine these guidelines and develop a security methodology for the chemical process industries. The first step is to complete a threat analysis (TA). The main purpose of this is to recognize or identify any threats that are plausible at a certain plant. Next, a vulnerability analysis (VA) is completed to pair a target asset with a threat to determine its vulnerability. Simultaneously, existing security measures are evaluated to determine their overall effectiveness. Additionally, the vulnerabilities should be ranked based on attractiveness and consequence. At this stage, the authors add a security risk factor table (SRFT) to assess the current risk of a facility. With the security risks known, countermeasures can then be implemented to stop and/or neutralize an attack. The final step is the mitigation and emergency response. The purpose of this step is to finalize an emergency plan when an attack occurs and to ensure the proper authorities will assist in response to the attack. To exemplify this approach, the authors complete a case study of a typical plant and give security recommendations based on the results.

Bajpai and Gupta (2007) further use this and apply it to typical oil and gas infrastructure, a refinery. Through the qualitative analysis, the overall risk was able to be determined and thus appropriate recommendations and countermeasures were made which could further increase the security of the refinery. The proposed methodology and use of the security risk factor table (SRFT) could further be improved if the SRFT was completed at each of the various 'zones' to provide a more accurate holistic view of security. With each zone defined, it would be easier to see where improvements could be made.

In order to help the Department of Homeland Security (DHS) to develop a standard SVA, the American Society of Mechanical Engineers (ASME) in conjunction with AcuTech Consulting Group collaborated to develop Risk Analysis and Management for Critical Asset Protection (RAMCAP) (Moore et. al 2006). Moore et. al (2006) describe RAMCAP as a common method for conducting SVAs for owner and operators and in addition help to report vital information on risk to the DHS. The RAMCAP method is a qualitative approach because the US chemical industry did not have enough experience with terrorist attacks to be able to use quantitative methodology to accurately predict an attack. The first step in the RAMCAP method was screening, which was to determine an asset list that would be of interest to the DHS. Its purpose is to determine if the RAMCAP SVA would need to be completed and submitted to the DHS.

The RAMCAP SVA approach consists of seven components of analysis. The first step is asset characterization, which helps to identify the notable assets of a chemical facility. The remaining analysis is only completed on the noted critical assets. Therefore, the next step, threat characterization is used to seek how an attack can be completed against the critical asset. Following this, a consequence analysis is conducted to determine the worst possible outcomes that could be produced from the threat characterization. A vulnerability analysis is then completed to establish the strengths and weaknesses of the asset. Then, there are two threat assessments completed one by the owner and one by the government. This is done to determine the attractiveness of an attack for that particular facility. The final two steps are risk assessment and risk management. Risk assessment will help to create strategies to protect the assets against an attack and risk management will ensure that risk is kept a standard level for a suitable cost.

In 2013, Moore (AcuTech Consulting) worked in conjunction with the American National Standards Institute (ANSI)/American Petroleum Institute (API) to release a Security Risk Assessment (SRA) Methodology (Standard 780) which would be used as a security standard for the petroleum industries (Moore, 2013). Moore (2013) states the purpose of the SRA is to estimate the chance of a threat against a chemical facility that would result in an unwanted consequence. This new ANSI/API Standard 780 is designed to provide the petroleum industry with a holistic SRA. This methodology illustrates that the security risk is the likelihood of a successful act against a chemical facility while assuming both the likelihood of the act happening and the chance for success causing a set of consequences. In order to decrease this risk, there are five inter related steps. The first step is characterization of critical assets followed by the threat assessment to identify attackers and the attractiveness of an attack. Subsequently, a vulnerability assessment is carried out to estimate the likelihood of the various scenarios. The fourth step is the risk evaluation to determine any weaknesses of the critical assets. Finally, risk treatment is completed to establish security countermeasures. The goal of this methodology is to highlight areas of improvement for management and to better define an organizations risk tolerance and requirements.

The current work aims to apply the existing safety barrier method to the security aspect of a chemical facility. Using the probabilistic risk approach, this work intends to provide a holistic view of security risk analysis, which can be applied to all chemical industries. In discussing probabilistic risk assessment, Bayesian Network relaxation assumptions will also be explored. Following this, in Section 3, the security barrier model using fault and event trees will be discussed. In Section 4, data sources will be investigated as there is a current availability for failure events. A case study will be presented in Section 5 to outline the application of the proposed methodology. The final section will be devoted to the conclusions drawn in this paper.

1.2 Probabilistic Risk Assessment

Probabilistic Risk Assessments (PRA) have been widely used in recent years in a safety aspect to help plant managers make informed risk management decisions. One of the highlights of this work is to transition a safety barrier approach method into a security barrier approach. As shown in the previous section, most work in security risk analysis is qualitative and lacks any quantitative methods. PRA is an organized approach to examine highly complex systems that exist in various industries. In its simplest terms, the PRA determines the risk value which is the product of consequence and probability. The main result of the PRA, as described by Modarres (2008) is finding out the system elements that contribute the greatest amount of risk to the system along with the usefulness of various risk reduction strategies. In this work, fault and event tree analysis is first utilized to develop a base case scenario. With the base case built, the fault trees are then subsequently mapped into Bayesian Networks (BN). Furthermore, various relaxation assumptions have been applied to the developed BNs in order to show which case best reflects reality. As uncertainties may arise through calculation, a Bayesian updating mechanism has been added to improve the accuracy of quantification along with a predictive component to further develop existing security strategies.

Fault tree analysis is the most widely used approach when determining the failure probability of barrier (or system). The system is defined by its top event while the tree is composed of other systems and events. These smaller sub systems and events are then combined with various Boolean logic gates that will cause the top event. Probabilities are then assigned to the basic events through historical data or expert judgment. Event tree analysis is used to show which sequence of events can lead to which consequences. Each barrier (system) is assumed to be independent with each branch representing a success or failure. The subsequent barrier is activated when the current barrier fails. The failure probabilities of each barrier when used in an event tree give the occurrence probabilities of the various consequences.

Mapping fault trees into BNs is a simple process that is best described by Bobbi et al (1999). When considering a fault tree with simple *AND/OR* gates (such as the fault trees proposed), the basic component of the fault tree (leaf node) now represents a root node in a BN. Subsequently, each gate of a fault becomes a BN node and should be labeled appropriately. Similar to that of a fault tree, the connections between a node and its gate will remain the same. These connections are described as arcs between nodes. The arc originates at the 'parent' node and ends at the 'child' node. This process is illustrated in Figure 1-4 below.

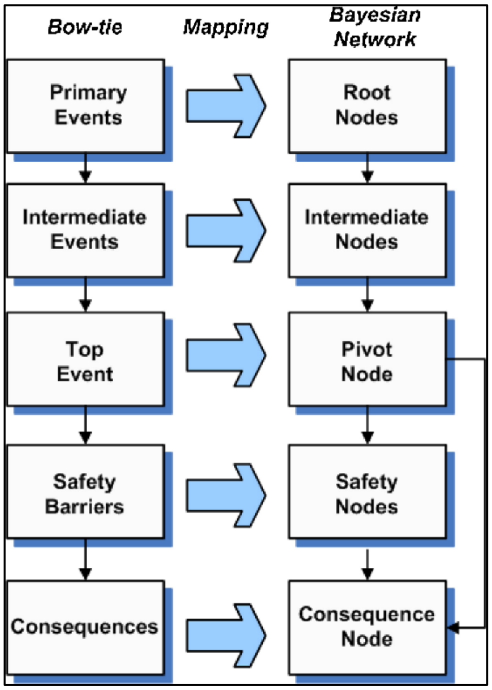

Figure 1 - 4: Mapping Flowchart (Khakzad et al. 2012)

However, a major difference is for each gate turned into a node, the conditional probability table (CPT) must match the logic of the gate (i.e. OR gate). This is an important factor as now the CPT can be manipulated based on various relaxation assumptions. With the CPT logic defined, the BN node probability can be calculated through the following Eq. 1-1 (Díez and Druzdzel 2007) :

$$P[X_1, X_2, \ldots X_n] = \prod_{i=1}^{n} P[X_i | Parent(X_i)] \tag{1-1}$$

An example of this mapping technique is shown in a later section of this paper.

As stated above, a key aspect of utilizing a BN over a fault and event tree analysis is the ability to manipulate the CPT. This paper outlines three techniques that can be applied to CPT. These techniques are called Leaky-OR, Noisy-OR, and Noisy-AND are covered in great detail by Díez and Druzdzel (2007) but will be briefly outlined here. The first relaxation assumption discussed is the Noisy-OR, where the term 'noisy' references the chance that the event may not occur because it was inhibited by an external independent factor. Simply, a parent node can occur /be present but the child node was not produced due to an inhibitor preventing it. This probability, denoted as c_i, is the probability that the parent produces the child while q_i is the probability that the inhibitor is active. This relationship is shown in Eq. 1-2,

$$c_i = 1 - q_i \tag{1-2}$$

When there are multiple parents to a child node, the child probability can then be calculated through the following Eq. 1-3:

$$P(Z | X_1, X_2, \ldots X_n) = \prod_{i \in x} (1 - c_i) = \prod_{i \in x} q_i \tag{3-1}$$

In the case of a Leaky-OR, a new variable is introduced to account parameters not in the model. As it is nearly impossible to include all causes of a certain effect, the leaky parameter (c_L) can account for it. The Noisy-OR is actually a particular case of the

Leaky-OR where its leaky parameter is equal to zero. Thus the equation to calculate the probability of the leak parameter is shown below in Eq. 1-4:

$$P(Z|X_1, X_2, \ldots X_n) = (1 - c_L) \times \prod_{i \in x}(1 - c_i) \qquad (1\text{-}4)$$

The last relaxation assumption that will be explored is the Noisy-AND. As Díez and Druzdzel explain, each condition of a child node can be either inhibited or substituted. Similar to Boolean logic, all parent nodes are required in order for the child node to be true. Noisy-AND introduces a new probability, s_i, which accounts for the parent node when it is not present. Hence, a parent node in a Noisy-AND model can either contribute an inhibitor or substituted factor based off whether it is present or not. The appropriate Eq. 1-5 for this model is shown below:

$$P(Z|X_1, X_2, \ldots X_n) = \prod_{i \in x} c_i \times \prod_{i \in x} s_i \qquad (1\text{-}5)$$

Based on prior and precursor data, an important feature of the proposed model is the ability to predict the number of abnormal security events. This prediction will be both qualitative and quantitative in order to best provide information to help improve a chemical plant's security strategies. The predictive model will follow a similar approach used in Rathnayaka et al. (2011) to help determine the number of events in the next time interval.

Hamada et al. (2008) proposed a general predictive Eq. 1-6 for discrete random variable *z*, based on observed data where the unknown parameter is symbolized by θ, the posterior distribution by $p(\theta/\pi)$, and the sampling distribution by $p(z/\theta)$ where π is the data in the posterior distribution.

$$p(z/\pi) = \sum_{all\,\theta} p(z/\theta)p(\theta/\pi) \tag{1-6}$$

Eq. 6 is now reestablished into Eq. 1-7 to determine the number of abnormal events where the posterior distribution now becomes *p(λ/data)* and the sampling distribution is *$p(y_{t+1}/\lambda)$*. The average number of abnormal events is now represented by the variable λ.

$$p\left(\frac{y_{t+1}}{data}\right) = \sum_{all\,\theta} p\left(\frac{y_{t+1}}{\lambda}\right) p\left(\frac{\lambda}{data}\right) \tag{1-7}$$

Rathnayaka (2011) points out that in the above equation, *data* is equal to the number of observed abnormal events during the time interval *t*, and the gamma distribution is the most widely used prior distribution for λ. Eq. 1-8 below represents the gamma distribution probability density with the parameters α and β.

$$p\left(\frac{\lambda}{\alpha,\beta}\right) = \frac{\beta^{\alpha}}{\Gamma\alpha}\lambda^{\alpha-1}e^{-\beta\lambda} \tag{1-8}$$

The number of abnormal events is to be considered a discrete and independent variable which follows a Poisson distribution with rate λ. In this assumption, the likelihood distribution for data (y_1, … y_n) is illustrated in Eq. 1-9:

$$p\left(\frac{data}{\lambda}\right) = \frac{\lambda^{\sum_{i=0}^{n} y_n} e^{-n\lambda}}{\prod(y_n!)} \tag{1-9}$$

Through the conjugate property, the posterior distribution will also follow the gamma distribution except its parameters $\alpha_p = \alpha + \sum_{i=0}^{n} y_n$ and $\beta_p = \alpha + n$. The total number of abnormal events is the summation of all the events over all of the time intervals. In Eq. 1-10, an updated value of λ can be found from the mean value of the posterior distribution.

$$\lambda_p = E\left(\frac{\lambda}{data}\right) = \frac{\alpha+\sum_{i=0}^{n} y_n}{\alpha+\beta} \tag{1-10}$$

In summary, Eq. 1-11 can determine the predictive probability distribution of occurrence for an abnormal event in the next time interval based on data through an approximated Poisson process.

$$p\left(\frac{y_{t+1}}{data}\right) = \frac{\lambda_p^{y_{t+1}} e^{\lambda_p}}{y_{t+1}!} \qquad (1\text{-}11)$$

Through quantification of the fault and event tree analysis, there is room for uncertainty to grow or for the accuracy of the consequence probabilities to decrease. This can arise by using point value form probabilities in addition to the error that may arise by using expert judgment or in literature. Therefore, a Bayesian updating mechanism is utilized to reduce the uncertainty that can occur. Bayes' theorem allows for initial beliefs to be updated through the use of likelihood probabilities from newly observed data. Similar to the predictive modeling approach, this probability updating method will very closely follow Rathnayaka et al (2011). This updated probability can be calculated by Eq. 1-12 where the denominator represents a normalizing factor:

$$p\left(\frac{x_i}{data}\right) = \frac{p(data/x_i)p(x_i)}{\sum p(data/x_i)p(x_i)} \qquad (1\text{-}12)$$

The prior probability is defined by *p(x_i)* calculated through fault tree analysis and the likelihood is represented by *p(data/x_i)* is calculated from abnormal event data. The first step in the likelihood calculation is to determine the number of abnormal events for each month and the relative success and failures of each barrier. In Eq. 1-13, $N_{F,i}$ and $N_{S,i}$ represent the number of failures and success at each barrier, respectively.

$$p\left(\frac{data}{x_i}\right) = \frac{N_{F,i}}{N_{F,i}+N_{S,i}} \qquad (1\text{-}13)$$

With the likelihood probabilities estimated and prior probabilities known, each can be placed into Eq. 12 to determine the new posterior probability. Finally, Eq. 1-14 can be used in event tree analysis to update the occurrence probabilities of the accident denoted by *p(c_k/data)*.

$$p\left(\frac{c_k}{data}\right) = \prod_{i=SB_k}\left(\frac{x_i}{data}\right)^{\theta_{i,k}}\left(1-\left(\frac{x_i}{data}\right)\right)^{1-\theta_{i,k}} \quad k = 1, 2, 3, 4, 5 \qquad (1\text{-}14)$$

1.3 Model Presentation

Previous security methods have been based on qualitative analysis. An attack is the result of an intentional act to cause harm. In its worst-case form (act of terrorism) it can cause consequential damage to not only human life but economic and environmental as well. The problem with attempting to model an attack is that it can happen in any number of ways and therefore the best countermeasure is to define security measures that can prevent them. Security measures can range in difficulty and thus the more sophisticated security system in place, the less likely an intentional failure can be accomplished. There are however two elements that can influence the attack process at any time, the Management and Organization barrier and the Political barrier. The relationship of all the barriers is shown in Figure 1-5.

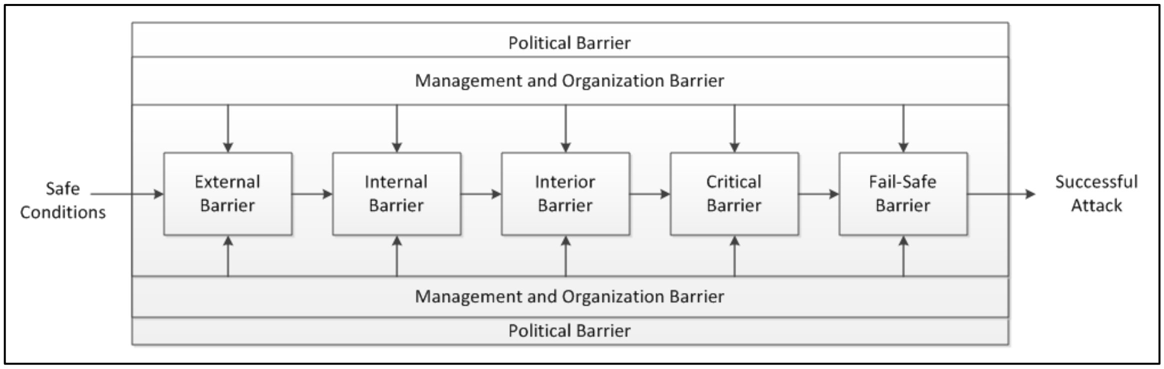

Figure 1 - 5: The Attack Model

The cause-consequence relationship is represented with fault and event tree analysis. In fault tree analysis (FTA), the top event signifies a failure for the entire barrier. Each top event will fail when the associated sub element barriers fail. The first four barriers (external, internal, interior, and critical) all have similar sub elements. Reniers (2010) proposed that physical security measures should be based on structural, electronic, a personnel barrier (or security checkpoint in case of external), which is implemented in this model. Even though the plant has been separated into barriers or zones, each measure is likely to overlap with another barrier. This however is not considered in this model. It is assumed that each barrier is a stand-alone entity and does not interact with each other.

The function of the external security barrier is to provide the first line of defense against an attack. Structural countermeasures for a chemical plant can be a perimeter fence, entrance/exit gates, bollards, and trenches. The electronic barrier is divided into power and intrusion detection devices because if the power is lost to the plant then the electronic barrier has failed. The intrusion devices are line of sight sensors, video motion and lighting. The final sub element of the external barrier is the personnel barrier. This barrier acts a security checkpoint in order to gain entrance into the chemical facility. At a security checkpoint there is a bag check, personal inspection (may be completed through image technology), vehicle inspection, and appropriate documentation for employees or contractors. The proposed fault tree for this barrier is shown below in Figure 1-6. Subsequent failure of this fault will allow access on the chemical facility’s grounds.

The purpose of the internal security barrier is to prevent an adversary from gaining access to structural buildings that are on the chemical plant property. The structural barrier is broken down into road conditions, manual locked doors and manual locked windows. Road conditions is a security measure that can often be overlooked. For instance, a well paved and maintained road will make moving around a chemical plant much easier for an attacker. Similar to the external barrier, the internal security electronic barrier is divided into power and intrusion devices. However, it adds a badge swipe component which will have the ability to electronically unlock doors. The personnel barrier includes both a reception area that can be a check-in desk past the security checkpoint and a mobile security unit. This unit would be tasked with making routine rounds throughout the plant. The fault tree for this security barrier is shown in Figure 1-7.

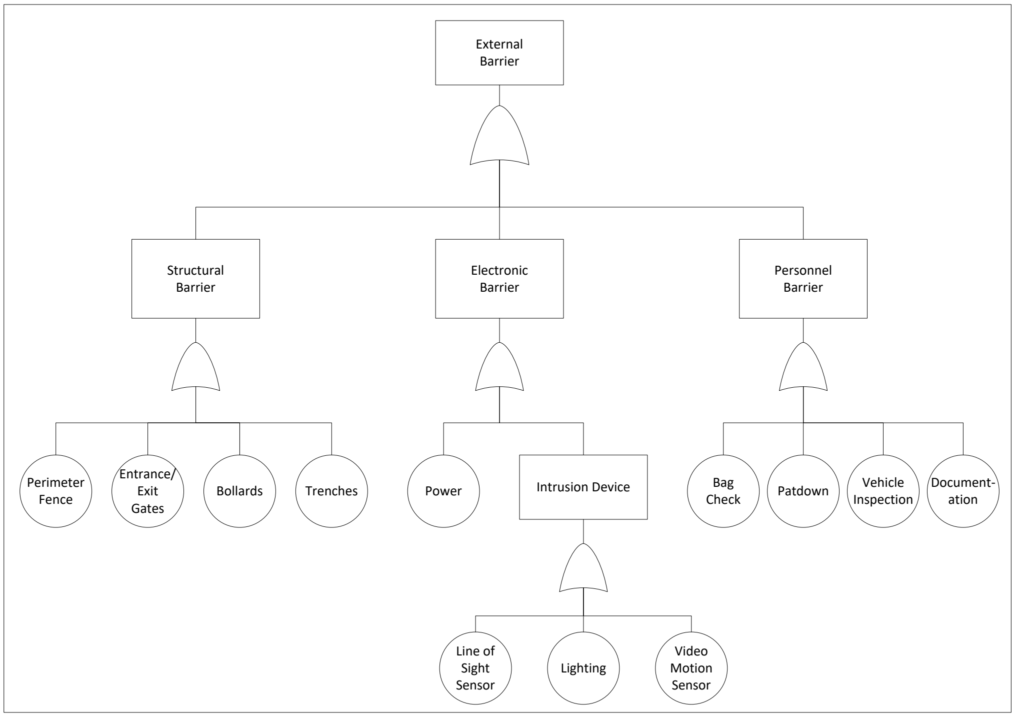

Figure 1 - 6: Proposed External Security Barrier Fault Tree

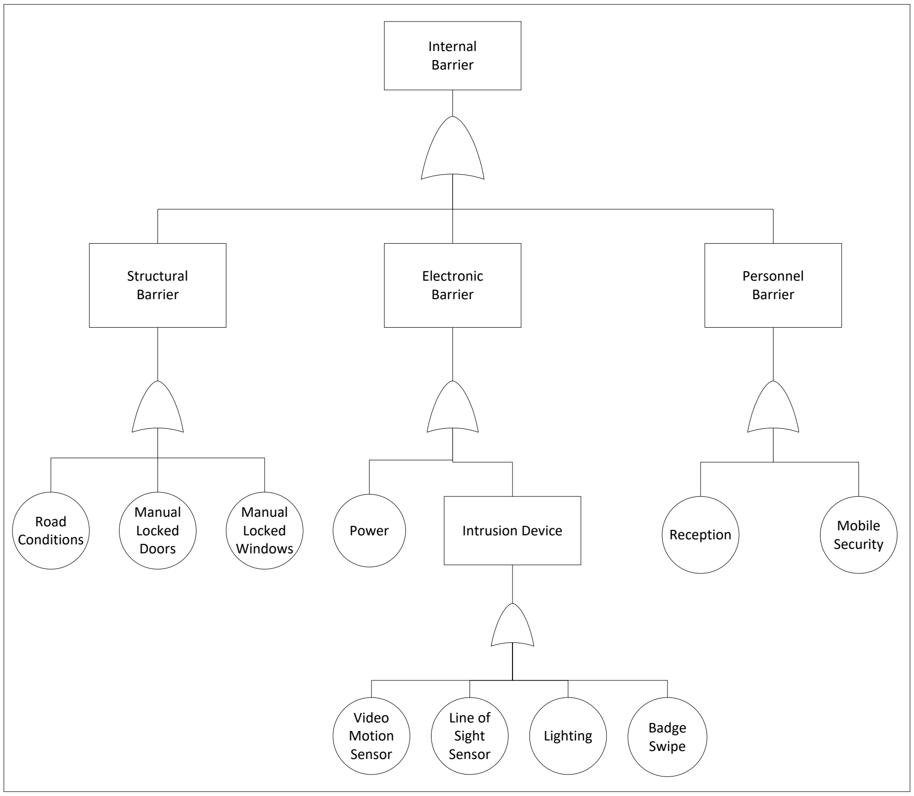

Figure 1 - 7: Proposed Internal Security Barrier Fault Tree

Following is the interior security barrier, which would deter unauthorized personnel from gaining access to employee workstations and offices. For the interior structural barrier, limiting the access points and having manual locked doors can deter an attacker. In addition, the electronic barrier includes biometric access and boundary penetration devices. These devices would detect when someone has gained unauthorized entry. However, the effectiveness of the personnel barrier is a function of the vigilance of the employees of the facility. Employees must be aware when unauthorized personnel are on site and should take notice of visitors. The interior security fault tree is shown in Figure 1-8.

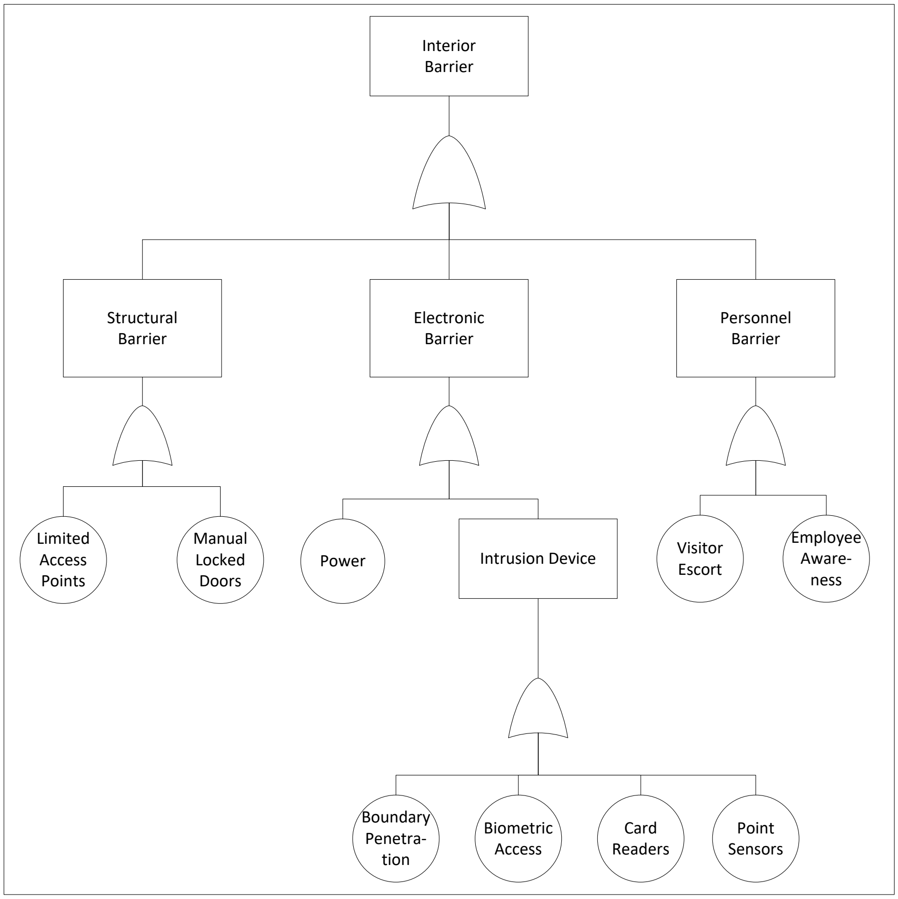

Figure 1 - 8: Proposed Interior Security Barrier Fault Tree

The critical security barrier is to prevent unwanted individuals from accessing the chemical plants control room. Similar to the interior barrier, the structural barrier consists of limited access points and manual locked doors. But in the electronic barrier, a firewall element has been added. The firewall is to prohibit unauthorized users from gaining proprietary information or manipulation of the process controls. Additionally, the personnel barrier should restrict visitor access to this security point. A proposed fault tree for this barrier is displayed in Figure 1-9.

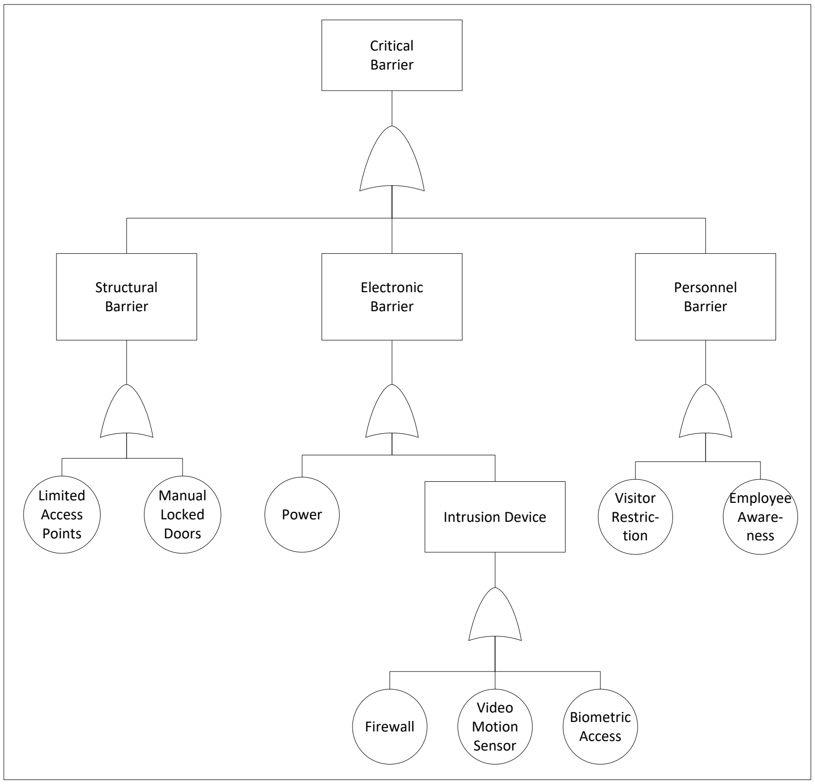

Figure 1 - 9: Proposed Critical Security Barrier Fault Tree

The last security barrier and last line of defense is the fail-safe security barrier. This barrier is separated into two categories of fail-safe mechanisms, manual and electronic. These mechanisms can come from an alarm or a shutdown. The alarm has the ability to warn employees of the unsafe conditions that the processing plant is incurring. Meanwhile the shutdown will end operations in order to revert back safe working conditions. The fault tree for this security barrier is represented in Figure 1-10.

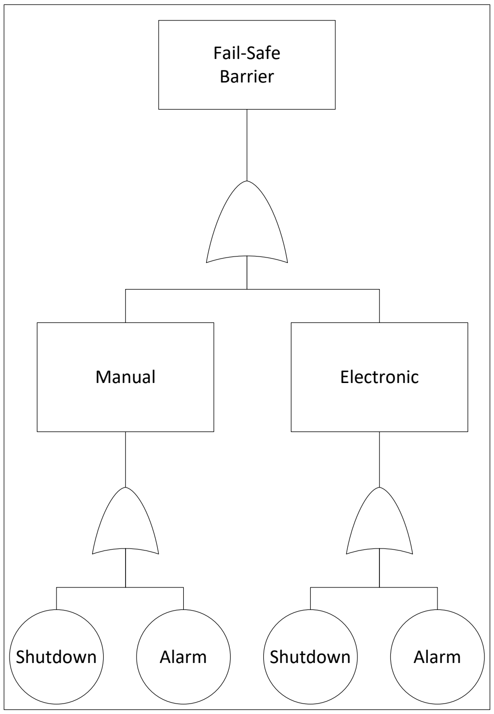

Figure 1 - 10: Proposed Fail-Safe Security Barrier Fault Tree

In regards to the above stated security barriers, each barrier's effectiveness will depend on the devices and security measures that are utilized. However, making economic and cost efficient selection for devices is imperative. For instance, it would be ideal to have biometric access at each door in order to ensure maximum security but the cost to supply this for an entire chemical facility is not feasible. Therefore, management should take the appropriate and practical actions to guarantee each security barrier is well equipped.

The management and organization barrier has the ability for its sub elements to intervene at any stage during an attack. This barrier is difficult to portray as each industry and individual companies will have various standards and protocols. Nevertheless, important factors were determined and a fault tree was designed as shown in Figure 1-11.

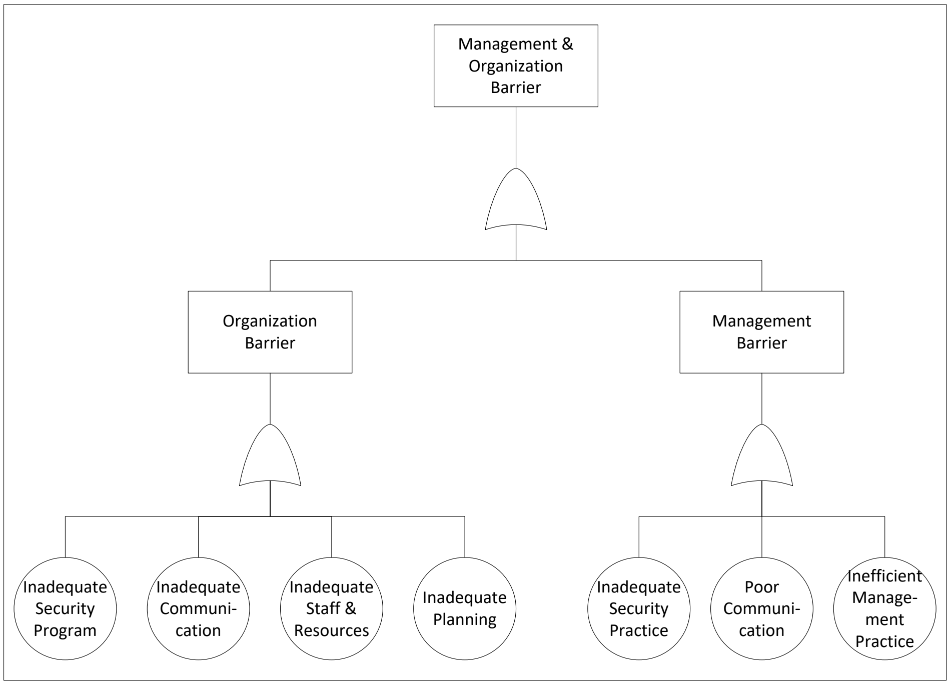
Management & Organization Barrier
Organization Barrier
Management Barrier
Inadequate Security Program
Inadequate Communi-cation
Inadequate Staff & Resources
Inadequate Planning
Inadequate Security Practice
Poor Communi-cation
Inefficient Manage-ment Practice

Figure 1 - 11: Proposed Management and Organization Security Barrier Fault Tree

The most important barrier in the model is the political barrier. This barrier takes into account the on-going situations around the chemical facility itself. Three main sub-barriers have been developed which are laws and enforcement, crime, and terrorism. The crime sub element is separated into hostage situations, stealing, and armed attack instances. There are five types of terrorism that would consider using a chemical plant as a target. Grothaus (2014) describes these types of terrorism as follows:

- State – government use of terror to regulate its population
- Religious – individual or groups use ideologies to justify use of terror
- Pathological – individual or groups that use terror for personal enjoyment
- Issue-Orientated – individual or groups inflict terror to bring awareness to a certain problem

- Separatist – a group that wishes to get rid of the current government and create a new state.

The laws and enforcement barrier is relative to the country or region as it looks at the measures in place to protect both the workers and the operation of the chemical facility. This fault tree is shown in Figure 1-12.

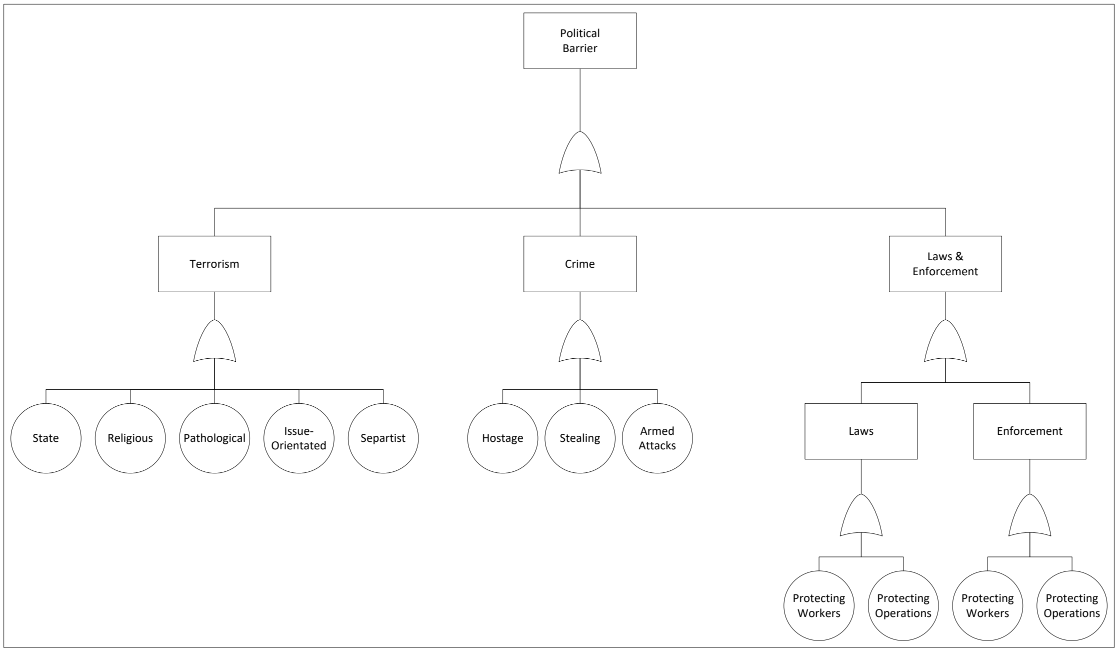

Figure 1 - 12: Proposed Political Security Barrier Fault Tree

In order to determine the consequences of the possible outcomes for an attack on a chemical plant, event tree analysis is applied in conjunction with an event network. The event tree is shown in Figure 1-13.

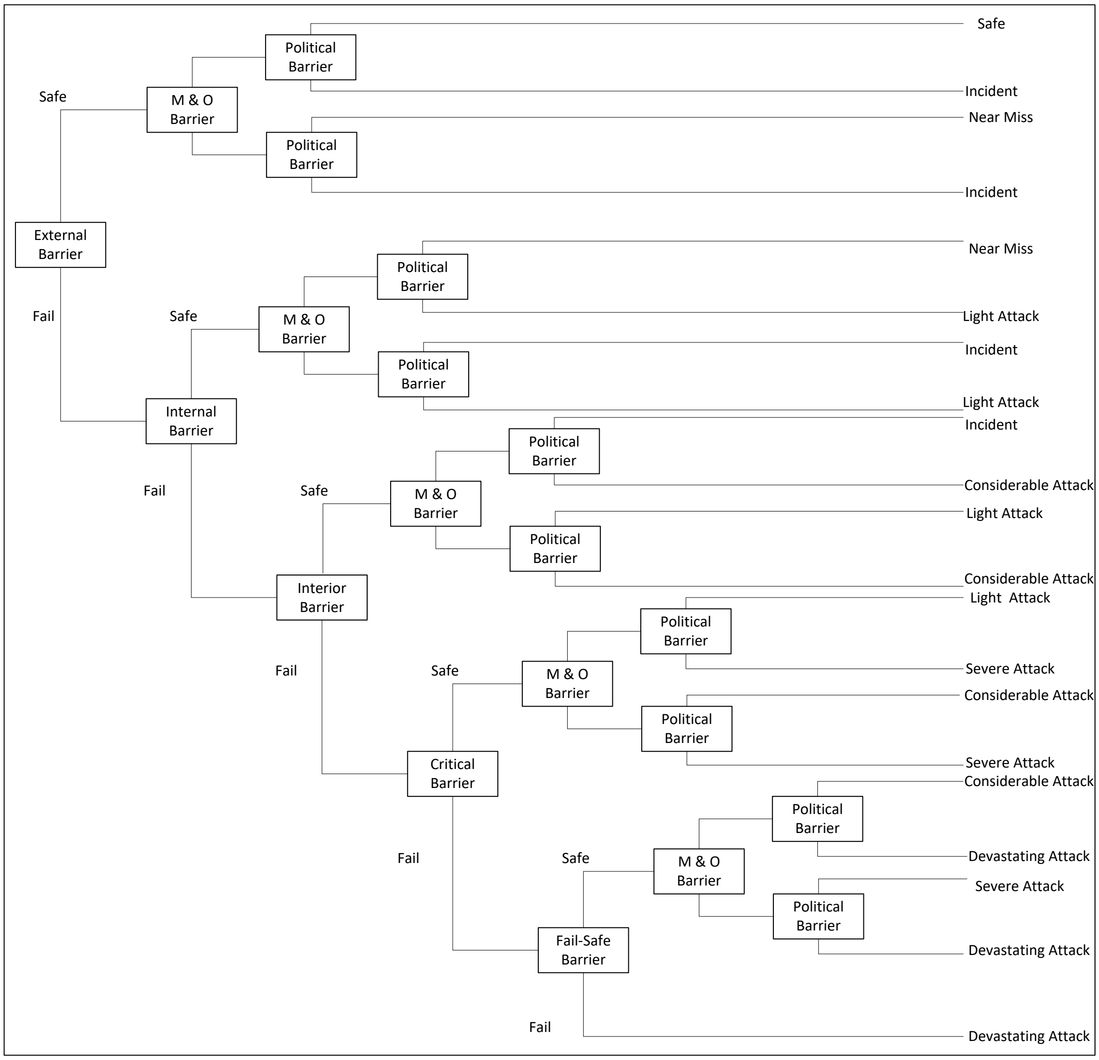

Figure 1 - 13: Attack Sequence Event Tree

Currently available literature does not provide definitions for security analysis consequences. Therefore, descriptions have been developed to accurately depict these security related events.

A ‘near miss’ is described as an event that has potential to cause damage or loss but does not result in any harm. An illustration of this would be a chemical facility receiving a threat of intent to inflict harm and they notify the proper authorities to prevent the action from being executed.

An ‘incident’ can be defined as an event that can cause minor damage to chemical facility and loss of production is negligible. For example, an intrusion device alerts security personnel that unauthorized individuals have cut the chain link fence and are currently trespassing on the grounds of the plant.

A ‘light attack’ is an event that could cause major damage to a chemical facility with minor loss in production and some harm against employees. One scenario for this case is if an individual breaks onto the processing plant grounds causes a leak in a storage tank and breaks a door down in attempt to gain access to sensitive information.

An event where a ‘considerable attack’ occurs would inflict injury to workers, cause greater financial damage and potential loss in production. In addition, this type of attack would draw local news coverage.

A ‘severe attack’ can be described as an event that may have one or more employee fatalities, major damage done to the environment and create national news. In addition there would be excessive financial losses and production would be stopped.

A ‘devastating attack’ is an event or series of events that would cause multiple fatalities, reach international news, and there would be catastrophic financial losses. Furthermore, the facility may be closed down for a lengthy period of time. An example of this is the recent attack on In Amenas gas refinery.

With the model herein outlined, the next step is to map the above fault trees into Bayesian networks. Shown in Figure 1-14, is an example of one of the barriers (external).

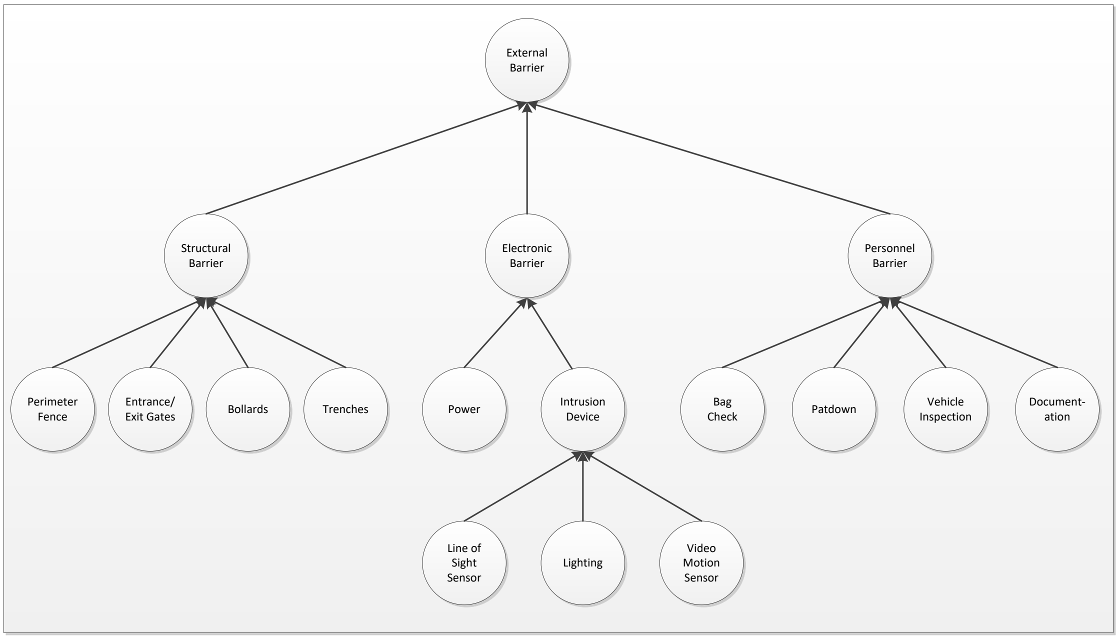

Figure 1 - 14: External Barrier Mapped in a Bayesian Network

The importance of this mapping is to verify the fault tree calculation by matching the conditional probability table (CPT) with the logic of the fault tree. In addition, using a BN allows for manipulation of the CPT to reflect various relaxation assumptions which will be shown in the case study. The next section will look into developing probability data that can be utilized for this proposed model.

1.4 Data Sources

When developing a risk model, uncertainties are created when assumptions are made. However, by comparing results of different models with different assumptions the critical components of failure can be recognized. This recognition is more useful than employing data sources as it displays an understanding of the risk model and its key components. Although only one case study is completed in this paper, the model is devised in such a way that it can be applied to multiple scenarios to develop a deeper understanding. The initial probabilities were developed through expert judgment, as there is currently a lack of data found in both industry and literature. To minimize the uncertainty that comes with expert judgment assigning probabilities, a soft computing theory has been utilized to help develop such probabilities.

In order to determine the failure probabilities of each basic event it must first be separated into two categories. The reason for this is shown in Figure 1-15. An event can come to failure through either a natural failure (i.e. component failure) or an unnatural (forced) failure. If natural failure data is available for the event described, such as biometric access, then it is sorted into category 2. Otherwise, it is given category 1 in which a probability is directly assigned based on expert judgment, as it cannot have a natural failure.

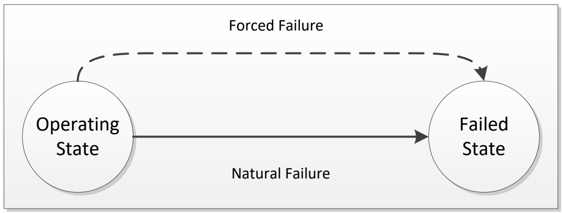

Figure 1 - 15: Basic Event Failure Pathways

Currently, forced failure data is unavailable and thus the unnatural failure must be calculated through Bayes Theorem shown in Eq. 1-15:

$$P(E|T) = \frac{P(T|E) \times P(E)}{P(T)} \tag{1-15}$$

Where *P(E)* denotes the probability of an event due to intended and unintended causes, *P(T)* is the probability of a threat, and *P(T|E)* is assuming the failure of the event E, what is the probability it came from a threat. As this is difficult to calculate, soft computing theory is utilized. Each event likelihood is given a specific term, which has an associated probability range, devised by the authors. These probability ranges were developed by the authors and is presented in Table 1-1.

Table 1 - 1: Likelihood Terms and Associated Probability Range

Event Likelihood Term	Probability Range
Very Likely	> 0.5
Frequent	0.25 - 0.50
Probable	0.10 - 0.25
Unlikely	0.01 - 0.10
Remote	.001 - .01
Rare	.0001 - .001
Improbable	< .0001

The key aspect in this is determining the probability of threat for a given chemical plant. This may lay in the location and conditions outside surrounding plant. To show how this method can be effectively used, a case study is presented in the subsequent section.

1.5 Case Study

A typical refinery is located in a region with turmoil and a recent uprising against foreign oil producers as the country is only a few years past a civil war. A neighboring country is currently dealing with civil demonstrations. However, a chemical plant has just been attacked by armed separatist group. The refinery, as shown in Figure 1-15, is located approximately 100km from the nearest town and 20km from the closest village. Due to its location, the refinery has its own power generation plant and it has been determined that a threat against the plant is unlikely.

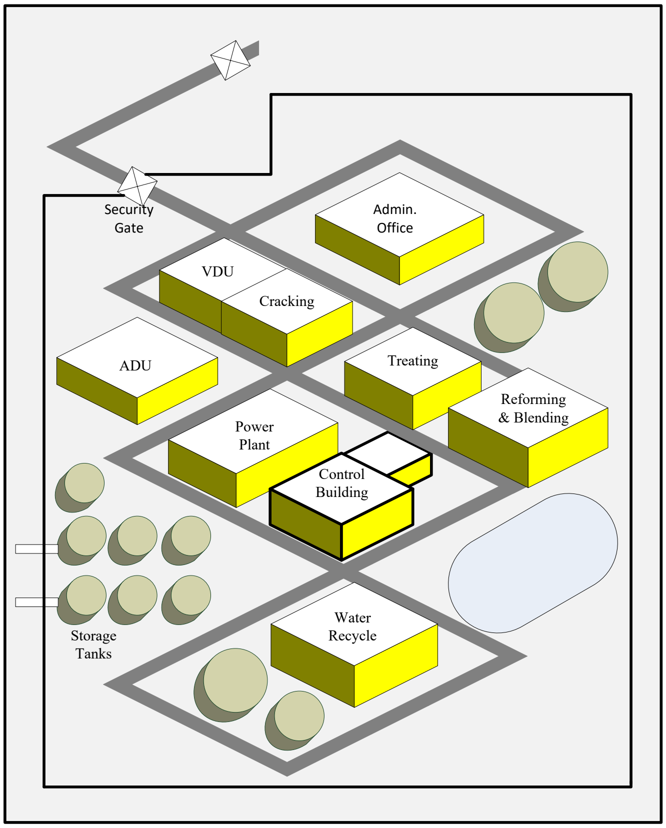

Figure 1 - 16: Case Study Refinery Layout

Recently, the management conducted a qualitative security vulnerability assessment to ensure that facility was up to date. With the current events in mind, management has decided to use the proposed quantitative analysis to determine the occurrence probability of various consequences. Management has a high concern for its control room shown in Figure 1-17.

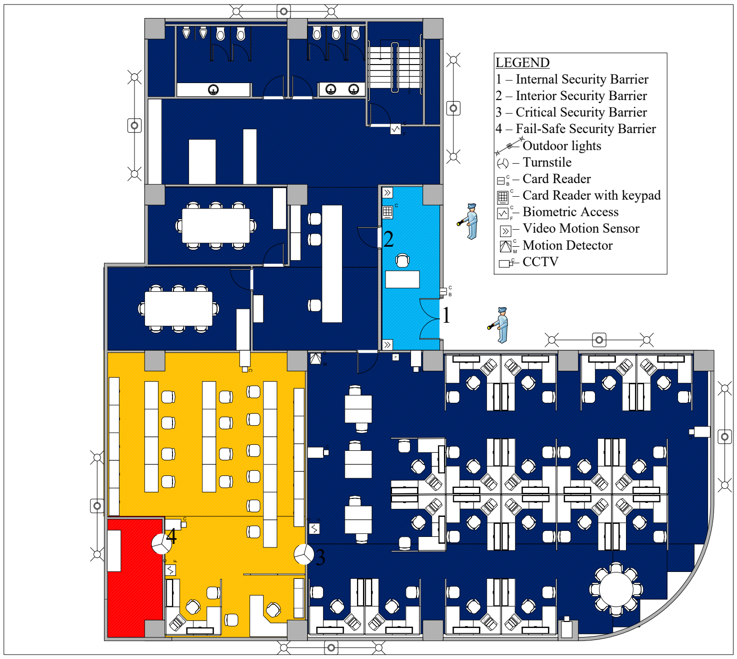
LEGEND
1 – Internal Security Barrier
2 – Interior Security Barrier
3 – Critical Security Barrier
4 – Fail-Safe Security Barrier
– Outdoor lights
– Turnstile
– Card Reader
– Card Reader with keypad
– Biometric Access
– Video Motion Sensor
– Motion Detector
– CCTV
1
2
3
4

Figure 1 - 17: Case Study Control Building Layout

Using the proposed model, probabilities for each basic event were assigned. The values tabulated in Tables 1-2 through 1-8 are assigned by expert judgement for the purpose of illustration of the described methodology.

Table 1 - 2: Basic event failure probability for External Security Barrier

Event Description	Failure Probability
Perimeter Fence	9.044E-03
Entrance/Exit Gates	2.276E-02
Bollards	3.126E-02
Trenches	4.044E-03
Power	1.685E-02
Line of Sight Sensor	7.814E-03
Video Motion	5.373E-03
Lighting	9.386E-03
Bag Check	3.894E-03
Person Inspection (Patdown)	1.184E-02
Vehicle Inspection	9.060E-03
Documentation	5.953E-03

Table 1 - 3: Basic event failure probability for Internal Security Barrier

Event Description	Failure Probability
Road Conditions	7.700E-04
Manual Locked Doors	1.784E-02

Manual Locked Windows	4.162E-02
Electronic Doors Lock	1.137E-02
Power	4.012E-03
Line of Sight Sensor	1.429E-02
Video Motion	1.573E-03
Lighting	8.719E-03
Reception	2.200E-03
Mobile Security	1.092E-02

Table 1 - 4: Basic event failure probability for Interior Security Barrier

Event Description	Failure Probability
Limited Access Points	7.800E-03
Manual Locked Doors	1.061E-02
Electronic Doors Lock	5.366E-03
Power	9.137E-03
Line of Sight Sensor	1.786E-03
Video Motion	8.164E-03
Lighting	9.098E-03
Visitor Escort	5.600E-04
Employee Awareness	5.300E-04

Table 1 - 5: Basic event failure probability for Critical Security Barrier

Event Description	Failure Probability
Limited Access Points	6.100E-04
Manual Locked Doors	9.845E-04
Biometric Access	3.240E-04
Power	4.581E-04
Line of Sight Sensor	2.100E-04
Video Motion	5.164E-04
Network Firewall	7.202E-04
Visitor Restriction	5.900E-04
Employee Awareness	9.000E-04

Table 1 - 6: Basic event failure probability for Fail-Safe Security Barrier

Event Description	Failure Probability
Manual Shutdown	3.267E-05
Manual Alarm	1.953E-05
Electronic Shutdown	5.082E-05
Electronic Alarm	8.215E-05

Table 1 - 7: Basic event failure probability for Management and Organization Barrier

Event Description	Failure Probability
Inadequate Security Program	3.800E-04
Inadequate Communication	4.200E-04
Inadequate Staff & Resources	2.700E-04
Inadequate Planning	4.800E-04

Poor Communication	9.800E-04
Inefficient Management Behaviors	7.400E-04
Inadequate Security Practice	3.600E-04

Table 1 - 8: Basic event failure probability for Political Barrier

Event Description	Failure Probability
State	8.800E-04
Religious	6.200E-04
Pathological	8.000E-05
Issue-Orientated	2.100E-04
Separatist	8.100E-04
Hostage	7.500E-04
Stealing	8.500E-03
Armed Attacks	7.100E-03
Protecting Workers	5.500E-03
Protecting Operations	3.800E-03
Worker Protection	3.800E-03
Operation Protection	6.800E-03

Using a fault tree simulation, the results for each barrier are shown in Table 1-9. With each barrier solved, the associated event tree model can be solved to determine the occurrence probability of each consequence. These results are shown in Table 1-10 additionally with the mapped Bayesian Network. Each consequence was developed through attack scenarios, their causes and their respective severity levels. As shown the model uses fault tree analysis in a barrier approach to determine the likelihood of each event. The probability for a chemical facility to remain ‘safe’ based on the event tree is 0.8344. This number needs to be increased. Furthermore, the probability for a ‘near miss’ is 0.1135, which is relatively high and should be lowered. This could be achieved by improving the security countermeasures in both the internal and external security barriers. However, the political barrier plays a major role in affecting the overall plant security and will be a major factor in the security of the plant.

Table 1 - 9: Failure probability data for each security barrier

Security Barrier	Failure Probability
External	1.2930E-01
Internal	1.0831E-01
Interior	5.1874E-02
Critical	5.3010E-03
Fail-Safe	6.4227E-04
Management and Organization	3.6250E-03
Political	3.8216E-02

Table 1 - 10: Consequence Occurrence Probability

Consequence	Event Tree Occurrence Probability	Event Network Occurrence Probability
Safe	8.3439E-01	8.3439E-01
Near Miss	1.1352E-01	1.1352E-01
Incident	4.6402E-02	4.6401E-02
Light Attack	5.1450E-03	5.1450E-03
Considerable Attack	5.0608E-04	5.1366E-04
Severe Attack	2.8001E-05	2.7630E-05
Devastating Attack	1.5000E-09	1.5000E-07
SUM:	9.999941E-01	1

It can be seen in Table 1-10 that both the event tree and BN produced the exact values except for the last three consequences. In addition, the summation of the probabilities should equal 1 but for the event tree this does not occur which could be assumed to be a computational error by the software. Furthermore, with the mapped BN matching in value to the fault tree, the relaxation assumptions can hence be applied.

With the Bayesian Network properly mapped, the relaxation assumptions can be applied. To display which technique can best reflect reality, each of the techniques will be used on the External Barrier as previously shown in Figure 1-13. In this case study, in order to seek continuity, the causation probabilities remained the same throughout each relaxation technique. Each causation probability was assigned on the basis that the parent event could cause the child event to fail when it was present. In the Leaky-OR assumption, a probability of 0.01 was assigned. This probability accounts for 1% of those parameters that are not modeled or unaccounted for. Meanwhile the substitution probability was assigned to be 0.05 as this probability when the parent node is not present. For the External Barrier, these probabilities are shown in Table 1-11.

Table 1 - 11: Assigned Relaxation Assumption Probabilities for each parent event

Barrier	Parameter	Causation Probability	Leak Probability	Substitution Probability
Intrusion Device	Line of Sight Sensor	0.60	0.01	0.05
	Lighting	0.80		
	Video Motion Sensor	0.70		
Electronic	Intrusion Device	0.70	0.01	0.05
	Power	0.80		
Structural	Perimeter Fence	0.80	0.01	0.05
	Entrance/Exit Gates	0.60		
	Bollards	0.70		
	Trenches	0.30		
Personnel	Bag Check	0.40	0.01	0.05
	Patdown	0.30		
	Vehicle Inspection	0.80		
	Documentation	0.75		
External	Electronic	0.85	0.01	0.05
	Structural	0.70		
	Personnel	0.60		

Using available software called Netica (https://www.norsys.com/netica.html), these probabilities were calculated through the outlined equations in Section 2. Thus, in Table 1-12, each of the failure probabilities are shown using the various techniques.

Table 1 - 12: Relaxation Techniques Failure Probabilities

Barrier	Mapped BN	Noisy-OR	Leaky-OR	Noisy-AND
Intrusion Device	0.021	0.015	0.025	0.024
Electronic	0.037	0.024	0.040	0.064
Structural	0.066	0.043	0.053	0.018
Personnel	0.030	0.017	0.027	0.021
External	0.128	0.062	0.096	0.023

Through the above table, it can be shown that the Leaky Noisy-OR relaxation assumption has the highest failure probability and the Noisy-AND has the lowest barrier failure probability based on the External barrier. The reasoning behind is that, the Noisy-AND requires a combination of parameters to have a failure while the Noisy-OR only needs one parameter. The leak probability adds complexity to the Noisy-OR, which further increases the probability of a barrier failure. However, it should be noted there are a few instances where the Noisy-And does not provide the lowest failure probability. This can be attributed to how the causation probabilities of the parent nodes interact with each other.

Nonetheless, the relaxation assumption that would most reflect reality and should be utilized is the Noisy-AND. The main reason for this is because an attacker on a chemical plant would likely attempt to break in through multiple ways. Using the Noisy-OR is expecting an attacker to only attack one avenue in the barrier. But in reality it can be assumed that there will be back-up plans, multiple personnel and access routes used to increase the likelihood of success.

One of the key aspects of this model is its ability to update and predict. Employing the approach used in Rathnayaka (2011), the number of cumulative abnormal events is displayed in Table 1-13. Assuming that the gamma distribution parameters are both uniform, α and β have the respective value of 0.01. Therefore, using Eq. (10), it was determined that the mean value for abnormal events λ_p was estimated to be 0.916. With this estimation placed into the predictive model, for the 13 month the average number of abnormal events was approximately 1.

Table 1 - 13: Cumulative Number of Abnormal Events over last 12 months

Month	Safe	Near Miss	Incident	Light Attack	Considerable Attack	Severe Attack	Devastating Attack
1	1	0	0	0	0	0	0
2	2	1	0	0	0	0	0
3	3	1	1	0	0	0	0
4	3	1	1	0	0	0	0
5	3	2	1	0	0	0	0
6	3	2	1	0	0	0	0

7	4	2	2	1	0	0	0
8	4	3	2	1	0	0	0
9	5	3	2	1	0	0	0
10	8	3	3	1	0	0	0
11	9	4	3	1	0	0	0
12	10	5	3	1	0	0	0

The final step in the proposed model is to update the barrier probabilities, as there is uncertainty with the initial probabilities since they were derived from expert judgment. A Bayesian mechanism is used to update the failure probabilities based on the fault trees and thus the consequence occurrence probabilities based on the event tree. The first step is to develop the likelihood probabilities based on the cumulative number of events shown in Table 1-13. Utilizing Eq. (13), these probabilities are shown in Table 1-14. Subsequently, applying the Eq. (12) based on Table 1-10 (prior) and Table 1-14 (likelihood), the posterior probabilities for each barrier could be estimated. These values are displayed in Table 1-15.

Table 1 - 14: Barrier Likelihood Probabilities

Month	External	Internal	Interior	Critical	M&O	Political
1	0.000	-	-	-	-	-
2	0.333	0.000	-	-	-	-
3	0.400	0.500	0.000	-	-	-
4	0.400	0.500	0.000	-	-	-
5	0.500	0.333	0.000	-	-	-
6	0.500	0.333	0.000	-	-	-
7	0.556	0.600	0.333	0.000	-	-
8	0.600	0.500	0.333	0.000	-	-
9	0.545	0.500	0.333	0.000	-	-
10	0.467	0.571	0.250	0.000	-	-
11	0.471	0.500	0.250	0.000	-	-
12	0.474	0.444	0.250	0.000	-	-

Table 1 - 15: Barrier Posterior Probabilities

Month	External	Internal	Interior	Critical	M & O	Political
1	0.000	-	-	-	-	-
2	0.065	0.000	-	-	-	-
3	0.086	0.108	0.000	-	-	-
4	0.086	0.108	0.000	-	-	-
5	0.129	0.054	0.000	-	-	-
6	0.129	0.054	0.000	-	-	-
7	0.162	0.162	0.026	0.000	-	-
8	0.194	0.108	0.026	0.000	-	-
9	0.155	0.108	0.026	0.000	-	-

10	0.113	0.144	0.017	0.000	-	-
11	0.115	0.108	0.017	0.000	-	-
12	0.116	0.087	0.017	0.000	-	-

With each the barrier posterior probabilities estimated, the consequence occurrence probabilities can be evaluated. These values are displayed in both Figure 1-18 and Figure 1-19.

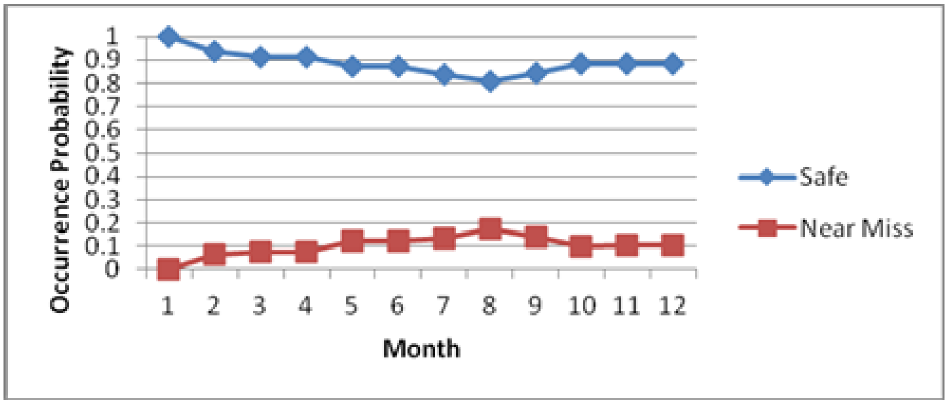

Figure 1 - 18: Updated Consequence Probability for Safe and Near Miss

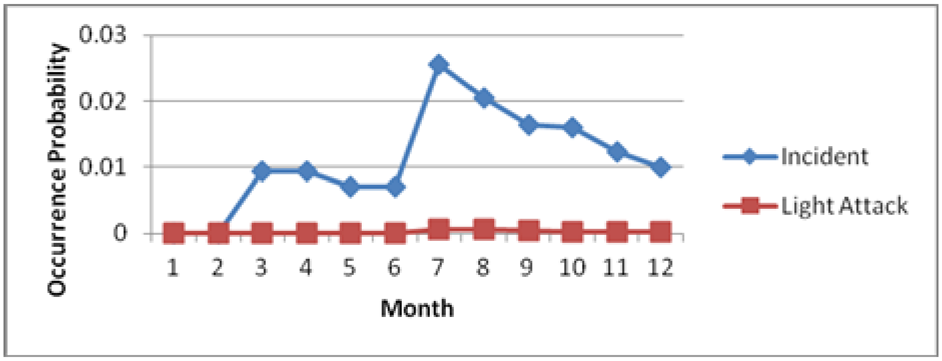

Figure 1 - 19: Updated Consequence Probability for Incident and Light Attack

Referring back to Table 9, both the external and internal barriers have high failure probabilities when compared to the rest. Even with the probabilities updated, the external barrier still remains high when compared to the rest. This clearly shows how important the first line of defense is against an impending attack. Therefore, counter measures can be made to further reduce their chance of failure. The recommendations are as follows are:

- Involve military personnel to restrict traffic to refinery business
- Install guard towers for the perimeter fence and involve security rounds along the perimeter
- Regularly inspect security device to ensure proper working order
- Develop a relationship with local enforcement to report any suspicious activity within range of the refinery

1.6 Conclusion

Through review of available security literature and the application of an existing probabilistic safety method, this model has been developed. In this proposed model, security barriers are developed in a sequential barrier approach method. Five barriers are placed in consecutive order with two barriers common to all of them. The five security barriers are: external, internal, interior, critical, and fail-safe, with the two common barriers being political, management and organization. The use of fault and event analysis has allowed for the barrier failure and consequence occurrence probabilities to be calculated. In addition, the fault trees have been mapped into respective Bayesian Networks, which allow for relaxation assumptions to be applied that better reflect reality. It was found the use of the Noisy-AND technique best reflects reality has an attacker will have multiple routes to ensure their attack is successful. This follows the logic for AND model has it represents that one condition is observed.

Nominally, basic event failure data is generated from reliability databases, literature and/or expert judgment. Alas, this is not the case for security related event. As it stands currently, there is a lack of data available related to security failures or forced failures. Therefore, soft computing theory in addition to Bayes theorem is used to calculate these probabilities. Furthermore, a predictive modeling and updating mechanism was applied to the model. This allowed for the model to become dynamic and adapt to changes as they happen in real time while the updating mechanism helped to reduce the uncertainty that may have been developed when values were assigned.

It should be noted that events threatening to a chemical facility are always changing and an attack on a plant can happen at any moment. Thus it is the mandate of the owners and management to ensure not only the safety of its workers but also others who may be affected by an attack.

The proposed methodology details a comprehensive security analysis and provides information to help in the underlying decision making of risk management. The goal of this work is to provide a model for quantitative analysis of security site risk and to create an awareness of the value of creating a database for security related failures.

1.7 References

Al-Bazee, Sabah. 2011. Iraq's largest oil refinery shut by bombing. *Reuters*, 26 February 2011,http://uk.reuters.com/article/2011/02/26/iraq-oil-refinery-dUKLDE71P00S20110226 (18 July 2014)

ANSI/API 780, Security Vulnerability Assessment, Methodology for the Petroleum and Petrochemical Industries. 2013. Washington, DC: API.

API, Security Vulnerability Assessment, Methodology for the Petroleum and Petrochemical Industries, Second Edition. 2003. Washington, DC: API.

Bajpai, S. and Gupta, J.P. 2005.Site security for chemical process industries. *Journal of Loss Prevention in the Process Industries* **18** (4-6): 301-309. doi:10.1016/j.jlp.2005.06.011

Bajpai, S. and Gupta, J.P. 2007. Securing oil and gas infrastructure. *Journal of Petroleum Science and Engineering* **55** (1-2): 174-186. doi:10.1016/j.petrol.2006.04.007

Baybutt, P. and Reddy, V. 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. *Homeland Defense Journal* **2** (1). http://www.primatech.com/images/docs/paper_assessing_risks_from_threats_to_process_plants_threat_and_vulnerability_analysis.pdf

BBC News. 2006. Saudis foil oil facility attack. *BBC News*, 24 February 2006, http://news.bbc.co.uk/2/hi/middle_east/4747488.stm (18 July 2014)

Bobbio, A., Portinale, L., Minichino, M. et al. 1999. Comparing Fault Trees and Bayesian Networks for Dependability Analysis. Computer Safety, Reliability and Security, Toulouse, France, 27-29 September. http://link.springer.com/book/10.1007/3-540-48249-0/page/1

CCPS (Center for Chemical Process Safety). 2003. *Guidelines for Analyzing and Managing Security Vulnerabilities of Fixed Chemical Sites*, New York, New York. http://www.aiche.org/ccps/publications/books/guidelines-analyzing-and-managing-security-vulnerabilities-fixed-chemical

Díez, F. and Druzdzel M. 2007. *Canonical Probabilistic Models for Knowledge Engineering Technical Report* CISAID, 06-01. Madrid, Spain: UNED. http://www.cisiad.uned.es/techreports/canonical.pdf

Grothous, N. 2014.Types of Terrorism. *Hand of Reason*, 2014, http://handofreason.com/2011/featured/types-of-terrorism (27 June 2014)

Hagen, Torgeiret et al. 2013. *The In Amenas Attack*. Statoil. http://www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf

Heinrich, W.H., 1941. *Industrial Accident Prevention*, Second Edition. New York, New York: McGraw-Hill.

Johnson, K. and Gilbert, D. 2013. Poorly Secured Remote Energy Facilities Invite Terrorist Attacks. *The Wall Street Journal*, 18 January 2013, http://online.wsj.com/news/articles/SB10001424127887323783704578250121106462696 (18 July 2014)

Khakzad, N., K han F., Amyotte, P. 2012 Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Journal of Process Safety and Environmental Protection* **91** (2): 46-53. http://dx.doi.org.qe2a-proxy.mun.ca/10.1016/j.psep.2012.01.005

Kujath, M.F., Amyotte, P.R. and Khan, F.I. 2010. A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries* **23** (2): 323–330. doi:10.1016/j.jlp.2009.12.003

Netica. 2014. Netica^{TM} Application. *Norsys Software Corporation*, 2014, https://www.norsys.com/netica.html

Nordland, R. and Al-Salhy, S. Extremists Attack Iraq's Biggest Oil Refinery. *The New York Times*, 18 June 2013, http://www.nytimes.com/2014/06/19/world/middleeast/iraqi-oil-refinery-ablaze-as-army-and-militants-clash.html (18 July 2014)

Rathnayaka, S., Khan, F.I., and Amyotte, P. 2011. SHIPP Methodology: Predictive Accident Modeling Approach. Part I: Methodology and Model Description. *Process Safety and Environmental Protection* **89** (3): 151-164. doi:10.1016/j.psep.2011.01.002

Reason, J. 1990. *Human Error*, First Edition. Cambridge, UK: Cambridge University Press.

Reason, J. 2000. Human error: models and management. *British Medical Journal* **320** (7237): 768-770. http://dx.doi.org/10.1136/bmj.320.7237.768

Reniers, Genserik L. L. 2010. *Multi-Plant Safety and Security Management in the Chemical and Process Industries*. Great Britain: Wiley-VCH, Weinheim.

Chapter 2: SVAPP Methodology: A Predictive Security Vulnerability Assessment Modelling Method

2.0 Abstract

Recent intentional attacks on the chemical industries in Middle East and Algeria have greatly influenced the risk management mindset. Nominally, probabilistic risk assessment and management has focused on safety and unintentional acts in the chemical and petroleum industry. The focus now needs to be broadened to include intentional acts that will inflict damage on a chemical facility. The proposed Security Vulnerability Assessment, Prevention and Prediction (SVAPP) methodology utilizes an existing safety barrier approach and adapts it to suit the security facet. In total, seven barriers are proposed of which five barriers are utilized to prevent or deter an attack with two overseeing barriers. The five barriers that help deter the security attack are external, internal, interior, critical, and the fail-safe barrier. To reduce the effect of uncertainty in the model, a Bayesian updating technique is proposed along with a predictive capability. This is a key aspect of the model because; with any new information as it accumulates, the model can be updated to better reflect the updated conditions. To illustrate how the model can be executed, a case study is conducted on a figurative liquefied natural gas treating plant. The goal of this work is to raise awareness for the development of security vulnerability assessment related databases in the chemical plants so that they can be used for continually updating the much needed probabilistic security vulnerability assessment in the prevailing environment.

Keywords: Security Risk; Probability; Bayesian analysis; Threat analysis; Vulnerability Analysis

2.1 Introduction

The terrorist attacks of September 11, 2001, raised the awareness of the need to improve chemical facilities risk assessments to counter possible security incidents. Chemical plants are possible targets for intentional attacks as they process and store high quantities of hazardous materials. A security risk assessment is similar to a safety risk assessment as it can help facilitate the mitigation of nuisance value of high frequency-low consequence and low frequency-high consequence events. The American Petroleum Institute (API) and the American Chemistry Council (ACC) both released documents to help processing plants complete risk assessments (API, 2003; ACC, 2001). These assessments are formally known as security vulnerability assessments (SVAs).

Throughout recent years, there have been some notable intentional attacks on chemical facilities. On February 24, 2006, there was a failed attack at Abqaiq in Saudi Arabia (Henderson, 2006). At the gate of the large refinery, assailants were killed along with two guards after a vehicular explosion and a minor skirmish. In January of 2013, armed militants attacked the Amenas gas refinery in Algeria and seized hostages that lasted over three days (Statoil, 2013). By the end of the third day, there were forty [40] casualties among the workers and production was shut down for some time. The most recent terrorist incident involves Iraq's largest refinery, the Baiji refinery. Since June of 2014, the refinery was under siege with Islamic State and Iraqi forces trading control of the facility. As of late December 2014, Islamic State militants had regained control of the refinery (Pandey, 2014). These examples substantiate the need to create a proper security risk assessment, prevention, and prediction in order to avoid financial loss, material loss, and most importantly avoid human loss.

2.2 Research Backgrounds

The security culture slowly began to change in the early 2000s, as a document was released by the Center for Chemical Process Safety (CCPS) (2003). This work provided systematic approaches for identifying, analyzing, and managing security vulnerabilities. In addition, the document illustrated the 'Rings of Protection' where an adapted version is shown in Figure 2-1. The *Outer* ring would provide perimeter security measures while the *Middle* may prevent an adversary from gaining further access to more critical areas. The *Inner* ring shall have most sophisticated security measures as it is the last line of defense for the critical infrastructure. In some cases, a security measure may have a wide range of applicability and can be utilized in multiple rings. For example, a badge check can be used for entrance onto the work site and additionally be required for access into a work site office.

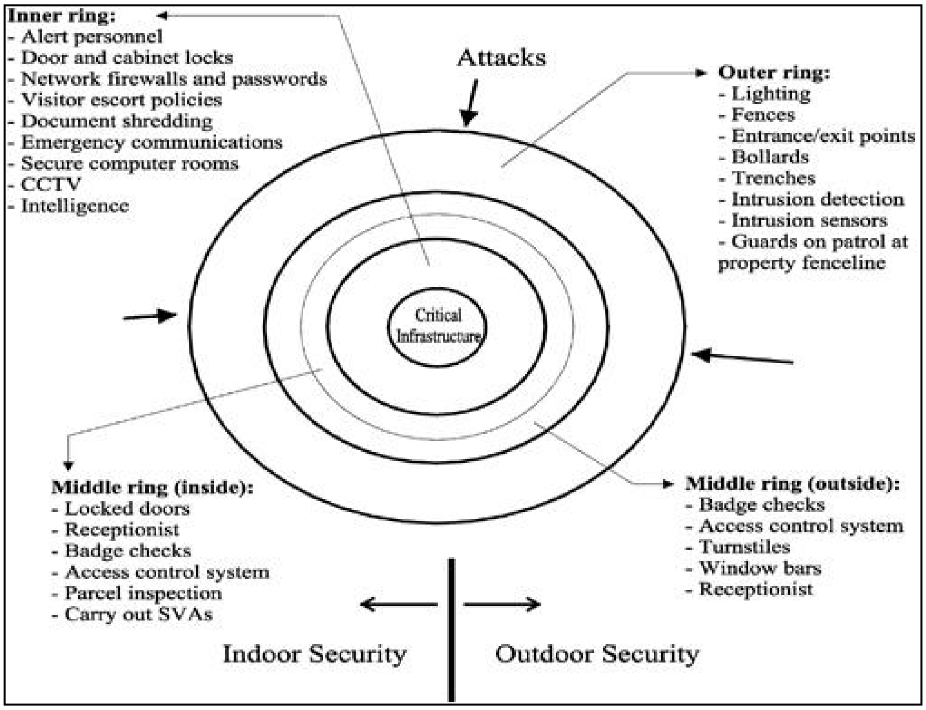

Figure 2 - 1: Rings of Protection based on Reniers (2010)

One of the first Security Vulnerability Assessments (SVA) to build up on the work provided by the CCPS was Air Products and Chemicals Inc. (APCI) (Dunbobbin et al. 2004). The APCI SVA methodology was developed to assist the company in conducting a robust approach that could be applied to a wide range of chemical facilities. This methodology expands on the CCPS work by documenting the flow of both employees and contractors to gain an understanding of people flow. Furthermore, it introduces a separate method to conduct an assessment of the current security systems on the chemical facility. Gap analysis is also presented to identify further improvements that could come through additional security, engineering or operations.

Bajpai and Gupta (2005) proposed a work that built on the then existing guidelines to develop a security methodology for chemical process industry. The initial step in the approach was to complete a threat analysis (TA) on a processing facility in order to recognize or identify possible threats. Subsequently, a vulnerability analysis (VA) was proposed to pair a potential target asset with a likely threat. They further proposed a review of security measures to verify the overall effectiveness. With this information, the vulnerabilities can be ranked based on the attractiveness and severity of consequence. Next a security risk factor table was created to assess the latest risks of the facility and the appropriateness of countermeasures that can be implemented. The final step in their work was to finalize a mitigation and emergency response plan that may include local authorities. To illustrate this approach, the authors presented a case study and gave security recommendations based off of results.

Moore et al. (2007) described an approach called Risk Analysis and Management for Critical Asset Protection (RAMCAP). At the behest of the Department of Homeland Security (DHS), USA; the American Society of Mechanical Engineers Innovative Technologies Institute and AcuTech consulting collaborated to develop sector-specific guidance on vulnerability analysis and management for critical asset protection for the chemical manufacturing, petroleum refining, and liquefied natural gas (LNG) sectors. RAMCAP is a qualitative method to conduct SVAs for either owner or operator of chemical facility, while also supplying key information back to the DHS. This information is used for a screening process by DHS to get an understanding of the assets that are important to protect against terrorist attack and to prioritize the activities. The RAMCAP-SVA is broken into seven main steps, where the first step is asset characterization. In this step, all non-credible target assets of the chemical facility are ignored and only credible targets are analyzed. The next step is threat characterization, which is similar to a threat analysis as it seeks information on how an attack can be completed against the critical asset. A consequence analysis is conducted to evaluate the worst possible outcomes followed by a vulnerability analysis to establish both the strengths and weaknesses of the asset. With this information, both the owner and the government will complete a threat assessment in order to determine the overall attractiveness for an attack. The final two steps of the RAMCAP-SVA method are risk assessment and risk management. The risk assessment helps to create strategies to protect the credible assets against an attack while risk management will ensure that risk is kept at a standard level for an appropriate cost.

Later, Moore (2013) of AcuTech Consulting worked with the American National Standards Institute (ANSI)/American Petroleum Institute (API) to help develop a security standard tailored to the petroleum industry. Security Risk Assessment (SRA) Methodology 780 (2013) established a tool for an industry to estimate the chance of a threat against its chemical plant that would result in any unwanted consequences. Similar to the previous work, there are five interrelated steps to complete the SRA. First, an asset characterization is done to deem which assets are most critical. Second a threat assessment is conducted to identify possible attackers and the attractiveness of an attack, which is followed by a vulnerability assessment to calculate the likelihood of the various scenarios. Next, a risk evaluation is completed to seek out any weaknesses of the identified critical assets. Risk treatment is the final step, which is to establish or improve existing security countermeasures. The main goal for this approach is to assist management by better defining organization risk tolerance and requirements. All of these steps are qualitative in nature.

In the proposed Security Vulnerability Assessment, Prevention and Prediction (SVAPP) methodology, the authors improve on the previous work of security vulnerability assessments which are mostly qualitative in nature with the work on the safety discipline which is quantitative barrier based approach which allows for continual updating of likelihood of security attack. A comparison of the above mentioned methodologies are illustrated in Table 2-1 below.

Table 2 - 1: Comparison of Security Methodologies

Method	Qualitative	Quantitative	Barrier Approach	Predictive Component	Updating Mechanism
CCPS (2003)	✓		✓		
Dunbobbin et al. (2004)	✓				
Bajpai and Gupta (2005)	✓	✓			
Moore et al. (2007)	✓				
Moore (2013)	✓				
SVAPP	✓	✓	✓	✓	✓

While there are existing qualitative approaches that consider both barrier and protection, they fail to provide the importance of both barrier and protection in quantitative terms that helps to develop priorities and procedure to act. Furthermore, the approaches are subjective in nature as the results and analysis are driven by analyst's experience and the understanding of the threats. As opposed to this a quantitative approach, SVAPP provides an objective understanding of the effectiveness of barriers and protection. Additionally, it helps to predict relative importance of different options while offering a clear and repeatable analysis. This is done by building the barriers upon the 'Rings of Protection' adopted from CCPS as shown in Figure 2-1, to have more descriptive and well-defined barriers. Figure 2-2 provides details of these rings of protection and security barrier analysis.

The authors recognize the current literature against the use probabilistic approaches involving intelligent adversaries (Brown and Cox 2011; National Research Council 2008). However, the use of a probabilistic risk approach is only to set initial probabilities based on existing conditions and these probabilities are updated based on events that occur. The goal of this paper is to bring awareness to the chemical industry about probabilistic security risk assessments and thus the need to create a database pertaining to security related failures. Probabilistic Risk Assessment (PRA) has widely been used by chemical facilities to help make informed safety risk management decisions (Ezell et al., 2010). As mentioned earlier, most of the available literature on security risk analysis is qualitative and there is a lack in the use of quantitative methods. This proposed method transitions a probabilistic safety barrier approach into a probabilistic security attack barrier approach. Modarres et al. (2006) states that the main purpose of the Probabilistic Risk Analysis is identifying the system components that contribute the highest amount of risk along with executing various risk reduction strategies. Simply, a PRA determines a risk value, based on the probability and a consequence. PRA can be conducted in multiple ways through fault or event tree analysis and/or Bayesian Networks. A Bayesian Network (BN) is a graphical technique composed of directed arcs between nodes that represent variables and their respective relationships.

Fault tree analysis is a well-known approach, which assists in the calculation of probability of system failure or barrier failure. The top event of a fault tree defines the system or barrier failure. The causation of the top event is represented as fault tree comprising of intermediate and basic events connected through logic gates. Each basic event is assigned a failure probability through historical data, literature, or in some cases expert judgment. Event tree analysis is used to show the sequence of conditions that lead to consequences. These conditions are represented as barriers, which are considered as independent of each other. When a barrier fails, the next subsequent barrier is activated. The failure probabilities or the events will lead to the occurrence probabilities of the different consequences.

Bayesian networks show relationships between events through the use of directed arcs and nodes (Ezell et al., 2010). These directed acyclic graphs connect existing fault and event trees through a technique called mapping. This mapping process is described by Bobbio et al. (2001), where the basic events (root cause of a system failure) of the fault tree become a parent node in a BN while the gate becomes a child node in the network. The connections in a BN are denoted by arcs which represent a direct causal relationship between the two nodes. A parent node will have a direct arc drawn to a child node. The conditional dependence of child node is represented in conditional probability table (CPT). This table match the logic defined in the fault tree (i.e. AND/OR logic). With the CPT logic well-defined, the BN child node probability can be evaluated using Equation 2-1, where X_i represents any child node:

$$P[X_1, X_2, .X_n] = \prod_{i=1}^{n} P[X_i | Parent(X_{i-1})] \tag{2-1}$$

Relaxation assumptions manipulate the CPT of existing nodes in the Bayesian Network in order to deviate away from its structured Boolean logic. This enables the CPT to better accurately depict the relationship between the nodes for a given situation.

Díez and Druzdel (2007) outline various CPT manipulation techniques such as Leaky-OR, Noisy-OR, and Noisy-AND. These CPT manipulation techniques or relaxation assumptions will be used in the methodology to represent various scenarios. Noisy-OR refers to the chance that a particular event may not occur because it was inhibited by an external factor. In other terms, each parent node is independent of the other and even if they are active it may not trigger the child node to be active. The probability that the parent produces the child is denoted by c_i while the probability that the inhibitor is active is denoted by q_i. The relationship is displayed in Equation 2-2:

$$c_i = 1 - q_i \tag{2-2}$$

In the case of multiple parent nodes to a single child node, the child node probability can be calculated by using Equation 2-3.

$$P(Z|X_1, X_2, \dots X_n) = 1 - \prod_{i \in x} q_i \tag{2-3}$$

Where Z represent the event of interest and $X_1, X_2, \dots X_n$ represents parents nodes (dependence).

The Noisy-OR technique is a particular case of the Leaky-OR, where is leaky parameter is equal to zero. The leaky parameter, c_L, is able to account for the modeling of combined influence factors that have not been explicitly modeled as it is nearly impossible to include all components for computation. With the leak parameter included, the child node probability can be calculated through the use of Equation 2-4, below:

$$P(Z|X_1, X_2,\ X_n) = 1 - \prod_{i \in x}(1 - c_i) \times (1 - c_L) \tag{2-4}$$

The other relaxation assumption illustrated by Díez and Druzdel (2007) is the Noisy-AND and in this technique the child node can either be substituted or inhibited. As in the case with Boolean logic, multiple parent nodes are active to cause the child node. If a node is not active then it is replaced with a substitution probability, denoted as s_i. Thus, a parent node will contribute either an inhibitor or substituted probability based on whether it is active or not. Equation 2-5, shows how the child node probability can be calculated.

$$P(Z|X_1, X_2, \dots X_n) = \prod_{i \in x} c_i \times \prod_{i \in x} s_i \qquad (2\text{-}5)$$

2.3 Proposed SVAPP Methodology

The goal of the SVAPP methodology is to perform a quantitative security vulnerability assessment and use it to assign initial failure probabilities to the barriers subjectively which are built on the 'Rings of Protection'; evaluate the consequences probabilistically and take measures to prevent the security attacks. Following this, the prior failure probabilities of barriers can be predicted and used to update the probabilities of the consequences. The SVAPP methodology has four main components which are (i) system definition, (ii) security vulnerability assessment modelling, (iii) decision making/strategy implementation and (iv) predict the prior failure probabilities of security barriers and continually update the security attack likelihoods as shown in Figure 2-2.

The first phase is to define the system in which the analysis will take place, which may include establishing system boundaries and establishing goals for the system. For a chemical facility, each system will have sub systems that may contain multiple elements that can interact with each other. It is crucial to have an understanding of each system as well as the interactions and dependencies.

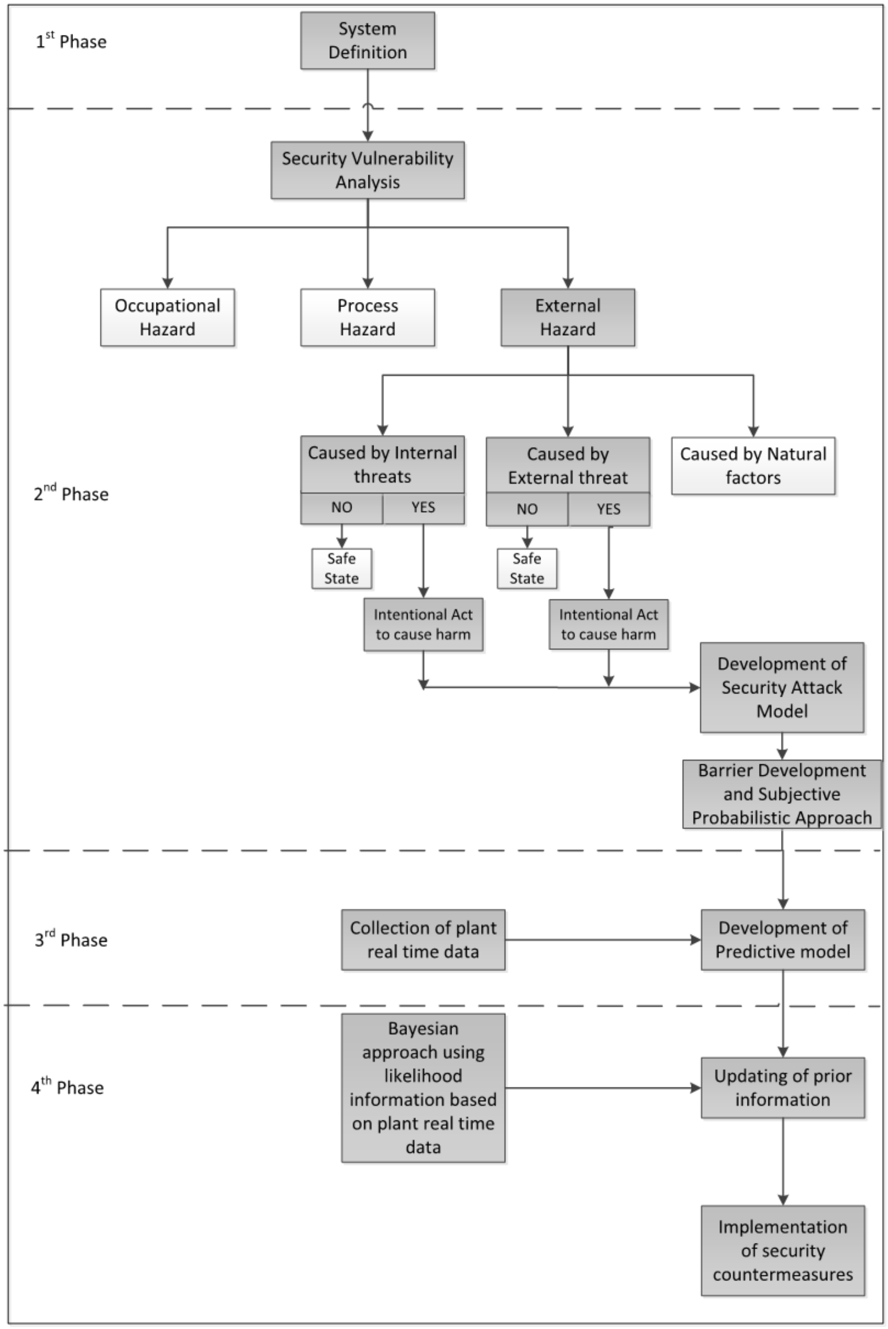
1st Phase
System Definition
Security Vulnerability Analysis
Occupational Hazard
Process Hazard
External Hazard
Caused by Internal threats
NO
YES
Caused by External threat
NO
YES
Caused by Natural factors
Safe State
Safe State
Intentional Act to cause harm
Intentional Act to cause harm
2nd Phase
Development of Security Attack Model
Barrier Development and Subjective Probabilistic Approach
3rd Phase
Collection of plant real time data
Development of Predictive model
4th Phase
Bayesian approach using likelihood information based on plant real time data
Updating of prior information
Implementation of security countermeasures

Figure 2 - 2: Proposed SVAPP Methodology Phases

The next step in the methodology is to complete the security vulnerability analysis and develop the security attack model. A Security Vulnerability Analysis (SVA) can be conducted by following API Recommend Practice 780 (2013) as it provides a holistic and comprehensive approach for conducting an SVA and therefore the reader is referred to API 780. Based on the outcomes of the chemical facility's SVA, an appropriate attack model path can be outlined and thus relevant security barriers can be developed to block such an attack. Previous security methods have been developed to prevent or limit the consequence of an attack, which is an intentional act to cause harm. The worst case form of attack would be an act of terrorism that could cause devastating economic, environmental and human damages. An attack can happen in a number of ways. Therefore, trying to model an attack can be quite challenging. As viewed in the 'Rings of Protection', an attacker would have to go through various layers of security in order to reach the critical process equipment. Following this logic, a proposed barrier based attack model is shown in Figure 2-3 below. The model shows that once *Safe Conditions* are no longer valid there are three barriers that could prevent the event from escalating. If the External barrier was to fail then the subsequent barriers would be available.

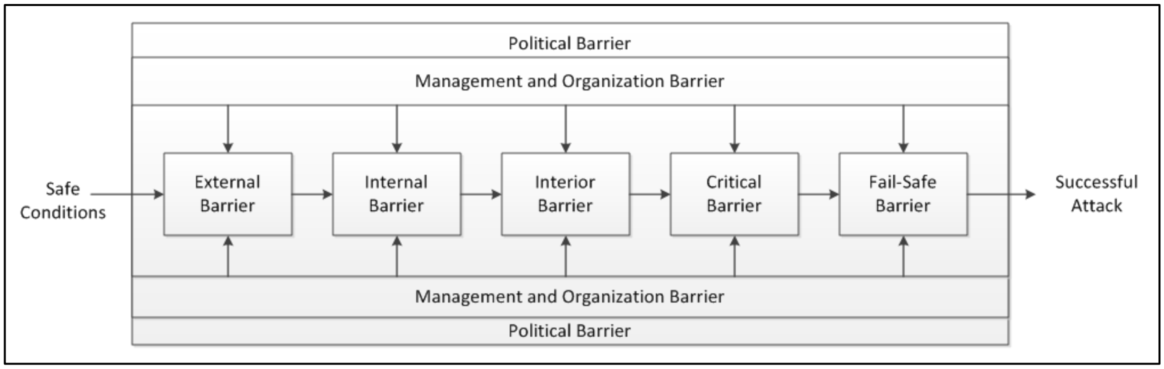

Figure 2 - 3: Proposed Attack Model

Reniers (2010) proposed that physical security should be broken down into three main areas: structural, electronic, personnel. This concept has been implemented into the External, Internal, Interior, and Critical barrier. The last barrier in the attack model is the

Fail-Safe barrier. Additionally, there are two external barriers that may affect the process of an attack, which are the Political and the Management and Organization Barriers. Each layer of protection or barrier can be modeled using fault and event tree analysis and thus mapped into Bayesian Networks.

The authors have previously developed a proposed fault tree for each barrier (van Staalduinen and Khan 2015), The reader is referred to this work for more elaboration on the fault tree analysis. The External security barrier is a chemical facility's first line of defense against an impending attack and is illustrated in Figure 2-4. Failure of this barrier allows an adversary access on the chemical plant's property. In order to prevent an adversary from gaining access to a chemical plant's buildings, the Internal security can be implemented, which is shown in Figure 2-5. The subsequent barrier is the Interior security barrier and the goal of this barrier is prevent unauthorized personnel or adversaries from accessing employee offices. The mapping of this barrier’s fault tree is displayed in Figure 2-6. The Critical security barrier is designed to prevent adversaries from accessing key access points in a chemical facility such as a process control room. Figure 2-7 shows mapping of the associated fault tree.

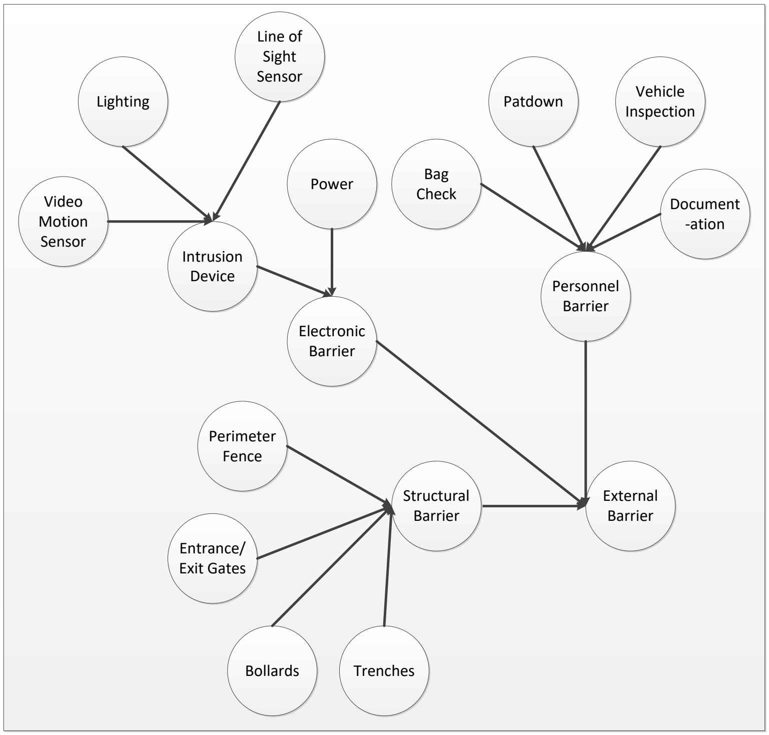

Figure 2 - 4: Proposed Mapping of fault tree for External Barrier

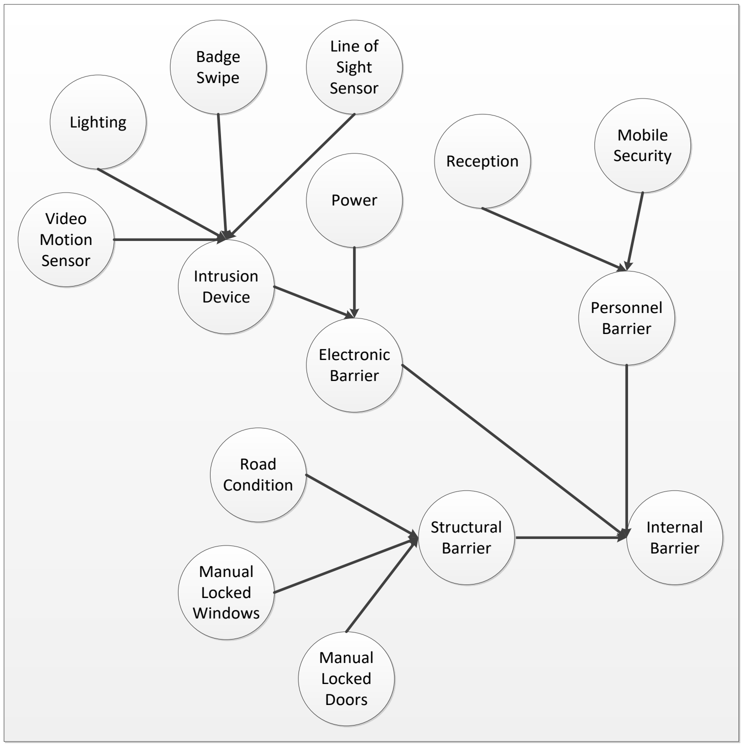

Figure 2 - 5: Proposed Mapping of fault tree for Internal Barrier

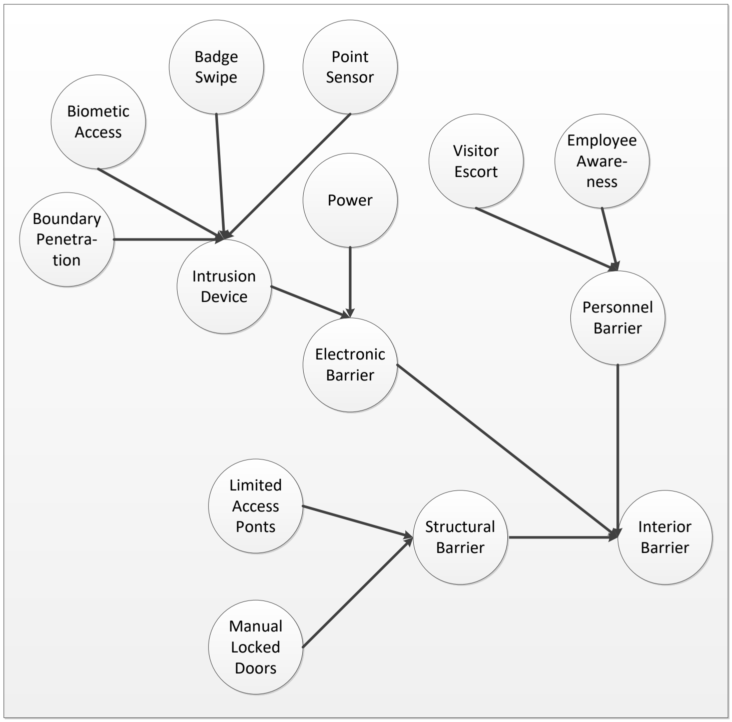

Figure 2 - 6: Proposed Mapping of fault tree for Interior Barrier

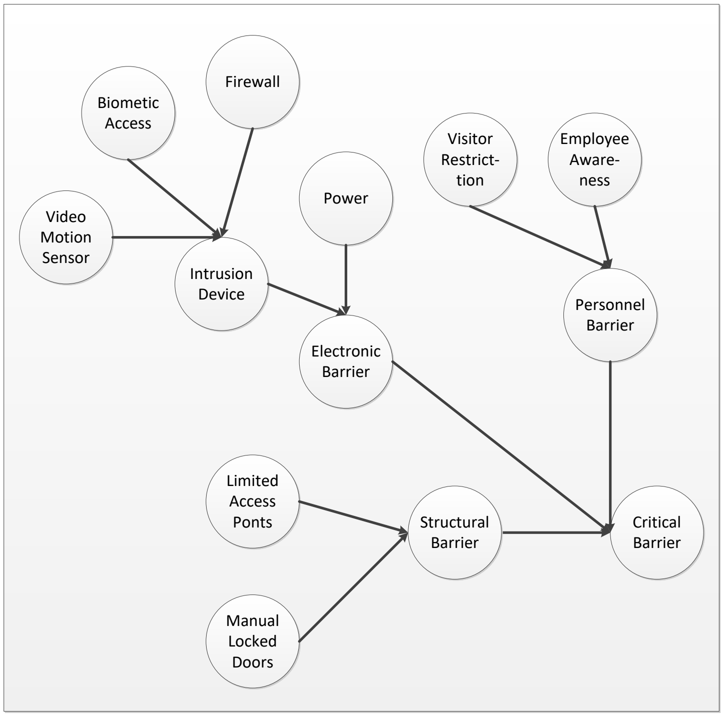

Figure 2 - 7: Proposed Mapping of fault tree for Critical Barrier

In a chemical plant, the last line of defense against an attacker is the Fail-Safe barrier. This fault tree mapping is shown in Figure 2-8. The Management and Organization barrier holds the ability to intervene any time during an impending attack. However, it is difficult to assess this barrier's effect as it may differ from industry to industry and even from company to company. Nonetheless, seven key factors have been identified and sorted into either the organization or management barrier. This is displayed in Figure 2-9.

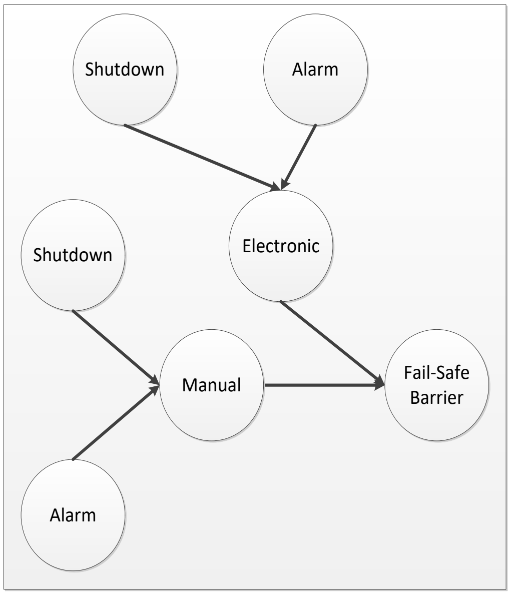

Figure 2 - 8: Proposed Mapping of fault tree for Fail-Safe Barrier

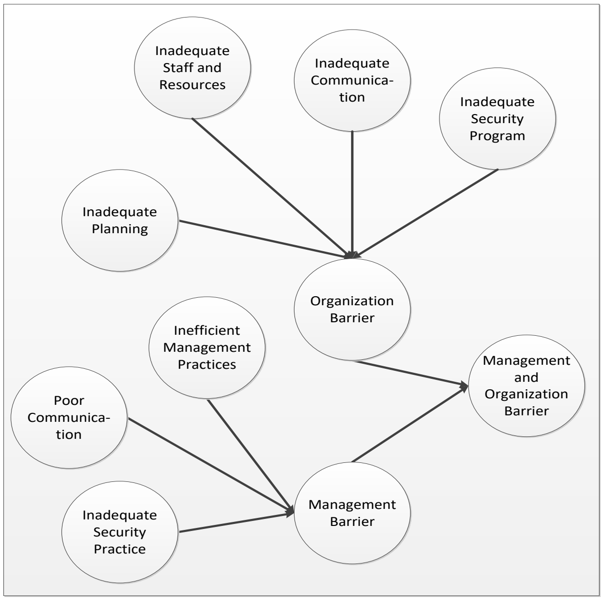
Inadequate Staff and Resources
Inadequate Communica-tion
Inadequate Security Program
Inadequate Planning
Organization Barrier
Inefficient Management Practices
Management and Organization Barrier
Poor Communica-tion
Inadequate Security Practice
Management Barrier

Figure 2 - 9: Proposed Mapping of fault tree for Management and Organization Barrier

The mapping of the fault tree for the Political barrier, shown in Figure 2-10, is a very crucial barrier in this model and accounts for conditions that are exogenous of a chemical facility. This barrier is broken into three main sub elements that are laws and enforcement, terrorism, and crime. The laws and enforcement barrier reflects the country/region that the facility is currently located in, to protect and keep safe the workers and the plant. Meanwhile, the crime barrier demonstrates the severity of hostage situations, stealing and armed attacks that may affect the operations. Finally, the terrorism barrier reveals the various forms of terrorism that can potentially hurt a chemical processing operation. Grothaus (2014) defines these types of terrorism below:

- State – the government uses it to regulate/control its population
- Religious –use of an ideology to justify use of terror
- Pathological – use of terror for personal enjoyment
- Issue-Orientated – group inflicts terror to bring awareness to a certain problem

- Separatist – use of terror to overthrow the current government and establish a new one

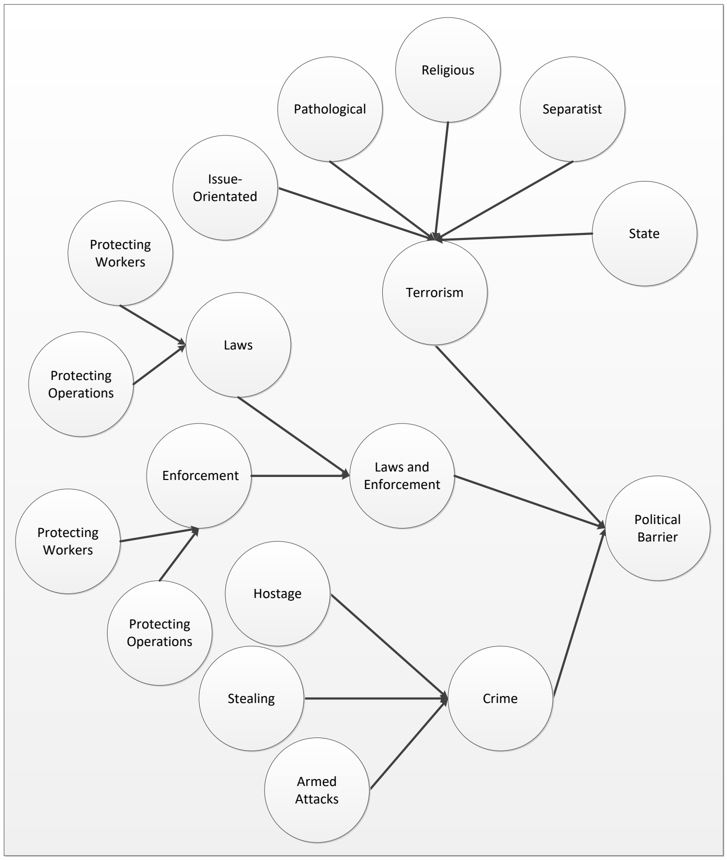

Figure 2 - 10: Proposed Mapping of fault tree for Political Barrier

Similar to the mapping of fault trees, event trees can be mapped in BN to form event networks.

The authors have previously developed a proposed event tree (van Staalduinen and Khan 2015), the reader is referred to this work for more elaboration on event tree analysis. For illustration, the event network is shown in Figure 2-12.

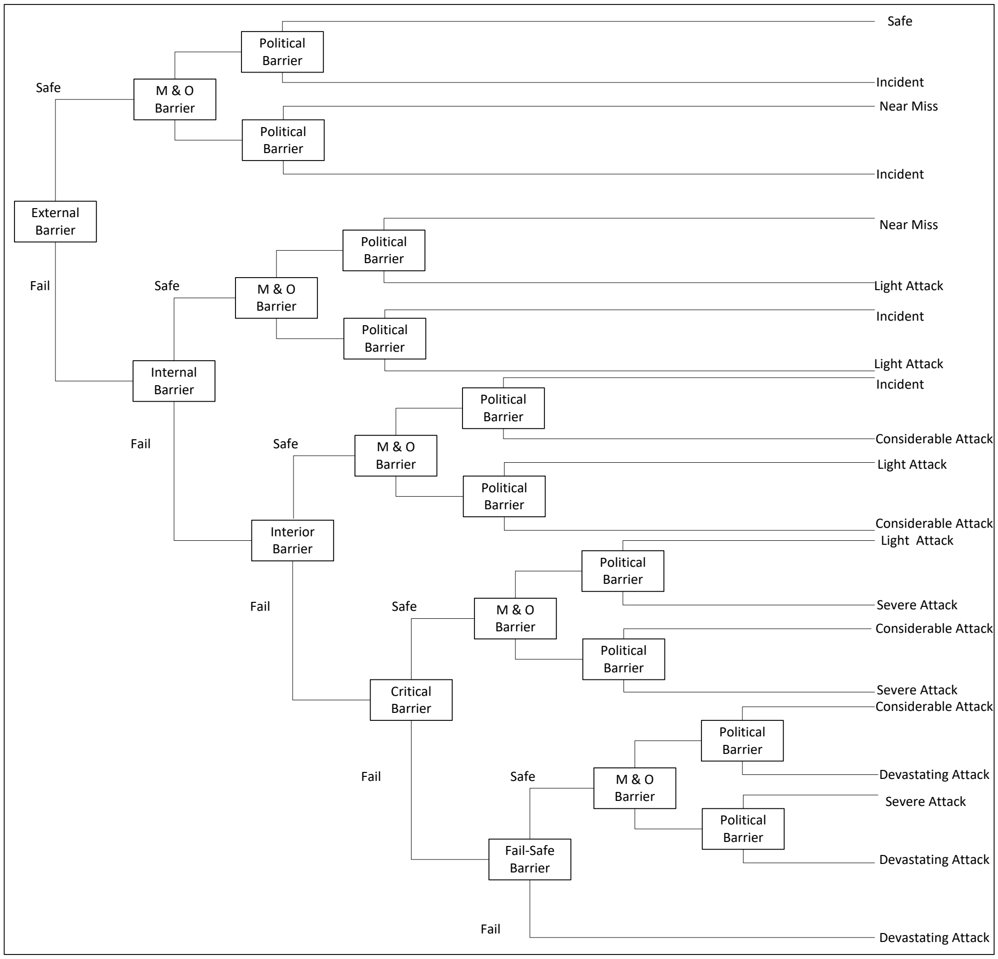

Figure 2 - 11: Proposed Event Tree (van Staalduinen and Khan, 2015)

The developed event network is shown in Figure 2-12. The consequences node is separated into seven various outcomes, which are herein described. Since there is no current available literature on security related consequence definitions, these descriptions have been developed to closely depict each situation.

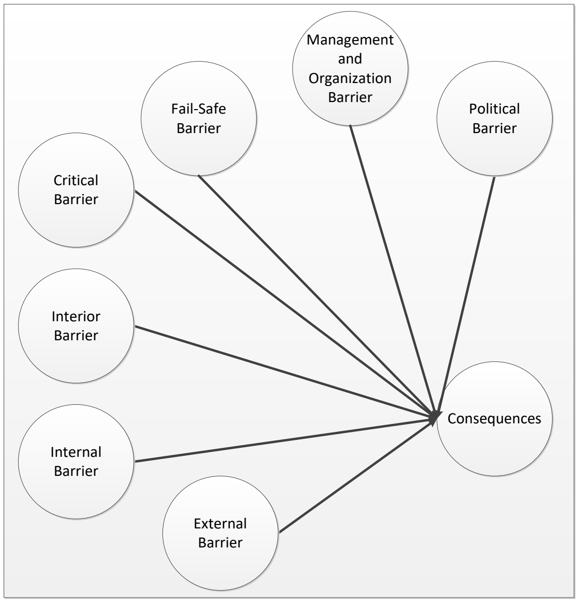

Figure 2 - 12: Proposed Mapping of the event tree for BN Network

A *Safe* term is defined as normal daily operating conditions, in which there are no issues.

A *Near Miss* is a situation in which there is potential for damage or losses to occur but however it does not. For example, if an adversary attempts to get past security with false documentation but is stopped by security.

An *Incident* can be described as an event that causes minor damage to a chemical facility while production still is operational. An illustration of this would be for an adversary is attempting to break into a building on chemical facility's property.

A *Light Attack* is a case where major damage has been caused to the facility with a minor loss in production. In addition, harm may come to employees. This event can be compared to an adversary gaining access to the facility and creating a leak in a pipeline or tank.

An event can be a *Considerable Attack* when there is greater financial damage to facility, loss in production, and workers have been injured. Furthermore, an attack at this level would draw local news coverage.

A *Severe Attack* is defined as event where operations are stopped, excessive financial damage has been accomplished and there may be employee fatalities. In addition, this type of event could inflict damage to the environment and create national news.

The last consequence, a *Devastating Attack* can be classified as event where multiple fatalities have occurred, financial losses and damages would be catastrophic and it would generate international news. Moreover, the plant would halt operations for months, possibly longer as with the case of the In Amenas gas refinery attack.

A summary of the various types of consequences is displayed in Table 2-2 below.

Table 2 - 2: Consequence Comparison

Consequence	Financial Loss	Production Loss	Worker Injuries	News Coverage
Safe	-	-	-	-
Near Miss	-	-	-	-
Incident	Insignificant	-	-	-
Light Attack	Minor	Minor	First Aid Treatment	-
Considerable Attack	Moderate	Moderate	Lost Time Injury	Local
Severe Attack	Major	Major	Fatality	National
Devastating Attack	Catastrophic	Catastrophic	Fatalities	International

With the appropriate barriers and mapped fault trees established, subjective quantification of the basic event’s probability can be found. The purpose of this is to establish initial probabilities that can later be updated based on real plant data.

The third phase and fourth phases in Figure 2-2 are dedicated to predicting the number of future abnormal events in the next interval and updating the barrier failure. Rathnayaka et al. (2011) have already explored and developed a highly detailed approach and therefore the reader is referred to their work as their method was applied directly. In the third phase, the predictive model is executed which is based on the development of the proposed BNs. This model predicts the occurrence of abnormal events in the next time interval considering history of the abnormal events and also current state of the operation. The fourth phase, executes a Bayesian updating mechanism to improve the initial beliefs of the system. These initial beliefs or prior probabilities are updated from the new data as likelihood probabilities to new posterior probabilities. Furthermore, this phase proposes and/or implements the risk reduction strategies.

2.4 Case Study

In order to illustrate the overall effectiveness of the proposed methodology, a case study is completed on an LNG processing plant, shown in Figure 2-13. As described previously the first step in the SVAPP methodology is to define the system. In a nominal LNG plant, there are typically three main processing areas: gas treatment, liquefaction, and storage. Each unit can hold various types of flammable chemicals which are potential targets for an adversary.

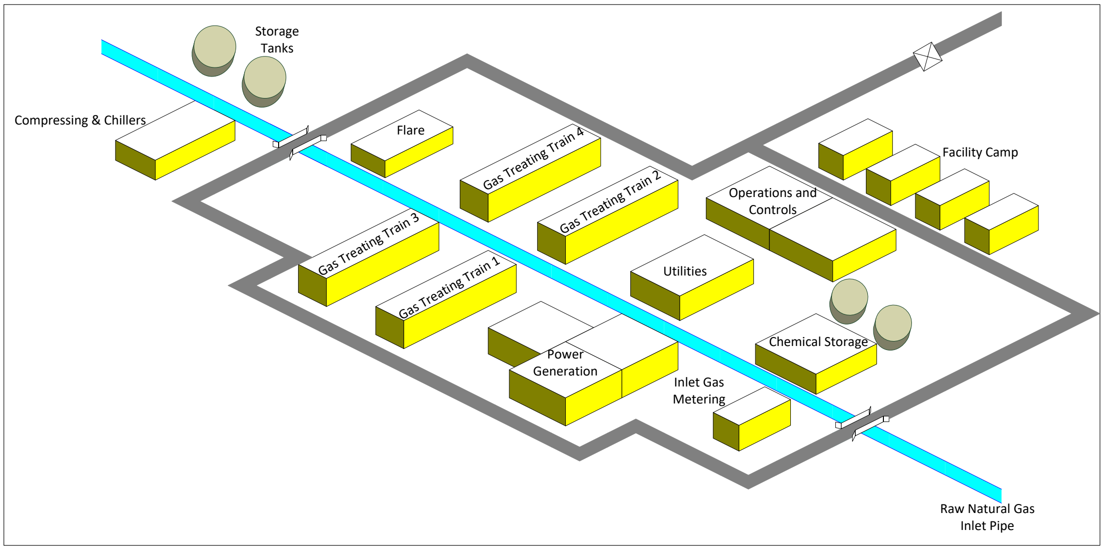

Figure 2 - 13: LNG Gas Treating Plant

The second phase is completion of a security vulnerability analysis (SVA) described by API (2013). A brief discussion on a SVA is described earlier, however for a more complete guide; the reader is referred to the original work. The initial step is planning, which will be composed outlining the objectives of the SVA by multi-skilled team to. Next step is facility characterization that aims to identify possible targets, layers of protection and determines the attractiveness of each target in addition to determining the possible consequences. For the LNG facility, possible targets are power generation unit, gas treating trains, and storage tanks. Threat assessment is the third step in conducting an SVA and the following threats have been identified with the help of ACC (2001):

- Control room cyber attack
- Intentional release of LNG storage tanks
- Intentional attack on processing equipment

- Loss of power

The subsequent step is the vulnerability analysis, which will pair both targets and threats. This will recognize probable process security vulnerabilities. Furthermore, existing security countermeasures are identified along with their effectiveness to reduce the vulnerability. By executing a variety of scenarios, the level of vulnerability for each asset is assessed. The final step is recommending further countermeasures that may be implemented in the chemical facility based on consequences and likelihood.

Throughout the conduction of the SVA, multiple scenarios of an attack would be discussed. This information would provide much needed insight in preparation of the third phase of the proposed methodology. As mentioned earlier, the third phase is the development of the attack model that places emphasis on layers of protection for a chemical facility. For the purpose of the case study, it is determined that a threat is unlikely. As described by Díez and Druzdel (2007), the causation probability is assigned based on expert judgment, which for the purpose of this methodology should be provided by security risk experts. For the purpose of this case study the values of probability are hypothetical and are displayed in Tables 2-3 – 2-9. The causation probability is designated on the basis of the parent probability that it is able to still able to cause the child node even if all other parent nodes are not active. In reality, this value should be discussed and determined by the Security Risk Assessment team. The numbers generated in this case study are illustrative to demonstrate how the methodology can be implemented.

Table 2 - 3: Basic Event Failure probabilities for External Barrier

BN Nodes	Failure	Assigned Causation

		Probability	Probability
Structural	Perimeter Fence	1.488E-03	0.75
	Entrance/Exit Gates	2.414E-02	0.60
	Bollards	3.265E-02	0.65
	Trenches	7.613E-03	0.45
	Perimeter Fence	1.488E-03	0.75
Electrical	Power	1.022E-02	0.65
	Line of Sight Sensor	5.156E-02	0.60
	Video Motion	8.848E-03	0.70
	Lighting	1.693E-02	0.70
Personnel	Bag Check	3.414E-03	0.50
	Person Inspection (Patdown)	8.661E-03	0.45
	Vehicle Inspection	9.611E-03	0.70
	Documentation	5.429E-03	0.75
External	Intrusion Device	-	0.60
	Electronic	-	0.70
	Structural	-	0.60
	Personnel	-	0.60

Table 2 - 4: Basic Event Failure probabilities for Interior Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Structural	Road Conditions	2.800E-04	0.7
	Manual Locked Doors	3.698E-02	0.6
	Manual Locked Windows	1.619E-02	0.55
Electrical	Badge Swipe	5.038E-03	0.7
	Power	9.638E-03	0.7
	Line of Sight Sensor	5.111E-03	0.65
	Video Motion	8.819E-03	0.75
	Lighting	1.283E-02	0.65
Personnel	Reception	8.400E-03	0.7
	Mobile Security	1.304E-02	0.75
Internal	Intrusion Device	-	0.65
	Electronic	-	0.75
	Structural	-	0.65
	Personnel	-	0.65

Table 2 - 5: Basic Event Failure probabilities for Internal Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Structural	Limited Access Points	6.400E-03	0.7
	Manual Locked Doors	8.056E-03	0.65
Electrical	Card Readers	5.108E-03	0.75
	Power	5.961E-03	0.75
	Boundary Penetration	5.954E-03	0.7
	Biometric Access	1.420E-03	0.65
	Point Sensors	6.463E-03	0.6
Personnel	Visitor Escort	3.200E-04	0.75
	Employee Awareness	6.100E-04	0.7

Interior	Intrusion Device	-	0.7
	Electronic	-	0.8
	Structural	-	0.7
	Personnel	-	0.7

Table 2 - 6: Basic Event Failure probabilities for Critical Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Structural	Limited Access Points	4.700E-04	0.75
	Manual Locked Doors	8.398E-04	0.7
Electrical	Biometric Access	4.507E-04	0.7
	Power	2.032E-04	0.8
	Video Motion	7.058E-04	0.75
	Network Firewall	1.303E-04	0.8
Personnel	Visitor Restriction	8.000E-03	0.8
	Employee Awareness	6.900E-04	0.75
Critical	Intrusion Device	-	0.75
	Electronic	-	0.85
	Structural	-	0.75
	Personnel	-	0.75

Table 2 - 7: Basic Event Failure probabilities for Fail-Safe Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Physical	Manual Shutdown	9.985E-05	0.85
	Manual Alarm	1.520E-05	0.85
Electronic	Electronic Shutdown	6.293E-05	0.8
	Electronic Alarm	3.441E-05	0.8
Fail-Safe	Electronic	-	0.9
	Structural	-	0.9

Table 2 - 8: Basic Event Failure probabilities for Management and Organization Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Organization	Inadequate Security Program	4.300E-03	0.8
	Inadequate Communication	3.300E-03	0.8
	Inadequate Staff & Resources	2.900E-03	0.8
	Inadequate Planning	4.100E-03	0.8
Management	Poor Communication	4.700E-03	0.8
	Inefficient Management Behaviors	4.400E-03	0.8
	Inadequate Security Practice	6.500E-03	0.8
Management and Organization	Organization	-	0.85
	Management	-	0.85

Table 2 - 9: Basic Event Failure probabilities for Political Barrier

BN Nodes		Failure Probability	Assigned Causation Probability
Terrorism	State	7.400E-04	0.75
	Religious	8.000E-03	0.7
	Pathological	6.000E-05	0.65
	Issue-Orientated	5.300E-03	0.6
	Separatist	7.700E-03	0.8
Crime	Hostage	5.000E-04	0.7
	Stealing	2.400E-04	0.65
	Armed Attacks	2.200E-03	0.7
Laws	Protecting Workers	1.900E-03	0.7
	Protecting Operations	8.100E-03	0.7
Enforcement	Worker Protection	6.900E-03	0.75
	Operation Protection	4.400E-03	0.75
Political Barrier	Laws	-	0.8
	Enforcement	-	0.8
	Laws & Enforcement	-	0.7
	Crime	-	0.7
	Terrorism	-	0.7

Based on the previous work of the authors (van Staalduinen and Khan 2015) it was found that the Noisy-AND relaxation technique that best reflected realistic conditions. The reader is referred to this work for more details. Utilizing the above basic failure probabilities and the Noisy-AND relaxation assumption with a constant substitution probability of 0.05, each respective barrier failure probability are calculated through the use software called *Netica* (2014). Using the Fail Safe barrier as an example, Table 2-10 below illustrates how Netica calculates the failure occurrence probability (this can be applied to any intermediate node). Since there are only two parent nodes for the Fail Safe barrier, there are only four logic scenarios. The BN condition is determined by the parent node failure probability while the Noisy-AND condition is determined by the causation and substitution probabilities. For instance, the failure probability of the Manual node was calculated using *Netica* to be *1.130E-02* and the Electronic node to be *3.800E-02*. Using these values and the causation probabilities in Table 2-12, the Fail Safe barrier failure probability can be calculated. The following equations clarify how Netica calculates the failure probability for each node. For the BN condition, the value is determined by the Manual failure probability multiplied by the Safe probability. When the Manual node is *Fail* and the Electronic node is *Safe*:

$$Failure\ probability\ using\ BN = 0.0113 \times (1 - 0.038) = 0.01087$$

$$Failure\ probality\ using\ Noisy - AND = \ 1 * (1 - 0.9) * (1 - 0.05) = 0.095$$

The value of the probability being ‘1’ illustrates that no inhibitor was present (i.e. fail condition).

Table 2 - 10: Example Calculation of Intermediate Node

Logic Scenarios		Network Conditions		Fail Safe Node
Manual	**Electronic**	**BN**	**Noisy-AND**	
Fail	Fail	4.294E-04	9.500E-01	4.079E-04
Fail	Safe	1.087E-02	9.500E-02	1.033E-03
Safe	Fail	3.757E-02	9.500E-02	3.569E-03
Safe	Safe	9.511E-01	9.500E-03	9.036E-03
		Fail Safe Failure Probability		1.400E-02

These values are displayed in the Table 2-11 below with the estimated prior occurrence probabilities that were determined through the event network that was constructed from the event tree. The occurrence probabilities are calculated by using the security barrier failure probabilities and the mapped event network. As shown by Rathnayaka et al. (2011), the prior probability of the consequence severity level k, (k=1,2,3, etc), denoted by *P(C$_k$)*, is shown in Equation 2-6:

$$P(C_k) = \ \prod_{j \in SB_k} x_i{}^{\theta_{i,k}} (1 - x_i)^{1-\theta_{i,k}} \tag{2-6}$$

Where *SB$_k$* denotes the security barrier associated with level *k*. If the level of k failure passes into the next security barrier, i, then $\theta_{i,k} = 1$; otherwise, $\theta_{i,k} = 0$. For example, using the Event Tree in Figure 2-11, the Safe Occurrence Probability is calculated using Equation 2-6 as follows:

$$P(C_{Safe}) = (1 - P(External)) \times (1 - P(M\&O)) \times (1 - P(Political))$$

$$= (1 - 0.0647) \times (1 - 0.0226) \times (1 - 0.0317) = \ 0.8852$$

Table 2 - 11: Failure and Consequence Occurrence Probabilities

Security Barrier	Failure Probability	Consequence *(C$_k$)*	Occurrence Probability *P(C$_k$)*
External	6.470E-02	**Safe**	8.852E-01
Internal	4.800E-02	**Near Miss**	7.876E-02
Interior	2.700E-02	**Incident**	3.386E-02
Critical	1.590E-02	**Light Attack**	2.096E-03
Fail- Safe	1.400E-02	**Considerable Attack**	9.993E-05
M & O	2.260E-02	**Severe Attack**	2.645E-06
Political	3.170E-02	**Devastating Attack**	6.034E-08

The final and key aspect of the third phase is the predictive modeling that assists in the forecasting of future security related events based on existing information. Table 2-12 shows the cumulative number of consequence events for the past twelve months.

Table 2 - 12: Cumulative Number of Consequence Events from past 12 months

Month	Safe	Near Miss	Incident	Light Attack	Considerable Attack	Severe Attack	Devastating Attack
1	1	1	0	0	0	0	0
2	2	1	0	0	0	0	0
3	3	1	1	0	0	0	0
4	4	1	1	0	0	0	0
5	4	2	1	1	0	0	0
6	5	2	1	1	0	0	0
7	6	2	2	1	0	0	0
8	6	3	2	1	0	0	0
9	8	3	3	1	0	0	0
10	8	4	3	2	0	0	0
11	9	4	3	2	0	0	0
12	10	4	3	2	0	0	0

Following the outlined model provided by Rathnayaka et al. (2011), the mean value of the posterior distribution was estimated to 1.58. Therefore, the average number of security consequence events in the next month is 2.

The final phase of the SVAPP methodology is to update the failure probabilities to minimize uncertainty through Bayesian updating and make important decisions on security countermeasures. Once again following the method by Rathnayaka et al. (2011), the likelihood probabilities have been developed and are shown in Table 2-13. The likelihood probabilities are based on consequence event data in Table 2-12. Due to the lack of severe attacks, in the past twelve months the later barriers cannot have likelihood probabilities developed. Subsequently, the posterior failure probabilities of the barriers can be calculated and are shown in Figure 2-14. However, since last four barriers in the table are unable to be updated they are assumed to have such a low failure rate that it is now negligible. With the updated barrier failure probabilities, the respective occurrence probabilities can also be determined. These values are displayed in Figures 2-15 – 2-18. The updated value for Light Attack is a reflection that as the Interior barrier increases in failure than the more likely a Light Attack will occur. Note that the values for the Critical barrier and beyond are zero as there were no incidents reported. This shows the Critical barrier was effective.

Table 2 - 13: Developed Likelihood Probabilities

Month	External	Internal	Interior	Critical	Fail Safe	M&O	Political
1	0.500	0.000	-	-	-	-	-
2	0.333	0.000	-	-	-	-	-
3	0.400	0.500	0.000	-	-	-	-
4	0.333	0.500	0.000	-	-	-	-
5	0.500	0.500	0.500	0.000	-	-	-
6	0.444	0.500	0.500	0.000	-	-	-
7	0.455	0.600	0.333	0.000	-	-	-

8	0.500	0.500	0.333	0.000	-	-	-
9	0.467	0.571	0.250	0.000	-	-	-
10	0.529	0.556	0.400	0.000	-	-	-
11	0.500	0.556	0.400	0.000	-	-	-
12	0.474	0.556	0.400	0.000	-	-	-

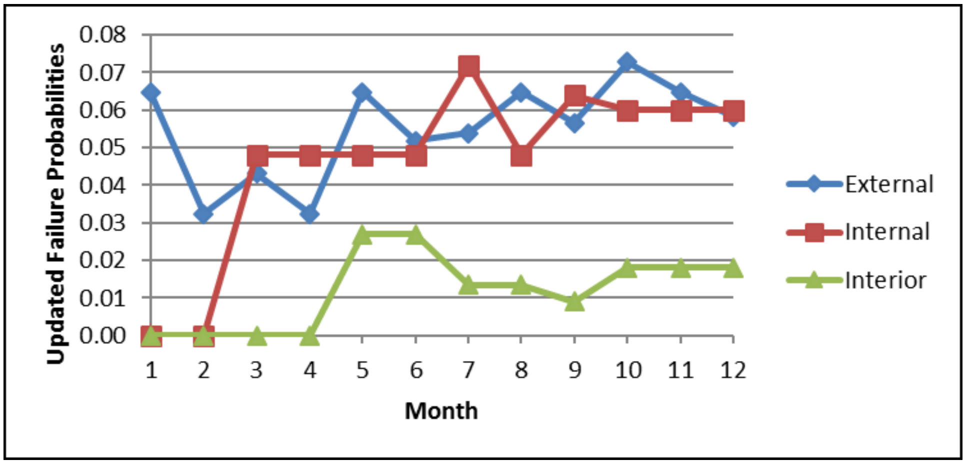

Figure 2 - 14: Posterior Failure Probability of Security Barriers

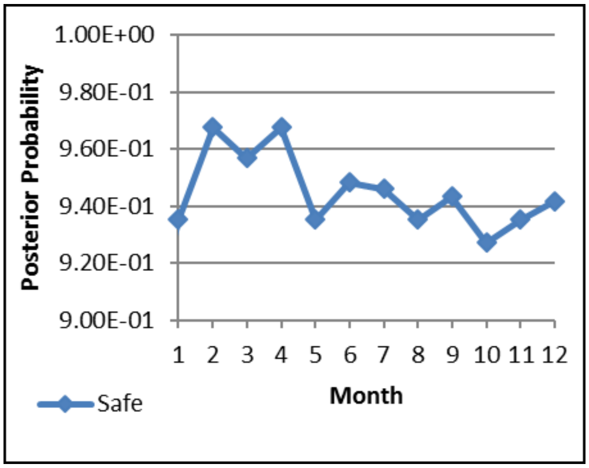

Figure 2 - 15: Updated Safe Consequence Occurrence Probability

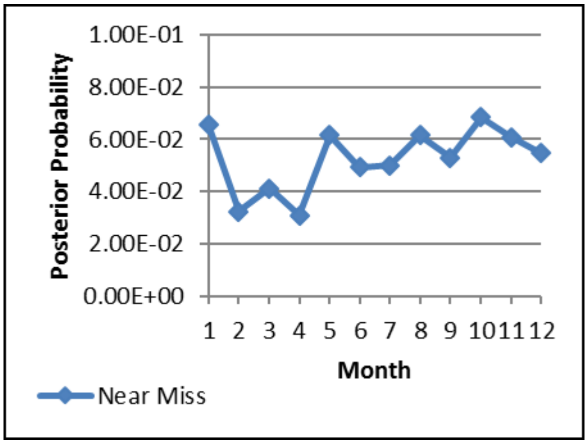

Figure 2 - 16: Updated Near Miss Consequence Occurrence Probability

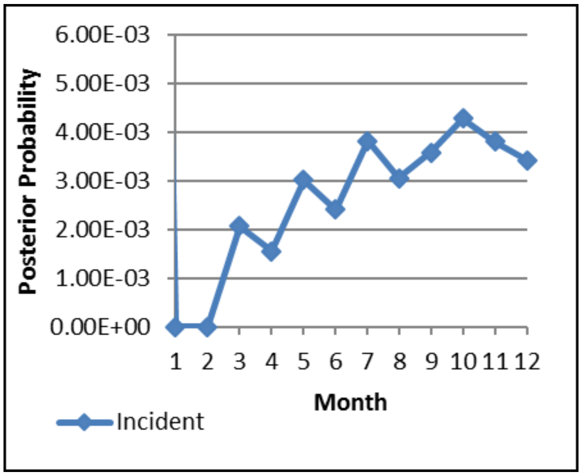

Figure 2 - 17: Updated Incident Consequence Occurrence Probability

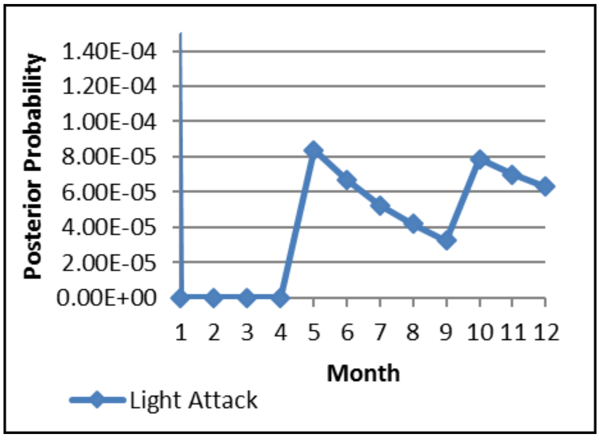

Figure 2 - 18: Updated Light Attack Consequence Occurrence Probability

For the sensitivity analysis, in order to see how each barrier has an impact on the consequences, one barrier failure probability was increased by 10% at a time while the others remained at the initial estimated prior probabilities as shown in Table 2-14. For example, Scenario 2 alters the External barrier while the other barrier failure probabilities remain the same. Scenario 3 returns the External barrier to the original value but alters the Internal failure probability. This continues for the remaining scenarios. The event network uses these probabilities to develop new occurrence probabilities which are shown in Figures 2-19 – 2-21. Through those figures it can be noted that Scenarios 5 to 7 do not affect the more severe consequences, therefore more attention can be focused improving the first few barriers of a plant's defense.

Table 2 - 14: Scenarios with Respective Probabilities

Barrier	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5	Scenario 6	Scenario 7	Scenario 8
External	6.47E-02	7.12E-02	6.47E-02	6.47E-02	6.47E-02	6.47E-02	6.47E-02	6.47E-02
Internal	4.80E-02	4.80E-02	5.28E-02	4.80E-02	4.80E-02	4.80E-02	4.80E-02	4.80E-02
Interior	2.70E-02	2.70E-02	2.70E-02	2.97E-02	2.70E-02	2.70E-02	2.70E-02	2.70E-02
Critical	1.59E-02	1.59E-02	1.59E-02	1.59E-02	1.75E-02	1.59E-02	1.59E-02	1.59E-02
Fail-Safe	1.40E-02	1.40E-02	1.40E-02	1.40E-02	1.40E-02	1.54E-02	1.40E-02	1.40E-02
M & O	2.26E-02	2.26E-02	2.26E-02	2.26E-02	2.26E-02	2.26E-02	2.49E-02	2.26E-02
Political	3.17E-02	3.17E-02	3.17E-02	3.17E-02	3.17E-02	3.17E-02	3.17E-02	3.49E-02

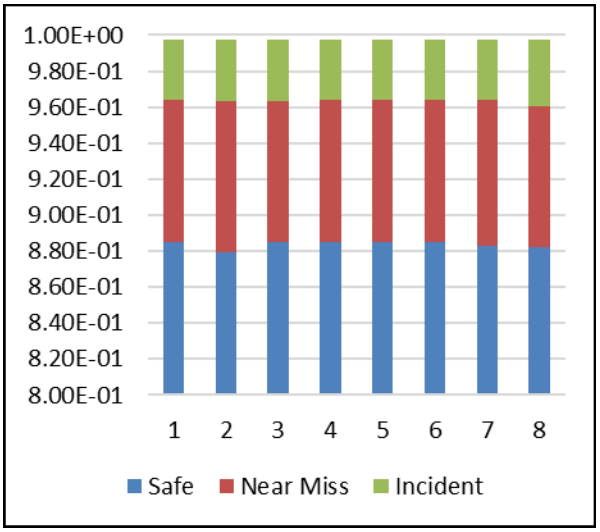

Figure 2 - 19: Scenario and Consequence Occurrence Probability

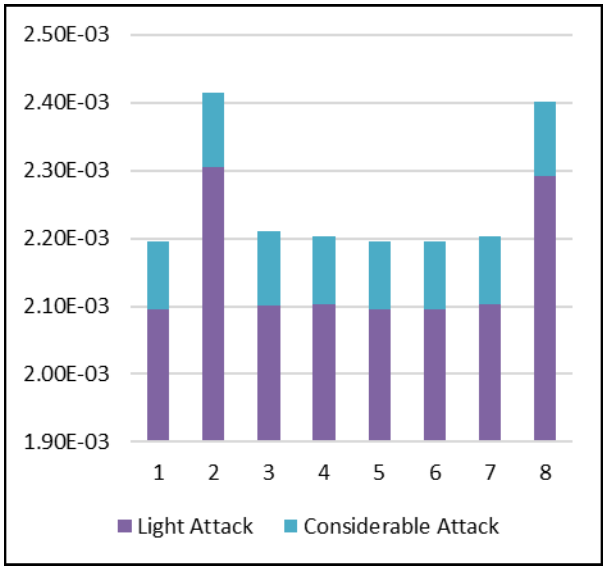

Figure 2 - 20: Scenario and Consequence Occurrence Probability

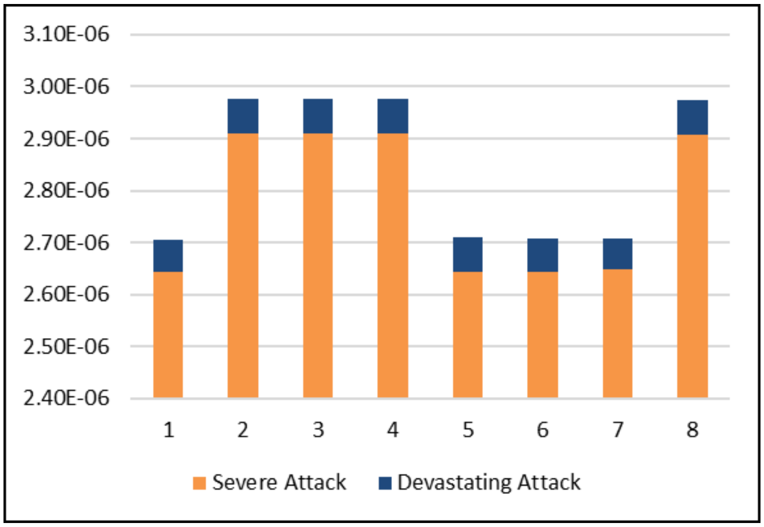

Figure 2 - 21: Scenario and Consequence Occurrence Probability

Further analysis can be completed on the event network and how each of the barriers may in reality interact with each other. Currently the network is set up as each barrier being d-separated from each other. The concept of d-separation was introduced by Geiger et al (1990). In a BN, two nodes are considered to be d-separated if a path between the two nodes is blocked by a diverging, serial, or converging pattern. Thus if they are d-separated then the nodes are considered independent. Figure 2-22 displays the new event network showing the dependency among the barriers.

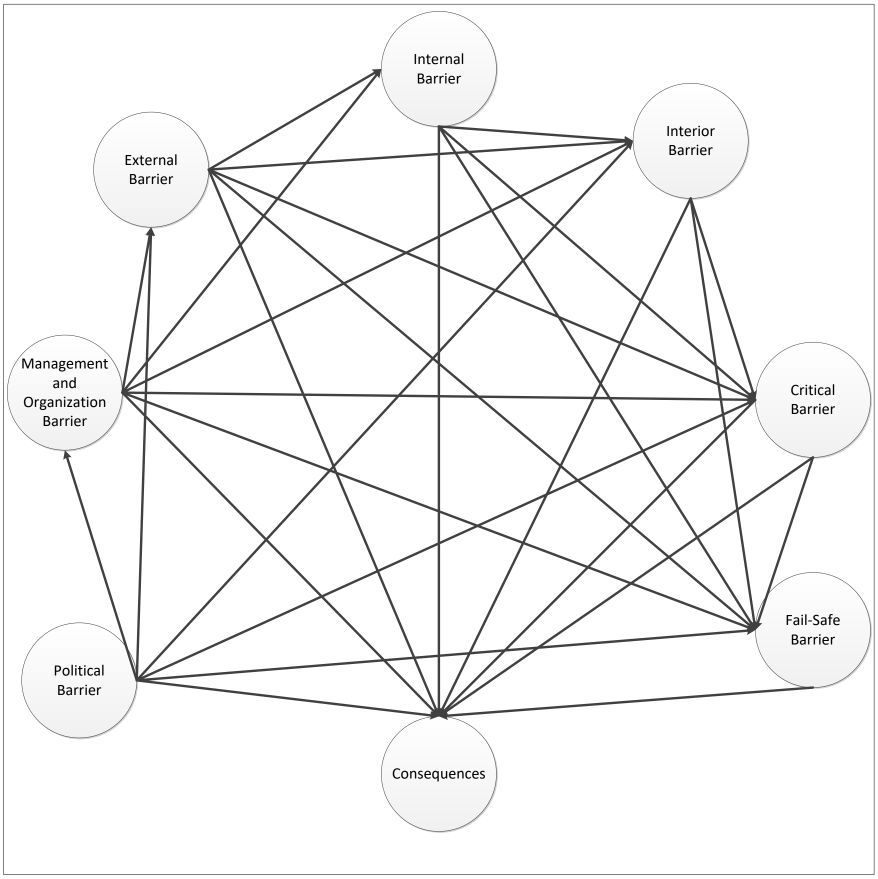

Figure 2 - 22: Event Network with Dependencies

In this new event network, the conditional probability tables of each barrier node can be manipulated to reflect the degree of dependency. Therefore, in order to see how each of the various degrees of dependency can affect the various consequences, five separate cases have been developed. The different cases are described as:

- Case 1 - utilizes AND/OR logic
- Case 2 - all CPT values equal to 0.50
- Case 3 - all CPT values equal to 0.50 except when all Fail conditions occur, then use 1 for Fail

- Case 4 - all CPT values equal to 0.50 except when all Safe conditions occur, then use 1 for Safe
- Case 5 - expert judgment is used to represent realistic conditions

To help clarify the differences in Cases 3 and 4, the CPT of the External Barrier are shown in Tables 2-15 and 2-16. For each case since the Political barrier was the influencing node, it remained constant throughout the analysis, with the initial prior estimated failure probability of 0.032. Figure 2-23 displays each barrier's calculated failure probability for the respective cases and Figure 2-24 shows how the consequence occurrence probabilities were affected.

Table 2 - 15: External Node CPT Case 3

Political Node		**Safe**		**Safe**	
Management and Organization Node		Safe	Fail	Safe	Fail
External Node	Safe	0.5	0.5	0.5	0
	Fail	0.5	0.5	0.5	1

Table 2 - 16: External Node CPT Case 4

Political Node		**Safe**		**Safe**	
Management and Organization Node		Safe	Fail	Safe	Fail
External Node	Safe	1	0.5	0.5	0.5
	Fail	0	0.5	0.5	0.5

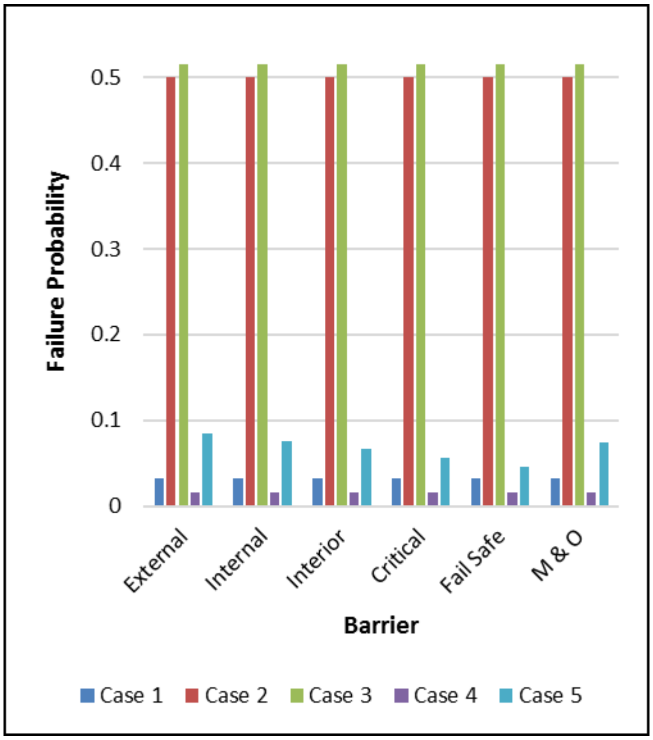

Figure 2 - 23: Case with Barrier Failure Probability

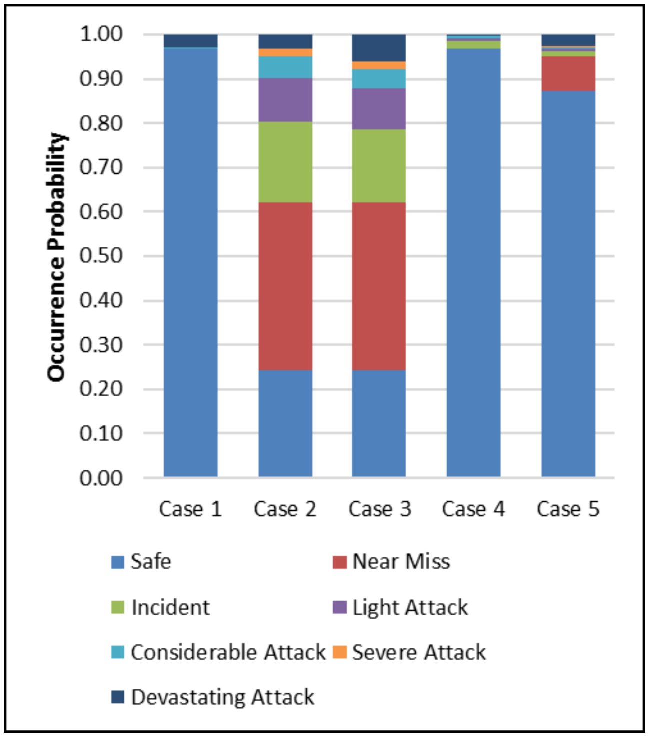

Figure 2 - 24: Case with Consequence Occurrence Probability

2.5 Analysis of Case Study

The proposed methodology utilizes five sequential barriers with two overseeing barriers to illustrate the attack process. The prior failure probability of each barrier was initially estimated using a subjective probabilistic approach with a relaxation assumption known as Noisy-AND. These probabilities were updated using illustrative plant's 'abnormal event' data that represent more realistic conditions. For example, the plant was initially operating a *Safe* condition at 88.5% but improved to 94.2%. A *Light Attack* probability decreased from initial estimate of 0.21 to 0.006 of occurring. Although some of the consequences eventually updated to a 0. Probability of occurring, this is simply not the case. These consequences will have a small probability of happening however; it is so small that it is reflected as 0.0% in the analysis.

When each barrier failure probability was changed one at a time, it became apparent how each barrier affected the possible consequences. For example, in Scenario 2, when the External barrier failure probability was increased all types of the attack probabilities increased. This was also the case for Scenario 8, when the failure probability of the Political barrier was increased. Based on this analysis, both the External and Political barriers are deemed the most important in the attack model sequence. This result is expected as the External barrier is a chemical facility's first line of defense in an attack prevention and the Political barrier attempts to model conditions that surround a chemical facility.

In the barrier dependency analysis, that the Political node has a direct correlation to the occurrence of a *Devastating Attack*. This is an expected result, as is the case with most attacks the intent is to cause as much damage as possible. When utilizing AND/OR logic, each node was calculated to have the same probability as the node which influenced, which is the Political node. The most interesting case is Case 5, which attempted to show realistic conditions. From an attack model's perspective this case makes the most sense as an attacker will typically attempt to create a *Devastating Attack* and the goal of chemical facility will be to attempt to prevent any attack from occurring which would count as a near miss.

2.6 Conclusion

In recent years, chemical processing plants have become targets for terrorists to attack as they hold toxic and flammable materials under pressurized conditions. The goal of these intentional attacks is to inflict damage to not only plant property but also the workers at the plant. Therefore, it is imperative to further develop security risk assessments to ensure that site security guidelines can be properly implemented.

The case study shows that the proposed SVAPP methodology applied to chemical facility security offers reliable information of modeling and predicting an intentional attack. In addition, the model displays various relaxation techniques that are applied to BN to best suit the interactions between events and barrier failure. The use of Bayesian updating allows for the uncertainty to reduce and allows the failure probabilities to reflect a more realistic value based on recent plant conditions. This in turn reflects reduced probability occurrence of possible consequences at chemical facility. The event barrier network was modified to show possible dependencies among the barriers. Through manipulation of the conditional probability tables a realistic condition was displayed, which reflected consequences nominally seen in security related attacks. These conditions are that chemical plants typically operate at a safe condition and that successful intentional attacks on them are usually classified as devastating. Utilizing this information, the overall security performance can be increased and effective countermeasures can be in put in place to prevent an intentional attack from occurring.

2.7 References

American Chemistry Council. Site Security Guidelines for the U.S. Chemical Industry. Washington (DC): American Chemistry Council; 2001 Oct. 56.

American Petroleum Institute. Security Vulnerability Assessment, Methodology for the Petroleum and Petrochemical Industries. Washington (DC): 2003.

American Petroleum Institute. Security Vulnerability Assessment, Methodology for the Petroleum and Petrochemical Industries. Washington (DC): 2013.

Bajpai S, Gupta JP. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries. 2005; 18 (4-6): 301-309.

Baybutt P, Reddy V. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defense Journal. 2003; 2 (1).

Brown G, Cox. A. How probabilistic risk assessment can mislead terrorism analysts. Risk Analysis. 2011; 31 (2): 196-204.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety. 2001; 71 (3): 249-260.

Center for Chemical Process Safety. Guidelines for Analyzing and Managing Security Vulnerabilities of Fixed Chemical Sites. New York: Center for Chemical Process Safety/AIChe; 2003. 240 p.

Díez F, Druzdzel M. Canonical Probabilistic Models for Knowledge Engineering Technical Report. Madrid (Spain): CISAID; 2007.

Dunbobbin B, Medovich T, Murphy M, Ramsey A. Security Vulnerability Assessment in the Chemical Industry. Process Safety Progress. 2004; 23 (3): 214-220.

Ezell BC, Bennett SP, von Winterfeldt D, and others. Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis. 2010; 30 (4): 575-589.

Geiger D, Verma T, Pearl J. Identifying Independence in Bayesian Networks. Networks. 1990; 20: 507-524.

Grothous N. Types of Terrorism. Hand of Reason. 2014 June 27.

Henderson S. Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil. The Washington Institute. 2006 Feb 26.

Modarres M. Risk Analysis in Engineering: Techniques, Tools, and Trends. Florida: CRC Press; 2006. 424 p.

Moore D. Security Risk Assessment Methodology for the petroleum and petrochemical industries. Journal of Loss Prevention in the Process Industries. 2013; 26 (6): 1685-1689.

Moore D, Fuller B, Hazzan, M, Jones J. Development of a security vulnerability assessment process for the RAMCAP chemical sector. Journal of Hazardous Materials. 2007; 142 (3): 689-694.

National Research Council. Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change. Washington, DC: National Academies Press; 2008. 171 p.

Netica. 2014. Netica^{TM} Application. Norsys Software Corporation. 2014.

Pandey A. ISIS in Iraq: Kurds Recapture Mount Sinjar As Islamic State Group Retakes Baiji Oil Refinery. International Business Times. 2014 Dec 22.

Rathnayaka S, Khan FI, Amyotte P. SHIPP Methodology: Predictive Accident Modeling Approach. Part I: Methodology and Model Description. Process Safety and Environmental Protection. 2011; 89 (3): 151-164.

Reniers G. Multi-Plant Safety and Security Management in the Chemical and Process Industries. Great Britain: Wiley-VCH; 2010. 290 p.

Statoil ASA. The In Amenas Attack. 2013 Feb. http://www.statoil.com/en/NewsAndMedia/News/2013/Pages/12Sep_InAmenas_report.aspx

van Staalduinen M, Khan F. A Barrier Based Methodology to Assess Site Security Risk. In: SPE E&P Health, Safety, Security, and Environmental Conference – Americas; 2015 Mar 16 – Mar 18, 2015; Denver, USA. Copy of the document available from Department of Process Engineering, Memorial University, St John's, Canada.

Chapter 3: Functional Quantitative Security Risk Analysis (QSRA) to Assist in Protecting Critical Process Infrastructure

3.0 Abstract

This article proposes a quantitative security risk assessment methodology that can assist management in the decision-making process where and when to protect critical assets of a chemical facility. An improvement upon previous work is the approach of conducting concurrent Threat and Vulnerability Assessments, as opposed to a sequential approach. Furthermore, this method introduces a Bow Tie risk model mapped into a Bayesian Network model that allows for various logical relaxation assumptions to be applied. Different uncertainty relaxation approaches such as "Noisy-OR" and "Leaky Noisy-OR" and "Noisy-AND" are tested to improve threat and vulnerability likelihood. Finally, integrating threat/vulnerability likelihood with potential losses, the security risk is quantified. The potential security countermeasures are characterized into either decreasing vulnerability or decreasing threat likelihood and are reassessed considering a cost analysis. A theoretical case study is conducted to exemplify the execution and application of the proposed method.

Keywords: quantitative security risk analysis, Bayesian network, bow-tie risk model

3.1 Introduction

The movement in the academic world to widen risk assessments to include security-related incidents began after the September 11, 2001 terrorist attacks in New York. In recent years, industry and policy makers have realized that chemical process facilities may be attractive soft targets for terrorists as they often store hazardous chemicals in large quantities. With the availability of hazardous materials, it becomes easier for a terrorist to inflict casualties, negatively impact the environment, cause huge property damage, and disrupt business operations and local or even global economies. For example, recent events in both Iraq and Algeria show the need to protect chemical plants from intentional acts to cause damage (Statoil ASA, 2013; Reuters News Agency, 2015).

Previously, risk assessments focused on unintentional, naturally occurring events to maintain plant safety and integrity. Recently, risk managers focus also on security countermeasures and their ability to control the loss due to possible deliberate acts of terrorism. There are two distinct approaches that can be executed to conduct a security risk assessment: 'asset-driven' and 'threat-driven' (or also called 'scenario-based'). McGill et al. (2007) define an asset-driven analysis as an approach that assesses the consequences and probability of an adversary's success for a given set of possible scenarios. The total risk is estimated using these scenarios with the threat likelihood, in turn based, amongst others, on the level of attractiveness of the process plant. Thus there is a need for intelligence on an adversary's intent and possible threats. In contrast, a threat-driven (or scenario-based) approach uses a set of predefined scenarios based on assumed adversary capabilities. The rate of occurrence can be predicted from historical data after studying the various hazards of a threat. The fallible component of this approach is that an innovative adversary may develop a new threat, previously unknown to the intelligence community.

The Center for Chemical Process Safety (2003) was among the first to release a document to assist industry in the procedure of completing a so-called security vulnerability assessment. In addition to presenting a systematic methodology, the document also provided insight into the concepts and background of chemical security such as the concept of “Rings of Protection”. The primary principle of this concept is that each ring will independently have the ability to block an adversary from accessing the next level and successfully achieving their malicious intent. The Center for Chemical Process Safety presents a five step method to complete a security vulnerability assessment (SVA): (1) Project Planning, (2) Facility Characterization, (3) Threat Assessment, (4) Vulnerability, (5) Identify Countermeasures. This methodology, when combined with other hazard reducing steps, can help to increase the success of security risk management.

Building upon this concept Bajpai and Gupta (2005) propose an alternative security risk assessment. This semi-quantitative approach is based on four main steps: (1) Threat Analysis, (2) Vulnerability Analysis, (3) Security Countermeasures, (4) Mitigation and Emergency Response. A novel idea presented in this method is the use of a security risk factor table. This table provides rankings from 1 (low) to 5 (high) of various risk factors affecting a given chemical facility. When summarized, these factors give the total current risk status of the facility. The model however does not capture the economic costs that may come from security countermeasures implementation.

Furthermore, McGill et al. (2007) subsequently propose a quantitative methodology helping investment decision-making regarding resource protection for critical assets. A key aspect of this method is the development of an annual risk profile for each critical asset along with a rate of occurrence. With a quantitative approach, the impact of possible security countermeasures through cost-benefit analysis becomes straightforward for management. However, the methodology provides no distinction of the type of benefit, whether it minimizes the threat or reduces the vulnerability.

White (2014) further extends the then current Department of Homeland Security (DHS) programs and proposes the Asset Vulnerability Model (AVM). The AVM is designed to assist in the development of an acceptable risk assessment approach for the industry. A risk baseline analysis is first established followed by a cost-benefit analysis which is utilized to support countermeasure decision making. This model does not provide a risk tracking or monitoring feature that is able to assist in continual analysis of the baseline risk.

Most recently, Argenti et al. (2015) studies the attractiveness of chemical installations being possible targets for terrorist activities. They adopted a semi quantitative approach to model the attractiveness of the target. The authors considered plant damage potential (in terms of causing fatalities) and perceived value (in terms of perceived political and socio-economic value) as two main factors, and used a scoring method to characterize these factors. It appears that socio-economic and political factors tend to play key role in defining the attractiveness of a target.

The goal of this current paper is to propose a methodology that can be used for security risk assessments and security risk mitigation through dynamic risk probabilities. Current literature sometimes criticises the use of fixed probabilities (National Research Council, 2008; National Research Council Press, 2010). This methodology allows for the probabilities to be reassessed if the risk is too high or a trigger calls for reassessment. Currently, the established precedent is to complete the Threat assessment and Vulnerability assessment in a sequential order (CCPS, 2003; Bajpai and Gupta, 2005;

API, 2013). However, this work suggests carrying out these two assessments concurrently as this will lead to information being helpful in either task to be shared. This methodology is constructed from the authors' previous work (van Staalduinen and Khan, 2015) and other available literature in the area of chemical security (McGill et al. 2007; Reniers et al., 2013). Section 2 explores the tools and techniques that are executed in the proposed method while Section 3 provides a holistic view of the proposed methodology. Section 4 displays how the method can be executed via a case study, the results being discussed in Section 5. Conclusions are provided in Section 6.

3.2 Analysis Techniques

3.2.1 Bow-Tie Model

A Bow-Tie (BT) model is a graphical technique composed of a fault tree on the left-hand side with a corresponding event tree on the right-hand side. Hence, a complete scenario with the causes on the left connected to a top event (or 'initiating event') with the subsequent consequences on the right is obtained (Delvosalle et al., 2005).

3.2.2 Bayesian Network

A Bayesian network (BN) or influence diagram is a graphical technique composed of directed arcs and nodes. These nodes and directed arcs represent variables and their relationships to each other, respectively. Conditional probabilities are assigned to each node displaying the conditional probability dependencies among the variables. A BN node probability can be calculated by Equation 3-1

$$P[X_1, X_2, . X_n] = \prod_{i=1}^{n} P[X_i | Parent(X_i)] \quad (3\text{-}1)$$

where *Parent(X$_i$)* is the parent set of *X$_i$* (Jensen and Nielson, 2007). Additionally, a BN uses Bayes Theorem, which can update the prior occurrence of primary events based on new evidence, E, that may become available in time. This relationship is shown in Equation 3-2:

$$P(X_i|E) = \frac{P(X_i,E)}{P(E)} = \frac{P(X_i,E)}{\sum_i P(X_i,E)} \tag{3-2}$$

Furthermore, when working within a BN, the conditional probabilities and hence the conditional probability tables (CPT) can be manipulated to show various relaxation assumptions such as the Noisy-OR, Leaky Noisy-OR, and Noisy-AND (Díez and Druzdzel, 2007). The Noisy-OR logic assumption is defined as a parent event may occur; however, the child may not occur as there was an inhibitor that prevented the occurrence. Meanwhile, the Leaky Noisy-OR follows this same logic but includes a leak parameter.

This leak parameter accounts for all possible parent events that are not explicitly modeled. The Noisy-AND logic follows that of Boolean logic however in this case the parent event will either be inhibited or substituted. The substitution factor replaces the parent if the event does not occur. These assumptions are extensively covered in a technical report presented at a conference (van Staalduinen and Khan, 2015). We refer the interested readers to this technical report for more information.

3.2.3 Bow-Tie Mapping

Both the fault and event tree of a developed BT can be mapped in a BN. Bobbio et al. (2001) provides a technique for mapping a fault tree. The primary and intermediate events in the fault tree become primary and intermediate nodes in a BN where the logic relationship is defined in the CPT. Meanwhile the event tree can be mapped by using the technique presented by Bearfield and Marsh (2005). In the mapped event tree, each node has two states, one for success and one for failure while the consequence node will include all possible consequences. It should be noted that a directed arc should be drawn from one barrier to another if that barrier influences the next barrier. In addition, a connection needs to be made from the barrier node to the consequence node. With both the fault and event tree mapped, the diagrams are then combined through the pivot node which is the top event of the fault tree. A generic mapped BT into a BN is shown in Figure 3-1. Furthermore, Khakzad et al. (2013) demonstrates that mapping a BT into a BN allows for a more relaxed structure of a BT and additional modeling aspects such as probability updating. Various barriers are developed which minimize the consequences of an attack while the number of available barriers may differ for each critical asset.

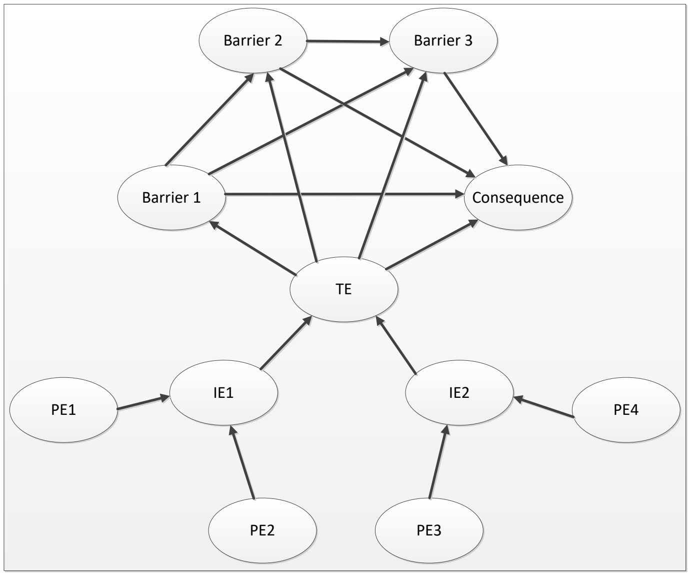

Figure 3 - 1: General Mapped Bow-Tie Model

3.3 Quantitative Security Risk Assessment Methodology (QSRA)

The first step in the QSRA methodology is to conduct an Asset Characterization of all assets to find out which ones are designated as critical. With critical assets recognized, a Threat and Vulnerability Assessment is conducted concurrently to ensure information is shared during the completion of the Attack Scenario Likelihood and Consequence Assessment. The Risk Assessment is finalized and the risk is determined to be acceptable or unacceptable. If the risk is deemed unacceptable, countermeasures are identified to either minimize the threat or vulnerability of the critical assets. A cost analysis of the recommended risk reduction strategies is completed to determine the most optimal solution which can be implemented. Once implemented, the methodology should be repeated to confirm that the risk is at an acceptable level. Risk monitoring and tracking is organized to have a reassessment of critical assets if a trigger is alerted. Execution of the proposed Quantitative Security Risk Assessment (QSRA), as shown in Figure 3-2 below, will help to develop a security plan and aid its implementation for improving plant security.

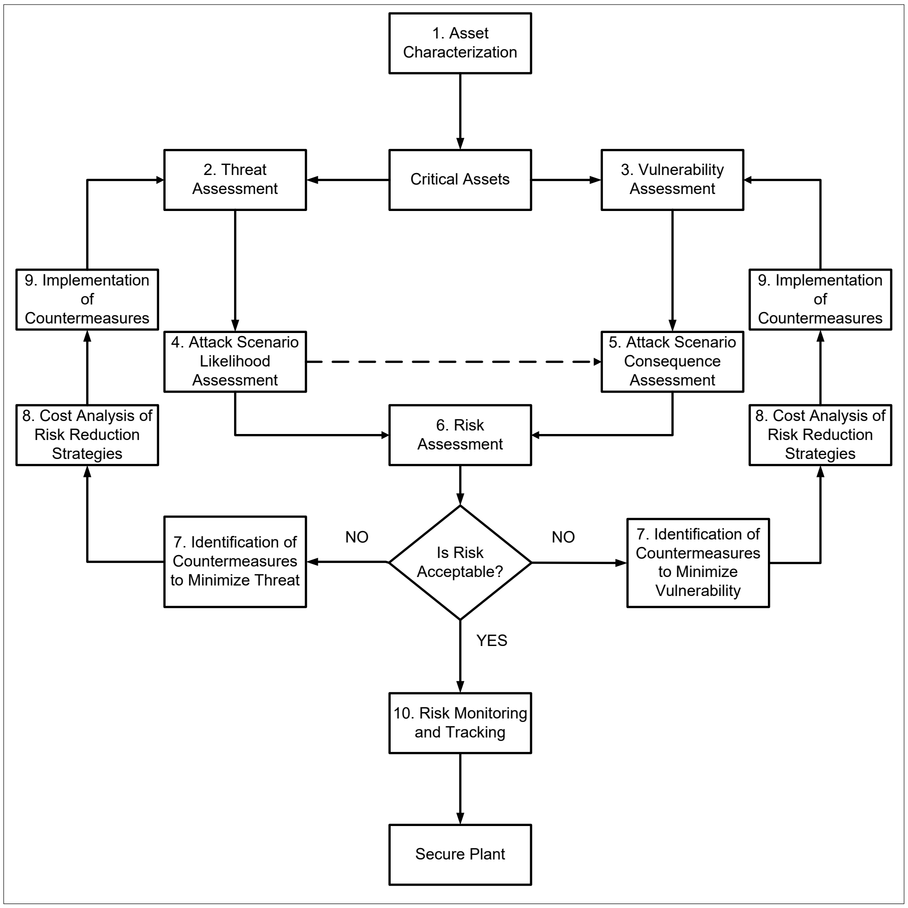
1. Asset Characterization
Critical Assets
2. Threat Assessment
3. Vulnerability Assessment
9. Implementation of Countermeasures
9. Implementation of Countermeasures
4. Attack Scenario Likelihood Assessment
5. Attack Scenario Consequence Assessment
8. Cost Analysis of Risk Reduction Strategies
6. Risk Assessment
8. Cost Analysis of Risk Reduction Strategies
7. Identification of Countermeasures to Minimize Threat
NO
Is Risk Acceptable?
NO
7. Identification of Countermeasures to Minimize Vulnerability
YES
10. Risk Monitoring and Tracking
Secure Plant

Figure 3 - 2: The Proposed Methodology

3.3.1 Asset Characterization

The first step in asset characterization is to identify all *potential* critical assets located on a chemical plant. This can be completed by a plant walk-through or by reviewing plant layout diagrams including piping and instrumentation diagrams (P&IDs). The next step is to determine the *criticality* of the assets through the analysis of three factors: (1) Social, (2) Economic, and (3) Political. Each factor is given a score out of ten, where 'one' is lowest and 'ten' is highest. The social factor considers how potential damage would impact society. The economic factor analyzes the financial costs. Lastly, the political factor relates to the potential that an adversary would see this asset as a target. In addition, the plant can be segregated into various zones that can group multiple potential assets together. The creation of zones allows for security countermeasure dependency to be displayed between each asset existing in the zone. At this stage all current security countermeasures should be identified. Reniers (2010) e.g. proposes that security countermeasures be broken down into distinct sections, such as Organizational, Physical, Electrical, and Personnel. Delineating security countermeasures into different groups, they can be better identified and organized for management. From this stage, only the selected critical assets will be counted in the assessment.

3.3.2 Threat Assessment

With the critical assets of a chemical facility determined, the next phase is to assess the possible threats with respect to the assets. Baybutt and Reddy (2003) state that a threat has several sources: internal and external sources. An internal threat may come from a disgruntled employee or contractor who may seek to cause economic loss to the company by disrupting the production of the plant. An external threat may be an adversary or terrorist group that wishes to exploit a chemical plant to cause maximum impact through casualties and damage to process equipment. A third type of threat is a combination of both an internal and an external threat: an outsider planning an attack with the help of an insider. This would allow for the worst-case scenario to develop. An inside threat allows the exploitation of the weaknesses within a facility. Based on these types of threats, the potential attacks can be determined through the availability of intelligence information.

3.3.2.1 Asset Attractiveness

Once the classes of threats are identified, the next step is to assess the asset attractiveness. Asset attractiveness is defined by API Recommended Practice 780 (2013) as an approximated value of a target to a threat, where the target is a critical asset of a plant. Therefore, asset attractiveness analysis must be taken from the perspective of the adversary where often the intent is to cause the maximum damage to a chemical plant. In order to assist in identifying the critical assets, a methodology has been proposed to assess site security risk (van Staalduinen and Khan, 2015). The Political barrier represented in the methodology allows the authors to establish the threat credibility. The authors have developed a table to assist with assigning a likelihood term once threat credibility is developed, shown in Table 3-1. The threat credibility is from the perspective of a potential attack.

Table 3 - 1: Threat Credibility

Ranking	Threat Credibility (Probability)	Threat Likelihood Term
1	< 0.01	Remote
3	0.01 – 0.10	Unlikely
4	0.10 – 0.25	Likely
5	0.25 – 0.50	Probable
6	> 0.50	Very Likely

3.3.3 Vulnerability Assessment

In the case of the vulnerability of an asset, the first step is to develop the various consequence scenarios on the chosen critical assets and zones. The key point in this step is to outline all possible scenarios in which the critical asset/zone could be attacked based on known weaknesses, and determines the type of consequence that would occur. Various types of consequences are shown in Table 3-2 that have been adapted from Haight (2013) who initially developed consequences based on a safety accident.

Table 3 - 2: Consequence Definition

Consequence Loss Term	Human Health	Environmental	Property Damage	Business Interruption
Insignificant	Multiple injuries	None	< 100K	< 5 days
Minor	Serious injuries inflicted	Localized clean up	> 100K	> 5 days
Major	Fatality	Exceed permit conditions	> 1M	> 10 days
Severe	Multiple fatalities	Observable effects	> 5M	> 30 days
Catastrophic	> 10 fatalities	Remediation required	> 10 M	> 60 days

3.3.4 Attack Scenario Likelihood Assessment

Once the various consequence scenarios have been developed the next step is to establish the likelihood for each type of attack scenario. Sorting the attacks into groups such as manned, vehicle, and aerial allows for simpler quantification. A manned attack is defined as an individual or group of people that executes force to enter the plant while a vehicle attack is a single or group of people with a motorized vehicle. The term aerial attack will be specific to drone attacks. The likelihood of an attack can be developed and quantified by modifying the Political barrier based on the type of attack. As noted in Figure 3-3, the likelihood of an attack relies on two major intermediate nodes, that is, Terrorism and

Crime, which are further detailed to provide simpler causes of an attack. This assessment can be modeled using a Bayesian Network of a mapped fault tree, with the top event being a successful attack. Figure 3-3 expands the original work of van Staalduinen and Khan (2015) which was developed based on recent incidents in the area of chemical security risk. However, extensive work to validate the figure through case studies is part of ongoing research.

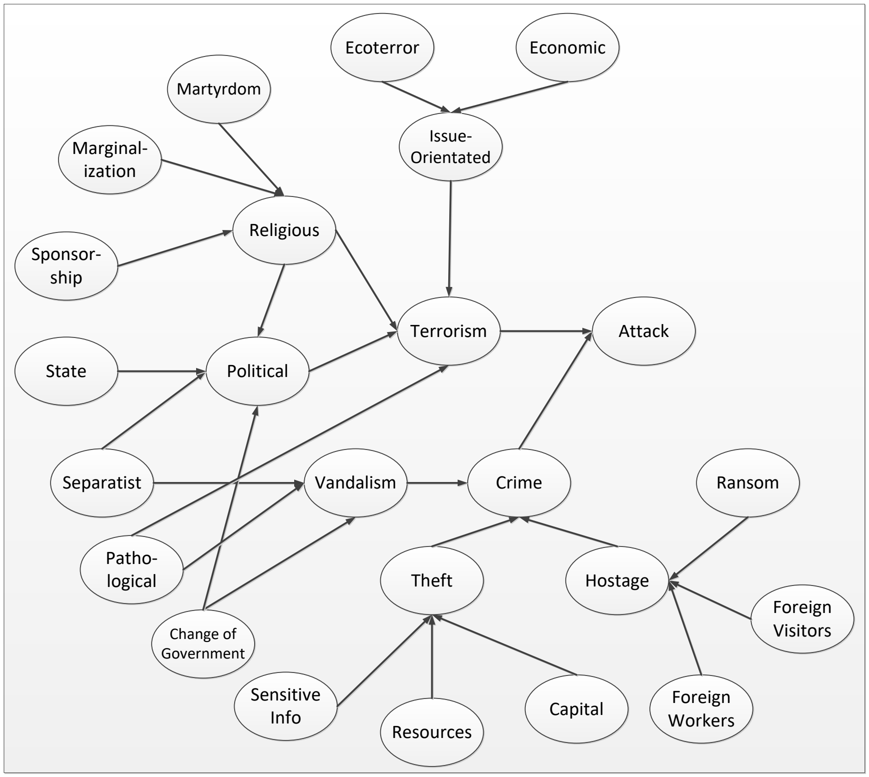

Figure 3 - 3: Mapped Fault Tree of Attack

The basic event probabilities can be estimated using expert judgment or with the help of an intelligence agency. A key factor to consider is that each probability of the basic events will be altered based on the type of attack scenario but the structure of the network will remain the same. Since the end goal of any threat is to conduct an attack, this model development will assist in the understanding of an attack likelihood.

3.3.5 Attack Scenario Consequence Assessment

Building upon the previous step, a Bow-Tie (BT) model can be developed. Various barriers are developed minimizing the consequences of an attack; however, the number of available barriers may differ for each critical asset. This methodology will consider that a facility will have three security barriers in response to an attack and a critical asset may have one or more of these barriers. Furthermore, not all the barriers may be activated as in the case of an aerial attack where the 'external barrier' will not be activated.

Similar to the previous work of the authors (van Staalduinen and Khan, 2015), the external barrier is a passive barrier designed to lessen the impact of an attack. The second barrier which is an internal barrier would be a transitional barrier from passive to reactive in which a mobile security team comes into action against an adversary. The critical barrier is the third security barrier of a plant. This barrier would be considered to have blast proof rooms for protection of workers and additionally a response of local law enforcement to deal with the adversary. Each barrier may play a different role in minimizing the consequence, as the external barrier is more passive while the critical barrier becomes reactive. The fully developed BT model is shown in Figure 3-4.

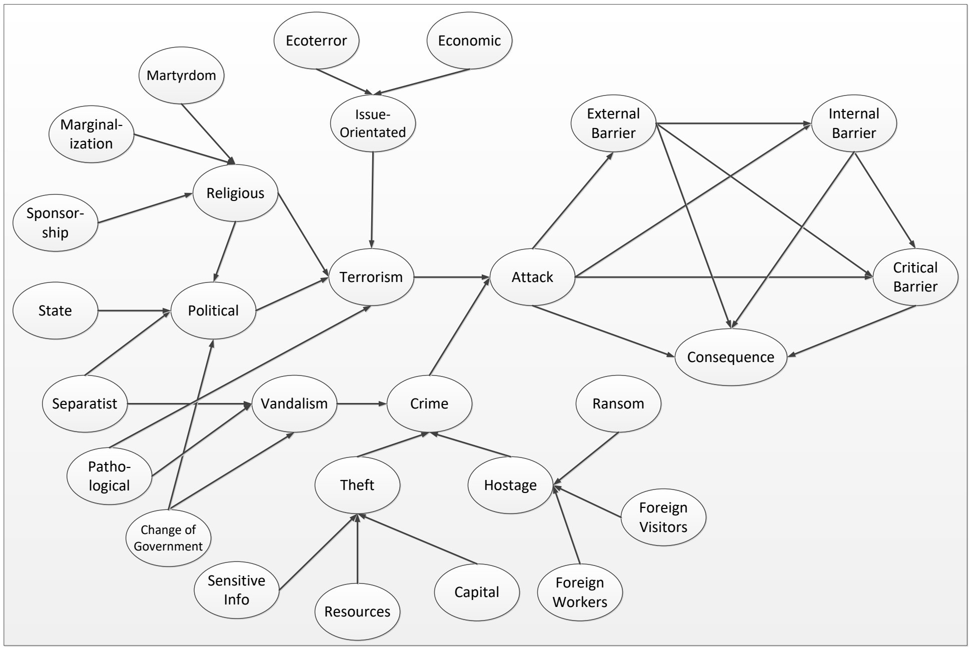

Figure 3 - 4: Mapped BT Model

However, for an aerial attack the BT model will need to be modified, as an aerial attack would bypass the External and Internal barriers, if these barriers do not take such aerial attack into consideration. This network is shown in Figure 3-5.

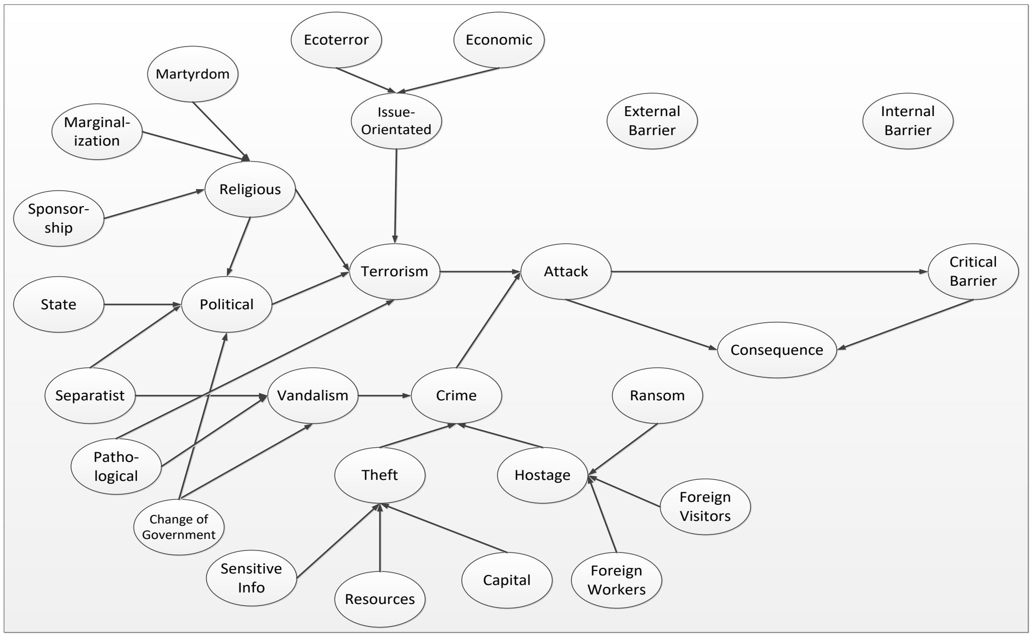

Figure 3 - 5: Aerial Attack BT Model

3.3.6 Risk Assessment

With the BT model completed, the baseline risk for the critical asset should be determined. To this end, the critical asset is placed into a specific asset group based on the criticality determined in the Asset Characterization. Table 3-3 matches the criticality score to the asset group number.

Table 3 - 3: Asset Group Designation

Criticality Range	Asset Group
0.00 – 5.99	1
6.00 – 6.99	2
7.00 – 7.99	3
8.00 – 8.99	4
9.00 – 10.0	5

Based on the consequence, a US dollar value can be matched against the asset group. Table 3-4 shows that the higher the criticality of an asset, the higher the cost becomes, as the severity of the consequence increases. This table is developed based on the losses associated with past security events. The values in the table are guiding values, these may be changed according to the region of application.

Table 3 - 4: Asset Group to Severity Matching

Consequence Severity	Asset Group 1	Asset Group 2	Asset Group 3	Asset Group 4	Asset Group 5
Insignificant	50 K	100 K	250 K	500 K	1 M
Minor	250 K	500 K	750 K	1 M	10 M
Major	500 K	1 M	5 M	10 M	50 M
Severe	1 M	10 M	25 M	50 M	100 M
Catastrophic	10 M	50 M	100 M	250 M	500 M

The baseline risk can be calculated for a given scenario by multiplying the consequence severity value by scenario likelihood. The calculated baseline risk will subsequently be used to compare different scenarios and also security countermeasures proposed/implemented. Therefore, any uncertainty and subjectivity in consequence assessment will have limited impact on the quality or interpretation of the study.

3.3.7 Identification of Countermeasures

The identification of security countermeasures is necessary to determine any security shortcomings in a chemical plant and to examine methods to improve security for a critical asset. Two types of security countermeasures can be distinguished (besides other possible classifications). Internal security countermeasures would increase protection within the plant, thus lessening the vulnerability of an asset. An external security countermeasure would increase protection on the external level with intent to decrease the threat of an attack. Additional security countermeasures will have an associated cost and therefore an economic analysis should be completed to determine the optimal solution.

3.3.8 Cost Analysis of Risk Reduction Strategies

With the baseline risk established, a list of possible security countermeasures is created along with their associated costs and a new estimated risk level with the selected measure implemented. To compare the importance of a countermeasure, a risk-reduction versus cost ratio is defined in Equation 3-3 as a modified version from White (2014):

$$\frac{Risk-Reduction}{Cost} = \frac{Baseline\ Risk-Estimated\ Risk\ after\ countermeasure}{Cost\ of\ countermeasure} \tag{3-3}$$

This ratio allows management to select the most cost effective protection of an asset within a defined budget. The *Estimated Risk after countermeasure* of the risk-reduction vs cost ratio is based on expected value theory. The advantage of this non-normative approach is that it is user-friendly for organizations, while the downside is that the approach gives the perception of accuracy, although it only has a limited predictive resolution, depending on the information available and on the assumptions made. The Bayesian decision theory, the most state-of-the-art in decision sciences, which is a neo-Bernoullian utility theory, sees the economics of operational safety as a normative decision support tool with considerable predictive resolution. However, the disadvantage of this approach is that its user-friendliness should be improved in order to be widely employed. In any case, one may opt to use one of both, or both, approaches to adequately deal with safety or security related decisions. Most important is that the approaches are carried out in a correct way.

In the present study, expected value theory is employed mainly due to the following arguments: i) *its user-friendliness*, ii) its point of reference, and (iii) being easy to understand. It should be stressed, however, that no matter what theory is used, results depend on the quality of input data and decision-makers should always be careful in their interpretation of the results and subsequent decision-making. Further research is needed to increase the quality of results and to ensure optimal decision-making.

3.3.9 Implementation of Countermeasure

With the security countermeasures selected for implementation based on the risk-reduction versus cost ratio, the methodology is redirected to the Critical Assets phase. Reassessing from the Critical Asset point will allow for more accurate determination of the new risk profile. Therefore, if the risk remains at an unacceptable level, then additional security countermeasures should be continually implemented until an acceptable level is reached.

3.3.10 Risk Monitoring and Tracking

To assist with the tracking of security risk for a chemical plant, security performance indicators should be established. Such indicators should complement those of safety and aim to establish, implement, and follow-up on corporate policies and acceptance criteria (Øien et al., 2011). Planned investigations of the organization and administrative procedures along with audits are tools that can be used for follow-up activities. Øien et al. (2011) found that there are typically two types of performance indicators: reactive and proactive. Reactive indicators are typically obvious after an event has occurred while proactive indicators employ factors and underlying causes to help provide an early warning. When the asset characterization, threat, vulnerability, and risk assessments are completed, the most effective security risk indicators can be determined.

Reniers et al. (2013) propose Threat Assessment (TA) triggers, which can be defined as an event or situation that results in changes in a threat level. While Reniers focuses on threat assessment, these same triggers can be sorted and viewed as security performance indicators as well. Nine triggers were proposed: (1) Technology, (2) Neighbouring activity, (3) Politics and prosperity, (4) Company's characteristics, (5) Incidents and accidents, (6) Remarks and suggestions, (7) Legislation and regulations, (8) Topicality and relevant factors, (9) Learning from external events. For a detailed explanation of these triggers, the reader is referred to Reniers et al. (2013) and the references therein. The TA trigger of company characteristics can be further broken into low and high level company characteristics. In 2012, the Department of Homeland Security (2012) released a guide to help raise security awareness in the chemical industry.

The DHS document (2012) lists five major security indicators: (1) Surveillance, (2) Elicitation, (3) Tests of security, (4) Acquiring supplies, (5) Suspicious people/behaviour.

Using the literature mentioned earlier, a holistic security performance indicator list can be developed based on sorting the indicators into either proactive or reactive. The finalized list is shown in Table 3-5 below.

Table 3 - 5: Security Risk Indicators

Security Risk Indicator	Proactive	Reactive
Technology	✓	
Neighbouring activity		✓
Politics and prosperity		✓
Low-level company characteristics	✓	
High-level company characteristics	✓	
Incidents and accidents	✓	
Remarks and suggestions	✓	
Legislation and regulations		✓
Topicality and relevant factors	✓	
Learning from external events		✓
Surveillance	✓	
Elicitation	✓	
Tests of security	✓	
Acquiring supplies	✓	
Suspicious people and/or behaviour	✓	

A slight change in any indicator may prompt for a re-assessment of the security program.

3.4 Case Study

To illustrate how the proposed methodology can be implemented on an existing chemical facility, the following example is herein presented. An illustrative Liquefied Natural Gas (LNG) plant will be considered as shown in Figure 3-6. For the purpose of illustration, we consider a plant which is in a remote location and is quite far from the nearest city. The numbers generated in this case study are illustrative to demonstrate how the methodology can be executed.

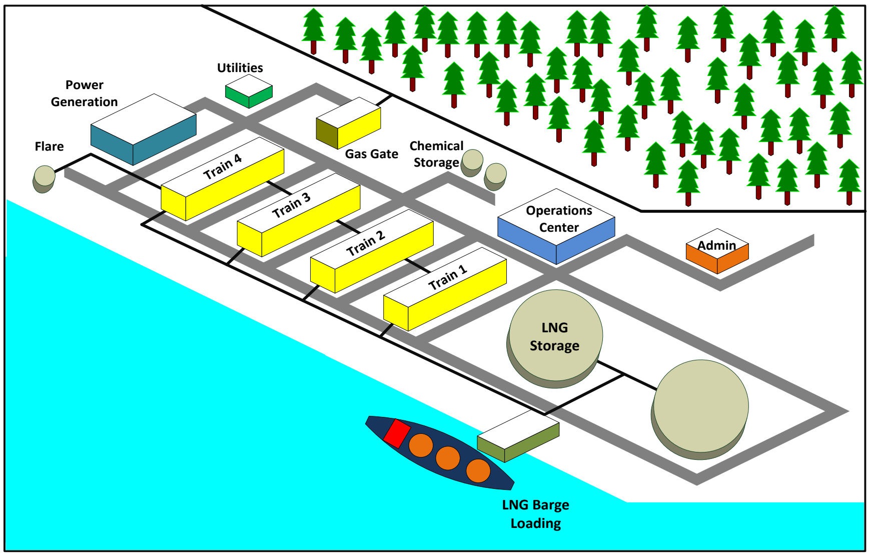

Figure 3 - 6: Case Study of LNG Facility

3.4.1 Asset Characterization

The purpose of this initial step is to determine which of the assets located on the plant are critical. Table 3-6 lists various assets and their appropriately assigned criticality scores on a Likert scale for the purpose of demonstration, where a score of 1 represents low impact and a score of 10 represents a highest impact. For example, the Admin building is assigned a score of 1 for a social factor as attack on it would have a least impact socially. However, it would have a medium economic impact due to the resources it may hold such as data storage and hence a score of 5 is assigned. The Admin building is more inclined to be attacked by an adversary as employees of the facility will be present during the working day and will have a higher political impact and hence a score of 7 is assigned. Taking the average of the three factors gives the Admin building a criticality score of 4.33. Likewise, other scores are assigned.

Table 3 - 6: Asset Criticality Designation

Asset	Social Factor	Economic Factor	Political Factor	Criticality
Admin	1	5	7	4.33

Operations Center	6	8	8	7.33
Utilities	7	8	8	7.67
Power Generation	3	8	8	6.33
Chemical Storage	8	7	9	8.00
Gas Gate	5	6	5	5.33
Flare	7	6	5	6.00
LNG Storage	7	8	10	8.33
Barge Loading	5	4	5	4.67
Gas Treating Train	9	9	9	9.00

We assume that the facility security program determines that any asset with a criticality higher than or equal to 6.5 is considered to be a critical asset. However, for the purpose of the case study only the Operations Center will be investigated. Once the critical assets have been selected, the existing security countermeasures need to be identified. The LNG facility has a fenced-in perimeter with security controlling entrance and exit gates. The security countermeasure for the operations center is displayed in Table 3-7.

Table 3 - 7: Operation Center Countermeasures

Countermeasure Class	Countermeasures
Physical	Locked doors, Limited access points
Electrical/Electronic	Lighting, CCTV, Motion detector, Card Readers
Personnel	Mobile Security, check-in desk

3.4.2 Threat Assessment

Once the critical assets and current security countermeasures have been identified, the next step is to complete a Threat Assessment. This begins with listing possible threats to the facility. For the purpose of this case study, we use only an external threat. We further assume that facility management has been in contact with intelligence agencies.

To assist with asset attractiveness, the threat credibility must first be determined. This is completed by using a part of a model previously proposed by van Staalduinen and Khan

(2015). The Political barrier considers the external conditions of a given chemical facility and helps to determine threat probability. This probability is matched to a likelihood term, thus allowing a threat credibility to be established. The threat probabilities were developed using expert judgment and available literature and the operations center threat probability from the Political barrier was set at 3.98E-02, which, based on Table 3-1, implies that a threat against the operations center is unlikely.

3.4.3 Vulnerability Assessment

In the initial stage of the vulnerability assessment all possible attack scenarios are developed based on the weaknesses of an asset and the type of threat perceived. The goal of this step is to illustrate the type of attack that can be achieved for a given threat, based on possible intrusion routes and deliveries of attacks. Various attack scenarios are shown in Table 3-8 for the operations center.

Table 3 - 8: Attack Scenarios for Operation Center

Intrusion Route	Delivery	Consequence
Main gate	Manned	Minor
	Vehicle	Minor
Forest	Manned	Minor
	Vehicle	Major
Waterway	Manned	Minor
Air	Aerial-Drone	Severe

3.4.4 Attack Scenario Likelihood Assessment

There are three types of attack scenarios that we employ in the suggested BT model to develop the attack likelihood. As discussed, earlier the basic event probabilities can be developed with expert judgment or with the aid of an intelligence agency. However, for the purpose of the case study the developed probabilities are used for illustrative purposes. In each BT model, for each additional logic relaxation assumption used, the corresponding probabilities have also been calculated (Causation, Leak, and Substitution). The causation probability is assigned on the basis that the parent event will cause the child event to occur when acting alone. The substitution probability is designated for the likelihood of the parent event and will be replaced if the original condition is not met. Table 3-9 displays all these probabilities for the primary nodes while Table 3-10 displays the probabilities for the intermediate nodes. The leak probability was assumed to be 1.00E-02 for all nodes which is designated under the assumption that the child node may still occur when none of the parent nodes are active. The primary node probabilities would be relative values as they would be assigned based on information from the intelligence community.

Table 3 - 9: Primary Node Probabilities

BN Node	Manned			Vehicle			Aerial		
	Basic Event	Causation	Substitution	Basic Event	Causation	Substitution	Basic Event	Causation	Substitution
Economic	1.15E-04	7.00E-01	1.00E-01	6.53 E-04	7.50E-01	5.00E-02	6.47 E-05	6.50E-01	1.00E-02
Eco-terror	5.39E-04			4.40 E-04			6.80 E-05		
Martyrdom	2.12E-04			6.56 E-04			5.91 E-05		
Marginal-ization	6.34E-04			4.87 E-04			5.31 E-05		
Sponsorship	9.01E-04			5.07 E-04			6.36 E-05		
State	1.22E-04			3.96 E-04			5.49 E-05		
Separatist	3.58E-04			1.00 E-04			4.00 E-05		
Change of Government	6.09E-04			4.21 E-04			8.15 E-05		
Pathological	9.61E-04			5.89 E-04			9.48 E-05		
Sensitive Info	3.52E-04	7.50E-01		2.22 E-03	8.00E-01		7.45 E-04	6.00E-01	
Resources	1.44E-04			7.02 E-03			1.61 E-04		
Capital	6.50E-04			7.83 E-03			3.18 E-04		
Foreign Workers	9.09E-04			2.64 E-03			3.75 E-04		
Foreign Visitors	2.86E-04			1.85 E-03			3.14 E-04		
Ransom	5.90E-			4.08			8.02		

	04			E-03			E-04		

Table 3 - 10: Intermediate Node Probabilities

BN Node	Manned		Vehicle		Aerial	
	Causation	Substitution	Causation	Substitution	Causation	Substitution
Issue-Orientated	7.50E-01	1.00E-01	7.50E-01	5.00E-02	7.00E-01	1.00E-02
Religious						
Political						
Terrorism	8.00E-01		8.00E-01		8.00E-01	
Vandalism	7.50E-01		7.50E-01		6.00E-01	
Theft						
Hostage						
Crime	8.50E-01		8.50E-01		8.50E-01	

Using the above probabilities and the various BN relaxation assumptions, the attack probability for each scenario, based on the different logics, was determined. This is illustrated in Figure 3-7. In the below figure, it is shown that a vehicle attack has the highest probability followed by manned then aerial attacks.

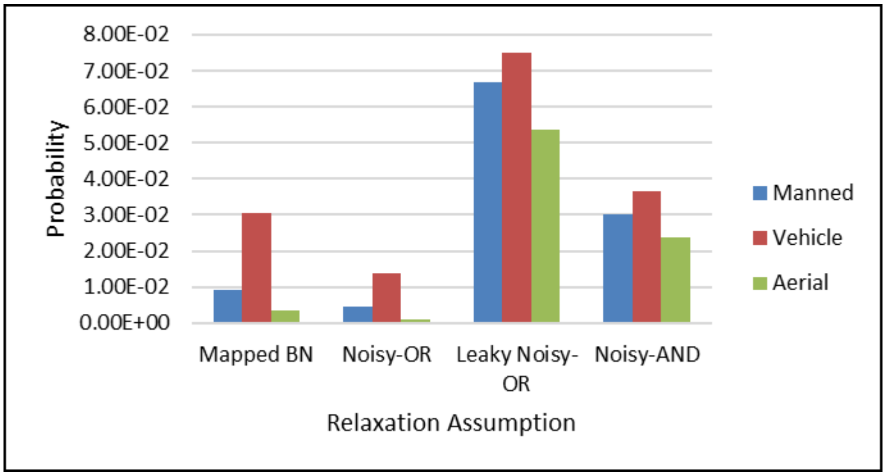

Figure 3 - 7: Graphical Display of Attack Likelihood for Type of Attack

3.4.5 Attack Scenario Consequence Assessment

With each type of attack likelihood developed, the consequences can be determined. For the mapped BN, the External barrier had a failure probability of 9.85E-02 and the Internal barrier had a failure probability of 3.67E-02. The Critical barrier had a failure probability of 1.30E-03 and the respective causation and substitution probabilities are shown below in Table 3-11.

Table 3 - 11: Barrier Node Probabilities

BN Node	Manned		Vehicle		Aerial	
	Causation	Substitution	Causation	Substitution	Causation	Substitution
Attack	8.00E-01	5.00E-02	7.00E-01	5.00E-02	7.00E-01	5.00E-02
External	8.50E-01		7.50E-01		-	
Internal	9.00E-01		8.00E-01		-	

With the probabilities established, each consequence state probability is determined. The results for each type of attack are shown Tables 3-12 – 3-14.

Table 3 - 12: Manned Attack Consequence Results

Consequence	Mapped BN	Noisy-OR	Leaky-Noisy OR	Noisy-AND
Insignificant	8.92E-01	9.95E-01	9.06E-01	7.83E-01
Minor	1.03E-01	4.00E-05	1.82E-02	1.52E-01
Major	4.01E-03	1.60E-04	3.60E-03	3.01E-02
Severe	9.10E-04	7.40E-04	1.84E-02	1.12E-02
Catastrophic	1.18E-06	3.70E-03	5.35E-02	2.34E-02

Table 3 - 13: Vehicle Attack Consequence Results

Consequence	Mapped BN	Noisy-OR	Leaky-Noisy OR	Noisy-AND
Insignificant	8.73E-01	9.86E-01	9.03E-01	6.49E-01
Minor	1.20E-01	3.80E-04	1.89E-02	1.93E-01
Major	4.66E-03	1.10E-03	7.40E-03	6.53E-02
Severe	3.02E-03	2.90E-03	2.17E-02	2.79E-02
Catastrophic	3.92E-06	9.50E-03	4.93E-02	6.50E-02

Table 3 - 14: Aerial Attack Consequence Results

Consequence	Mapped BN	Noisy-OR	Leaky-Noisy OR	Noisy-AND
Insignificant	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Minor	0.00E+00	0.00E+00	0.00E+00	0.00E+00
Major	9.95E-01	9.99E-01	9.37E-02	8.31E-01
Severe	4.79E-03	2.30E-04	2.01E-02	1.45E-01
Catastrophic	4.55E-08	9.20E-04	4.30E-02	2.37E-02

3.4.6 Risk Assessment

The baseline risk profile can be calculated by matching the criticality asset group to the probabilities shown in the above tables. From Asset Characterization, the operations center was found to have a criticality rating of 7.33. Therefore, it is in Asset Group 3 from Table 3-4. Figure 3-8 – 3-11 below display the risk for the operations based on each type of attack with the use of various logic assumption.

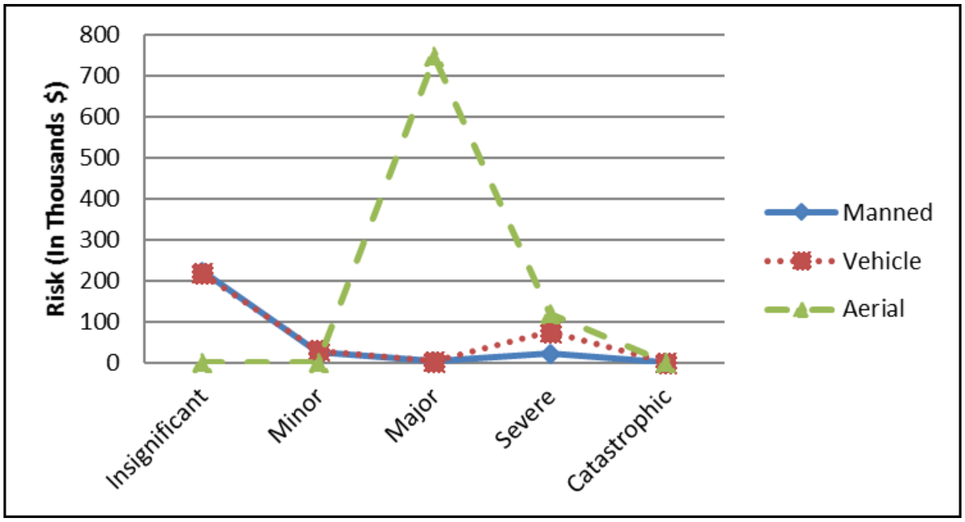

Figure 3 - 8: Risk Profile based on Mapped BN

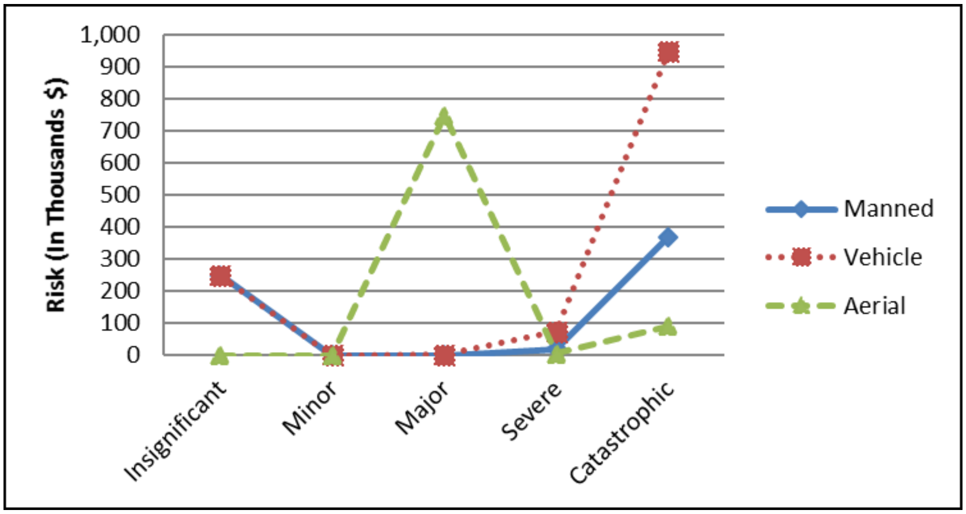

Figure 3 - 9: Risk Profile based on Noisy-OR

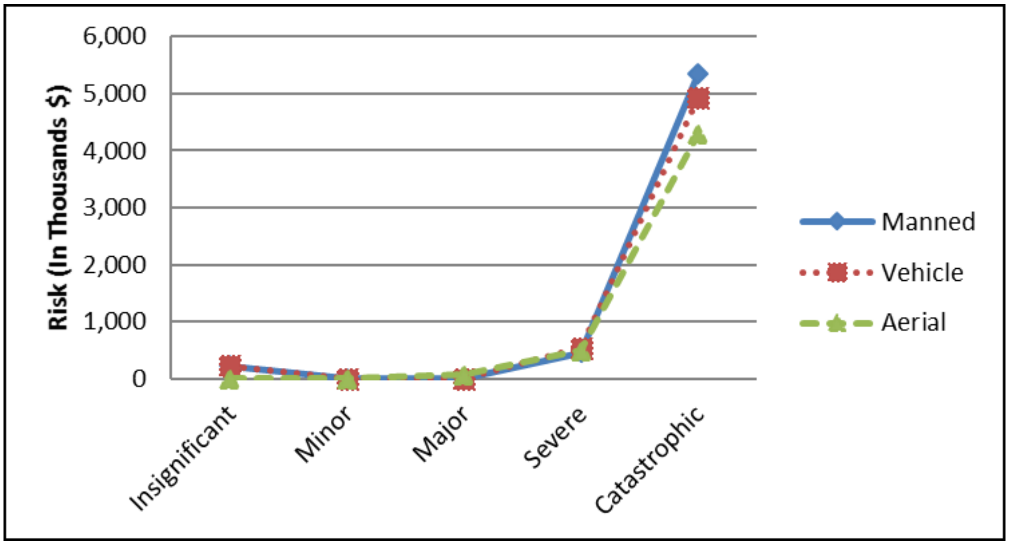

Figure 3 - 10: Risk Profile based on Leaky Noisy-OR

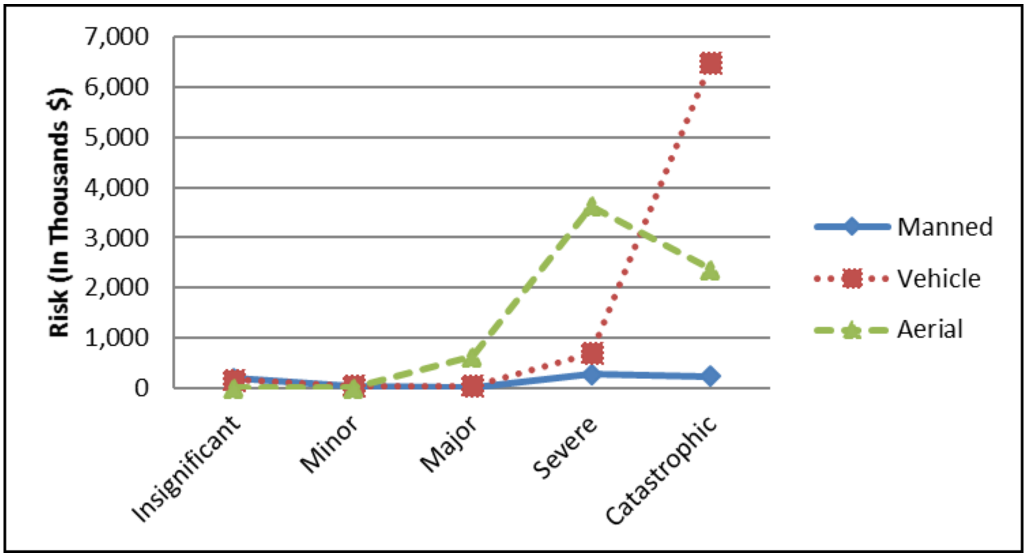

Figure 3 - 11: Risk Profile based on Noisy-AND

Based on the results of the risk assessment, Figures 3-9 through 3-11 indicate that a vehicle attack is at the highest risk for a catastrophic consequence. Therefore, security countermeasures must be added to reduce this risk. Figure 3-8 and 3-9 shows that without the use of the relaxation assumptions executed within the model, the results would not reflect reality accurately. As shown in Figure 3-10, the Leaky Noisy-OR relaxation best illustrates an attack on the plant as the most devastating consequences have the highest risk. Recent incidents on chemical facilities from the past years illustrate that a coordinated vehicle attack poses the greatest risk. However, it should be noted that with the increase in drone technology, aerial attacks may become more frequent and may therefore entail a higher risk than anticipated based on casuistic information.

3.4.7 Identification of Countermeasures

To reduce the risk of the critical asset, additional countermeasures can be implemented. These security countermeasures can either attempt to minimize the asset vulnerability or minimize the threat to the asset. A list should be created of possible security countermeasures to implement along with the associated cost. Table 3-15 shows an illustrative list of additional security countermeasures that might be proposed for this LNG facility. The list is not at all exhaustive or comprehensive and many additional measures could be considered.

Table 3 - 15: Security Countermeasure Proposals

Countermeasure	Description	Cost ($/yr.)
Facility Response Team (FRT)	Create a facility response team that will immediately respond to a security alarm on the facility	80,000
Communication (C)	Increase correspondence with local law enforcement and emergency response teams	40,000
Fortification (F)	Install guard towers equipped for both day and night surveillance	110,000
FRT + C	Facility Response Team plus Communication	120,000
FRT + F	Facility Response Team plus Fortification	190,000
C + F	Communication plus Fortification	150,000
FRT + C + F	Implement all three options	230,000

3.4.8 Cost Analysis of Risk Reduction Strategies

With the security countermeasures developed, the next step in the methodology is to complete a cost analysis. Chemical facilities will have budget restraints on the implementation of new security countermeasures. Therefore, it is imperative that maximum security be gained for a minimal cost. With the security countermeasures and costs listed, the ensuing step is to estimate the effect of the security measure on the baseline risk. Table 3-16 shows the results of security countermeasure cost analysis based on Leaky Noisy-OR logic relaxation assumption. It was determined that this logic assumption best reflected realistic conditions. The baseline risk was calculated from using the catastrophic risk state probability of the Leaky Noisy-OR logic under a vehicle attack along with the matched severity for Asset Group 3 found in Table 3-4. The new estimated risk is determined by expert judgement based on the implementation of the security countermeasure through expected value theory.

Table 3 - 16: Security Countermeasure Cost Analysis

Countermeasure	Baseline Risk ($)	New Estimated Risk ($)	Risk-reduction (Benefit)	Risk-reduction versus Cost Ratio
FRT	4,930,000	3,200,000	1,730,000	21.63
C	4,930,000	4,000,000	930,000	23.25
F	4,930,000	2,800,000	2,130,000	19.36
FRT + C	4,930,000	2,270,000	2,660,000	22.17
FRT + F	4,930,000	1,070,000	3,860,000	20.32
C + F	4,930,000	1,870,000	3,060,000	20.40
FRT + C + F	4,930,000	140,000	4,790,000	20.83

From the illustrative cost analysis, it was found that the most optimal solution for the company is to fortify its perimeter with continual surveillance (Fortification countermeasure).

3.4.9 Implementation of Countermeasures

Once the optimum security countermeasure has been determined, it needs to be implemented into the LNG plant. The methodology must be repeated from Threat Assessment to accurately determine the risk level for the critical asset. This includes updating the developed BT for each attack scenario to ensure that the baseline risk level reflects the changes.

Starting with the Threat Assessment step, the threat credibility for the operations center will need to be reassessed, as a fortified perimeter will affect the asset attractiveness. With re-examination of the Political barrier, it was found that threat credibility was lowered to 9.23E-03 which changed the threat likelihood to ‘Remote’ based on Table 3-1. The Vulnerability Assessment phase will remain constant as the development for an attack to be carried, will not change.

The implementation of the security countermeasure will require an updated Attack Scenario Likelihood Assessment. Basic event probabilities will be changed to reflect the new conditions and consulting with an intelligence agency or through the use of expert judgement can complete this. While the fortification of the perimeter would also affect a manned attack, only a vehicle attack is being considered. In the Leaky Noisy-OR conditions, the new attack likelihood is compared to previous likelihood in Figure 3-12 below. Furthermore, the consequence state will be altered in the Attack Scenario Consequence Assessment. From these two steps, the new risk profile can be developed through the Risk Assessment step. The updated risk profile is compared with risk profile prior to the implementation of the security countermeasure. Through the analysis, the risk of a catastrophic event was actually $2.55 M, not $2.80 M that was previously estimated as illustrated in Figure 3-13.

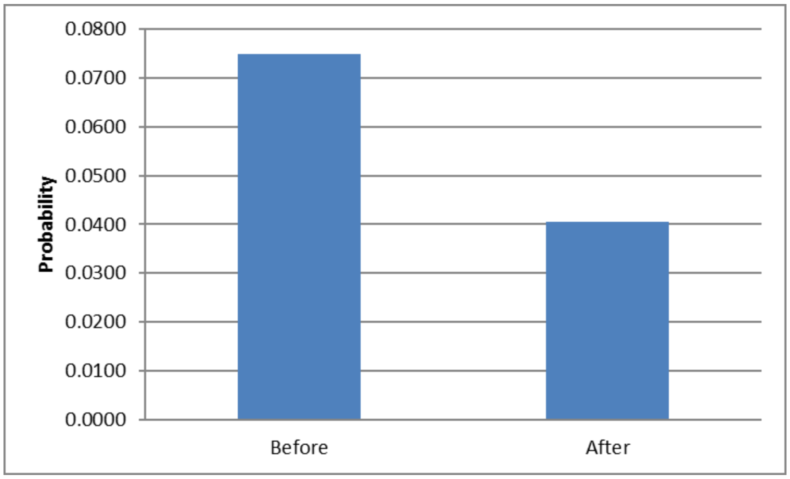

Figure 3 - 12: Comparison of Changed in Attack Likelihood

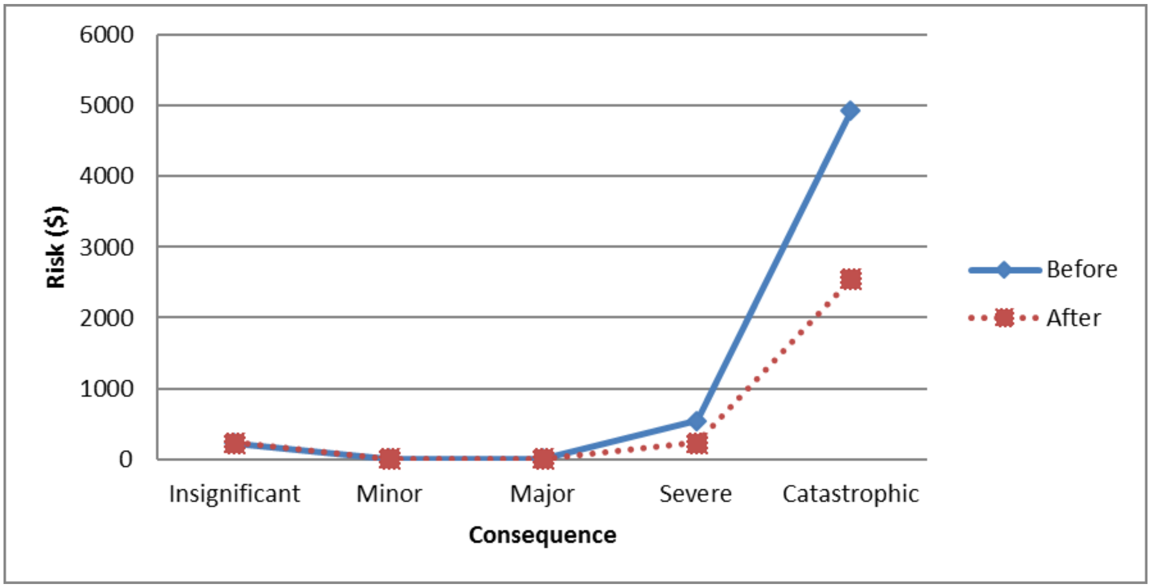

Figure 3 - 13: Comparison of Risk Profiles

3.4.10 Risk Monitoring and Tracking

The final step of the methodology is to create a risk monitoring and tracking program within the LNG facility. However, it may not be feasible to monitor and track all the security risk indicators listed in Table 3-5. Based on the location of the plant with the current surrounding conditions, the QSRA determined that the following indicators should be tracked: (1) External technology, (2) Neighbouring activity, (3) Incidents and accidents, (4) Topicality and relevant factors, (5) Surveillance, and (6) Tests of security.

3.5 Discussion of Case Study Results

The elaborated QSRA methodology approach has been demonstrated through a case study on a typical LNG facility with the operations center selected as the critical asset. The various relaxation assumptions within the BT model, allow for the selection of the idealistic conditions which in our case was the Leaky Noisy-OR. This is an expected result, as an attack will only need one individual or group to initiate an event to commit the attack, not a combination as is seen in the Noisy-AND condition. Furthermore, the leak parameter accounts for components that are not explicitly modeled and therefore accounts for any missing component that may lead to an attack on the facility.

Through the risk analysis, it has been shown that the plant has the highest risk for either low frequency-high consequence or high frequency-low consequence events. Therefore, it is imperative that security countermeasures be put in place to reduce both these types of events. The case study exemplified that with additional security countermeasures the risk can be lowered with an optimum cost. Furthermore, the case study illustrated that the greatest risk for the LNG facility was a coordinated vehicular attack. Previous history of attacks on chemical facilities was typically in the form of vehicle attacks; however, with increasing drone technology, aerial attacks may become more important in the future.

3.6 Conclusion

As chemical plants have become targets for terrorist groups in recent years, the need has arisen to develop a holistic security risk methodology. The QSRA methodology discussed in this paper expands upon the five sequential steps suggested in the well-known API document (2013) and adds concurrent steps that lead to the security risk assessment. A Bow-Tie model mapped in a Bayesian Network is utilized to allow for easy updating when certain plant conditions change and further assists in quantifying the security risk. The methodology herein described implements originality as it completes both a Threat and Vulnerability assessment concurrently rather sequentially. A key aspect of this methodology is the reliance on analysis and probability as there are no current statistics on the type of situations that security risk managers are faced with. The potential improvement in the proposed approach includes the consideration of uncertainty analysis, the inclusion of data gathering and processing, and the integration of the proposed approach with an online monitoring system.

Future research will be aimed at advancing the quality of the input data while employing the expected value theory in our suggested QSRA method, as well as making Bayesian Theory, the current state-of-the-art in decision analysis, more user-friendly and incorporate it into the QSRA method, to further improve security risk decision-making.

3.7 References

Argenti F, Landucci G, Spadoni G, Cozzani V. The assessment of the attractiveness of process facilities to terrorist Attacks. Safety Science. 2015; 77: 169–181

American Petroleum Institute. ANSI/API 780 Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries. Washington (DC): 2013.

Bajpai S, Gupta JP. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries. 2005; 18 (4-6): 301-309.

Baybutt P, Reddy V. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defense Journal. 2003; 2 (1): 1-7.

Bearfield G, Marsh W. Generalising event trees using Bayesian networks with a case study of train derailment. Lecutre Notes in Computer Science. 2005; 3688: 52-66 p.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety. 2001; 71 (3): 249-260.

Center for Chemical Process Safety. Guidelines for Analyzing and Managing Security Vulnerabilities of Fixed Chemical Sites. New York: Center for Chemical Process Safety/AIChe; 2003.

Delvosalle C, Fievez C, Pipart A, Casal Fabrega J, Planas E, Christou M, Mushtaq F. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety. 2005; 90 (2-3): 238-246.

Díez F, Druzdzel M. Canonical Probabilistic Models for Knowledge Engineering Technical Report. Madrid (Spain): CISAID; 2007.

Haight J. Handbook of Loss Prevention Engineering. Germany: Wiley-VCH; 2013.

Jensen FV, Nielson TD. Bayesian Networks and Decision Graphs. New York: Springer; 2007.

Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection. 2013; 91 (1-2): 46-53.

McGill W, Ayyub B, Kaminsky M. Risk Analysis for Critical Asset Protection. Risk Analysis. 2007; 27 (5): 1265-1281.

National Research Council. Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change. Washington, DC: National Academies Press; 2008. Available at: http://www.nap.edu/catalog/12206/department-of-homeland-security-bioterrorism-risk-assessment-a-call-for (last checked on Jan 20, 2016)

National Research Council. Review of the Department of Homeland Security's Approach to Risk Analysis. Washington, DC: National Academies Press; 2010.

Øien K, Utne IB, Tinmannsvik RK, Massaiu S. Building Safety Indicators: Part 2 – Application, practices and results. Safety Science. 2011; 49 (2): 162-171.

Reuters News Agency. Islamic State militants breach Iraq refinery perimeter, repelled. 2015 April 13. http://www.reuters.com/article/us-mideast-crisis-iraq-refinery-idUSKBN0N414W20150413

Reniers G. Multi-Plant Safety and Security Management in the Chemical and Process Industries. Berlin, Germany: Wiley-VCH; 2010.

Reniers G, Herdewel D, Wybo JL. A Threat Assessment Review Planning (TARP) decision flowchart for complex industrial areas. Journal of Loss Prevention in the Process Industries. 2013; 26 (6): 1662-1669.

Statoil ASA. The In Amenas Attack. 2013 Feb. http://www.statoil.com/en/NewsAndMedia/News/2013/Pages/12Sep_InAmenas_report.aspx

U.S. Department of Homeland Security. Chemical Sector Security Awareness Guide. Washington (DC): Department of Homeland Security. 2012.

van Staalduinen M, Khan F. A Barrier Based Methodology to Assess Site Security Risk. In: SPE E&P Health, Safety, Security, and Environmental Conference – Americas; 2015 Mar 16 – Mar 18, 2015; Denver, USA. Copy of the document available from Department of Process Engineering, Memorial University, St John's, Canada.

White R. Towards a Unified Homeland Security Strategy: An Asset Vulnerability Model. Homeland Security Affairs. 2014; 10: 1-15.

Summary

Security incidents may not be a common occurrence within the chemical industry however, the need to address these risks continues to exist. Chemical facilities hold hazardous materials and have dangerous operating conditions which a threat to the plant may look to exploit. Therefore, a robust and versatile risk based methodology to assist decision-makers needs to be established. The subjective approach illustrates adaptability to build networks to suit a specific facility based on its own security measures and external conditions. Two comprehensive methodologies have been proposed, SVAPP and QSRA, to contribute in the foundation for future work in the area of chemical security risk analysis. Both methodologies are structured on mapped BN which are advantageous for learning casual relationships to allow for a forecast of possible consequences. One key limitation of this work was the data for basic event probabilities. The collection of security data can be collected and maintained by a company, however due to the sensitivity of this data it is unlikely that it would be shared. This is one of the disadvantages of Bayesian Networks, as prior beliefs can misrepresent the entire network to give unacceptable results. Therefore, the use of an updating mechanism as executed in chapter 1 and 2 can help to eliminate that concern.

The SVAPP methodology utilizes similar techniques that have been previously established in a safety methodology known as SHIPP. This would allow for an effortless combination of both methodologies to create one heuristic risk model to cover both safety and security.

In the QSRA methodology both the loss and cost-benefit are simplified. This simplification is user-friendly and provides a quick estimation, however, the accuracy of the results can suffer through this assessment. Future work should consider ways to further advance assessing consequence severity into a monetary value. Additionally, a method should be explored to enhance the assessment of additional security countermeasures.

The SVAPP and QSRA methodologies proposed illustrate how the approach can assist risk managers to make an informed decision. The case studies utilized subject approach to build the barriers and expert judgement to form the initial failure probabilities. While both methodologies are mapped into Bayesian Networks, the key difference is that the QSRA employs a BT. The graphical technique of BN allows for CPT manipulation, however, these causation and substitution probabilities rely on expert judgment. This is one key limitation of the studies as gathering appropriate data is difficult to due the sensitivity of the security subject for corporations.

Additionally, the current proposed methodologies apply a logic model to an illogical adversary. This can be corrected to incorporate the use of game theory which models conflict between two decision-makers.

Bibliography and References

Abimbola, M., Khan, F., Khakzad, N. Risk-based safety analysis of well integrity operations. Safety Science, Volume 84, April 2016, Pages 149–160.

Adedigba, S. A., Khan, F., & Yang, M. (2016). Dynamic safety analysis of process systems using nonlinear and non-sequential accident model. Chemical Engineering Research and Design. http://doi.org/10.1016/j.cherd.2016.04.013

Bird, F.E., Germain, G.L. Practical Loss Control Leadership Georgia: Det Norske Veritas, USA (1996)

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety. 2001; 71 (3): 249-260.

Center for Chemical Process Safety. Guidelines for Analyzing and Managing Security Vulnerabilities of Fixed Chemical Sites. New York: Center for Chemical Process Safety/AIChe; 2003. 240 p.

Delvosalle C, Fievez C, Pipart A, Casal Fabrega J, Planas E, Christou M, Mushtaq F. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety. 2005; 90 (2-3): 238-246.

Department of Homeland Security (DHS). (2003). Presidential Directive N 7. https://www.dhs.gov/homeland-security-presidential-directive-7

Department of Homeland Security (DHS). (2007). Chemical facility anti-terrorism standards. https://www.dhs.gov/chemical-facility-anti-terrorism-standards

Díez F, Druzdzel M. Canonical Probabilistic Models for Knowledge Engineering Technical Report. Madrid (Spain): CISAID; 2007.

Ezell BC, Bennett SP, von Winterfeldt D, et al. Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis. 2010; 30 (4): 575-589.

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

National Research Council. Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change. Washington, DC: National Academies Press; 2008. 171 p.

Pearl, J. Probabilistic Reasoning in Intel ligent Systems. Morgan Kaufmann, San Mateo, CA, 1988.

Rathnayaka S, Khan FI, Amyotte P. SHIPP Methodology: Predictive Accident Modeling Approach. Part I: Methodology and Model Description. Process Safety and Environmental Protection. 2011; 89 (3): 151-164.

Reason, J. Human Error. University press, Cambridge (1990)

Sadiq, A.-A. (2013), Chemical Sector Security: Risks, Vulnerabilities, and Chemical Industry Representatives' Perspectives on CFATS. Risk, Hazards & Crisis in Public Policy, 4: 164–178. doi: 10.1002/rhc3.12032